

UNIVERSIDAD TÉCNICA FEDERICO SANTA MARÍA
DEPARTAMENTO DE INFORMÁTICA
VALPARAÍSO - CHILE



“EXPERIENCIA CON UNA METODOLOGÍA DE
DESARROLLO DE SOFTWARE SEGURO DESPLEGADO EN
SERVICIOS DE CLOUD COMPUTING”

PABLO BETANCOURT

MEMORIA PARA OPTAR AL TÍTULO DE
INGENIERO CIVIL EN INFORMÁTICA

Profesor Guía: Raúl Monge Anwandter
Profesor Correferente: Mauricio Figueroa

Agosto - 2025



CONSTANCIA DE VALIDACIÓN Y CONFIDENCIALIDAD DE MONOGRAFÍA A REPOSITORIO ACADÉMICO

1.- IDENTIFICACIÓN DEL TRABAJO ACADÉMICO

Tipo de monografía (marcar una opción): ☒ Memoria o trabajo de título; ☐ Tesis de Postgrado;

Título del trabajo: EXPERIENCIA CON UNA METODOLOGÍA DE DESARROLLO DE SOFTWARE SEGURO DESPLEGADO EN SERVICIOS DE CLOUD COMPUTING

Nombre del candidato(a): Pablo Betancourt

Carrera / Grado: Ingeniería Civil Informática

Campus: Casa Central Valparaíso ; **Departamento:** Informática

2.- VALIDACIÓN DEL PROFESOR GUÍA/DIRECTOR DE TESIS

Yo, Raúl Monge Anwandter, en mi calidad de profesor(a) guía/director(a) del trabajo académico mencionado anteriormente **DEJO CONSTANCIA** que:

- He revisado esta versión del documento y corresponde a la versión final aprobada del trabajo.
- El trabajo cumple con los requisitos académicos y de formato establecidos por la institución

3.- EVALUACIÓN DE CONFIDENCIALIDAD POR PROPIEDAD INDUSTRIAL

☒ El trabajo **NO contiene información que amerite confidencialidad** y puede ser publicado de inmediato en repositorio con acceso abierto.

☐ El trabajo **CONTIENE** información con potenciales implicancias de propiedad industrial o intelectual y requiere un periodo de confidencialidad (embargo) por:

☐ 6 meses; ☐ 12 meses; ☐ 2 años; ☐ 3 años; ☐ 5 años; ☐ 10 años

Fundamentación de la necesidad de confidencialidad (obligatorio si se solicita embargo):

4.- FIRMAS

Profesor(a) guía o director(a) de memoria o tesis:

Fecha:

; Firma:

Raúl Monge

Estudiante o Candidato(a):

Fecha: 01/08/2025

; Firma:

Betancourt

Este formulario debe ser insertado como página 2 de la memoria o tesis, completado y firmado por estudiante y profesor(a) antes de la entrega en portal PRISMA de Biblioteca USM.

DEDICATORIA

Este trabajo se lo dedico con todo mi cariño a mi familia, y especialmente a mis padres, por su amor incondicional, su constante apoyo y por estar siempre presentes en cada paso de mi camino académico. Sin su ayuda, no habría sido posible siquiera realizar este trabajo.

AGRADECIMIENTOS

Agradezco especialmente a mi familia por haberme apoyado durante todo el proceso de mi formación profesional. A mis amigos, quienes compartieron conmigo sus opiniones y experiencias, lo que me permitió enriquecer mi propio trabajo. Y, por supuesto, a mi profesor guía ya que su orientación y conocimientos fueron claves para la realización de esta memoria.

RESUMEN

Resumen— La seguridad en tecnologías Cloud, y específicamente en el desarrollo de soluciones basadas en estas, permite mitigar riesgos que afectan aspectos como la reputación, la legalidad y los ataques que una empresa puede sufrir a causa de ciberdelincuentes. Durante la pandemia del COVID-19, el uso de esta tecnología de información se incrementó sustancialmente, lo que llevó a muchas empresas a migrar sus sistemas locales a sistemas Cloud. Sin embargo, este proceso no estuvo acompañado de una mayor seguridad de la información. En este trabajo, se propone una metodología de desarrollo seguro basada en un modelo de mejora continua, que abarca aspectos como DevSecOps, infraestructura Cloud, desarrollo Cloud y cumplimiento. Este enfoque se sustenta en un marco teórico robusto, con estándares como CCM, CIS, ISO, NIST y las investigaciones realizadas sobre seguridad en Cloud.

Como resultado de la experiencia con una metodología de desarrollo de software para Cloud, se detectaron desviaciones, que fueron clasificadas y se construyeron controles para remediarlas en cada uno de los dominios revisados. El plan de remediación se aplicó en un plazo de un mes. En este ciclo, se logró iniciar el proceso de implementación de los marcos CCM y CIS, enfocados en los servicios de Amazon, mejorar los procesos de desarrollo e incorporar las amenazas más importantes relacionadas con Cloud en un catálogo de amenazas. Al final del ciclo, se cuantificó que se implementó un 80 % de los controles esperados en el modelo de responsabilidad compartida y un 71 % de los controles esperados según la CIS Amazon Web Services Foundations Benchmark. Además, en todos los proyectos desarrollados se realizaron pruebas de seguridad en cada etapa de su ciclo, y se incorporaron 10 amenazas detectadas por la CSA sobre Cloud Computing. Estas mejoras, excepto el incremento del marco CIS, se encuentran dentro de los umbrales de aceptación de la metodología, por lo que se indica que el 75 % de las metas planteadas fueron alcanzadas.

Palabras Clave— Cloud Computing, Cloud Security, Modelo responsabilidad compartida, DevSecOps, Pandemia del COVID-19

ABSTRACT

Abstract— Security in Cloud technologies, and specifically in the development of solutions based on them, helps mitigate risks that affect aspects such as reputation, legal compliance, and the attacks a company may suffer from cybercriminals. During the COVID-19 pandemic, the use of this information technology increased substantially, leading many companies to migrate their on-premises systems to Cloud-based systems. However, this process was not accompanied by an increase in information security. In this work, a secure development methodology is proposed based on a continuous improvement model, covering aspects such as DevSecOps, Cloud infrastructure, Cloud development, and compliance. This approach is supported by a robust theoretical framework, including standards such as CCM, CIS, ISO, NIST, and research conducted on Cloud security.

As a result of experience with a software development methodology for Cloud, deviations were identified, classified, and controls were created to remediate them in each of the reviewed domains. The remediation plan was applied within a one-month timeframe. In this cycle, the implementation of the CCM and CIS frameworks—focused on Amazon services—was initiated, development processes were improved, and the most significant Cloud-related threats were incorporated into a threat catalog. By the end of the cycle, it was quantified that 80 % of the expected controls in the shared responsibility model were implemented, as well as 71 % of the controls according to the CIS Amazon Web Services Foundations Benchmark. Additionally, security testing was conducted at each stage of the development cycle in all projects, and 10 threats identified by the CSA regarding Cloud Computing were incorporated. These improvements—except for the increase in CIS framework implementation—fell within the methodology's acceptance thresholds, leading to the conclusion that 75 % of the established goals were achieved.

Keywords— Cloud Computing, Cloud Security, Shared Responsibility Model, DevSecOps, COVID-19 pandemic

ÍNDICE DE CONTENIDOS

RESUMEN	IV
ABSTRACT	V
ÍNDICE DE FIGURAS	VIII
ÍNDICE DE TABLAS	VIII
INTRODUCCIÓN	1
CAPÍTULO 1: DEFINICIÓN DEL PROBLEMA	4
1.1 Contexto	4
1.2 Objetivos de la memoria	8
CAPÍTULO 2: MARCO CONCEPTUAL	10
2.1 Las características principales de Cloud	10
2.1.1 Modelo de responsabilidad compartida	13
2.2 Las características de DevSecOps en Cloud Computing	17
2.3 Seguridad de la información en el contexto de Cloud Computing	19
2.3.1 Fuentes de información	20
2.3.2 Controles de seguridad	21
2.3.3 Inteligencia de amenazas	22
2.3.4 Indicadores	23
2.4 Modelo de mejora continua	24
CAPÍTULO 3: PROPUESTA DE SOLUCIÓN	26
3.1 Análisis de la organización (Planear)	27
3.1.1 Definición de áreas organizacionales	27
3.1.2 Análisis de contexto y dominios de la solución	28
3.1.3 Construcción de objetivos	29
3.1.4 Construcción del Plan de remediación	29
3.2 Implementación del Plan (Hacer)	31
3.2.1 Aplicación del Plan de remediación	32
3.2.2 Auditorías del proceso	32
3.2.3 Cálculo de indicadores intermedios	33
3.2.4 Registro de complicaciones o incidencias	33
3.3 Revisión del proceso (Verificar)	34
3.3.1 Revisión de indicadores finales vs metas	34
3.4 Actuar y cierre (Actuar)	34
CAPÍTULO 4: VALIDACIÓN DE LA SOLUCIÓN	36
4.1 Análisis de la organización (Planear)	36
4.1.1 Definición de actores	36

4.1.2	Análisis de contexto y dominios de la solución	37
4.1.3	Construcción de objetivos	40
4.1.4	Construcción del Plan de remediación	40
4.2	Implementación del Plan (Hacer)	42
4.2.1	Aplicación del Plan de remediación	42
4.3	Revisión del proceso (Verificar)	42
4.3.1	Revisión de indicadores finales vs metas	42
4.4	Actuar y Cierre (Actuar)	43
CAPÍTULO 5: CONCLUSIONES		46
5.1	Resultados	46
5.2	Alcance y Limitaciones de la memoria	48
5.3	Trabajo Futuro	49
GLOSARIO		51
ANEXOS		52
5.1	Cuestionario análisis de contexto	52
5.2	Análisis de Contexto	53
5.3	Plan de tratamiento durante aplicación de la metodología	58
5.4	Registro Cambios durante aplicación de la metodología	63
5.5	Informe Verificación de resultados	64
5.6	Informe resultados finales	67
REFERENCIAS BIBLIOGRÁFICAS		72

ÍNDICE DE FIGURAS

1	Crecimiento Cloud durante pandemia	5
2	Consumo Zoom	6
3	Responsables de Cloud Security	7
4	Árbol del problema	8
5	Diferencias entre MultiCloud y Cloud híbrido	12
6	Modelo de responsabilidad compartida de servicios AWS	16
7	Comparación modelo DevSecOps vs DevOps	18
8	Comparación amenazas 2022 y 2024	24
9	Ciclo de mejora continua	25
10	Flujo en etapa Análisis de la organización	32
11	Flujo en etapa Implementación del Plan	33
12	Flujo en etapa Revisión del proceso	35
13	Flujo en etapa Actuar y Cierre	36

ÍNDICE DE TABLAS

1	Top 11 vulnerabilidades en Cloud Computing en 2020	2
2	Comparación entre instalación On-premise y usando Cloud Computing	11
3	Evaluación de Prioridad de Dominios de Seguridad	38
4	Niveles de Madurez de Controles	38
5	Matriz de Dominio/Nivel de Madurez del control.	41

INTRODUCCIÓN

Cloud Computing es una tecnología que consiste en abstraer la infraestructura tecnológica para convertirla en recursos computacionales unitarios, los cuales permiten la construcción de servidores fácilmente escalables. Esto posibilita que las empresas especializadas en esta tecnología ofrezcan dichos recursos como un servicio de infraestructura virtual, permitiendo así a otras organizaciones desarrollar sus propios sistemas en estos entornos y pudiendo ajustar sus capacidades tecnológicas a las necesidades de sus organizaciones. [Borra, 2024].

Estos servicios permiten a desarrolladores, organizaciones o empresas crear aplicaciones web, modelos de inteligencia artificial y cualquier otro tipo de solución que requiera potencia computacional sin la necesidad de contar con una infraestructura física dedicada. De este modo, se favorece el desarrollo de soluciones tecnológicas más escalables, las cuales, en el caso de utilizar infraestructura propia, estarían limitadas por la inversión realizada por la organización. Algunos de los beneficios que entrega el uso de servicios de Cloud Computing son: mayor flexibilidad de capacidades computacionales, reducción en costes de ejecución, automatización de actualización de software y hardware, entre otros. [Xue y Xin, 2016].

Durante la pandemia del COVID-19, esta tecnología experimentó un incremento significativo en su uso, debido a su facilidad de implementación y su eficiencia en el ajuste de la capacidad de los sistemas construidos, aspectos que permitieron resolver los problemas que se vieron acentuados por el contexto. Sin embargo, este aumento en la adopción del Cloud Computing no estuvo acompañado de un mayor conocimiento sobre la protección de dichos sistemas. Como resultado, en muchos casos, la seguridad de las soluciones implementadas fue deficiente [Mandal y Khan, 2020a], lo que podría acarrear graves consecuencias para las organizaciones, tales como ataques de Ransomware [Sajjan y Ghorpade, 2017], Malware [Watson *et al.*, 2015], Denegación de Servicio [Bonguet y Bellaïche, 2017], entre otros. La CSA a partir de su informe anual sobre amenazas en Cloud Computing, presentó cuáles fueron las amenazas mas importantes durante la pandemia del COVID-19, donde muestra datos como la criticidad de cada amenaza ponderado a partir del conocimiento de mas de 700 expertos del área. Esto se presenta en la tabla 1, donde adicionalmente, se agrega una breve descripción de cada amenaza.

Nº	Puntaje	Problema	Descripción
1	7.73	Gestión débil de credenciales y privilegios	Accesos mal gestionados permiten comprometer datos sensibles.
2	7.59	Interfaces y APIs inseguras	APIs mal diseñadas exponen servicios a ataques.
3	7.42	Mala configuración y cambios no controlados	Fallas en configuraciones permiten vulnerabilidades.
4	7.41	Falta de estrategia de seguridad en Cloud Computing	Ausencia de controles claros incrementa riesgos.
5	7.28	Desarrollo inseguro de software	Errores en código abren puertas a ataques.
6	7.21	Recursos de terceros no seguros	Proveedores externos pueden introducir brechas.
7	7.14	Vulnerabilidades del sistema	Software sin parches puede ser explotado.
8	7.11	Divulgación accidental de datos	Configuraciones erróneas exponen información.
9	7.10	Riesgos en serverless y contenedores	Configuración débil facilita ataques rápidos.
10	7.09	Amenazas APT / hackers	Delincuentes sofisticados se enfocan en Cloud Computing.
11	7.09	Exfiltración de datos en Cloud Computing	Robo de datos sin detección desde Cloud Computing.

Tabla 1: Top 11 vulnerabilidades en Cloud Computing en 2020

Fuente: [CSA, 2020b]

En cuanto a las soluciones existentes, hay modelos o marcos de trabajo (*frameworks*) de cumplimiento que buscan asegurar los sistemas tecnológicos, tales como la ISO/IEC 27001 [Calder, 2020], el NIST CSF [Ibrahim et al., 2018], entre otros. Sin embargo, la realidad es que estos modelos no cuentan con un enfoque técnico específico para Cloud Computing. Aunque existen estándares complementarios a las normativas mencionadas para abordar aspectos relacionados con el uso de servicios de Cloud Computing, como la normativa ISO/IEC 27017 [TENELEMA et al., 2020] y NIST SP 800-144 [Jansen y Grance, 2011], su aplicación puede resultar compleja e incompleta sin un sistema de gestión de seguridad de la información (SGSI) formalmente establecido. La falta de un SGSI dificulta la implementación efectiva de estos estándares [Vaca Báez, 2023].

Como solución a este problema, se propone una metodología enfocada en desarrollar un plan de trabajo para tratar aspectos de seguridad en entornos de Cloud Computing.

Como la seguridad en Cloud Computing es un problema multidisciplinario que abarca todas las áreas relacionadas con el desarrollo de soluciones tecnológicas, el enfoque de la solución a este problema se debe centrar en las tres áreas con mayor participación debido al alcance de la memoria, estas áreas son: Infraestructura en Cloud, Desarrollo en Entornos de Cloud

y Seguridad de la Información [CSA, 2021]. Esta última es la responsable de implementar la solución propuesta.

Se considera como alcance de la metodología propuesta para organizaciones que no han enfocado sus esfuerzos en la protección de sus entornos en Cloud. Es decir, la solución es aplicable tanto para organizaciones que utilizan un Sistema de Gestión de Seguridad de la Información (S GSI) no enfocado en Cloud Computing, como para organizaciones emergentes que necesitan asegurar sus sistemas desplegados en Cloud. La propuesta se encuentra basada en marcos de trabajo (*frameworks*) utilizados para la protección de la seguridad de la información, tanto en general como en aspectos relacionados con la seguridad en Cloud Computing y las amenazas más frecuentes en sistemas basados en Cloud Computing.

El trabajo desarrollado en esta memoria abarca desde el análisis del problema hasta la construcción y validación de la solución. En este contexto, este documento se organiza en los siguientes capítulos:

1. En el Capítulo 1, se define el problema y se investiga el contexto de la situación, así como la gravedad de los problemas de seguridad en entornos de Cloud Computing. También se establece el alcance y los objetivos del trabajo.
2. En el Capítulo 2, se construye un marco conceptual sobre los temas más relevantes relacionados con el contexto del problema, tales como una descripción de lo que es Cloud Computing, cómo se adapta el desarrollo seguro a este entorno y las distintas alternativas que se utilizan actualmente para resolver los problemas de seguridad.
3. En el Capítulo 3, se presenta una propuesta de solución, en la que se conectan los elementos anteriores en una metodología que permita utilizar el marco conceptual como una herramienta para asegurar los entornos Cloud, sin perder de vista la flexibilidad que la solución debe tener según el contexto, y el tiempo en el que se implemente.
4. En el Capítulo 4, se argumenta cómo la metodología cumple con los objetivos definidos en el Capítulo 1 y se presentan los avances reales obtenidos en la aplicación de la metodología en una empresa de tecnología.
5. Finalmente, en el Capítulo 5, se presenta una conclusión de la memoria, que profundiza en los elementos fundamentales desarrollados a lo largo del trabajo, las ventajas y desventajas del uso de la metodología propuesta, las posibles mejoras a implementar y las áreas de trabajo futuro necesarias para continuar con el desarrollo de la solución.

CAPÍTULO 1

DEFINICIÓN DEL PROBLEMA

1.1. Contexto

Cloud Computing es una tecnología que transforma una infraestructura tecnológica tradicional en recursos computacionales virtuales para procesar información, gestionar servidores, desarrollar aplicaciones, entre otras funciones. Esta tecnología se destaca por ser utilizada por empresas con robustas infraestructuras físicas, estas ofrecen sus unidades computacionales a otras organizaciones o usuarios a través de un modelo de negocio basado en el principio de “paga por lo que usas”, es decir, el consumidor del servicio solo paga por los recursos que realmente consume [Borra, 2024].

Este modelo ofrece múltiples beneficios a sus clientes. Permite implementar servicios en períodos cortos de tiempo de manera ágil, facilita el aumento o la disminución de la capacidad computacional de los sistemas según las necesidades de la organización, y automatiza tareas relacionadas con la actualización de hardware y software. Además, proporciona una significativa reducción en los costos operativos, siendo esta última la principal razón por la cual, inicialmente, la computación en la nube resulta una opción atractiva para las empresas. [Xue y Xin, 2016].

Si bien Cloud Computing ha mantenido un crecimiento positivo en la última década, en los últimos años, su crecimiento se ha visto potenciado, principalmente por el aumento explosivo de la demanda por su uso. Sin embargo, su masificación no se debe únicamente a los beneficios inherentes de su uso, sino también al contexto global vivido en 2020 debido a la pandemia del COVID-19 y a los problemas de capacidad que afectaron a la infraestructura tecnológica de ese entonces. Como indicio de que este incremento surge debido a la pandemia, StackOverflow presentó durante 2021, un artículo donde presenta el volumen de preguntas realizadas bajo los Tags relacionados a Cloud Computing. En éste se observa que a inicios de 2020 se presentaba un incremento importante en las consultas acerca de Cloud Computing el cuál estaba muy alejado a las predicciones de crecimiento esperadas; este incremento coincide con la fecha de inicio de la pandemia del COVID-19 y sugiere una relación entre la pandemia y el aumento del uso de Cloud Computing. El gráfico que presenta lo anteriormente descrito se encuentra en la figura 1.

La pandemia del COVID-19 fue declarada durante el año 2020, debido a un virus altamente contagioso y difícil de tratar. La principal medida adoptada en ese momento fue prevenir los contagios, lo que llevó a cada país a implementar estrategias de distanciamiento social y aislamiento. Como resultado, se redujo significativamente la interacción social entre las personas, lo que afectó enormemente al comercio, la producción y la educación. Algunas medidas tomadas en estos momentos fueron: la suspensión de clases presenciales, trabajos de oficinas se trasladaron a una modalidad en línea y las reuniones sociales quedaron

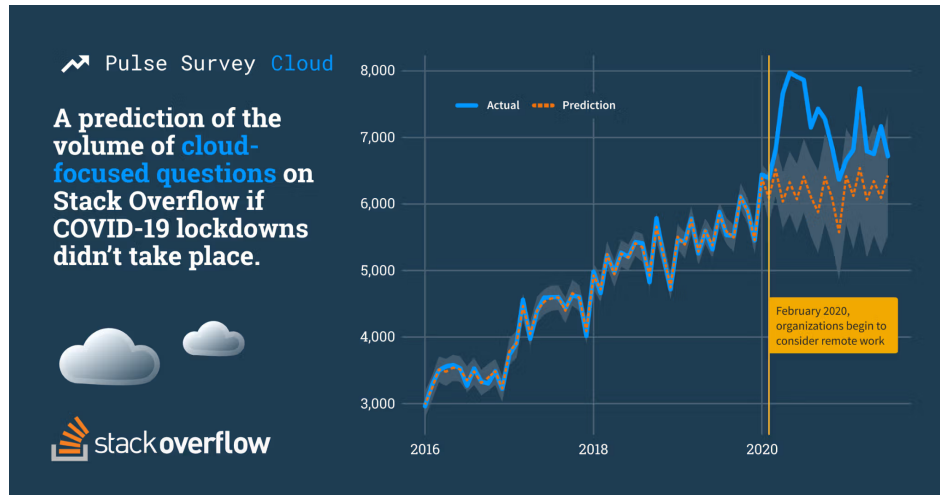


Figura 1: Crecimiento Cloud durante pandemia
Fuente: StackOverflow [Overflow, 2021]

prohibidas [Singh et al., 2021].

Es difícil cuantificar la cantidad exacta de personas que no pudieron retomar sus actividades habituales debido a las circunstancias, y que se vieron obligadas a iniciar un proceso de digitalización. Como ejemplo, podemos analizar el ámbito educativo; la UNESCO estimó que durante la pandemia, se suspendieron las clases presenciales a cerca de 1600 millones de niños y jóvenes [UNESCO, 2025]. Con este ejemplo, podemos notar que surgieron problemas para retomar la productividad sin salir de casa, lo que se ve alineado con las soluciones ya existentes de teletrabajo o en este caso, educación en línea, por lo que se incrementó el uso de tecnologías como clases en línea, trabajos remotos y la digitalización de diversas actividades productivas, siempre que fuera factible.

Otro ejemplo, pero a nivel del consumo de las aplicaciones Cloud, es la aplicación Zoom [Kerravala, 2025]. Se realizó una publicación que presenta la instalación y descarga de la plataforma con un incremento exponencial durante el año 2020 (figura 2). Lo cual nos da indicios de que esta tecnología fue necesitada para labores tales como teletrabajo o clases en línea y por lo cual Zoom necesitó un escalamiento rápido para solventar tal demanda.

Este incremento de uso de servicios digitales generó una mayor demanda de elementos computacionales tales como: almacenamiento de datos, procesamiento computacional y servicios de internet, los cuales pocas empresas podían satisfacer con su propia infraestructura física. A pesar de esto, la falta de capacidades no era un problema nuevo, sino uno que la tecnología de Cloud Computing venía resolviendo desde hacía años.

Las características del Cloud Computing permitieron un aumento de capacidades rápido, efectivo y sin necesidad de la implementación de infraestructura física. En concreto, en el contexto de la pandemia, se necesitó una aceleración sustancial en la implementación de teletrabajo, educación en línea, construcción de entornos mas sustentables

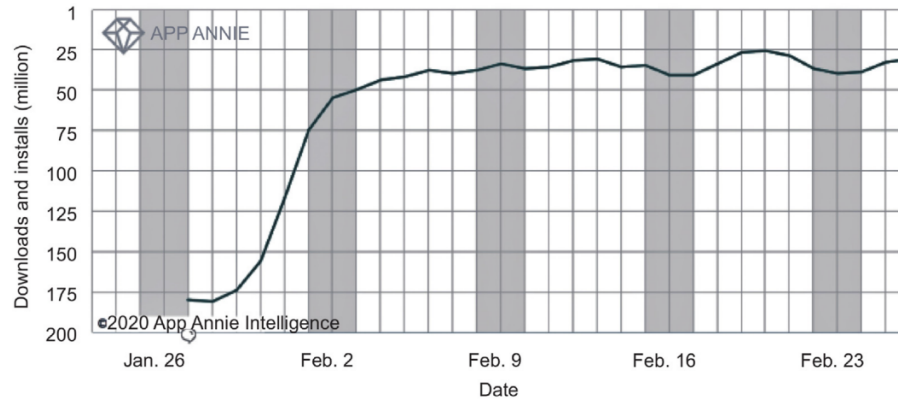


Figura 2: Consumo Zoom
Fuente: [Alashhab et al., 2021]

[Ezema y Rivera, 2021]. Sin embargo, esto también acarreo nuevas dificultades, tales como el desconocimiento de los equipos tecnológicos acerca del aseguramiento, problemas de uso para los usuarios de este tipos de herramientas y mayor cantidad de ataques debido al contexto de confinamiento global [Mandal y Khan, 2020b].

El artículo, “State of Cloud Security Concerns, Challenges, and Incidents” [CSA, 2021] realizado por la CSA junto en colaboración con la organización AlgoSec, presenta un panorama de adversidades que se están viviendo respecto al uso de esta tecnología, que a grandes rasgos, permite destacar lo siguiente:

1. Se consultó acerca de cuales son las áreas encargadas de la seguridad de la información en entornos Cloud y se llegaron a las ponderaciones de: Operaciones de seguridad (35 %), Equipos de Cloud (18 %), Operaciones TI (16 %), Operaciones de redes (9 %), Ingenieros DevOps(8 %), entre otras. Estos resultados se presentan en la figura 3
2. Existe un 55 % de empresas que reconocen una falta de conocimiento en certificaciones y capacitaciones dentro del apartado de Cloud Security.
3. Un 8 % de las empresas posee su infraestructura completa en algún servicio de Cloud Computing y se estima que para el año 2021, se incrementará a un 21 %.
4. Un 20 % de los encuestados declaran no haber tenido incidentes relacionados a Cloud Computing, un 41 % no está seguro y 11 % si los ha tenido.

La información previamente presentada muestra la tecnología es un área multidisciplinaria con múltiples aristas responsables de la seguridad de sus servicios, no siendo suficiente con los controles de seguridad implementados por el proveedor de servicios, aún así, por motivos de alcance de la memoria, el análisis se centrará en las áreas de desarrollo, áreas dedicadas a la infraestructura Cloud y áreas relacionadas a seguridad de la información, con

la intención de dedicar trabajo futuro en el resto de las áreas involucradas. Si bien Cloud puede traer grandes beneficios para una organización, debe ser implementada por personal capacitado. Esto se debe, entre otros aspectos, a los grandes riesgos que conllevan este tipo de herramientas respecto a la seguridad de la información, y a que si bien este problema ya existía cuando surgió esta tecnología, su rápida implementación en el transcurso de los últimos años provocó que las empresas no estuviesen preparadas desde un punto de vista técnico, y pusiesen en riesgo su información.

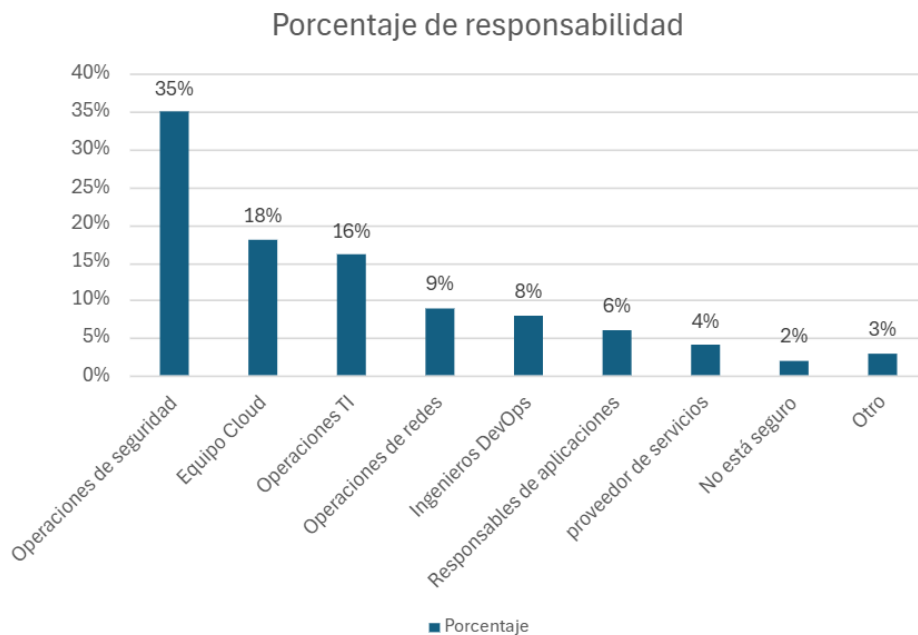


Figura 3: Responsables de Cloud Security

Fuente: [CSA, 2021]

Respecto a las amenazas relacionadas a Cloud, anualmente la CSA realiza un reporte sobre las mayores de amenazas presentadas en entornos de Cloud Computing[CSA, 2024], estas amenazas están cambiando constantemente y están arraigadas a problemas como: el manejo de accesos a los servicios en Cloud, manejo inadecuado del control de cambios, APIs desarrolladas de forma insegura y falta de conocimiento en arquitectura Cloud. El alcance de la metodología planea en primera instancia gestionar la mitigación de las amenazas mencionadas según su importancia y contexto de la empresa.

El impacto de estas amenazas puede ser muy grave para las organizaciones, independiente de su tamaño, sus consecuencia pueden ejemplificarse en: Fuga de datos sensibles, degradación de rendimiento operacional, Ransomware, incumplimiento normativo y legal, entre otros [CSA, 2024].

Inclusive, si se llegasen a mitigar todas las amenazas presentadas en los reportes mencionados, no sería suficiente, porque como se mencionó anteriormente, las amenazas cambian constantemente según el contexto de la organización y el global, por lo tanto, se requieren

medidas que permitan un aprendizaje constante por parte de los equipos de tecnología, para mantenerse actualizado respecto a los desafíos y los riesgos actuales del uso de Cloud Computing [Peña-Robayo et al., 2024].

En resumen, actualmente se presenta una situación donde la falta de conocimiento sobre Cloud security, principalmente en áreas relacionadas al desarrollo e infraestructura en el contexto de seguridad de la información, generan riesgos importantes para los sistemas desarrollados por las empresas.

Con estos antecedentes, podemos mostrar el problema a partir del siguiente diagrama de árbol:

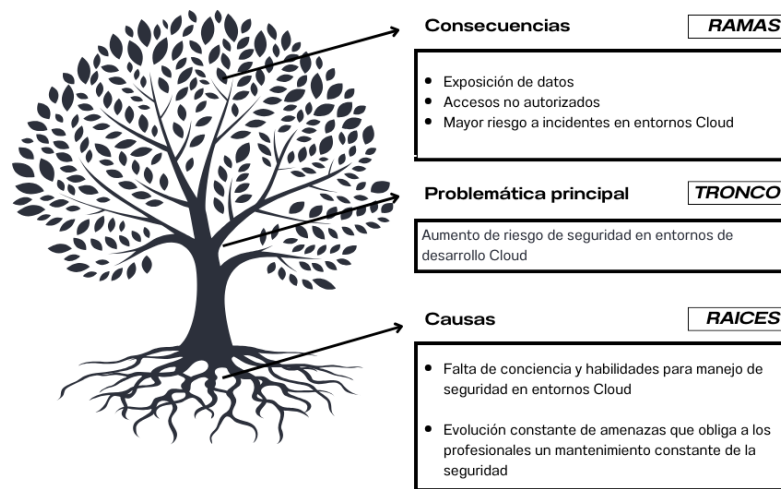


Figura 4: Árbol del problema
Fuente: Elaboracion Propia

1.2. Objetivos de la memoria

A partir de lo presentado, se propone como solución construir una metodología de desarrollo seguro en Cloud Computing que permita gestionar el proceso de protección de los activos de información u otros recursos tecnológicos de una organización según su contexto. Esta será contruida a partir de los siguientes objetivos:

Objetivo principal

1. Diseñar una metodología de desarrollo seguro de aplicaciones y sistemas de software para Cloud Computing, la cual esté basada en estándares de seguridad reconocidos a nivel internacional, y permita a empresas de madurez baja o intermedia en aspectos de seguridad construir y auditar controles tecnológicos.

Objetivos específicos

1. Seleccionar y analizar estándares de seguridad relevantes para el desarrollo en Cloud, identificando los elementos críticos que permitan garantizar la seguridad de las aplicaciones que desarrolle una organización específica.
2. Elaborar indicadores que permitan evaluar y cuantificar el progreso de implementación de controles de seguridad en el desarrollo de software en Cloud.
3. Diseñar un marco de seguridad que cubra las etapas del ciclo de vida del desarrollo de software en entornos Cloud.
4. Establecer procesos de mejora continua que faciliten la actualización y adaptación de la metodología a lo largo del tiempo.

Para cumplir estos objetivos, se deben abordar aspectos clave como las configuraciones de los entornos Cloud, el desarrollo de aplicaciones y la seguridad de la información. Además, contemplar una línea de implementación adaptable según el nivel de madurez y los controles que se utilicen en la organización donde se va a aplicar la metodología. Con esto, se espera construir una herramienta que permita visibilizar los riesgos existentes, incorpore la capacitación constante de los responsables, se adapte a la madurez de la organización y ayude a la mejora continua en estos aspectos.

CAPÍTULO 2

MARCO CONCEPTUAL

Para comprender correctamente cómo abarcar el problema se requiere indagar en aspectos de Cloud Computing, desarrollo de Software y seguridad de la información. Por lo que este capítulo se ha dividido en las siguientes 4 secciones, a saber: (1) las características principales de Cloud, (2) las características de DevSecOps en Cloud Computing, (3) seguridad de la información en el contexto de Cloud Computing y (4) modelo de mejora continua. Si bien la última sección no es un tema asociado a Cloud Computing, tiene una gran relevancia en la construcción de la metodología asociada a esta memoria.

2.1. Las características principales de Cloud

Esta sección busca abarcar el concepto de Cloud como servicio de infraestructura tecnológica y las principales características en torno a estos usos.

¿Qué es Cloud Computing? Corresponde a una tecnología que abstrae la infraestructura física de servidores, centros de datos o hardware, transformándola en recursos computacionales. Estos recursos, al estar virtualizados, permiten la creación de múltiples servidores virtuales o servicios aislados entre sí, lo que facilita el aumento o la reducción de sus capacidades en función del uso de una mayor o menor cantidad de unidades. Todo esto se realiza con total transparencia respecto a las capas físicas del hardware.

A partir de estas características se desarrollan los servicios de Cloud Público bajo el modelo de "paga por lo que usas". Estos servicios son ofrecidos por un proveedor de servicios Cloud (Cloud Service Provider, CSP), y permiten que un consumidor de servicios Cloud (Cloud Service Consumer, CSC) utilice todos los recursos necesarios para construir su infraestructura computacional. Posteriormente, generalmente de forma mensual, el CSC realiza un pago basado en la cantidad de recursos computacionales utilizados y el tiempo de uso. [Patidar et al., 2012].

Diferencias entre Cloud Computing y un datacenter "on premise": Un servicio *on premise* se define como el uso de servicios de infraestructura a partir de un datacenter propio. A diferencia del servicio contratado de Cloud Computing requiere un alto coste de inicialización y un equipo con conocimientos de hardware e infraestructura física para su mantención y futuro escalamiento, el cuál está limitado por las capacidades físicas del datacenter. Pesa a lo anterior, se considera una buena opción debido a que permite un control absoluto sobre la seguridad física de la infraestructura, aplicación de redes locales o privadas. La selección del método a utilizar dependerá exclusivamente del contexto de la organización y del uso que se le pretende dar.

Las diferencias se resumen en la siguiente tabla: 2

Categoría	On-premise	Cloud Computing
Tiempo de salida al mercado	Configuración más lenta por compra de hardware	Configuración más rápida, solo requiere apps y conexión a Internet
Costo	Costos iniciales por hardware, licencias y servidores físicos	No requiere una inversión inicial
Escalabilidad	Requiere más tiempo, esfuerzo y dinero	Escalable fácilmente en todas las ubicaciones
Confiabilidad de las conexiones a internet	Depende del proveedor Cloud	Depende del proveedor de internet de la organización
Continuidad del negocio	Cambio manual de servidor ante desastres genera demoras	Transición fluida y sin demoras ante desastres

Tabla 2: Comparación entre instalación On-premise y usando Cloud Computing

Fuente: [Ameyo, 2024]

Tipos de arquitectura Cloud Existen 4 tipos de arquitecturas principales en Cloud, éstas son un punto clave puesto que su comprensión implica tomar mejores decisiones sobre como desplegar una solución en Cloud:

1. Cloud Público: Es cuando el proveedor del servicio Cloud es un usuario externo al cliente, es el caso mas común de Cloud.
2. Cloud Privado: Es cuando el cliente tiene su propio Centro de Datos basado en la tecnología de Cloud Computing, esto lo puede realizar a partir de Arquitectura propia o utilizando herramientas como OpenStack o Apache CloudStack
3. Cloud Híbrido: Es cuando se entremezclan ambos modelos para tener la potencia de los elementos de Cloud público y el resguardo de un Cloud privado. Es necesaria principalmente cuando la empresa tiene datos sensibles intranferibles a un proveedor externo.
4. Cloud Comunitario: Es cuando se combinan servicios de Cloud públicos y privados al igual que en el caso anterior, como tener la infraestructura para poseer un Cloud privado es altamente costoso se realizan alianzas entre empresas para poseer un Cloud privado entre un número limitado de entidades. No es tan seguro como lo sería un Cloud privado para una única empresa, pero es mas barato en términos de despliegue.

MultiCloud: Es cuando una organización utiliza servicios públicos de dos o más proveedores distintos, por ejemplo AWS, Azure y Google Cloud, de forma coordinada e integrada. Su propósito es optimizar rendimiento, disponibilidad y costos, así como evitar la dependencia de un solo proveedor.

No se debe confundir MultiCloud con Cloud Híbrido. Mientras que el enfoque MultiCloud se basa en utilizar múltiples servicios Cloud públicos de diferentes proveedores para aprovechar lo mejor de cada uno y evitar la dependencia de un solo proveedor, el modelo de Cloud Híbrido busca integrar la infraestructura local (on-premises) o privada con servicios de Cloud público, permitiendo una gestión unificada y flexible de cargas de trabajo. Es decir, MultiCloud se centra en la diversificación de proveedores, mientras que el Cloud Híbrido prioriza la combinación de entornos locales y en Cloud para una mayor continuidad operativa y control. En la figura 5 se puede apreciar esta diferencia en la comunicación de los servicios.

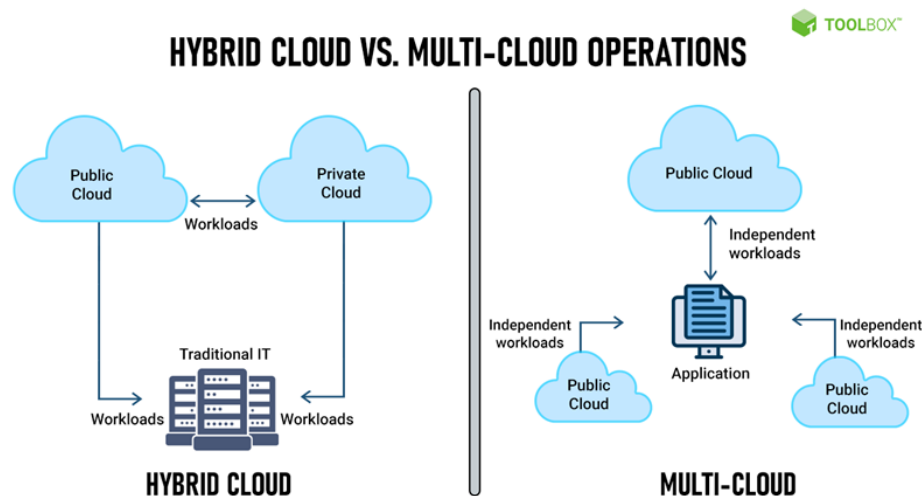


Figura 5: Diferencias entre MultiCloud y Cloud híbrido
Fuente: Artículo de SpiceWorks [Kanade, 2022]

Tipos de servicios en Cloud: Los recursos de un servidor Cloud se pueden configurar para entregar distintos servicios según se requiera, independiente de la arquitectura, entre ellos, la NIST define los siguientes tipos de servicios [Mell y Grance, 2011]:

1. **Serverless y Microservicios:** Según el artículo de CloudFlare [Cloudflare, 2025], podemos considerar un microservicio como una fragmentación independiente de un programa, por lo que a este tipo de elementos dentro de Cloud Computing les podemos atribuir un modelo *serverless*, este implica la atribución dinámica de recursos al servicio solo en caso de necesitarlo, en caso contrario no será necesario contratar un servidor para que pueda ser llamado.
2. **Software as Service (SaaS):** Es un modelo en el cual se utilizan aplicaciones del proveedor que se ejecutan en una infraestructura Cloud. Estas aplicaciones son fácilmente

accesibles, normalmente a partir de un sitio web. El usuario no gestiona ni controla la infraestructura de la aplicación, es decir, no tiene control sobre la red, servidores, sistemas operativos o almacenamiento, y solo puede realizar configuraciones limitadas a nivel de aplicación.

3. Platform as Service (PaaS): Son servicios que entregan al consumidor un entorno para desplegar sus propias aplicaciones (creadas o adquiridas) en la infraestructura Cloud del proveedor, utilizando herramientas y lenguajes de programación soportados. El usuario no administra la infraestructura base (redes, servidores, sistemas operativos, almacenamiento), pero sí tiene control sobre las aplicaciones desplegadas y algunas configuraciones del entorno de ejecución.
4. Infrastructure as Service (IaaS): Son servicios que entregan proporciona al consumidor la capacidad de provisionar recursos informáticos fundamentales como procesamiento, almacenamiento y redes. El usuario puede instalar y ejecutar cualquier software, incluidos sistemas operativos y aplicaciones. Aunque no controla la infraestructura física subyacente, tiene control completo sobre los sistemas operativos, el almacenamiento, las aplicaciones implementadas y, en algunos casos, ciertos elementos de red como los firewalls de host. Es el tipo de servicio que permite una mayor personalización del desarrollo, pero también requiere un mayor nivel de securización por parte del consumidor.

Adicionalmente, por el tipo de modelo “Pagas por lo que usas”, pueden existir numerosos mas servicios del tipo “as a service”. Estos son los conocidos “XaaS”, entre los que se encuentran por ejemplo Database as a service, Function as a service, Storage as a service, entre otros.

2.1.1. Modelo de responsabilidad compartida

Cuando se utiliza un servicio de Cloud público, existen 2 organizaciones principales que interactúan directamente con el entorno: el proveedor del servicio Cloud (Cloud service provider, o en su sigla, CSP) y el consumidor del servicio Cloud (Cloud service consumer, o en su sigla, CSC). Si bien se podría creer que el proveedor del servicio es el responsable de la seguridad de la información, pero no es cierto debido a que los datos y configuraciones realizadas por el CSC dentro de los entornos Cloud son transparentes para el CSP.

Como existen múltiples tipos de servicios en Cloud, existe el denominado Modelo de responsabilidad compartida, donde se realiza la división de las responsabilidades de seguridad para las partes involucradas, según el tipo de servicio y el CSP contratado [REYES y MENDOZA, 2023].

Responsabilidades “Fijas”

Como se mencionó anteriormente las responsabilidades de cada una de las partes varían según el proveedor y el tipo de servicio, pero hay algunas responsabilidades que no tienden a cambiar. Según lo mencionado por la CSA [CSA, 2020a] son denominadas responsabilidades fijas.

Por el lado del proveedor, como los servicios de Cloud Público son esencialmente un servicio de préstamo de infraestructura física, el CSP se responsabiliza de los aspectos relacionados al mantenimiento de la parte física y de su gestión, por lo que es responsable de:

1. Red física, Host físicos y datacenters: El proveedor necesita el Hardware suficiente para proveer a sus clientes de los servicios contratados. Es por ello que todas las comunicaciones entre el datacenter, los hosts y la red deben estar estrictamente asegurados en aspectos como la restricción del acceso físico de los servidores, el monitoreo físico de los servidores y la preparación de planes de contingencia para recuperar el servicio en caso de incidentes.
2. Capa de la virtualización: El concepto de Cloud no es la prestación de datacenters, sino de unidades computacionales que permiten construir distintos tipos de productos como los mencionados en el apartado anterior, por lo que en un servidor se pueden alojar los servicios de múltiples usuarios. Es por ello que se necesita una gestión de la virtualización adecuada, es decir, una segmentación y aislamiento apropiado para recursos como la CPU, GPU, almacenamiento, RAM, etc.

La incorrecta gestión de la virtualización genera amenazas tales como filtración de datos entre usuarios o un aprovisionamiento incorrecto de los recursos que contrata cada cliente.

Por el lado del consumidor del servicio, éste utilizará aplicaciones, configurará su entorno y servicios, gestionará el acceso tanto del propio entorno Cloud como de sus propias aplicaciones construidas en base de éste y tendrá datos con cierta sensibilidad según su contexto organizacional; por lo tanto, en la mayoría de los casos es el responsable de la seguridad de la información en los siguientes aspectos:

1. Datos e Información: El proveedor de ninguna manera tendrá visibilidad o control alguno sobre la información del consumidor. Es por ello que la protección, encriptación, uso y acceso a ésta es responsabilidad del consumidor.
2. Código y aplicación lógica: El consumidor tiene la libertad de construir sus aplicaciones según sus necesidades y facilidades, lo que también implica que él debe asegurarse de que su código sea seguro antes de ser desplegado.
3. Identidad y Acceso: El consumidor es responsable de quienes acceden a su entorno Cloud, debe configurar tanto las contraseñas, permisos para cada usuario, MFA, keys, certificados, reglas de reinicio de contraseñas, etc.

4. Plataforma y recursos para la configuración: Todo servicio de Cloud Computing, ya sea *serverless* o no requiere algún tipo de configuración por parte del CSC. Es responsabilidad del CSC realizar la configuración adecuada según el contexto de la aplicación desarrollada.

Zonas Grises Existen ciertos elementos que varían en la responsabilidad según el tipo de servicio utilizado, o bien, según el tipo de proveedor que se utiliza. La CSA menciona como “zonas grises” [CSA, 2020a], y son las siguientes:

1. Identificación e infraestructura de directorio: El manejo de las identidades con acceso a los servicios de AWS utilizados por terceros y el uso de Active Directory u otro servicio que se contrate, es responsabilidad compartida. En caso de ser un servicio PaaS o SaaS, es altamente probable que la configuración sea realizada por el proveedor.
2. Aplicaciones: Cuando se utiliza un servicio PaaS o SaaS, existen aplicaciones dispuestas por parte del proveedor ya preparadas para ser utilizadas, por lo que no necesitan que sean aseguradas por el consumidor. Mientras que, cuando se instala una aplicación por parte del consumidor en entornos IaaS, la seguridad de ese entorno es responsabilidad única del consumidor.
3. Controles de Redes: El proveedor tiene sus propias redes aseguradas, si se utilizan redes externas a las proporcionadas por el proveedor, es responsabilidad del consumidor protegerlas.
4. Sistema Operativo: PaaS y SaaS entregan una menor flexibilidad pero permiten al consumidor un entorno seguro hasta la capa del sistema operativo. Si se requiere más flexibilidad se debe utilizar un entorno IaaS. El proveedor normalmente proveerá una licencia y un catálogo de SO, pero es responsabilidad del consumidor informarse sobre su seguridad y proveer a su sistema de parchados/revisiones periódicas.

El modelo de responsabilidad compartida de seguridad es un concepto variable según la interpretación del CSP contratado, por lo que la definición presentada anteriormente se debe considerar como una presentación del modelo a grandes rasgos.

Se puede conocer el modelo específico por aplicar si se conoce quien es el CSP y los tipos de servicio empleados por la organización en concreto, por ejemplo, si se va a utilizar un modelo IaaS con el proveedor de servicios AWS, bastará con revisar el modelo de seguridad de información que plantean (figura 8), permitiendo concretar cuáles son las responsabilidades de seguridad de cada parte involucrada.

Una vez se conoce cuáles son las responsabilidades de la organización en torno a infraestructura de seguridad, es necesario aplicar controles que permitan cumplir estas responsabilidades, un buen acercamiento a estos controles es la matriz de controles Cloud desarrollado por la CSA (Cloud control matrix, es sus siglas, CCM)¹.

¹[CSA, nd]

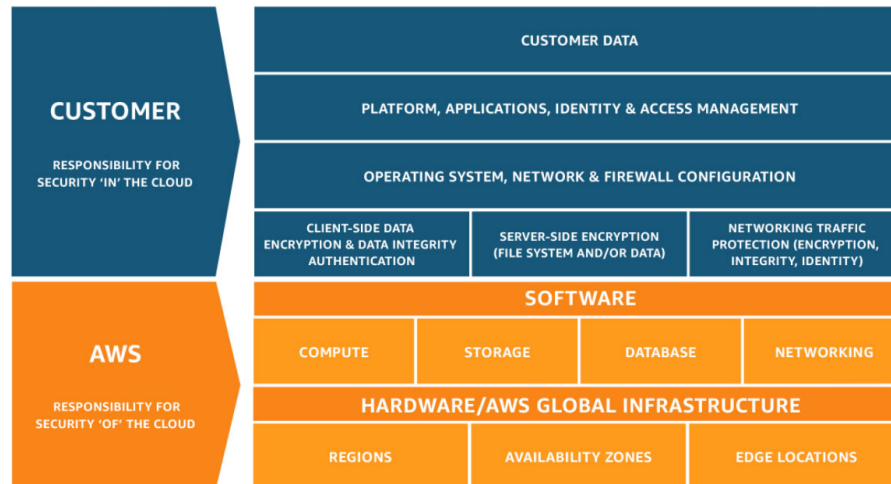


Figura 6: Modelo de responsabilidad compartida de servicios AWS
Fuente: Artículo de AWS [AWS, 2025a]

Cloud Control Matrix (CCM)

La CCM es un *framework* de Ciberseguridad de Cloud, el cual presenta 197 controles divididos en 17 dominios, es una guía sobre qué controles deben aplicarse en un entorno de Cloud Computing tanto por el CSP como por el CSC y clasifica sus controles según sus tipos de servicios, frameworks aplicados, áreas de la organización, entre otros.

Sus principales atractivos son:

1. Entrega una estandarización del modelo de responsabilidad compartida, siendo sus controles catalogados según quién es el responsable de aplicarlos (proveedor, consumidor, compartido), el tipo de servicio (SaaS, IaaS, PaaS) y el área responsable dentro de la empresa (RRHH, arquitectura, seguridad de la información, etc.).
2. Tiene equivalencias con otros frameworks de cumplimiento; es decir, si ya se posee una certificación de seguridad, existe un *mapping* que facilita la construcción y determinación de la(s) brecha(s) de seguridad existente(s).
3. Es un *framework* especializado en Cloud Computing, por lo que es ideal cuando se tiene una seguridad generalizada y se busca abarcar el contexto específico de Cloud security.
4. Cuenta con una certificación llamada CSA STAR, la cual se entrega a los proveedores que cumplen con sus controles de seguridad. Actualmente esta certificación es cumplida por los proveedores mas populares de servicios Cloud, es decir: AWS, Microsoft Azure y Google Cloud.

Como parte de la investigación se revisó un análisis de efectividad de la CCM externo a lo presentado por la propia empresa desarrolladora del *framework*. Se revisó el estudio “Analysis of the Effectiveness of Cloud Control Matrix for Hybrid Cloud Computing” [Tariq, 2018], donde para el análisis se revisó una lista de 37 amenazas comunes dentro de Cloud Computing en el año 2018, luego de los experimentos, se llegó a la conclusión de que todos los riesgos revisados estaban siendo controlados por este framework en alguna medida, con una tendencia favorable hacia los controles relacionados a los dominios de “Aplicaciones e interfaces de seguridad” (Application & Interface Security, en su sigla, AIS) y manejo de vulnerabilidades (TVM: Threat & Vulnerability Management, en su sigla, TVM), y que efectivamente, el conjunto de controles propuesto por la CSA permite un control correcto de los riesgos de Cloud, por lo menos en los casos estudiados.

2.2. Las características de DevSecOps en Cloud Computing

Uno de los elementos mencionados dentro de reportes e investigaciones acerca del problema de seguridad en entornos de desarrollo Cloud, es la falta de comunicación entre desarrolladores/infraestructura y el área encargada de la seguridad [CSA, 2021]. Una de las formas para mejorar la comunicación entre ambas áreas es transicionar de una metodología basada en prácticas DevOps hacia una DevSecOps.

DevOps viene del conjunto de las palabras desarrollo y operación, consta del ciclo de vida desde el desarrollo hasta la operación de la aplicación sin realizar pruebas de seguridad, o bien, realizándose únicamente en las etapas finales del desarrollo, por lo que, además de ser una práctica sin una integración efectiva de la seguridad de la información en el desarrollo, también provoca problemas de comunicación entre los equipos de desarrollo y seguridad, puesto que sus tareas se encuentran segmentadas entre sí y no hay una retroalimentación durante el ciclo de vida del software.

DevSecOps viene a solucionar este problema, es la práctica de la integración de revisiones de seguridad en entornos de desarrollo durante todo el ciclo de vida de desarrollo de software (SDLC). Es decir, desde su análisis de requisitos inicial hasta su implementación e iteraciones continuas, esto independiente de la metodología de desarrollo utilizada o bien al entorno que se va a utilizar, en este caso Cloud Computing [AWS, 2025b]. Esto se puede apreciar en la figura 7, realizada por la empresa dynatrace.

En esta figura se observa la etapa de seguridad de la información como una capa exterior del ciclo de desarrollo, que afecta a todas y cada una de las etapas que lo conforman.

Los beneficios del uso de esta práctica no sólo aplican en aspectos de seguridad, sino también en los propios costos y optimización del tiempo de desarrollo; podemos enumerar los siguientes beneficios:

1. Detección temprana de vulnerabilidades: Cuando las pruebas de seguridad sólo se

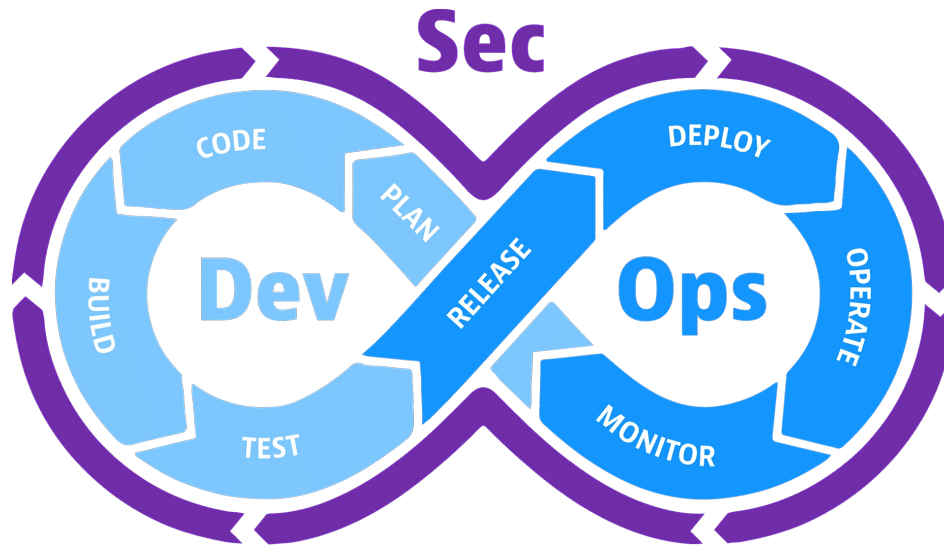


Figura 7: Comparación modelo DevSecOps vs DevOps

Fuente: [Dynatrace, 2025]

realizan en una fase final del proyecto se puede elevar los costos de remediación de los hallazgos, pues obviar hallazgos que en etapas más tempranas de desarrollo eran más evidentes o no permitir tener una visión global sobre qué tan seguro es la aplicación a medida que pasa el tiempo. Por esto y otros motivos se recomienda utilizar el método DevSecOps, inclusive si es un desarrollo en Cloud Computing.

2. Reducir el tiempo de comercialización: Parte de DevSecOps trata de utilizar pruebas de seguridad automatizadas dentro del desarrollo de la aplicación. Lo que permite reducir el tiempo del desarrollo en las últimas etapas de revisión de seguridad
3. Garantizar el cumplimiento de las regulaciones: Permite realizar revisiones constantes al cumplimiento de las regulaciones de seguridad del proyecto, debido a las recurrentes revisiones durante el desarrollo
4. Crear una cultura consciente de la seguridad: Los desarrolladores son constantemente revisados y corregidos respecto a prácticas dentro del código relacionadas a la seguridad de éste. Lo que les da una retroalimentación activa y les permite ser más conscientes de los riesgos que conlleva una mala gestión de seguridad de la información.
5. Desarrollar nuevas características de forma segura: Mejora la relación entre el DevOps tradicional y seguridad. Lo que conlleva a la búsqueda de aportar valor a los desarrollos de forma mas homogénea, permitiendo mejoras en las evaluaciones e informes de seguridad.

Según la investigación de [Ibrahim et al., 2022] los aspectos clave a considerar para implementar DevSecOps en una organización son los siguientes:

1. Enfoque de seguridad hacia la izquierda: La seguridad se debe revisar en cada etapa de desarrollo del software, es importante la constante comunicación del equipo encargado de la seguridad y el equipo desarrollador, desde una etapa de requisitos hasta las próximas iteraciones de la misma aplicación
2. Pruebas y monitoreo continuo de seguridad: Adicional a esto, la aplicación debe ser constantemente monitoreada y testeada por el equipo de seguridad, esto con el objetivo de detectar amenazas y vulnerabilidades en las etapas mas tempranas de desarrollo
3. Análisis de seguridad automatizados y gestión de vulnerabilidades: En sistemas mas maduros es recomendable la utilización de herramientas de manejo de vulnerabilidades más automatizadas, que permitan una mayor eficiencia en la detección de problemas de seguridad

Si bien estos aspectos clave son aplicables para cualquier tipo de desarrollo, en el contexto específico de Cloud, se proponen las siguientes herramientas que normalmente están anexas a DevSecOps en Cloud:

1. Infraestructura como código (IaC): El Código como infraestructura permite construir entornos Cloud estandarizados sin la necesidad de una configuración manual.
2. Contenedores y despliegue de microservicios: El uso de contenedores y microservicios correctamente gestionados y configurados permite un control de acceso, control de versiones e implementación de parches y pruebas de seguridad mucho mas eficiente.
3. Monitoreo de entornos Cloud y respuesta a incidentes: Se debe aprovechar las herramientas entregadas por el propio proveedor de Cloud público para realizar un monitoreo de desviaciones dentro de la seguridad de la organización, además de contar con herramientas adicionales como un SIEM (Security Information and Event Management), la cual es una herramienta que permite un análisis en profundidad de los datos mediante la recolección, correlación y visualización centralizada de eventos de seguridad.

2.3. Seguridad de la información en el contexto de Cloud Computing

Además de conocer las características de Cloud, es necesario conocer que fuentes podemos consultar para informar y capacitar a los equipos de tecnología de la organización, como podemos implementar medidas para defender los sistemas, que amenazas existen actualmente para la organización en aspectos de seguridad de la información y como podemos visibilizar que los planes o medidas aplicadas están siendo implementadas correctamente y entregando los resultados esperados.

2.3.1. Fuentes de información

Existen instituciones y proveedores que cuentan con equipos dedicados a investigar los riesgos asociados a Cloud Computing y las estrategias para su mitigación. A su vez, estos organismos ofrecen soluciones y recomendaciones a los usuarios de dicha tecnología. Algunas de estas entidades son:

1. Cloud Security Alliance (CSA)² : Es una organización estadounidense formada en 2008 y sin fines de lucro. Tiene el objetivo de promover el uso de las mejores practicas de seguridad respecto a Cloud Computing y proveer educación en el uso de la tecnología. Actualmente posee cerca de 80000 afiliados a lo largo del mundo. Entre las investigaciones que realiza se encuentran: Reportes sobre las mayores amenazas de Cloud, reportes del estado actual de Cloud security y una certificación de seguridad para proveedores de servicios Cloud (CSA STAR) que actualmente es utilizada por proveedores relevantes del área, tales como Google, Amazon y Microsoft.
2. Instituto Nacional de Estándares y Tecnología (NIST)³ : Institución estadounidense relacionada a la gobernanza y la gestión de sistemas. Si bien no se destaca por su dedicación a Cloud posee estándares que permiten la segurización de sistemas y la construcción de SGSI con algunos controles de Cloud security (NIST Cybersecurity Framework).
3. Organización Internacional de Normalización (ISO)⁴ : Institución relacionada a la gobernanza y la gestión de sistemas. En el caso de un SGSI, para Cloud aplica controles tales como la 27001, 27002 y mas específico la 27017. De hecho, en el año 2022, la ISO27002 recibió una nueva versión debido a la relevancia actual de la tecnología Cloud, donde, entre otros cambios, se incluyó un control nuevo relacionado a la seguridad en entornos Cloud y otro respecto a inteligencia de amenazas.
4. Proveedores Cloud: Debido al modelo de responsabilidad compartida, los proveedores tienen claridad sobre cuales son los elementos que deben proteger y cuáles son responsabilidad del usuario. Para el usuario construyen tanto *frameworks*, herramientas y reportes que permitan reducir la brecha de seguridad en sus respectivos sistemas, normalmente se basan en investigaciones de otras instituciones tales como la CSA y la NIST presentadas anteriormente. Entre ellos, se puede mencionar a AWS, Microsoft y Google.
5. Consultoras de Cloud Security: Debido al crecimiento de Cloud existen numerosas empresas que se dedican a construir soluciones a distintos entornos de Cloud Computing, muchas de ellas también tienen equipos de investigación que construyen informes y

²Cloud Security Alliance. (s.f.). *Cloud Security Alliance*. Recuperado el 13 de abril de 2025, de <https://Cloudsecurityalliance.org>

³National Institute of Standards and Technology. (s.f.). *National Institute of Standards and Technology*. Recuperado el 13 de abril de 2025, de <https://www.nist.gov>

⁴International Organization for Standardization. (s.f.). *International Organization for Standardization*. Recuperado el 13 de abril de 2025, de <https://www.iso.org>

metodologías que adopten sus soluciones y entreguen información sobre los problemas que abarcan, como ellos los solucionan y cuales son sus resultado actuales. Entre estas algunas que se podrían mencionar son Sophos, Palo Alto Networks, AlgoSec, Netskope, entre muchas mas.

2.3.2. Controles de seguridad

Una vez se tiene conocimiento de los riesgos actuales de la tecnología y los objetivos de la organización, se requerirá alguna forma de reducir su riesgo; esto se realiza a partir de controles de seguridad.

Los controles de seguridad, que normalmente se encuentran gestionados a partir de un sistema de gestión de seguridad de la información, son medidas aplicadas al negocio con el objetivo de reducir la criticidad de los riesgos encontrados, normalmente se extraen de normativas o *frameworks*.

¿Qué es un Sistema de Gestión de Seguridad de la Información (SGSI)?

Es un conjunto de principios o procedimientos que se utilizan para identificar riesgos y definir los pasos de mitigación de riesgos que deben llevarse a cabo. Es importante notar que a grandes rasgos, esta memoria no presenta una metodología para construir un SGSI pero si entregará un ciclo con algunos controles, indicadores, objetivos y definición de requisitos. Sin embargo, podrían permitir ser el inicio de uno, o bien, una parte de un SGSI dedicada únicamente a aspectos de Cloud.

Un SGSI se puede basar en *frameworks* o modelos tales como:

1. ISO/IEC 27001 [ISO/IEC, 2013]: Es un *framework* que construye y madura un SGSI a partir de un ciclo de mejora continua, dentro a lo que respecta a sus controles de seguridad de la información. En relación a Cloud Computing, la normativa contiene el control “A5.23, políticas de seguridad de la información en la nube”, el cuál es el único control dedicado a este entorno.

La propia implementación de un sistema como la ISO permitirá, en general, permite mitigar riesgos relacionados a la seguridad de la información en Cloud, pero sin objetivos correctamente definidos no permitirá un control óptimo de la seguridad de la información. Posee una certificación asociada.

2. Security, Trust, Assurance and Risk(CSA STAR)[Cloud Security Alliance, 2025]: Es un programa de certificación y evaluación de seguridad desarrollado por la Cloud Security Alliance (CSA). Este es evaluado a partir de la CCM, por lo que permite una estandarización de los requisitos de seguridad solicitados a la organización, y en consecuencia, se puede tener un conocimiento mas específico sobre cuáles son las responsabilidades a nivel empresarial. Por lo que, si se utiliza este *framework*,

no es relevante el tipo de proveedor a utilizar siempre cuando éste cumpla con la certificación correspondiente.

3. NIST Cybersecurity Framework (NIST CSF) [Pascoe et al., 2024]: Proporciona directrices a la industria, agencias gubernamentales y otras organizaciones para gestionar los riesgos de seguridad cibernética.
4. CIS Critical Security Controls [CIS, 2021]: Son un conjunto priorizado de salvaguardias para mitigar los ciberataques más prevalentes contra sistemas y redes. Están mapeados y referenciados por múltiples marcos legales, regulatorios y de políticas. Existen *mappings* de CIS para los proveedores de servicios públicos en la vanguardia (Google, Microsoft, Amazon), estos se utilizan principalmente para la configuración de sus entornos.

En el contexto de Cloud Computing, existen otros *frameworks* más enfocados en estos entornos tales como:

1. ISO/IEC 27017 [ISO/IEC, 2015]: Framework realizado por la ISO que amplía los controles existentes en la ISO/IEC 27002, enfatizado únicamente en controles relacionados a Cloud Computing, tanto por el lado del proveedor como del consumidor.
2. ENISA Cloud Computing Security Risk Assessment
[ENISA, 2009]: Es un *framework* de la Unión Europea diseñado para el análisis de riesgos en Cloud Computing. Muy similar a la ISO/IEC 27017.
3. Amazon Web Services (AWS) Well-Architected Framework - Security Pillar
[AWS, 2024]: Es un *framework* que posee controles respectivos a seguridad dentro de entornos de AWS. Si bien esta última es sólo aplicable en este entorno, se enfatiza la importancia de la investigación del contexto, puesto que existe la posibilidad de que su proveedor ya provea controles y buenas practicas de seguridad recomendadas dentro de sus propios servicios.

2.3.3. Inteligencia de amenazas

La inteligencia de amenazas consiste en el uso de fuentes públicas de buena reputación para mejorar la propia seguridad de la empresa. Estas fuentes públicas entregan una buena base de investigación para prevenir posibles riesgos de seguridad.

Si bien las amenazas en entornos de Cloud Computing son cambiantes, existen instituciones que cada año destacan las mayores amenazas para estos sistemas, entre estas se destaca la CSA, OWASP y en aspectos de inteligencia de amenazas, MITRE.

1. Top threats Cloud Computing⁵: La CSA anualmente realiza una encuesta donde participan más de 10.000 expertos en materias de Cloud Security para evaluar las amenazas mas comunes en estos entornos. Estas son clasificadas según su frecuencia e impacto ya explicadas. También presenta casos concretos donde fueron explotadas y como pueden ser mitigadas a partir del uso de la CCM. Su actualización anual permite una mejor priorización de las amenazas a considerar, puesto que, como se puede apreciar en la figura 8, las amenazas puede cambiar su criticidad en periodos cortos de inclusive 2 años.
2. OWASP Cloud-Native Application Security Top 10⁶: Durante 2022, la OWASP realizó un proyecto que recopilaba el top 10 de mayores amenazas de Cloud Computing. Si bien no es un proyecto muy actualizado, se debe considerar debido a la importancia de la OWASP en temas de seguridad de la información.
3. MITRE ATT&CK for Cloud⁷: Es una extensión del marco MITRE ATT&CK que categoriza y documenta las tácticas, técnicas y procedimientos (TTPs) utilizados por actores maliciosos específicamente en entornos Cloud.

Estas fuentes son útiles para tareas de prevención y anteponerse ante posibles amenazas de adversarios, por lo que se debe considerar su revisión en actividades de inteligencia de amenazas.

2.3.4. Indicadores

Uno de los elementos de mayor importancia del sistema es la visibilidad del cumplimiento de metas y objetivos, es decir, si los planes implementados están entregando resultados acorde a los objetivos organizacionales y cómo se pudiese mejorar los planes construidos. Esta normativa presenta 2 tipos de indicadores, según la ISO27004 [ISO/IEC, 2022].

1. Indicadores de eficacia: Son aquellos que buscan un cumplimiento de las acciones realizadas, responde a la pregunta de ¿Se esta cumpliendo o no?. Se utilizan para medir el cumplimiento de los planes en etapas iniciales de implementación sin considerar la optimización de recursos.
2. Indicadores de eficiencia: Plantean la efectividad del control mas de su propio cumplimiento. Responden a la pregunta de ¿Qué tanto me funciona este control? o ¿Cuanto me está costando aplicar este control en función de sus resultados?. Se utilizan para medir qué tanto funciona un control en relación a los objetivos organizacionales y a los recursos utilizados para su cumplimiento.

En primera instancia se utilizará un indicador de eficacia para realizar la implementación de los controles, una vez se alcance la meta de este indicador se podrá proceder a implementar indicadores de eficiencia para optimizar el control o medida relacionada. Los controles o

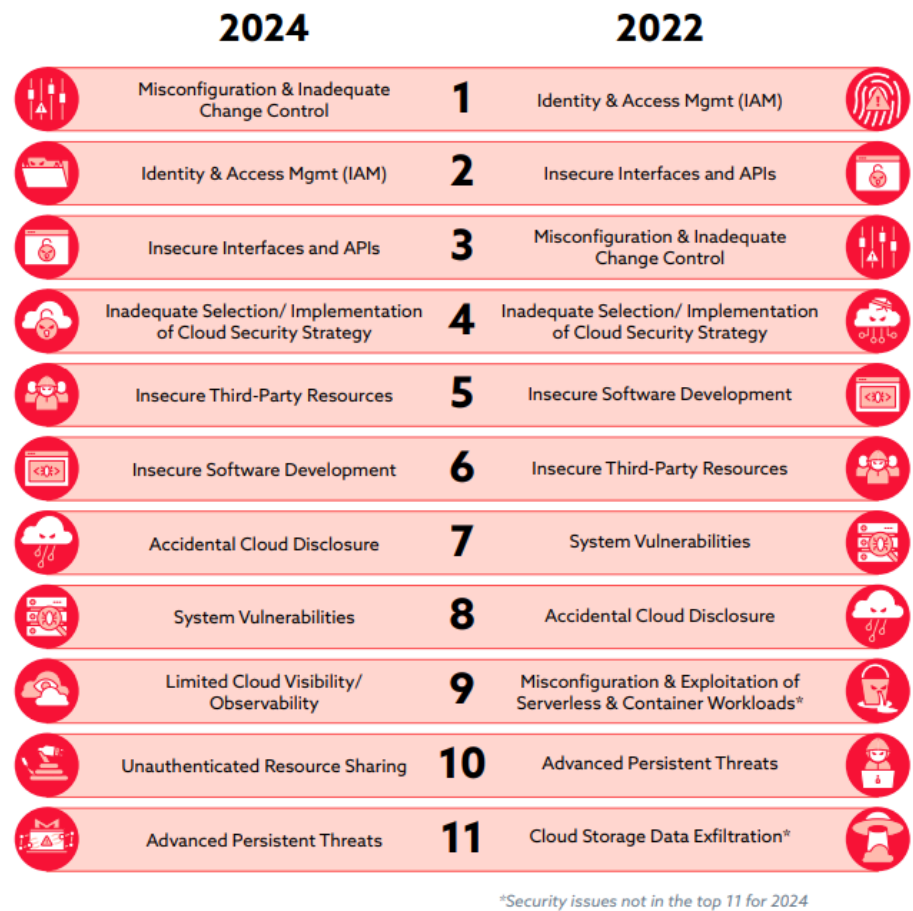


Figura 8: Comparación amenazas 2022 y 2024
Fuente: [CSA, 2024]

medidas relacionadas pueden tener ambos tipos de indicadores al mismo tiempo, pero los indicadores de efectividad no tendrán sentido una vez el control o la medida sea completamente incorporada.

Adicionalmente podemos considerar como indicador el porcentaje de cumplimiento de cada normativa o *framework* utilizado, ya que permite conocer el estado de avance de la propia implementación.

2.4. Modelo de mejora continua

Un modelo de mejora continua es una metodología que se retroalimenta a sí misma con el objetivo de perfeccionar los procesos existentes mediante el aprendizaje obtenido en cada iteración. En el contexto de seguridad de la información, permite que los procesos relacionados se mantengan actualizados y optimizados con el tiempo.

En general, las metodologías de seguridad de la información se basan en el ciclo PDCA (Plan-Do-Check-Act), como se muestra en la Figura 9. Este consta de cuatro fases fundamentales:

1. Planear: Se identifican oportunidades de mejora y se establecen objetivos y procesos necesarios para lograr resultados conforme a los requisitos esperados.
2. Hacer: Se implementa el plan realizado en la fase anterior. Aquí se ponen en práctica las acciones planificadas y se recopilan datos para su posterior análisis.
3. Verificar: Se evalúan los resultados obtenidos comparándolos con los objetivos. Se analizan los datos recolectados para ver si hubo mejoras, desviaciones o errores.
4. Actuar: Se ajustan, estandarizan o corrigen las acciones según los resultados. Si la mejora fue efectiva, se implementa a mayor escala; si no, se replantea el plan.

Las etapas son iteradas constantemente para mejorar los procesos de la organización, esto se ve representado en la figura 9.



Figura 9: Ciclo de mejora continua

Fuente: [Fattocses, 2019]

CAPÍTULO 3

PROPUESTA DE SOLUCIÓN

Considerando el entorno en el cual se va a desplegar la solución, es decir, desde organizaciones con un nivel bajo de seguridad de la información en Cloud hasta organizaciones con un nivel de madurez medio, se deben considerar los siguientes aspectos como requisitos no funcionales para la construcción de la metodología:

1. Debe ser Integrable: Los *frameworks* revisados durante la construcción, tales como la ISO/IEC 27001, como tal poseen una estructura general donde se inicia con la construcción de requisitos, luego se realizan metas y finalmente se aplican planes, los cuales se deben implementar a partir de múltiples iteraciones. Ya sea que la metodología se aplique a una empresa sin SGSI, con un SGSI sin madurar o uno de gran maduración, es importante que la solución propuesta tenga esta estructura, debido a que así se facilitará la implementación de cada etapa propuesta dentro de las organizaciones que ya poseen controles de seguridad; y, en otros casos, permitirá a organizaciones sin un SGSI iniciarse con un ciclo adaptado a las mejores prácticas, lo que se traduce en mayor eficiencia para mejorar su seguridad a partir de estándares.
2. Debe ser flexible: La metodología deberá adaptarse a la madurez y capacidades de la organización, por lo que su análisis debe ser a alto nivel y considerando aspectos como: gestión de la seguridad actual, contexto de la organización, capacidades de trabajo, exigencias legales, solicitudes de clientes, objetivos organizacionales, metodologías de desarrollo, entre otros.
3. Debe ser medible: Si bien el modelo podrá implementar controles de seguridad en entornos Cloud, debe existir algún mecanismo que permita la medición de la efectividad de estos controles, según los propios objetivos de la organización, puesto que la efectividad de los controles es directamente dependiente de las propias necesidades de la organización y sus metas.
4. Debe ser cíclico: Las amenazas y vulnerabilidad cambian constantemente, lo que hace imposible realizar un sistema capaz de mitigar todas las vulnerabilidades, por lo que la solución debe de alguna manera iterar en sí misma para detectar nuevas amenazas, planificar mejoras en el sistema actual, implementarlas y medir su efectividad, pero también para avanzar en un mayor nivel de madurez.

Adicionalmente, se definen las áreas organizacionales que serán relevantes para la aplicación de la solución:

1. Dirección de tecnología: Es un individuo o el grupo de colaboradores de la organización encargados del funcionamiento del área tecnológica, principalmente de los aspectos

de desarrollo, infraestructura de Cloud y seguridad de la información. Son aquellos que toman las decisiones acerca de los cambios que se pueden realizar o no dentro del sistema.

2. Área de seguridad de la información: Es el área encargada de dirigir, planificar y auditar cada uno de los cambios realizados. Idealmente, debe ser un área que no depende de ninguna otra área tecnológica, que esté dedicada únicamente a la seguridad de la información y aislada de las propias implementaciones propuestas.
3. Área(s) de implementación: Son todas las áreas tecnológicas operativas que tienen relación con el plan de implementación. Según el alcance de la memoria, abarca a las áreas de infraestructura, desarrollo y seguridad con respecto al uso y gestión de la tecnología Cloud Computing.

Es importante considerar que no se requiere que estas áreas tengan exactamente la misma definición formalizada dentro de la organización, pero es fundamental que exista alguna equivalencia entre estas áreas y las existentes en la organización. Además, en organizaciones de menor tamaño, es posible que algunas de estas áreas sean asumidas por una sola persona.

Se decidió basar la solución en un modelo de mejora continua, puesto que la mayoría de las normativas están fundamentadas en este enfoque (como, por ejemplo, la estructura de la ISO/IEC 27001). Esto facilita la integración de la metodología con otros SGSI. Además, la seguridad de la información requiere una revisión constante, dado que las amenazas críticas cambian con el tiempo; por esta razón, un enfoque de mejora continua resulta ideal para mantener los sistemas actualizados y alineados con el contexto.

En las próximas subsecciones se abarcará cada una de las etapas del ciclo con un mayor detalle.

3.1. Análisis de la organización (Planear)

En esta etapa se construye todo el análisis de la organización para conocer su nivel de madurez, cuáles son sus objetivos más críticos y que se realizará para cumplirlos.

3.1.1. Definición de áreas organizacionales

Inicialmente se requiere claridad sobre las responsabilidades y funciones de cada uno de los colaboradores relacionados a la metodología. Por lo que se debe realizar un registro de las responsabilidades que tendrá cada cargo según las áreas organizacionales mencionadas: Dirección de tecnología, Área de seguridad y Área de implementación. Estas áreas pueden cambiar en cada ciclo según corresponda.

3.1.2. Análisis de contexto y dominios de la solución

Luego, se realizará una revisión del contexto de la organización en base a 4 dominios, esto con el objetivo de conocer el funcionamiento del área tecnológica de la organización, que relación tiene la organización con la tecnología de Cloud Computing, que aspectos normativos debe cumplir y cuales controles utiliza actualmente la organización para controlar sus riesgos de seguridad de la información. Para obtener esta información es necesario comunicarse con la Dirección de tecnología, se recomienda obtener esta información mediante una entrevista a todos los colaboradores que sean parte del Área de tecnología, o bien, se podría enviar un cuestionario actualizado según los aspectos que se plantean analizar. Esta fase se divide en la investigación de 4 dominios estrechamente relacionados con el marco teórico presentado.

1. Análisis de contexto: Este dominio tiene como objetivo conocer la organización y su relación con las tecnologías de Cloud Computing, por lo que es crucial conocer aspectos relacionados al tamaño de la empresa, su misión, visión, usos de Cloud, proveedores de servicios Cloud, certificaciones, análisis FODA, procesos críticos, organigramas, tipos de clientes y cualquier otra información que se considere útil para entender a la organización y su necesidad de seguridad de la información. Adicionalmente, en base a lo anterior se debe consultar que controles se están aplicando actualmente para reducir los riesgos y cuales son los riesgos asociados a la tecnología de Cloud mas críticos identificados. Algunas preguntas claves son: ¿Para que se utiliza Cloud?, ¿Cuáles son los procesos mas sensibles?, ¿Qué medidas de seguridad se realizan actualmente?, ¿Como se organiza el área de tecnología?. Se recomienda revisar la sección 2.1 en caso de requerir realizar preguntas relacionadas a los servicios Cloud que utiliza la organización.
2. Desarrollo de software: Este dominio tiene el objetivo de conocer la comunicación entre los equipos de seguridad de la información y los de desarrollo, por lo que se pretende conocer las metodologías de gestión de proyectos relacionadas a Cloud Computing. Algunas preguntas recomendadas son: ¿Qué tipos de servicios se utilizan en Cloud? ¿Cuáles son sus proveedores? ¿Cómo se gestiona el código? ¿Qué metodología de desarrollo se utiliza? ¿Qué pruebas de seguridad se realizan?. Se recomienda revisar la sección 2.2 del documento para conocer los aspectos más importantes de DevSecOps.
3. Cumplimiento normativo: Según el contexto de la organización es posible que tenga objetivos, certificaciones o frameworks implementados. Por lo que se debe descubrir cuáles son y en qué etapa de implementación se encuentran, esto para integrarlos a la solución desde un inicio. Algunas de las preguntas recomendadas son: ¿Se realiza alguna certificación de seguridad o se planea aplicar alguna? ¿Los clientes necesitan algún tipo de certificación? ¿La organización debido a su negocio tiene obligaciones legales de seguridad?. Se recomienda revisar la sección 2.1 y 2.3.2 del documento para conocer algunos de los estándares de seguridad de la información.

4. **Inteligencia de amenazas:** Se debe conocer cuáles son las fuentes de información que utiliza el Área de seguridad con el propósito de implementar medidas tácticas para la mitigación de incidencias de seguridad de la información. Es posible que las empresas inicialmente no tengan un procedimiento de inteligencia de amenazas, en estos casos se considera como un aspecto a implementar. Algunas de las preguntas recomendadas son: ¿Se realizan aspectos de monitoreo de amenazas?, ¿Qué medidas preventivas se realizan ante amenazas? ¿Se conoce las amenazas que podrían causar mas impacto a la organización?. Se recomienda revisar la sección 2.3.3 para conocer algunas fuentes de inteligencia de amenazas.

Se entrega un catálogo de preguntas en el Anexo 5.1.

3.1.3. Construcción de objetivos

Una vez se haya realizado la revisión completa, se debe proponer los objetivos de seguridad que abarcará la metodología. Estos objetivos deberán ser aprobados por la Dirección de Tecnología y deberán enfocarse tanto en la seguridad de la información en Cloud Computing como en el apoyo a los objetivos organizacionales.

Si la organización ya cuenta con objetivos de seguridad propios en materia de seguridad, no será necesario modificarlos, bastará con seleccionar aquellos que aborden específicamente la seguridad en entornos Cloud. Sin embargo, en caso de no contar con objetivos formales, se deben considerar los siguientes aspectos clave:

- Los objetivos deben alinearse a la visión y misión de la organización.
- Los objetivos deben considerar cualquier incidente de seguridad registrado como medida de mitigación.
- Los objetivos deben considerar los objetivos organizacionales.

3.1.4. Construcción del Plan de remediación

A partir del análisis de contexto y los objetivos construidos, se formarán no conformidades de seguridad de la información. Es decir, aspectos que no cumplen con los estándares de madurez esperados ni con los objetivos de seguridad realizados, tales como, falta de pruebas de seguridad de la información, normativas no implementadas correctamente, buenas prácticas no aplicadas en Cloud, procesos críticos no protegidos, entre otras. Estas deben ser identificadas en un informe fundamentado con las respuestas recibidas anteriormente.

El primer dominio permitirá realizar un análisis de contexto, mientras que el resto permitirá revisar la seguridad de la información de la organización a partir del siguiente análisis:

- **Prioridad del dominio:** Cada dominio tendrá una mayor prioridad según el contexto de la empresa, por lo que es importante clasificar su importancia.
- **Análisis de las preguntas:** Al revisar las preguntas se debe tener en consideración si la respuesta es la esperada, la respuesta debe permitir detectar si se han tomado las medidas de seguridad necesarias o no. En caso de que las medidas se consideran insuficientes, se ha detectado una no conformidad.
- **Recomendaciones:** Una vez se conoce lo aproximado que se está al nivel de seguridad real con el esperado, se pueden proponer las primeras medidas para remediar las no conformidades identificadas.

Se recomienda revisar la propuesta presentada en el Anexo 5.2, donde se aplican cada una de estas secciones, y adicionalmente se definen los criterios de evaluación para cada pregunta.

Una vez se tenga claridad sobre las no conformidades de la organización, se elaborará un plan de remediación a partir de estas y considerando las capacidades del área de implementación, los objetivos establecidos, el contexto de la organización y la criticidad de cada hallazgo para su propuesta de remediación. La criticidad se determinará a partir de la importancia del dominio de la metodología asociado al control y su relevancia específica.

La elaboración del plan debe realizarse en coordinación con el Área de implementación, ya que esta posee el mayor conocimiento sobre los procesos y capacidades del área tecnológica. No es necesario que el plan inicial abarque la totalidad de las brechas identificadas, pero sí debe contemplar una proyección futura que indique los pasos a seguir una vez concluida su implementación.

El plan debe ser un documento centralizado y aprobado por el Área de Implementación junto con la Dirección de Tecnología. Idealmente, no debería requerir modificaciones una vez aprobado; sin embargo, si se presentan cambios en etapas posteriores, será fundamental mantener un control de versiones junto con un registro detallado de las modificaciones realizadas, con el fin de facilitar el monitoreo y trazabilidad del ciclo implementado.

El plan tendrá una fecha límite que no podrá ser modificada bajo ninguna circunstancia. Esto evitará la prolongación del ciclo y permitirá una evaluación precisa de su efectividad, así como de los indicadores asociados a lo planificado.

Se deberán definir indicadores de eficacia y desempeño para cada uno de las medidas de remediación propuestas y aprobados dentro del plan de remediación, estos ya se encuentran definidos en la sección 2.3.4.

En general, en caso de implementar algún *framework* o normativa de seguridad de la información, se utilizarán indicadores de eficacia, mientras que, si se busca mejorar controles ya existentes, se aplicarán indicadores de eficiencia. Estos indicadores serán aprobados en conjunto con el Plan de trabajo.

La estructura propuesta para el plan de remediación se encuentra en el Anexo 5.3, que considera cada uno de los puntos anteriormente mencionados con la siguiente estructura:

- **Introducción:** Explicación ejecutiva que explica el documento y el proceso realizado.
- **Gap Identificado:** Presentación de cada no conformidad encontrada durante el análisis, estas son clasificadas según el dominio donde fueron encontradas.
 - **Descripción del Gap:** Explica brevemente cual fue la no conformidad encontrada.
 - **Prioridad:** A partir de criterios presentados en el propio documento, clasifica la no conformidad según su importancia para la organización.
 - **Plan de acción:** Presenta una lista de acciones secuenciales que pretenden solucionar la no conformidad identificada
 - **Área responsable:** Es el área o individuo que estará a cargo del plan de acción.
 - **Duración:** Calculo aproximado acerca de cuando tardará la aplicación del plan de acción.
- **Plan de remediación:** Selección de no conformidades y planes de acción que se realizarán durante una iteración específica, con un tiempo determinado para aplicarlas.
- **Indicadores:** Representación cuantitativa del avance de cada uno de los planes de acción que constituyen al plan de remediación.
- **Anexos específicos:** Normativas, estándares, *frameworks* o controles necesarios para la realización del plan de remediación.

Una vez aprobado todo lo anterior, se podrá iniciar la implementación de las medidas. En la Figura 10 se presenta un esquema que resume todas las etapas descritas en esta fase. Cabe destacar que este diagrama representa una recomendación del flujo de actividades a seguir, y su aplicación concreta dependerá del contexto específico de cada organización tecnológica.

3.2. Implementación del Plan (Hacer)

Esta etapa es realizada principalmente por el Área de Implementación y el Área de Seguridad, en caso de que algunas de las implementaciones son realizadas por la propia área de seguridad, se recomienda que sea auditada por un área externa a seguridad de la información (como un área gerencial), debido a que un área no debe auditarse a sí misma.

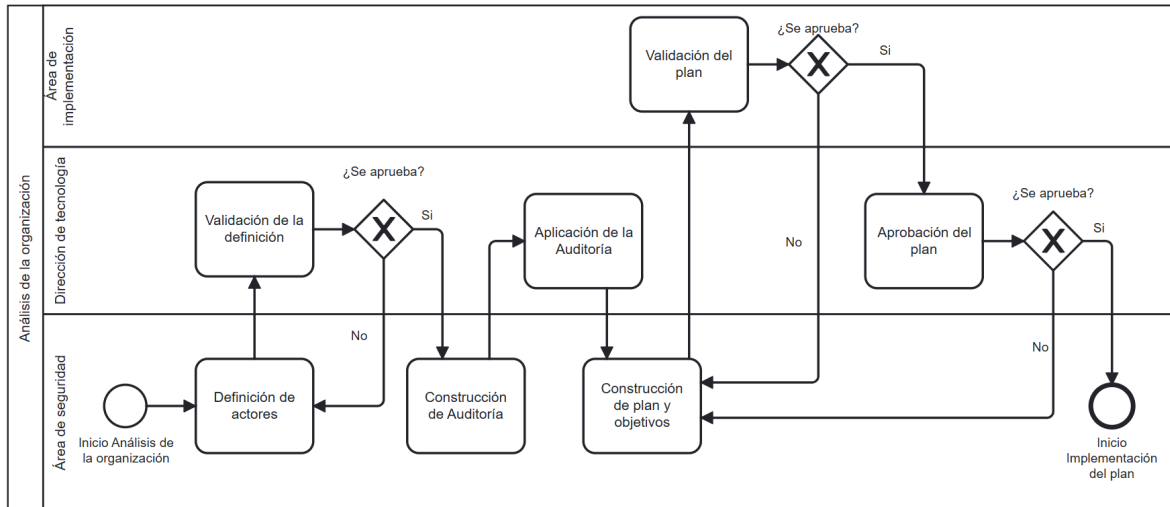


Figura 10: Flujo en etapa Análisis de la organización
Fuente: Elaboración propia

3.2.1. Aplicación del Plan de remediación

El plan de remediación se aplicará en el plazo definido, ante cualquier incidencia, retraso o solicitud de cambio, ésta debe ser registrada por el Área de seguridad indicando los motivos y justificaciones para los cambios o problemas existentes. La implementación del plan puede ser anexada a otros planes de seguridad de la organización, pero el registro inicialmente solo debe ser parte de los aspectos de Cloud por el alcance de la metodología. Los cambios registrados no pueden modificar el tiempo de duración de esta fase.

Se recomienda identificar los cambios realizados en una tabla o planilla similar a la presentada en el Anexo 5.4, la cual contiene los siguientes elementos:

- Fecha: Fecha en la cuál se notificó el cambio realizado en el plan.
- Plan: Presenta el nombre del plan específico que fue modificado.
- Responsable: Es el usuario que solicitó la modificación del plan.
- Cambios realizados: Descripción ejecutiva acerca de en qué consiste el cambio realizado.

3.2.2. Auditorías del proceso

Cada cierto periodo de tiempo se debe registrar a partir de auditorías el avance técnico de las soluciones a implementar, el objetivo de esto es conocer si lo implementado por cada

área está alineado con el propio plan de implementación, si existen diferencias se pueden modificar el plan de implementación o realizar observaciones, aun así, todos estos cambios siempre deben quedar registrados.

3.2.3. Cálculo de indicadores intermedios

Cada cierto periodo de tiempo se solicitarán datos para realizar el cálculo de los indicadores, esto con el objetivo de ver el progreso de las metas propuestas en el Plan de remediación. Si los indicadores no están siguiendo el comportamiento deseado, se pueden proponer revisiones al plan de implementación. Todo comportamiento no deseado o modificación al plan de implementación debe quedar registrado.

3.2.4. Registro de complicaciones o incidencias

Cómo se ha enfatizado anteriormente, durante la implementación es posible que se requieran hacer muchos cambios durante la aplicación de las remediaciones, es por ello que se debe tener organizado los problemas de la forma más detallada posible. Puesto de que estos documentos serán altamente relevantes durante las próximas etapas para el análisis del proceso.

A partir de las acciones presentadas, se muestra en la figura 11 el siguiente diagrama de flujo como recomendación para aplicar el proceso.

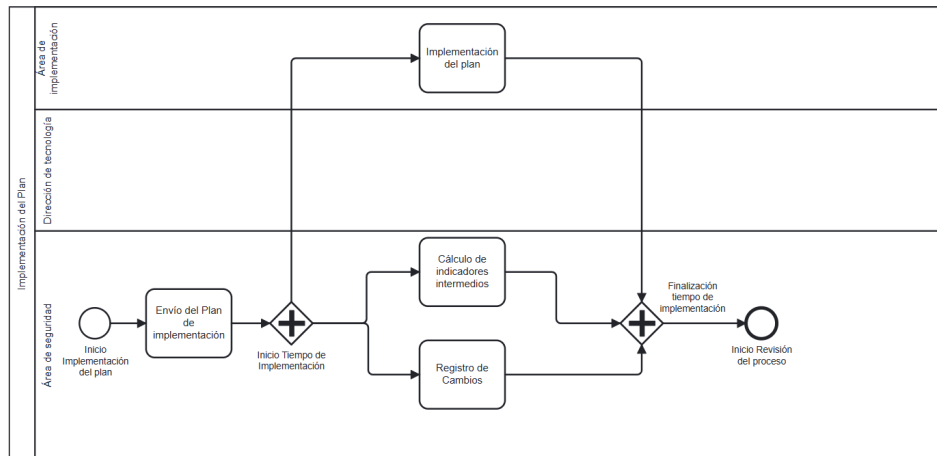


Figura 11: Flujo en etapa Implementación del Plan
Fuente: Elaboración propia

3.3. Revisión del proceso (Verificar)

3.3.1. Revisión de indicadores finales vs metas

Al cumplirse el plazo establecido en el Plan de Remediación, se procederá al cálculo de los indicadores correspondientes a cada uno de los controles implementados. Estos serán evaluados por el Área de Seguridad para determinar el grado de cumplimiento del plan respecto a las metas proyectadas. En caso de que el resultado final sea insatisfactorio, se elaborará un plan de corrección, el cual se definirá con un alcance y un tiempo determinados, y se orientará exclusivamente a mejorar el cumplimiento de las metas. Una vez elaborado, será enviado al Área de Implementación.

Como ejemplo, se presenta el documento en el Anexo 5.5, el cual contiene las siguientes secciones:

- **Resumen ejecutivo:** Breve resumen del proceso realizado hasta este momento.
- **Indicadores alcanzados:** Presentación de cada uno de los indicadores del plan, tanto de los que alcanzaron su meta, como los que no.
- **Problemáticas identificadas:** Complicaciones encontradas durante la aplicación del proceso
- **Plan de remediación:** Versión reducida del plan de remediación original, con el objetivo de alcanzar las metas presentadas en los objetivos.

La figura 12 presenta el flujo recomendado para aplicar este proceso.

3.4. Actuar y cierre (Actuar)

Una vez entregado el plan de corrección, se esperará su ejecución. Tras la finalización de su implementación, se elaborará un informe final basado en los resultados obtenidos a lo largo de todo el proceso. Este informe incluirá un análisis de los indicadores finales de la iteración, así como una sección de mejora continua que abordará los ajustes necesarios para la próxima iteración. En concreto, debe contener al menos los siguientes elementos:

- No conformidades del plan: Elementos críticos que fueron omitidos durante la implementación del plan. Su tratamiento será obligatorio en la próxima iteración de la metodología, y se considerarán como controles de mayor prioridad que en la iteración actual.

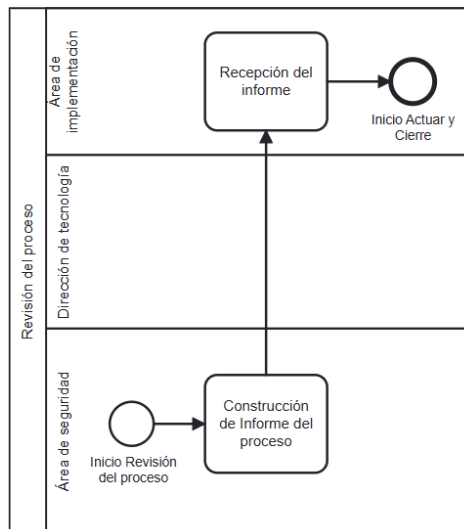


Figura 12: Flujo en etapa Revisión del proceso
Fuente: Elaboración propia

- Mejoras de los procesos: En caso de que el proceso no se haya ajustado adecuadamente a las necesidades organizacionales durante las fases anteriores, ya sea por un plan inadecuado para las capacidades de la empresa, información errónea, objetivos no alineados, entre otros, se debe incluir en esta sección, junto con una propuesta de la solución a estos problemas. El objetivo es implementar mejoras en el flujo de actividades para alinear el proceso con la realidad organizacional.

Se presenta como ejemplo el documento Anexo 5.6.

Una vez finalizado el informe, se presentará a la Dirección de Tecnología para dar visibilidad al proceso descrito. Finalmente, a partir de los resultados obtenidos, se iniciará nuevamente la fase 1. Si la organización no ha sufrido cambios relevantes en su estructura o áreas tecnológicas, se podrá omitir la fase de análisis y avanzar directamente a la construcción del plan, basándose en la brecha identificada en el plan recientemente revisado y en las proyecciones futuras. El proceso recomendado para aplicar esta fase se muestra en la figura 12.

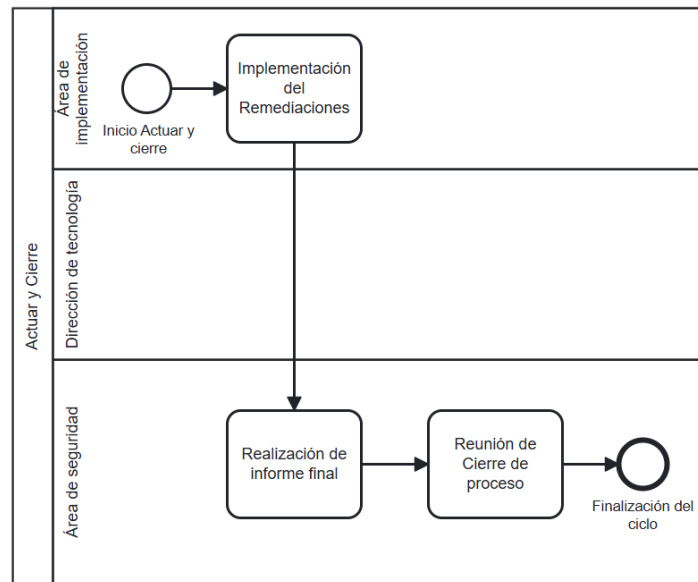


Figura 13: Flujo en etapa Actuar y Cierre
Fuente: Elaboración propia

CAPÍTULO 4

VALIDACIÓN DE LA SOLUCIÓN

Una vez planteada la metodología, se aplicó en una empresa del sector tecnológico como una iteración inicial, con el objetivo de fortalecer la seguridad de la información en sus procesos relacionados con Cloud, incorporar prácticas de DevSecOps en su ciclo de desarrollo y mejorar los controles establecidos en la normativa ISO/IEC 27001 vinculados a la seguridad en entornos Cloud. La implementación fue coordinada en conjunto con el Director de TI de la empresa y el oficial de seguridad de la organización.

Por razones de confidencialidad, en esta sección no se incluirán nombres ni datos que puedan permitir la identificación de la empresa o comprometer su seguridad. No obstante, se presentarán los detalles del proceso ejecutado y los aspectos que se proponen mejorar en la próxima iteración.

4.1. Análisis de la organización (Planear)

4.1.1. Definición de actores

El ciclo fue presentado durante una reunión del Comité de Seguridad, en la cual se presentó el trabajo desarrollado en el proyecto y la propuesta a implementar. Al finalizar la presentación,

se definieron los actores responsables de aplicar la metodología:

1. Director de Tecnología: El principal responsable será el Director de TI, en conjunto con la gerencia de desarrollo y la gerencia de seguridad de la información.
2. Área de Seguridad: La empresa cuenta con un área de seguridad ya establecida, la cual participará activamente en la metodología.
3. Área de Implementación: Estará compuesta por el área de desarrollo, el área de infraestructura en AWS y, en algunos casos, el área de seguridad.

4.1.2. Análisis de contexto y dominios de la solución

Luego de la reunión, se envió un cuestionario compuesto por 35 preguntas, estas se encuentran en el Anexo 5.1. Las preguntas están orientadas a los cuatro dominios definidos para la evaluación. Además, se solicitó información complementaria, como el organigrama de la empresa, su misión y su visión. Las respuestas fueron elaboradas de forma colaborativa por las tres gerencias que componen el rol de Director de TI:

- El Oficial de Seguridad respondió los dominios relacionados con Cumplimiento e Inteligencia de Amenazas.
- El Director de TI abordó el contexto organizacional y el uso de Cloud Computing.
- El Jefe de Desarrollo respondió el dominio de Desarrollo, proporcionando detalles sobre las metodologías actualmente empleadas.

Una vez contestados, cada uno de los dominios fue categorizado según la tabla 3 para conocer su relevancia en torno al negocio. A partir de las respuestas también se cuestionarios posibles controles esperados, tales como implementaciones de modelos de responsabilidad compartida, controles de seguridad Cloud, inteligencia de amenazas entre otros. La aplicación de cada uno de estos controles consultados fue categorizado a partir de la tabla y el promedio de cada uno será presentado en el análisis para tener una idea sobre qué tan avanzado va cada dominio respecto a controles de seguridad (ver figura 4).

Una vez respondido el cuestionario, cada uno de los dominios fue categorizado según la tabla 3, con el objetivo de determinar su nivel de relevancia en relación con el contexto organizacional. A partir de las respuestas, se identificaron también los controles esperados, tales como la implementación de modelos de responsabilidad compartida, controles de seguridad en entornos Cloud, e inteligencia de amenazas, entre otros. La aplicación de estos controles fue evaluada utilizando la tabla 4, y el promedio de las categorizaciones obtenidas para los

Nivel	Descripción
Bajo	El dominio presenta riesgos mínimos para la organización. Su implementación puede posponerse sin impacto significativo en la seguridad general o continuidad del negocio.
Medio	El dominio presenta riesgos moderados que requieren atención planificada. Su implementación debe considerarse en el mediano plazo para mantener un nivel adecuado de seguridad.
Alto	El dominio es crítico para la seguridad organizacional. Presenta riesgos significativos que requieren implementación inmediata para proteger activos críticos o cumplir con obligaciones regulatorias.

Tabla 3: Evaluación de Prioridad de Dominios de Seguridad
Fuente: Elaboración propia

Nivel	Descripción
0 – Inexistente	El control no está implementado ni planeado.
1 – Inicial	El control existe, pero de forma informal, reactiva y no documentada.
2 – Incompleto	El control se aplica parcialmente, con algo de documentación, pero sin estandarización.
3 – Definido	El control está formalmente definido, documentado y comunicado.

Tabla 4: Niveles de Madurez de Controles
Fuente: Criterios internos de la empresa

controles esperados en cada dominio será presentado en el análisis de contexto, con el propósito de evidenciar el grado de avance de cada dominio en relación con la implementación de controles de seguridad.

Con las respuestas del cuestionario se construyó un análisis de contexto para la empresa, este se encuentra documentado en el Anexo 5.2. Adicionalmente, a partir de las respuestas entregadas, se elaboró el siguiente resumen de la empresa.

Contexto de la Empresa

La empresa se define como un *contact center* bajo el modelo de negocio B2B con una amplia trayectoria en el mercado y con un tamaño cercano a los 1300 trabajadores. Actualmente su operación depende de infraestructura tecnológica basada en servicios Cloud, siendo su único proveedor Amazon, se utiliza un modelo principalmente de Platform as a Service (PaaS) y con una arquitectura *serverless*. Su actividad requiere el tratamiento de información sensible de clientes y usuarios finales, por lo que la seguridad de la información representa un aspecto crítico del negocio.

A continuación se presenta el análisis detallado de cada uno de los dominios de la metodología:

1) Contexto general de la organización en relación con Cloud Computing

Se considera este dominio de prioridad Alta, ya que toda la operación de TI de la organización depende de servicios en la nube. Esto implica que cualquier debilidad en su gestión representa un riesgo elevado para la continuidad y seguridad de las operaciones. Se considera que los controles de este dominio se encuentran en un estado Inicial debido a que:

- No existen controles dedicados a los servicios utilizados en AWS.
- No se ha aplicado formalmente un modelo de responsabilidad compartida.
- Solo se aplica el principio de mínimo privilegio como buena práctica en Cloud Computing. Debería aplicarse un *framework* completo.
- No se realizan revisiones de buenas prácticas relacionadas a el uso de arquitecturas serverless.

2) Desarrollo

Según la información recopilada, este dominio se clasifica con prioridad Alta, ya que los desarrollos actuales impactan directamente la operación central y están constantemente realizando mejoras o extensiones a modelos ya implementados. Debido al contexto de la información se considera que los controles de este dominio se encuentran en un estado Inicial debido a que:

- Actualmente si se realizan pruebas de seguridad, pero sólo en la fase final del proyecto
- No se implementan herramientas y servicios que podrían contribuir a la seguridad de la información, tales como: Infraestructure as code, uso de contenedores, microservicios o herramientas de monitoreo del proveedor.

3) Cumplimiento normativo

De acuerdo con las respuestas entregadas, se asigna a este dominio una prioridad Alta, ya que el incumplimiento normativo podría derivar en sanciones legales, pérdida de confianza de los clientes o afectación directa a la reputación institucional. Debido al contexto de la información se considera que los controles de este dominio se encuentran en un estado Repetible pero Informal

- Actualmente si se gestionan los aspectos normativos solicitados por clientes y aspectos legales relacionados con seguridad de la información.

- No se tiene conocimiento de las normativas cumplidas por los proveedores, incluyendo los relacionados en Cloud Computing.

4) Inteligencia de amenazas

Según la información recopilada, se asigna a este dominio una prioridad media, ya que actualmente se encuentra en etapa de planificación y no impacta directamente las operaciones ni los controles de seguridad vigentes. No obstante, su desarrollo es clave para cumplir con los requisitos de la certificación ISO/IEC 27001:2022. Debido al contexto de la información se considera que los controles de este dominio se encuentran en un estado Inexistente por lo que se debe iniciar un proceso desde 0 para su implementación.

4.1.3. Construcción de objetivos

Una vez finalizado el análisis del contexto, se revisaron los objetivos de seguridad establecidos por la organización. Actualmente, la empresa se rige por 7 objetivos propios, los cuales abordan aspectos como la seguridad legal, el cumplimiento normativo, la protección de información personal identificable, entre otros. Considerando la criticidad de la tecnología Cloud en el entorno actual, se definió el siguiente objetivo específico orientado a fortalecer la seguridad en entornos Cloud.

- *“Fortalecer la gestión integral de riesgos tecnológicos en los sistemas productivos en Cloud mediante la implementación de controles para vulnerabilidades críticas, configuraciones seguras y posturas de seguridad, estableciendo y manteniendo niveles de protección alineados con las mejores prácticas de la industria para minimizar la exposición a amenazas.”*

El plan de remediación va a girar en torno al objetivo presentado.

4.1.4. Construcción del Plan de remediación

Para el plan de remediación se consideraron las desviaciones más críticas, esto fue calculado a partir de la tabla 5 en función de la importancia de cada dominio y de cada control en específico.

Por cuestión de tiempo, se planeó 1 mes de implementación con una posible prórroga dentro de la etapa de actuar de 2 semanas. Los Controles aplicados fueron los siguientes:

1. Modelo de responsabilidad compartida CCM (Parcial): Se pretende abarcar únicamente los 15 controles iniciales considerando 1 mes de implementación, durante cada implementación de este ciclo, se espera aplicar una mayor cantidad de controles.

Dominio/Nivel de madurez	Inexistente	Inicial	Incompleto	Definido
Bajo	Media	Baja	Baja	Baja
Medio	Alta	Media	Baja	Baja
Alto	Crítica	Alta	Media	Baja

Tabla 5: Matriz de Dominio/Nivel de Madurez del control.

Fuente: Elaboración propia.

2. CIS Framework (Parcial): Se pretende abarcar al menos 21 controles presentados en la CIS Amazon Web Services Foundations Benchmark.
3. Pruebas de seguridad durante todo el SDLC: Se estima que debido al uso de metodologías ágiles y el uso de Jira se podrá implementar pruebas de seguridad en todo el ciclo de vida del 100 % de los proyectos nuevos.
4. Construcción catálogo de amenazas Cloud: Inicialmente se considerará únicamente aplicar un catálogo de amenazas en torno al marco de Top threats Cloud Computing, esto debido a la propia implementación de la CCM, la cual está fuertemente derivada en este aspecto. Una vez finalizada se procederá a aplicar otros marcos teóricos igual de relevantes.

El plan de remediación completo se encuentra en el Anexo 5.3

Indicadores iniciales

Los indicadores iniciales asociados a los controles a aplicar y al objetivo presentado son:

1. % de aplicación de la CCM (Cloud Controls Matrix): Mide el porcentaje de controles seleccionados del modelo CCM (Cloud Controls Matrix) que han sido implementados dentro del SGSI y aplicados en procesos de desarrollo, infraestructura y operación.
2. % de proyectos que se realizaron pruebas de seguridad durante su desarrollo: Mide la proporción de proyectos de desarrollo que incorporaron pruebas de seguridad (automáticas o manuales) durante todas las fases del ciclo de vida del software y antes de ser puestos en producción.
3. % de amenazas analizadas del marco teórico Top Threats Cloud Computing: Mide el nivel de incorporación de amenazas provenientes del informe Top Threats to Cloud Computing de la CSA al catálogo de amenazas de la organización.

Debido a que inicialmente no se ha aplicado ninguno de los controles por aplicar, no existe convalidación, por lo que todos los indicadores inician en un 0 %

4.2. Implementación del Plan (Hacer)

4.2.1. Aplicación del Plan de remediación

La implementación del plan tuvo una duración de 1 mes y solo se realizó 1 revisión intermedia durante la aplicación, las auditorías durante esta fase fueron realizadas únicamente por el Área de seguridad de la información a pesar de que 1 control era su responsabilidad.

Solicitudes de cambios

Se realizaron durante el proceso 7 registros distintos, entre los más relevantes fueron:

1. CIS Framework: Se detectó 1 control no aplicable dentro del marco teórico.
2. Pruebas de seguridad durante todo el SDLC: Existen procesos registrados que dependen del área de desarrollo, estos procesos siempre se realizan de la misma forma y ya fueron auditados, por lo tanto, se solicitó que estuviesen fuera del alcance para agilizar la operación.
3. Modelo de responsabilidad compartida CCM: Se detectaron 3 controles no aplicables por parte de seguridad de la información.

El detalle de estos registros se encuentra en el Anexo 5.4.

4.3. Revisión del proceso (Verificar)

4.3.1. Revisión de indicadores finales vs metas

Luego del mes de implementación se realizó una reunión con las Áreas de implementación para presentar los avances y tener conocimiento acerca del cumplimiento de cada control.

Se obtuvieron inicialmente los siguientes resultados:

1. % de aplicación de la CCM (Cloud Controls Matrix): No se cumplió la meta esperada. Se alcanzó un 60 % con 9 de los 15 controles seleccionados implementados, frente al 80 % proyectado.
2. % de aplicación del marco CIS (CIS Framework): Se alcanzó un 52 %, con 11 de 21 controles implementados. La meta establecida era del 90 %.

3. % de proyectos con pruebas de seguridad durante el desarrollo: Se cumplió completamente la meta, alcanzando un 100 % (2 de 2 proyectos ejecutados), respecto al 90 % esperado.
4. % de amenazas analizadas del marco *Top Threats to Cloud Computing*: Se alcanzó un 91 %, con 10 de 11 amenazas clasificadas y analizadas, superando la meta del 90 %.

Informe de verificación

Debido a que no se cumplieron las metas presentadas en el plan de remediación, se realizó el siguiente plan de corrección:

1. Implementación de los controles de la CCM: IVS-06, IVS-07 y IVS-09
2. Implementación de los controles de la CIS Framework: 1.6, 1.8, 1.9, 1.12.

Con el cumplimiento de los siguientes elementos es posible cumplir las metas asociadas, se dará 2 semanas para su implementación.

El documento de verificación de resultados se encuentra en el Anexo 5.5.

4.4. Actuar y Cierre (Actuar)

Una vez finalizadas las 2 semanas, se volvieron a calcular los indicadores y se preparó un análisis completo del Sprint

Indicadores finales

Considerando las 2 semanas utilizadas para el plan de corrección, se pudo completar parcialmente el plan de remediación, lo que llevó a los siguientes resultados:

1. % de aplicación de la CCM (Cloud Controls Matrix): Se cumplió la meta establecida, alcanzando un 80 % con 12 de los 15 controles seleccionados implementados. La meta era del 80 %.
2. % de aplicación del marco CIS (CIS Framework): Se alcanzó un 71 % con 15 de 21 controles implementados, frente a una meta del 90 %.
3. % de proyectos con pruebas de seguridad durante el desarrollo: Se logró un 100 %, con 2 de 2 proyectos ejecutados con pruebas de seguridad. La meta esperada era del 90 %.

4. % de amenazas analizadas del marco *Top Threats to Cloud Computing*: Se alcanzó un 91 %, con 10 de 11 amenazas catalogadas y analizadas, superando la meta del 90 %.

Con esto, finalmente se tendría un cumplimiento de 3 de los 4 controles aplicados

No conformidades del plan

Durante el proceso se identificaron los siguientes aspectos que dificultaron la aplicación efectiva del plan de remediación:

1. Limitaciones técnicas del equipo de infraestructura AWS: Se evidenciaron brechas de conocimiento técnico dentro del equipo, lo cual afectó la correcta ejecución de ciertos controles y tareas planificadas.
2. Complejidad en la implementación de controles: El tiempo estimado para implementar los controles fue insuficiente, especialmente en lo relacionado con la Cloud Controls Matrix (CCM) y el marco CIS (CIS Framework), lo que impidió alcanzar algunos de los objetivos establecidos.
3. Interrupciones por urgencias operativas: La ocurrencia de incidentes durante la iteración redujo las capacidades dedicadas al plan de remediación, generando retrasos no esperados.

Mejoras del proceso

En base en las no conformidades detectadas, se proponen las siguientes acciones de mejora para la próxima iteración:

- Programa de capacitación técnica en AWS: Se sugiere implementar sesiones de formación específicas para el equipo de infraestructura, enfocadas en los servicios de AWS más relevantes para la seguridad y cumplimiento de controles.
- Mayor duración de la iteración: Se recomienda ampliar la duración del próximo ciclo a tres meses, con el fin de disponer de más tiempo para la implementación efectiva de los controles.
- Reuniones de seguimiento más frecuentes: Se establecerán reuniones quincenales para monitorear los indicadores clave y facilitar una toma de decisiones más oportuna ante desviaciones o bloqueos.

El Informe de resultados finales se encuentra en el Anexo 5.6

Próxima iteración

Los resultados de este informe fueron presentados en la reunión mensual de seguridad de la información, donde el Comité de Crisis fue informado acerca de los resultados del proceso completo. Se llegó al consenso de que el proceso fue exitoso, ya que permitió mejorar diversos aspectos de seguridad relacionados con entornos Cloud y, especialmente, visibilizar nuevos riesgos que no habían sido considerados con los controles previamente existentes en la empresa.

Sin embargo, debido a las limitaciones actuales de capacidad del equipo, se acordó postergar la próxima iteración hasta la finalización de labores críticas por parte del área de seguridad. Para la siguiente fase, se espera retomar el plan propuesto, incorporando aquellos elementos que no pudieron ser implementados por falta de tiempo. Esta vez, la iteración se ejecutará en un ciclo de tres meses, lo cual permitirá una mayor brecha de mejora en cada ciclo.

CAPÍTULO 5

CONCLUSIONES

En esta parte se presentarán las conclusiones del trabajo, tanto los aspectos metodológicos del proyecto como su aplicación. El trabajo realizado se ha dividido en las siguientes 3 secciones: Resultados, Alcance y limitaciones de la memoria y Trabajo futuro.

5.1. Resultados

A continuación, se presentan los resultados del proceso en función del análisis de los objetivos específicos definidos en esta memoria:

1. ***Seleccionar y analizar estándares de seguridad relevantes para el desarrollo en Cloud, identificando los elementos críticos que permitan garantizar la seguridad de las aplicaciones que desarrolle una organización específica.***

En el marco teórico se incluyó una sección dedicada al análisis del cumplimiento de los estándares de seguridad, en la que se describen marcos relevantes de la industria, como los desarrollados por NIST, OWASP, ISO y CSA, entre otros.

Dado que este aspecto se consideró crítico, la metodología propuesta incorpora, en su fase de análisis, un dominio específico para la gestión de estándares y el cumplimiento, con el fin de evaluar de manera estructurada estos elementos clave.

Durante la validación del proyecto, se consideraron los estándares de la CCM y el CIS Amazon Web Services Foundations Benchmark.

2. ***Elaborar indicadores que permitan evaluar y cuantificar el progreso de implementación de controles de seguridad en el desarrollo de software en Cloud.***

El marco teórico menciona dos tipos de indicadores definidos en la norma ISO/IEC 27004: los indicadores de eficacia y los indicadores de eficiencia. Adicionalmente, se consideran los porcentajes de implementación de los *frameworks* de seguridad seleccionados durante su aplicación.

Dentro de la metodología, los indicadores juegan un papel fundamental en la definición la fase de planificación, puesto que se utilizan para visibilizar el funcionamiento del plan completo a partir de la definición de metas. Estos indicadores se analizan en las fases de verificación y la de actuar.

Durante la validación del proyecto, se utilizaron 4 indicadores: 3 de cumplimiento y 1 de eficacia. Esto permitió evaluar el avance del plan, identificar las brechas existentes durante la fase de planificación y calificar la iteración con un 75 % de éxito, ya que se cumplieron 3 de las 4 metas acordadas inicialmente

3. *Diseñar un marco de seguridad que cubra las etapas del ciclo de vida del desarrollo de software en entornos Cloud.*

En el marco teórico se desarrolló una sección dedicada al enfoque DevSecOps y su relevancia en el ciclo de vida del desarrollo. El enfoque se abordó desde la perspectiva de una empresa que no utiliza DevSecOps y la de una que sí lo implementa, pero que no aplica controles específicos para la seguridad en Cloud Computing.

Dentro de la metodología, esto se aplica específicamente en la Fase de análisis, ya que se diseñó un dominio orientado a los controles de desarrollo en entornos Cloud, abordando tanto la aplicación general de DevSecOps como la incorporación de buenas prácticas específicas para la seguridad en entornos de desarrollo Cloud.

Durante la validación del proyecto, se pudo apreciar la nula aplicación de DevSecOps en la organización, ya que las pruebas se realizaban únicamente durante la fase de implementación de los proyectos. Este hallazgo fue detectado por la metodología, lo que permitió iniciar pruebas a lo largo de todo el ciclo de desarrollo del software.

4. *Establecer procesos de mejora continua que faciliten la actualización y adaptación de la metodología a lo largo del tiempo.*

En el marco teórico se identificaron fuentes de información que se actualizan periódicamente sobre amenazas y vulnerabilidades, lo que permite que la metodología se fortalezca progresivamente con su uso.

Respecto a la metodología, esta se fundamenta en el ciclo de mejora continua, bajo la premisa de que las amenazas y riesgos en seguridad de la información están en constante evolución, lo cual requiere una revisión y adaptación permanentes. Asimismo, al ser una metodología de alto nivel, puede adaptarse a las capacidades, el nivel de madurez y el contexto particular de cada organización.

Durante la validación del proyecto, se estableció una línea de implementación en función de lo que se consideraba más crítico para la organización, en este caso, los controles aplicados a la infraestructura y la gestión de riesgos. Además, debido a la estructura de la organización, se seleccionaron 4 controles con el objetivo de que se participaran todas las áreas de implementación (Infraestructura AWS, Desarrollo y Seguridad de la Información). Asimismo, los *frameworks* utilizados tienen la reputación de actualizarse con frecuencia.

Con este análisis podemos concluir que la metodología propuesta y la memoria en general cumple con los lineamientos inicialmente establecidos.

Considerando únicamente los resultados prácticos obtenidos se puede decir:

1. La metodología mejoró el sistema donde fue implementada: Su integración permitió mejorar aspectos de cumplimiento dentro de la ISO/IEC 27001, lo cual representa un valor significativo para la empresa en la que se implementó.

2. Permitió identificar brechas de seguridad relevantes: Se detectaron brechas tales como la falta de procesos de inteligencia de amenazas, pruebas deficientes de seguridad en el desarrollo de la información, la no aplicación de buenas prácticas de configuración en entornos Cloud, la ausencia de controles dedicados a los servicios utilizados en la infraestructura Cloud, y la falta de un modelo de seguridad compartida formalmente documentado.
3. Permitió construir soluciones a partir de *frameworks* reconocidos: Se encontraron soluciones a través de la aplicabilidad de *frameworks* como la CCM, el CIS Amazon Web Services Foundations Benchmark y Top Threats to Cloud Computing 2024 de la CSA.

A pesar de lo anterior, la efectividad de las medidas presentadas depende directamente de las capacidades del equipo encargado de su implementación, lo cual puede ser un factor determinante para identificar qué se puede implementar y qué no. La capacitación del equipo es un elemento clave, que en algunos aspectos limitó el primer ciclo de aplicación.

Desde un enfoque cuantitativo, los resultados fueron positivos: se construyó un plan de remediación con 11 medidas distintas, de las cuales se seleccionaron 4, y se aplicaron 3 dentro del plazo estimado. Esto representa un 75 % de los objetivos cumplidos, con la posibilidad de incrementar ese porcentaje en las siguientes iteraciones.

Los inconvenientes registrados durante la aplicación fueron debidamente analizados y utilizados para proponer ajustes en el proceso, con el fin de mejorar la efectividad en futuras iteraciones.

Finalmente, la propia metodología respalda otros procesos formales de cumplimiento. En este caso, el proceso aplicado generó registros formales útiles para auditorías y cumplimiento externo, los cuales serán empleados para una próxima recertificación en aspectos de seguridad.

5.2. Alcance y Limitaciones de la memoria

Debido a la naturaleza del problema inicial identificado, esta memoria se enfoca únicamente en tecnologías de infraestructura de Cloud Computing y desarrollos relacionados. Además, en la etapa inicial del estudio solo se consideraron áreas tecnológicas asociadas a dicho ámbito. Esta última delimitación impide que la metodología pueda abarcar la totalidad del espectro de responsabilidades vinculadas a la seguridad de la información en entornos Cloud.

Desde el punto de vista estructural, la incorporación de los elementos antes mencionados no afectaría el funcionamiento general del proceso metodológico; sin embargo, sería necesario ampliar la cantidad de dominios abordados, definir una mayor diversidad de actores que interactúen con la metodología, y reestructurar el marco teórico para adecuarlo al nuevo alcance. Por tanto, aunque el alcance actual permite construir una solución eficiente para

problemáticas de seguridad asociadas a áreas tecnológicas y de desarrollo, su expansión implicaría necesariamente complejizar y escalar la metodología.

Otra limitación relevante es que, al no estar respaldada ni desarrollada por alguna entidad reconocida en el ámbito de la seguridad de la información, la metodología no otorga certificaciones ni posee un reconocimiento formal como un mecanismo válido de aseguramiento organizacional. Esta carencia se ve parcialmente mitigada mediante el dominio de cumplimiento, dado que si para una empresa es crítico contar con una certificación que respalde ante terceros sus prácticas de seguridad, la propia metodología priorizará la adopción de controles y marcos normativos que respondan a dicha necesidad.

Aun así, el alcance de la metodología está considerablemente alejado de los requisitos exigidos por una certificación formal, por lo que serían necesario aplicar otro tipo de metodología en paralelo para cumplir el alcance de una certificación formal. Pero contribuye para lograr alguna certificación al estar alineada con sus exigencias.

Finalmente, aunque la metodología no exige la existencia de un área de seguridad formalizada, sí requiere un equipo capacitado o con la posibilidad de dedicarse a la revisión de controles de seguridad. La metodología asume que el equipo encargado de su implementación posee conocimientos sobre las prácticas que se pretenden analizar e incorporar. Si bien es factible que los equipos se capaciten progresivamente según las demandas del proceso, este aspecto deberá ser integrado en futuras iteraciones de la metodología, para que el equipo sea capaz de realizar análisis de mayor complejidad y permita mejorar la madurez de la organización en aspectos de seguridad de la información. Esto último se concluye debido a que durante la aplicación de la metodología, se evidenció que el nivel de conocimiento del los responsables del proceso guarda una relación directa con la calidad de los resultados obtenidos.

5.3. Trabajo Futuro

Como trabajo futuro, se plantean tres elementos principales: realizar un mayor número de pruebas en distintos contextos, desarrollar nuevos dominios que permitan abarcar otras aristas de la seguridad de la información, y construir un marco teórico flexible y sostenible en el tiempo.

Pruebas de la metodología

La metodología fue validada únicamente en una empresa con un SGSI definido y una madurez media. Esta validación inicial no es suficiente para comprender el comportamiento de la metodología en organizaciones con diferentes niveles de madurez. Por tanto, se propone realizar nuevas pruebas en organizaciones sin SGSI, así como en aquellas con un SGSI altamente maduro. El objetivo es comparar qué elementos de la metodología funcionan mejor en función del nivel de madurez del sistema.

Nuevo dominios

Si bien la metodología actualmente se aplica al entorno de Cloud Computing, es importante considerar otras tendencias tecnológicas emergentes, como el uso de inteligencia artificial o la gestión de información personal identificable. También deben contemplarse elementos dependientes del contexto, como aspectos legales o propios de la organización. Se propone la creación de dominios adicionales a los 4 que se presentaron y que sean seleccionables dentro de un catálogo, de acuerdo con las necesidades específicas de cada organización.

Marco teórico flexible

Aunque la base del marco teórico actual es suficiente para que un equipo comprenda los aspectos más relevantes, no se puede asegurar que esta vigencia se mantenga en durante el tiempo. Se requiere un mecanismo de actualización sostenible de información, que permita retroalimentar a la metodología, que categorice las fuentes de información según el tipo de dominio que abordan y que considere la madurez de la organización a la que está dirigido.

GLOSARIO

AIS: Application & Interface Security
AWS: Amazon Web Services
CCM: Cloud Controls Matrix
CIS: Center for Internet Security
CPU: Central Processing Unit
CSC: Cloud Security Consumer
CSA: Cloud Security Alliance
CSA STAR: Security, Trust, Assurance and Risk (programa de certificación de CSA)
CSP: Cloud Service Provider
DevOps: Development and Operations
DevSecOps: Development, Security, and Operations
IEC: Comisión Electrotécnica Internacional
ENISA: European Union Agency for Cybersecurity
GPU: Graphics Processing Unit
IAAS: Infrastructure as a Service
IAC: Infrastructure as Code
ISO: International Organization for Standardization
IT: Information Technology
KPI: Key Performance Indicator
MFA: Multi-Factor Authentication
MTCS: Multi-Tier Cloud Security
NIST: National Institute of Standards and Technology
NIST CSF: NIST Cybersecurity Framework
NIST SP: NIST Special Publication
OWASP: Open Worldwide Application Security Project
PAAS: Platform as a Service
PDCA: Plan Do Check Act
RAM: Random Access Memory
RRHH: Recursos Humanos
SAAS: Software as a Service
SDLC: Software Development Life Cycle
SGSI: Sistema de Gestión de Seguridad de la Información
SIEM: Security Information and Event Management
SO: Sistema Operativo
TVM: Threat & Vulnerability Management
UNESCO: United Nations Educational, Scientific and Cultural Organization
XAAS: Anything as a Service

ANEXOS

5.1. Cuestionario análisis de contexto

Dominio 1 - Contexto de la empresa

1. ¿Cómo describiría la misión y visión de la organización? ¿Qué actividades realiza y desde cuándo? ¿Cuál es su trayectoria en el sector?
2. ¿Cuál es el público objetivo o mercado principal al que se dirige la organización?
3. ¿Cuántas personas componen la organización y cómo está estructurada internamente en términos de personal?
4. ¿Cómo están organizadas las áreas tecnológicas dentro de la empresa (equipos de TI, desarrollo, infraestructura, etc.)?
5. ¿La organización maneja información sensible de clientes, empleados o de la propia empresa?
6. Para los clientes y partes interesadas, ¿es crucial que la organización tenga un alto nivel de madurez en seguridad tecnológica? ¿Se solicita algún tipo de requerimiento de seguridad para trabajar con ellos?
7. ¿Existen áreas específicas de la organización encargadas de gestionar la ciberseguridad y los riesgos asociados con los servicios en la nube o la infraestructura tecnológica?
8. ¿Cuál es la importancia de la infraestructura en Cloud dentro de la organización y qué proporción de la infraestructura total de la organización se encuentra en Cloud?
9. ¿Qué servicios en la nube está utilizando actualmente la organización? (IaaS, PaaS, SaaS, otros) ¿Está utilizando la organización alguna solución de Cloud privado?
10. ¿Qué tipo de arquitectura en la nube está adoptando la organización (por ejemplo, monolítica, microservicios, serverless, etc.)?
11. ¿Cuáles son los servicios de Cloud más utilizados dentro de la empresa?
12. ¿Cómo se gestiona el modelo de responsabilidad compartida en la empresa con respecto a la infraestructura en la nube?

Dominio 2 - Desarrollo

1. ¿Se realizan pruebas de seguridad en los desarrollos en la nube antes de pasar a producción?

2. ¿Se realizan pruebas de seguridad durante todo el ciclo de vida de desarrollo?
3. ¿Se aplican prácticas de DevSecOps tales como análisis automatizados o monitoreo continuo?
4. ¿Se usan prácticas de desarrollo en Cloud como Infrastructure as Code, contenedores o microservicios?

Cumplimiento normativo

1. ¿La empresa tiene requisitos normativos por parte de sus clientes y los cumple?
2. ¿Existen requisitos normativos internos o del negocio y se cumplen?
3. ¿Existen requisitos normativos legales del país y se cumplen?
4. ¿Se conoce el cumplimiento normativo de los proveedores de Cloud?

Dominio 4 - Análisis de amenazas

1. ¿Se tiene un inventario de fuentes de inteligencia de amenazas?
2. ¿Se utilizan referencias como Top Threats Cloud Computing de la CSA?
3. ¿Se conoce el marco MITRE ATT&CK y se usa para amenazas Cloud?

5.2. Análisis de Contexto

1) Introducción

El presente informe presenta un análisis de seguridad enfocado en las tecnologías de Cloud Computing, con el fin de evaluar el nivel de implementación y madurez de los controles de seguridad asociados.

El objetivo principal de este análisis es establecer el estado actual de la seguridad en entornos de Cloud Computing, identificar brechas (GAPs) y entregar recomendaciones orientadas a su mejora continua.

La evaluación se estructura en cuatro áreas clave:

- Contexto de la empresa en relación con Cloud Computing
- Desarrollo

- Cumplimiento normativo
- Inteligencia de amenazas

Para desarrollar este análisis, se utilizó un cuestionario basado en buenas prácticas reconocidas en seguridad de la información. Las respuestas fueron obtenidas a partir de la revisión de documentación entregada por la empresa durante la auditoría, así como de entrevistas con cargos estratégicos: Dirección de TI, Subgerencia de Desarrollo y Gerencia de Seguridad de la Información. La participación de estos actores fue autorizada por el director de TI, y el proyecto cuenta con la aprobación del Comité de Seguridad.

Finalmente, para medir el grado de avance en la implementación de estos aspectos, se aplicó el siguiente modelo de madurez:

Nivel	Descripción
0 – Inexistente	El control no está implementado ni planeado.
1 – Inicial	El control existe, pero de forma informal, reactiva y no documentada.
2 – Incompleto	El control se aplica parcialmente, con algo de documentación, pero sin estandarización.
3 – Definido	El control está formalmente definido, documentado y comunicado.

.2) Contexto de la empresa

la organización es una empresa de contact center B2B con una amplia trayectoria en el mercado y un tamaño cercano a los 1300 trabajadores. Su operación depende completamente de infraestructura tecnológica basada en servicios de nube pública, siendo el único proveedor Amazon, se utiliza un modelo Platform as a Service (PaaS) y una arquitectura serverless. Su actividad requiere el tratamiento de información sensible de clientes y usuarios finales, por lo que la seguridad de la información representa un aspecto crítico del negocio.

En términos generales, la organización cuenta con una estructura tecnológica bien definida y un nivel de seguridad aceptable respecto a servicios Cloud. Se percibe un nivel de madurez medio en la forma en que comprende y gestiona los riesgos asociados a su entorno operativo. A continuación, se presenta el análisis detallado de cada uno de los dominios revisados a partir de la auditoría realizada.

2) Resultados del análisis

2.1) Contexto general de la organización en relación con Cloud Computing

Este dominio evalúa el grado de conocimiento y control que tiene la organización sobre los servicios de Cloud Computing que utiliza, incluyendo la identificación de proveedores, los tipos de servicios contratados y los controles de seguridad aplicados.

Se considera este dominio de **prioridad Alta**, ya que toda la operación de TI de la organización depende de servicios en la nube.

N	Pregunta y Respuesta	Nivel
1	¿Se gestiona la seguridad en Cloud? Sí, se gestiona a partir del propio SGSI de la empresa, existen una política propia para aspectos de Cloud Computing.	2
2	¿Se utilizan controles definidos para gestionar el modelo de responsabilidad compartida? Las máquinas virtuales y los accesos se controlan como antes de la migración a AWS, no existen controles adicionales para serverless.	1
3	¿Se utilizan controles definidos para buenas prácticas de arquitectura Cloud? Actualmente solo se utiliza el principio de mínimo privilegios en los accesos de AWS.	1
4	¿Se mantiene conocimiento en las medidas de seguridad de los proveedores? Sí, sus boletines son revisados y se conoce su cumplimiento normativo con la ISO y la CCM STAR, pero esto no ha sido registrado ni formalizado.	2
5	¿Se dedican controles según la arquitectura utilizada? Actualmente, no existen controles dedicados a la arquitectura serverless.	0

Recomendaciones:

- Realizar controles adicionales para cada servicio utilizado en Cloud.
- Aplicar un framework como la CCM o el propio de AWS para gestionar el modelo de responsabilidad compartida.
- Utilizar el CIS framework para complementar las prácticas ya existentes.
- Registrar y formalizar las revisiones de seguridad del proveedor.
- Realizar controles dedicados a una arquitectura Serverless.

2.2) Desarrollo

Este dominio analiza el contexto de los proyectos de desarrollo que la organización implementa en entornos de Cloud Computing, considerando su alcance, criticidad y relación con los sistemas existentes. Se clasifica con **prioridad Alta**.

N	Pregunta y Respuesta	Nivel
1	¿Se realizan pruebas de seguridad en el desarrollo? Sí, no se puede enviar a producción ningún proyecto sin antes aplicarse pruebas de seguridad (Incluyendo Cloud).	2
2	¿Las pruebas se realizan durante todo el ciclo de vida? No, existen proyectos con pruebas intermedias, pero la mayoría se le realizan una vez se inicia el paso a producción.	0
3	¿Se aplican controles de DevSecOps como análisis automatizados, monitoreo continuo? Solo se realiza monitoreo continuo mediante Cloud-Watch centralizado vía Splunk.	1
4	¿Se utilizan aspectos de desarrollo en Cloud claves? No, no se utilizan ni se han auditado por parte del equipo de seguridad.	0

Recomendaciones:

- Aplicar pruebas de seguridad durante todo el ciclo de vida del desarrollo.
- Implementar pruebas automatizadas y enfoque hacia la izquierda.
- Implementar controles de seguridad en el desarrollo relacionados directamente con Cloud: Infraestructure as code, contenedores, microservicios y herramientas de monitoreo del proveedor.

2.3) Cumplimiento normativo

Este dominio evalúa cómo la organización gestiona el cumplimiento de las normativas y regulaciones que afectan el uso de servicios de Cloud Computing. Se asigna **prioridad Alta**.

N	Pregunta y Respuesta	Nivel
1	¿Se tienen requisitos normativos por parte de los clientes, se cumplen? ISO27001 actualmente se cumple.	3
2	¿Se tienen requisitos normativos por parte del negocio? Son solicitados por operaciones y gestionados en el SGSI.	3
3	¿Se tienen requisitos normativos por parte del país? Revisión en planificación para la ley de protección de datos.	2
4	¿Se ha dedicado tiempo para conocer el cumplimiento normativo del proveedor? Sí, pero no registrado ni formalizado.	2

Recomendaciones:

- Definir procesos de revisión de requisitos país con mayor urgencia.
- Definir procesos de revisión para proveedores dentro de los procesos de auditoría.

2.4) Análisis de amenazas

Este dominio analiza el nivel de madurez de las herramientas y procesos de inteligencia de amenazas implementados por la organización. Se asigna **prioridad Media**.

N	Pregunta y Respuesta	Nivel
1	¿Se tiene un inventario de fuentes de inteligencia de amenazas? Algunas fuentes consideradas pero no inventariadas.	0
2	¿Se utilizan referencias como el informe CSA? Se tiene conocimiento, pero no se han aplicado.	0
3	¿Se tiene conocimiento del marco MITRE ATT&CK? Se tiene conocimiento, pero no se ha aplicado.	0

Recomendaciones:

- Hacer un catálogo de amenazas Cloud a partir de las fuentes conocidas.
- Analizar informes de Top Threats Cloud Computing para gestionar amenazas.
- Incorporar al catálogo de amenazas aquellas identificadas en el marco MITRE ATT&CK y otras fuentes relevantes.

5.3. Plan de tratamiento durante aplicación de la metodología

1. Introducción

El presente informe contiene un plan de tratamiento relacionado al desarrollo en Cloud Computing dentro de la empresa, desde su planificación hasta su mantenimiento. Este análisis abarca aspectos como uso de Cloud Computing, DevSecOps, Cumplimiento e inteligencia de amenazas. El plan de tratamiento se basa en las respuestas proporcionadas por el equipo de tecnología a partir de un cuestionario enviado y analizado anteriormente.

El objetivo de este informe es establecer el estado actual de cumplimiento, identificar brechas (GAPs) y entregar recomendaciones para su mejora continua. La evaluación se ha realizado considerando los siguientes niveles de madurez: Inexistente, Inicial, Incompleto, Definido, Bajo, Medio, Alto y Crítico.

2. Gap identificado

2.1 - Contexto general de la organización en relación con Cloud Computing

2.1.1 - Controles de seguridad para servicios Cloud

A pesar de que el 100 % de la operación productiva de la empresa se encuentra en AWS, los servicios individuales construidos no poseen securización especializada. Se pretende construir controles técnicos basados en los servicios utilizados.

Prioridad: Medio

Plan de acción:

- Análisis de controles para Lambda, CloudFront, ECS, EC2, S3, Load Balancer, WAF, RDS.
- Presentación de medidas y discusión con infraestructura.
- Implementación de medidas acordadas.
- Registro de controles actualizados en PSI06: Política de Cloud Computing.

Área responsable: Seguridad de la información + Infraestructura AWS.

Duración: 3 Meses.

2.1.2 - Modelo de responsabilidad compartida CCM

Se pretende implementar controles de la CCM según criticidad.

Prioridad: Alto

Plan de acción:

- Análisis del modelo de responsabilidad compartida CCM lite.
- Análisis de mejoras desde Top Threats Cloud Computing CSA.
- Implementación y registro en el SGSI.

Área responsable: Seguridad de la información, Infraestructura AWS y Desarrollo.
Duración: 4 Meses.

2.1.3 – CIS Framework

Buenas prácticas en Cloud Computing no cuantificadas ni reflejadas en el SGSI.

Prioridad: Alto

Plan de acción:

- Construcción de lista de controles de CIS Framework.
- Aplicación de los controles solicitados.

Área responsable: Seguridad de la información + Infraestructura Cloud.
Duración: 3 Meses.

2.1.4 – Controles Proveedor

Se debe conocer y registrar información sobre el proveedor de servicios Cloud.

Prioridad: Medio

Plan de acción:

- Suscripción a boletines y fuentes de información de AWS.
- Elaboración de informes mensuales sobre hallazgos.
- Registro de estas prácticas en políticas de Cloud.

Área responsable: Seguridad de la información.
Duración: 1 Mes.

2.1.5 – Controles dedicados a arquitectura Serverless

No existen controles específicos para servicios serverless.

Prioridad: Crítico

Plan de acción:

- Clasificación de todos los servicios serverless.
- Identificación de vectores de ataque comunes.
- Implementación de controles por parte de Infraestructura AWS.

- Establecer controles dedicados y agregarlos a las auditorías.

Área responsable: Seguridad de la información + Infraestructura AWS.
Duración: 2 Meses.

2.2 – Desarrollo

2.2.1 – Pruebas de seguridad durante todo el SDLC

Actualmente solo se realizan al final, se implementarán durante todo el ciclo.

Prioridad: Crítico

Plan de acción:

- Ingresar tareas de pruebas de seguridad en Jira.
- Aplicar pruebas de seguridad (código asistido, revisión manual, software especializado).
- Actualizar documento de buenas prácticas de desarrollo seguro.
- Construir indicadores sobre pruebas aplicadas y hallazgos corregidos.

Área responsable: Seguridad de la información + Desarrollo.
Duración: 2 Meses.

2.2.2 – Uso de buenas prácticas DevSecOps

Prioridad: Alto

Plan de acción:

- Analizar procesos de revisión continua.
- Aplicar pruebas y consultar efectividad con el equipo de desarrollo.
- Construir indicadores para medir reducción de amenazas.

Área responsable: Seguridad de la información.
Duración: 1 Mes.

2.2.3 – Uso de buenas prácticas DevSecOps Cloud

Prioridad: Crítico

Plan de acción:

- Analizar procesos para implementar: Infrastructure as Code, contenedores, microservicios y herramientas del proveedor.

- Aplicar pruebas y medir efectividad.
- Construir indicadores de reducción de amenazas.

Área responsable: Seguridad de la información + Infraestructura Cloud + Desarrollo.
Duración: 1 Mes.

2.3 – Cumplimiento normativo

2.3.1 – Planes de auditoría para cumplimiento legal

Prioridad: Bajo

Plan de acción:

- Revisar nueva ley de protección de datos.
- Implementar procedimientos de revisión de legislación nacional.
- Aplicar controles para cumplimiento legal.

Área responsable: Seguridad de la información.
Duración: 1 Mes.

2.3.2 – Planes de auditoría para cumplimiento proveedores Cloud

Prioridad: Bajo

Plan de acción:

- Definir criterios de seguridad para proveedores Cloud.
- Incluir revisión documental y técnica del proveedor en auditorías.

Área responsable: Seguridad de la información + Infraestructura AWS + Desarrollo.
Duración: 1 Mes.

2.4 – Análisis de amenazas

2.4.1 – Construcción catálogo de amenazas Cloud

Prioridad: Alta

Plan de acción:

- Revisar catálogo de amenazas actual y ajustarlo a contexto Cloud.

- Recolectar información de Top Threats Cloud Computing y MITRE ATT&CK.
- Identificar y categorizar amenazas específicas según servicios utilizados.
- Integrar amenazas al catálogo institucional y mapearlas a activos críticos.
- Aprobar y registrar catálogo actualizado dentro del SGSI.

Área responsable: Seguridad de la información.

Duración: 3 Meses.

3. Plan de remediación

Se aplicará inicialmente un plan de 1 mes:

- 2.1.2 – Modelo de responsabilidad compartida CCM (parcial)
- 2.1.3 – CIS Framework (parcial)
- 2.2.1 – Pruebas de seguridad durante el SDLC (completo)
- 2.4.1 – Catálogo de amenazas Cloud (parcial)

4. Indicadores

- % de aplicación de la CCM = $(\text{Controles CCM implementados} / \text{Total controles CCM seleccionados}) \times 100$.
- % de aplicación CIS Framework = $(\text{Controles CIS aplicados} / \text{Controles CIS relevantes}) \times 100$.
- % de proyectos con pruebas de seguridad = $(\text{Proyectos con pruebas} / \text{Total proyectos}) \times 100$.
- % de amenazas analizadas CSA = $(\text{Amenazas CSA incorporadas} / \text{Total amenazas CSA}) \times 100$.

5. Controles específicos del primer ciclo de implementación

5.1 Controles CCM lite

Se seleccionaron los primeros 15 controles aplicables de la CCM lite: A&A-02, A&A-06, AIS-02, AIS-06, CCC-01, DCS-06, DSP-01, DSP-05, DSP-06, DSP-07, DSP-10, IVS-03, IVS-06, IVS-07, IVS-09.

5.2 Controles CIS Framework

Se aplicarán los 21 controles iniciales del dominio IAM de CIS AWS Foundations Benchmark v5: 1.1, 1.2, 1.3, 1.4, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11, 1.12, 1.13, 1.14, 1.15, 1.16, 1.17, 1.18, 1.19, 1.20 y 1.21.

5.4. Registro Cambios durante aplicación de la metodología

Fecha	Plan	Responsable	Cambios realizados
30/4/2025	2.1.3 – CIS Framework	Infraestructura AWS	Se convalidan los controles 1.4 y 1.5. Debido a que en auditorías anteriores se habían aplicado los mismos cambios.
30/4/2025	2.1.2 – Modelo de responsabilidad compartida CCM	Seguridad de la información	Los controles de la CCM: DSP-01 y el IVS-03 se están realizando actualmente.
02/05/2025	2.2.1 – Pruebas de seguridad durante todo el SDLC	Desarrollo	Para proyectos de levantamiento de campañas no se requerirá pruebas en la sección de requerimientos, debido a que todos poseen los mismos requerimientos y ya han sido aprobados por el área de seguridad.
07/05/2025	2.1.2 – Modelo de responsabilidad compartida CCM	Seguridad de la información	Los controles de la CCM A&A-02 y A&A-06 no son realizables actualmente, debido a que se está en una fase inicial de integración de controles Cloud.

Fecha	Plan	Responsable	Cambios realizados
12/05/2025	2.1.3 – CIS Framework	Infraestructura AWS	El control de la CIS 1.15 no es aplicable debido a que si bien existe una gestión de roles no se ha hecho a partir de grupos; si se realiza el proceso incorrectamente podría afectar a la operatividad. Se realizará prontamente un control propio para este aspecto.
15/05/2025	2.1.3 – CIS Framework	Infraestructura AWS	Falta de capacidades para aplicar los controles de la CIS, debido a que existen más controles complejos de aplicar y con un riesgo alto de impactar a la operación.
17/05/2025	2.1.3 – CIS Framework	Infraestructura AWS	Debido a problemas de disponibilidad en plataforma de Call Center, el equipo no realizó avances durante los días 16 y 17 de mayo.

5.5. Informe Verificación de resultados

1. Resumen Ejecutivo

Este informe presenta la verificación del cumplimiento del Plan de Tratamiento Cloud implementado durante abril-mayo de 2025, así como un plan de remediación de una semana para mejorar los indicadores identificados con oportunidades de mejora.

2. Verificación de Cumplimiento

2.1 Indicadores Alcanzados

1. % de aplicación de la CCM (Cloud Controls Matrix)

Meta esperada: $\geq 80\%$

Resultado Final: 60 % (9 de 15 controles seleccionados implementados)

Estado: CUMPLIDO

Control	Descripción	Estado
A&A-02	Realizar auditorías y evaluaciones independientes al menos una vez al año.	No realizado
A&A-06	Establecer un plan de acciones correctivas basado en riesgos.	No realizado
AIS-02	Requisitos básicos de seguridad para aplicaciones.	Realizado
AIS-06	Estrategias para implementación de aplicaciones seguras.	Realizado
CCC-01	Políticas para gestión de riesgos en cambios de activos.	No realizado
DCS-06	Catalogar y rastrear activos físicos y lógicos.	Realizado
DSP-01	Políticas de clasificación, protección y manejo de datos.	Realizado
DSP-05	Documentación del flujo de datos.	Realizado
DSP-06	Documentar propiedad y administración de datos.	Realizado
DSP-07	Seguridad desde el diseño en sistemas y productos.	Realizado
DSP-10	Procesos para proteger transferencias de datos.	Realizado
IVS-03	Monitorear, cifrar y restringir comunicaciones entre entornos.	Realizado
IVS-06	Segmentar y restringir accesos entre inquilinos.	No realizado
IVS-07	Usar canales seguros y cifrados para migraciones.	No realizado
IVS-09	Procesos de defensa integral ante ataques.	No realizado

2. % de aplicación de la CIS Framework

Meta esperada: $\geq 90\%$

Resultado Final: 52 % (11 de 21 controles implementados)

Estado: NO CUMPLIDO

Control	Descripción	Estado
1.1	Mantener los datos de contacto actuales	Realizado
1.2	Registrar información de contacto de seguridad	Realizado
1.3	Sin clave de acceso para usuario 'root'	Realizado
1.4	MFA habilitado para 'root'	Realizado
1.5	MFA físico habilitado para 'root'	Realizado
1.6	Eliminar uso de 'root' en tareas diarias	No realizado
1.7	Política de contraseñas ≥ 14 caracteres	Realizado
1.8	Política que prevenga reutilización de contraseñas	No realizado
1.9	MFA habilitado para usuarios de IAM	No realizado
1.10	No crear claves de acceso iniciales para usuarios	Realizado
1.11	Deshabilitar credenciales inactivas ≥ 45 días	Realizado
1.12	Una clave activa por usuario	No realizado
1.13	Rotar claves cada 90 días	Realizado
1.14	Permisos solo vía grupos	No realizado
1.15	No adjuntar políticas con privilegios completos	No realizado
1.16	Rol de soporte para incidentes AWS	Realizado
1.17	Usar roles de instancia de IAM	Realizado
1.18	Eliminar certificados expirados	Realizado
1.19	Habilitar analizador de acceso externo	Realizado
1.20	Gestión centralizada de usuarios IAM	Realizado
1.21	Restringir acceso a AWSCloudShellFullAccess	Realizado

3. % de proyectos con pruebas de seguridad durante desarrollo

Meta esperada: $\geq 90\%$

Resultado Final: 100 % (2 de 2 proyectos ejecutados)

Estado: CUMPLIDO

Nombre del Proyecto	Etapas actual	Estado
Aplicación de gestión de tickets de Soporte	Implementado	Realizado
Aplicación para la automatización del levantamiento de campañas	En desarrollo	Realizado

4. % de amenazas analizadas del marco Top Threats Cloud Computing

Meta esperada: $\geq 90\%$

Resultado Final: 91 % (10 de 11 amenazas catalogadas)

Estado: CUMPLIDO

N	Nombre	Estado
1	Mala Configuración y Control de Cambios Inadecuado	Agregado
2	Gestión de Identidad y Acceso (IAM)	Agregado
3	Interfaces y APIs Inseguras	Agregado
4	Estrategia de Seguridad en la Nube Inadecuada	Agregado
5	Recursos de Terceros Inseguros	Agregado
6	Desarrollo de Software Inseguro	Agregado
7	Divulgación Accidental de Datos	Agregado
8	Vulnerabilidades del Sistema	Agregado
9	Visibilidad/Observabilidad Limitada en la Nube	Agregado
10	Compartición de Recursos No Autenticada	Agregado
11	Amenazas Persistentes Avanzadas	Agregado

2.2 Problemáticas Identificadas

- Limitaciones técnicas del equipo de infraestructura AWS: problemas de conocimiento inicial.
- Complejidad de implementación de controles: tiempo estimado poco realista, principalmente para CCM y CIS Framework.
- Interrupciones por urgencias operativas: incidentes que afectaron ligeramente el rendimiento de los equipos.

3. Plan de Remediación

Objetivo: Elevar el cumplimiento del CIS Framework y la CCM a partir del enfoque en pocos controles, extendiendo el plazo final a 2 semanas.

Actividades Programadas:

- **CCM:** Implementación de los controles: IVS-06, IVS-07 y IVS-09.
- **CIS Framework:** Implementación de los controles: 1.6, 1.8, 1.9, 1.12.

5.6. Informe resultados finales

1. Resumen Ejecutivo

Este informe final presenta los resultados completos de la implementación de la metodología de tratamiento de no conformidades Cloud, incluyendo las mejoras obtenidas durante el plan de remediación de desarrollo en Cloud computing.

2. Resultados Finales Post-Remediación

2.1 Indicadores Finales Consolidados

1. % de aplicación de la CCM (Cloud Controls Matrix)

Meta esperada: $\geq 80\%$

Resultado Final: 80 % (12 de 15 controles seleccionados implementados)

Estado: CUMPLIDO

Control	Descripción	Estado
A&A-02	Auditorías y evaluaciones independientes anuales	No realizado
A&A-06	Plan de acciones correctivas basado en riesgos	No realizado
AIS-02	Requisitos básicos de seguridad para aplicaciones	Realizado
AIS-06	Estrategias y capacidades para implementación segura	Realizado
CCC-01	Políticas para riesgos en cambios de activos	No realizado
DCS-06	Catalogar y rastrear activos físicos y lógicos	Realizado
DSP-01	Políticas para clasificación y manejo de datos	Realizado
DSP-05	Documentación del flujo de datos	Realizado
DSP-06	Propiedad y administración de datos documentados	Realizado
DSP-07	Seguridad desde el diseño en sistemas y productos	Realizado
DSP-10	Procesos técnicos para protección de datos	Realizado
IVS-03	Monitoreo, cifrado y restricciones de comunicación	Realizado
IVS-06	Segmentación y control de accesos entre inquilinos	Realizado
IVS-07	Canales seguros y cifrados para migraciones	Realizado
IVS-09	Procesos de defensa integral ante ataques	Realizado

2. % de aplicación de la CIS Framework

Meta esperada: $\geq 90\%$

Resultado Final: 71 % (15 de 21 controles implementados)

Estado: NO CUMPLIDO

Control	Descripción	Estado
1.1	Mantener datos de contacto actuales	Realizado
1.2	Información de contacto de seguridad registrada	Realizado
1.3	Sin clave de acceso para usuario 'root'	Realizado
1.4	MFA habilitado para 'root'	Realizado
1.5	MFA físico habilitado para 'root'	Realizado
1.6	Eliminar uso de 'root' en tareas diarias	Realizado
1.7	Política de contraseñas ≥14 caracteres	Realizado
1.8	Prevenir reutilización de contraseñas	Realizado
1.9	MFA habilitado para usuarios IAM con contraseña	Realizado
1.10	No crear claves de acceso iniciales	Realizado
1.11	Deshabilitar credenciales inactivas ≥45 días	Realizado
1.12	Solo una clave activa por usuario	Realizado
1.13	Rotar claves cada 90 días	Realizado
1.14	Permisos solo a través de grupos	No realizado
1.15	No adjuntar políticas con privilegios completos	No realizado
1.16	Rol de soporte para incidentes AWS	Realizado
1.17	Usar roles de instancia para acceso a recursos	Realizado
1.18	Eliminar certificados SSL/TLS expirados	Realizado
1.19	Analizador de acceso externo habilitado	Realizado
1.20	Gestión centralizada de usuarios IAM	Realizado
1.21	Restringir acceso a AWSCloudShellFullAccess	Realizado

3. % de proyectos con pruebas de seguridad durante desarrollo

Meta esperada: ≥ 90 %

Resultado Final: 100 % (2 de 2 proyectos ejecutados)

Estado: CUMPLIDO

Nombre del Proyecto	Etapas actual	Estado
Aplicación de gestión de tickets de Soporte	Implementado	Realizado
Aplicación para la automatización del levantamiento de campañas	En desarrollo	Realizado

4. % de amenazas analizadas del marco Top Threats Cloud Computing

Meta esperada: ≥ 90 %

Resultado Final: 91 % (10 de 11 amenazas catalogadas)

Estado: CUMPLIDO

N	Nombre	Estado
1	Mala Configuración y Control de Cambios Inadecuado	Agregado
2	Gestión de Identidad y Acceso (IAM)	Agregado
3	Interfaces y APIs Inseguras	Agregado
4	Estrategia de Seguridad en la Nube Inadecuada	Agregado
5	Recursos de Terceros Inseguros	Agregado
6	Desarrollo de Software Inseguro	Agregado
7	Divulgación Accidental de Datos	Agregado
8	Vulnerabilidades del Sistema	Agregado
9	Visibilidad/Observabilidad Limitada en la Nube	Agregado
10	Compartición de Recursos No Autenticada	Agregado
11	Amenazas Persistentes Avanzadas	Agregado

2.2 Beneficios del Plan de Remediación

- Incremento del cumplimiento CCM del 60 % al 80 %.
- Incremento del cumplimiento CIS Framework del 52 % al 71 %.

3. Lecciones Aprendidas

3.1 Fortalezas Identificadas

- Efectividad del enfoque progresivo de implementación.
- Alto compromiso de los equipos de tecnología.
- Capacidad de adaptación ante urgencias operativas.

3.2 Oportunidades de Mejora Validadas

- Necesidad de mayor capacitación técnica en el equipo de tecnología para aplicar controles de seguridad.

4. Mejoras próxima iteración del proceso

- Mayor Duración: 3 meses (post-auditoría programada).
- Mayor cantidad de reuniones de seguimiento: Reuniones quincenales de indicadores.
- Incremento del alcance: completar controles restantes y expandir cobertura.

4.2 Objetivos Próxima Iteración

- Completar 100 % de implementación CCM (A&A-02, A&A-06, CCC-01).
- Implementar control CIS restante (1.14).
- Expandir cobertura a 10 controles CCM adicionales.

6. Conclusiones

La primera iteración de la metodología Cloud Security generó resultados positivos. El plan de remediación permitió alcanzar o superar la mayoría de los indicadores establecidos. Éxitos principales:

- Mejoras en el manejo de configuraciones en Amazon AWS.
- Aplicación de un modelo formal de responsabilidad compartida.
- Mayor control en proyectos del área de desarrollo.
- Visibilidad a riesgos del uso de tecnologías Cloud.
- Evidencia de falta de capacidades ante problemas relacionados con Cloud Security.

REFERENCIAS BIBLIOGRÁFICAS

- [Alashhab et al., 2021] Alashhab, Z. R., Anbar, M., Singh, M. M., Leau, Y.-B., Al-Sai, Z. A., y Alhayja'a, S. A. (2021). Impact of coronavirus pandemic crisis on technologies and cloud computing applications. *Journal of Electronic Science and Technology*, 19(1):100059.
- [Ameyo, 2024] Ameyo (2024). On-premise vs cloud contact center software – what's the difference? Consultado el 20 de abril de 2025.
- [AWS, 2024] AWS (2024). *Security Pillar - AWS Well-Architected Framework*. Accedido: 2025-04-13.
- [AWS, 2025a] AWS (2025a). Modelo de responsabilidad compartida. Accedido: 2025-04-29.
- [AWS, 2025b] AWS (2025b). ¿qué es devsecops? Consultado el 3 de mayo de 2025.
- [Bonguet y Bellaiche, 2017] Bonguet, A. y Bellaiche, M. (2017). A survey of denial-of-service and distributed denial of service attacks and defenses in cloud computing. *Future Internet*, 9(3):43.
- [Borra, 2024] Borra, P. (2024). An overview of cloud computing and leading cloud service providers. *International Journal of Computer Engineering and Technology (IJCET) Volume*, 15:122–133.
- [Calder, 2020] Calder, A. (2020). *Information Security based on ISO 27001/ISO 27002*. Van Haren.
- [CIS, 2021] CIS (2021). *CIS Critical Security Controls v8*. Center for Internet Security. Accedido: 2025-04-13.
- [Cloud Security Alliance, 2025] Cloud Security Alliance (2025). Certificación csa star. Accedido: 2025-04-13.
- [Cloudflare, 2025] Cloudflare (2025). What is a serverless microservice? Revisado el 22 de julio de 2025.
- [CSA, 2020a] CSA (2020a). Shared responsibility model explained. Accedido: abril 12, 2025.
- [CSA, 2020b] CSA (2020b). Top threats to cloud computing: Pandemic eleven. Accessed: 2025-04-07.
- [CSA, 2021] CSA (2021). State of cloud security concerns: Csa.
- [CSA, 2024] CSA (2024). Top threats to cloud computing 2024: Csa.
- [CSA, nd] CSA (n.d.). Cloud controls matrix. Accessed: 2025-05-03.

- [Dynatrace, 2025] Dynatrace (2025). Devsecops: desarrollo, seguridad y operaciones. Revisado el 22 de julio de 2025.
- [ENISA, 2009] ENISA (2009). Cloud computing security risk assessment. Technical report, ENISA. Accedido: 2025-04-13.
- [Ezema y Rivera, 2021] Ezema, E. y Rivera, L. (2021). The pandemic accelerated cloud: Application, impact and challenges of cloud computing in covid-19 pandemic. *Impact and Challenges of Cloud Computing in COVID-19 Pandemic (December 13, 2021)*.
- [Fattocses, 2019] Fattocses (2019). Twit fattocses. Tweet del 26 de junio de 2019.
- [Ibrahim et al., 2018] Ibrahim, A., Valli, C., McAteer, I., y Chaudhry, J. (2018). A security review of local government using nist csf: a case study. *The Journal of Supercomputing*, 74:5171–5186.
- [Ibrahim et al., 2022] Ibrahim, A., Yousef, A. H., y Medhat, W. (2022). Devsecops: A security model for infrastructure as code over the cloud. En *2022 2nd International Mobile, Intelligent, and Ubiquitous Computing Conference (MIUCC)*, pp. 284–288. IEEE.
- [ISO/IEC, 2013] ISO/IEC (2013). Iso/iec 27001:2013 - information technology - security techniques - information security management systems - requirements. Accedido: abril 12, 2025.
- [ISO/IEC, 2015] ISO/IEC (2015). Iso/iec 27017:2015 - code of practice for information security controls based on iso/iec 27002 for cloud services. Accedido: abril 12, 2025.
- [ISO/IEC, 2022] ISO/IEC (2022). ISO/IEC 27004:2022 - information security, cybersecurity and privacy protection — information security management — monitoring, measurement, analysis and evaluation. <https://www.iso.org/standard/73906.html>. Consultado el 3 de mayo de 2025.
- [Jansen y Grance, 2011] Jansen, W. y Grance, T. (2011). Sp 800-144. guidelines on security and privacy in public cloud computing.
- [Kanade, 2022] Kanade, V. (2022). Multi-cloud vs. hybrid cloud: 10 key comparisons. <https://www.spiceworks.com/tech/cloud/articles/multi-cloud-vs-hybrid-cloud/>.
- [Kerravala, 2025] Kerravala, Z. (2025). Webex meetings or zoom: Peering into performance. Accedido: 19 de abril de 2025.
- [Mandal y Khan, 2020a] Mandal, S. y Khan, D. A. (2020a). A study of security threats in cloud: Passive impact of covid-19 pandemic. En *2020 International Conference on Smart Electronics and Communication (ICOSEC)*, pp. 837–842. IEEE.
- [Mandal y Khan, 2020b] Mandal, S. y Khan, D. A. (2020b). A study of security threats in cloud: Passive impact of covid-19 pandemic. En *2020 International Conference on Smart Electronics and Communication (ICOSEC)*, pp. 837–842.

- [Mell y Grance, 2011] Mell, P. y Grance, T. (2011). The nist definition of cloud computing. Special Publication 800-145, National Institute of Standards and Technology, Gaithersburg, MD, USA. Accedido el 22 de julio de 2025.
- [Overflow, 2021] Overflow, S. (2021). Pandemic lockdowns accelerated cloud migration by three to four years. Accessed: 2025-04-07.
- [Pascoe et al., 2024] Pascoe, C., Quinn, S., y Scarfone, K. (2024). The nist cybersecurity framework (csf) 2.0. Technical Report NIST CSWP 29, National Institute of Standards and Technology. Accedido: 2025-04-13.
- [Patidar et al., 2012] Patidar, S., Rane, D., y Jain, P. (2012). A survey paper on cloud computing. En *2012 second international conference on advanced computing & communication technologies*, pp. 394–398. IEEE.
- [Peña-Robayo et al., 2024] Peña-Robayo, Martha and del Pílar Moreno, Ana and others (2024). Amenazas emergentes en la computación en la nube: desafíos de seguridad y respuesta. *Revista Vínculos*, 21(1).
- [REYES y MENDOZA, 2023] REYES, C. y MENDOZA, C. (2023). Exploring the impact of shared responsibility models on cloud security posture and vulnerability management.
- [Sajjan y Ghorpade, 2017] Sajjan, R. S. y Ghorpade, V. R. (2017). Ransomware attacks: Radical menace for cloud computing. En *2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, pp. 1640–1646. IEEE.
- [Singh et al., 2021] Singh, R. P., Haleem, A., Javaid, M., Kataria, R., y Singhal, S. (2021). Cloud computing in solving problems of covid-19 pandemic. *Journal of Industrial Integration and Management*, 6(02):209–219.
- [Tariq, 2018] Tariq, M. I. (2018). Analysis of the effectiveness of cloud control matrix for hybrid cloud computing. *International Journal of Future Generation Communication and Networking*, 11(4):1–10.
- [TENELEMA et al., 2020] TENELEMA, E. N., MÉNDEZ, P. M., VILLA, H. M., y CAIZA, D. G. (2020). Modelo de seguridad para mitigación de vulnerabilidades en ambientes de almacenamiento en la nube con base en las normas iso 27017 y 27018. *Espacios*, 41:17–20.
- [UNESCO, 2025] UNESCO (2025). Education response to covid-19: Initiatives. Accedido: 19 de abril de 2025.
- [Vaca Báez, 2023] Vaca Báez, J. F. (2023). *Sistema de gestión de la seguridad de la información (SGSI) basado en la norma ISO 27001: 2013 para el centro médicoÇotacachi*. Tesis doctoral, PUCE Ibarra.
- [Watson et al., 2015] Watson, Michael R and Marnerides, Angelos K and Mauthe, Andreas and Hutchison, David and others (2015). Malware detection in cloud computing infrastructures. *IEEE Transactions on Dependable and Secure Computing*, 13(2):192–205.

[Xue y Xin, 2016] Xue, C. T. S. y Xin, F. T. W. (2016). Benefits and challenges of the adoption of cloud computing in business. *International Journal on Cloud Computing: Services and Architecture*, 6(6):01–15.