UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

Resolución: **RPC-SO-02-No.053-2021**

PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGÍSTER

Título del proyecto:
Propuesta de un esquema de gestión de riesgos tecnológicos para modelos de servicio de tipo Infraestructura como servicio "IAAS" utilizando la metodología OCTAVE dentro del ciclo de mejora continua PHVA.
Línea de Investigación:
Proyecto de Graduación
Campo amplio de conocimiento:
Propuesta de un esquema de gestión de riesgos tecnológicos.
Autor:
Ing. Muñoz Gutiérrez Cristian Andrés
Tutor:
Msc. Vaca Benalcázar Christian Patricio CPA

Quito – Ecuador

2022

APROBACIÓN DEL TUTOR

Yo, Christian Vaca con C.I: 171936855-5 en mi calidad de Tutor del proyecto de investigación titulado: Propuesta de un esquema de gestión de riesgos tecnológicos para modelos de servicio de tipo Infraestructura como servicio "IAAS" utilizando la metodología OCTAVE dentro del ciclo de mejora continua PHVA.

Elaborado por: Cristian Andrés Muñoz Gutiérrez, de C.I: 172134069-1, estudiante de la Maestría: Seguridad Informática de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., 09 de Septiembre de 2022

Firma

DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE

Yo, Cristian Andrés Muñoz Gutiérrez con C.I: 172134069-1, autor/a del proyecto de titulación denominado: Propuesta de un esquema de gestión de riesgos tecnológicos para modelos de servicio de tipo infraestructura como servicio "IAAS" utilizando la metodología OCTAVE dentro del ciclo de mejora continua PHVA. Previo a la obtención del título de Magister en Seguridad Informática.

1. Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar el respectivo trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.
2. Manifiesto mi voluntad de ceder a la Universidad Tecnológica Israel los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autor@ del trabajo de titulación, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital como parte del acervo bibliográfico de la Universidad Tecnológica Israel.
3. Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de prosperidad intelectual vigentes.

Quito D.M., 09 de septiembre de 2022

CRISTIAN ANDRES MUNOZ GUTIERREZ
Firmado digitalmente por CRISTIAN ANDRES MUNOZ GUTIERREZ
Fecha: 2022.09.11 20:19:24 -05'00'

Firma

Tabla de contenidos

Índice de tablas

Índice de figuras

INFORMACIÓN GENERAL

Contextualización del tema

Hoy en día existe una tendencia muy marcada respecto al uso de infraestructuras cloud "en la nube", en el mercado tecnológico hay un sin número de proveedores de servicio con varios esquemas de operación. Una de las características de mayor relevancia es la escalabilidad de recursos bajo demanda y el fácil acceso a la gestión de servidores y servicios corporativos. Existen diferentes servicios y capas que ofrece este tipo de infraestructura, las principales características de este modelo de servicio son: costos variables (pago por consumo), escalabilidad, elasticidad, trabajo colaborativo, ahorro energético, optimización de recursos humanos que conozcan del manejo de la plataforma en producción, ahorro monetario en comparación a una arquitectura física, coherencia y ubicuidad.

Ampliando el panorama tecnológico el incremento en el volumen de incidentes de seguridad en el 2021 y 2022 son a mayor escala y más costosos según la investigación realizada por (*Top Threats to Cloud Computing*, s. f.), por lo que el disponer de un resquema de manejo de riesgos sobre una arquitectura en la nube es de gran importancia para diferentes tipos de empresas hoy en día, con la necesidad de contar con características de elasticidad en sus recursos de hardware, esta arquitectura brinda una opción de despliegue para una gran variedad de servicios y en tiempos bastante ágiles que en diferentes giros de negocios significa ganancias o pérdidas. "Los métodos de intrusión utilizados tienen una tendencia como noticias falsas "fake news", ciberataques a la cadena de suministro, guerra fría, filtraciones de datos, criptodivisas, robo de información, ataques a dispositivos móviles, identificación de vulnerabilidades de microservicios, tecnología "deepfake" y ataques de ransomware. En 2022, la sofisticación y la escala de los ciberataques siguen batiendo récords y se espera un aumento de secuestros informáticos y ataques móviles" según lo mencionado por la "red seguridad" (*¿Qué ciberamenazas serán tendencia en 2022?*, 2021). Debido a estos posibles incidentes de seguridad "las empresas deben asegurarse de que cuentan con las medidas adecuadas para

prevenir los ciberataques más avanzados, ser proactivas y no dejar ninguna parte de su superficie sin proteger o supervisar", observa Mario García, director de Check Point para España y Portugal "Igual que los ataques, la seguridad tiene que evolucionar de manera constante, 2022".

De acuerdo con el informe (*Deepfakes, Cryptocurrency and Mobile Wallets*, 2021) — elaborado por *Check Point Software Technologies* para el año 2022 los cibercriminales encontrarán nuevas oportunidades de ataque con las deepfakes, las criptodivisas, los wallets, entre otros. Además de las nuevas tendencias de ataque antes mencionados existen técnicas de ataque conocidas y bastante efectivas según el modelo de seguridad con el que se disponga en la arquitectura tecnológica.

Según lo indicado por *Lumu Technologies*, compañía de ciberseguridad los ataques de ransomware han afectado considerablemente la economía de varios sectores estratégicos, las organizaciones que tuvieron incidentes con ransomware fueron: 68% en 2021; 62% en 2020; 56% en 2019 y 55% en 2018 («Ataques de ransomware aumentó 6% más en 2021», 2022).

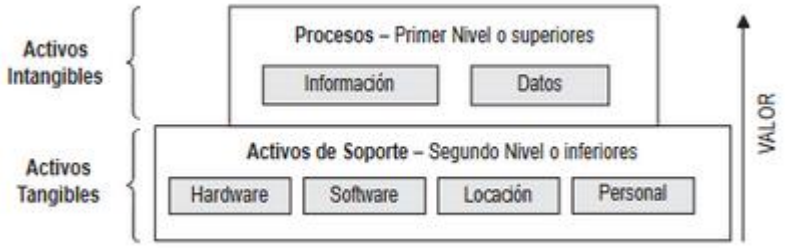
Respecto a la gestión de riesgos existen diferentes normativas que le permiten a un empresa identificar y gestionar los riesgos que están presentes desde que el servicio se encuentra publicado y dependiendo su funcionalidad este riesgo puede incrementar considerablemente.

El ciclo de mejora continua Planificar, Hacer, Verificar y Actuar (PHVA) facilita un proceso infinito de evaluación en cuanto a la administración de los riesgos a los cuales diferentes servicios e información se encuentran expuestos, además brinda una conceptualización base según las normas ISO 27001 (Sistema de Gestión de Seguridad de la información SGSI) e ISO 27002 de tal manera interpretar las reglas que se necesitan para poder gestionar estos riesgos de forma adecuada. "La mejor metodología para la gestión de riesgos tecnológicos está orientada en procesos teniendo en cuenta que esto facilita el entendimiento sobre el funcionamiento de la organización y la definición de interacciones para la identificación de activos críticos" según lo indicado en el artículo de investigación (de Caldas, s. f.).

Estos riesgos están categorizados según los activos sobre los que tienen afectación; activos tangibles y activos intangibles, ambos de igual importancia para una empresa, sin embargo, tienen diferente valor al momento de priorizar los servicios que brindan y que impacto tienen en el giro de negocios. Según lo identificado en la Figura. 2. se tiene una categorización de estos activos:

Figura *1.*

Manejo de activos según la metodología Octave



Nota. Categorización de activos manejados en la metodología. Adaptada de la metodología Octave, 2001 (https://resources.sei.cmu.edu/asset_files/TechnicalReport/2001_005_001_13871.pdf).

Según lo mencionado en los artículos de investigación (Castro & Bayona, 2011) y (Bezanilla et al., 2018) “la gestión de riesgos en las nubes privadas adquiere relevancia debido a que, en este tipo de escenario, las amenazas a los centros de datos tradicionales coexisten junto a las que provocan el empleo de los recursos compartidos y otras características de la computación en la nube y la virtualización”. Por tal motivo el disponer de un plan de acción frente a estos riesgos tiene es de gran importancia, el contar con una línea base de seguridad permitirá optimizar los tiempos de respuesta y el diseño de una metodología a seguir.

Existen diferentes esquemas de seguridad orientados a sistemas o aplicaciones particulares bajo un modelo de “Infraestructura como servicio”, que sirven en ocasiones hasta cierto punto para poder referenciar como actuar frente a un riesgo de seguridad, según lo expuesto en

(Agudelo, 2018) se obtiene como resultado un conjunto de actividades y recomendaciones técnicas que permiten mitigar estos riesgos bajo un procedimiento dado.

Como parte de las características del modelo de infraestructura como servicio, existen diferentes capas de seguridad que puede habilitarse sobre una instancia o plataforma. Cada una brinda una configuración recomendada según el tipo de servicio y para una gran variedad de aplicaciones desarrolladas al interno o de uso común. Según lo indicado en el estudio (*Optimización de una IaaS en cloud computing haciendo uso de una nube privada*, s. f.) el uso de la tecnología en la nube permite tener eficiencia en el consumo de energía en las empresas y proporcionalmente costos por el mantenimiento de equipos de cómputo y los riesgos asociados a este entorno.

Como requerimiento principal para la gestión de riesgos corresponde el conocer a que nos enfrentamos, el nivel y tipo de vulnerabilidades que puede tener un servicio y en base a estos poder relacionarlos con los riesgos que podríamos manejar. Considerando que uno de los puntos de mayor interés en una empresa es su economía en la investigación (Mateo, 2017) se evidencia el crecimiento y volumen monetario que han tenido incidentes de seguridad con gran afectación en diferentes partes del mundo y su evolución en la última década.

Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE) nos permite obtener la valoración y gestión del riesgo contemplando la identificación, estimación, análisis y evaluación de riesgos e identificación de opciones para tratarlos, apoyándose en la unificación de criterios básicos que permitan referenciar cambios adversos en el cumplimiento de objetivos estratégicos en la operación de una arquitectura IaaS para luego definir probabilidades e impactos en la materialización de amenazas dentro de su alcance y límites. Así mismo se dispone del ciclo de mejora continua “Deming” PHVA, como apoyo a los requerimientos del SGSI (Sistema de gestión de seguridad) definido en el ISO/IEC 27001, por lo que se hará énfasis en el proceso de iteraciones continuas que permiten tener un esquema ágil respecto la valoración y manejo proporcionado por la metodología Octave.

Problema de investigación

¿Existe alguna metodología que permita realizar la identificación y manejo de riesgos basado en activos o aplicativos de una infraestructura como servicio en la nube y que además disponga de un ciclo de mejora continua como parte de su implementación?

Objetivo general

Establecer una propuesta de un esquema de gestión de riesgos mediante la metodología OCTAVE utilizando el ciclo de mejora continua PHVA para disponer de un marco de referencia que permita gestionar de forma correcta eventos e incidentes de seguridad en un modelo de Infraestructura como servicio "IAAS".

Objetivos específicos

Contextualizar los fundamentos teóricos sobre una infraestructura en la nube de tipo IAAS, la metodología Octave y el ciclo de mejora continua PHVA, mediante la revisión de las principales consideraciones y características para disponer de un esquema de seguridad y manejo de riesgos que permita asegurar la información y servicios alojados en esta infraestructura.

Describir la aplicación de los marcos metodológicos mediante su revisión y lineamiento base para disponer de un esquema de manejo de riesgos basados la metodología Octave utilizando el ciclo de mejora continua PHVA.

Diseñar un esquema de seguridad empleando el ciclo de mejora continua PHVA y la metodología Octave para la definición de un proceso de aseguramiento de la información que brinde integridad, disponibilidad y confidencialidad sobre los servicios alojados en una infraestructura en la nube.

Identificar el nivel de criticidad de los incidentes de seguridad a los que una infraestructura en la nube tipo IAAS se encuentran expuestos mediante la implementación del ciclo de mejora

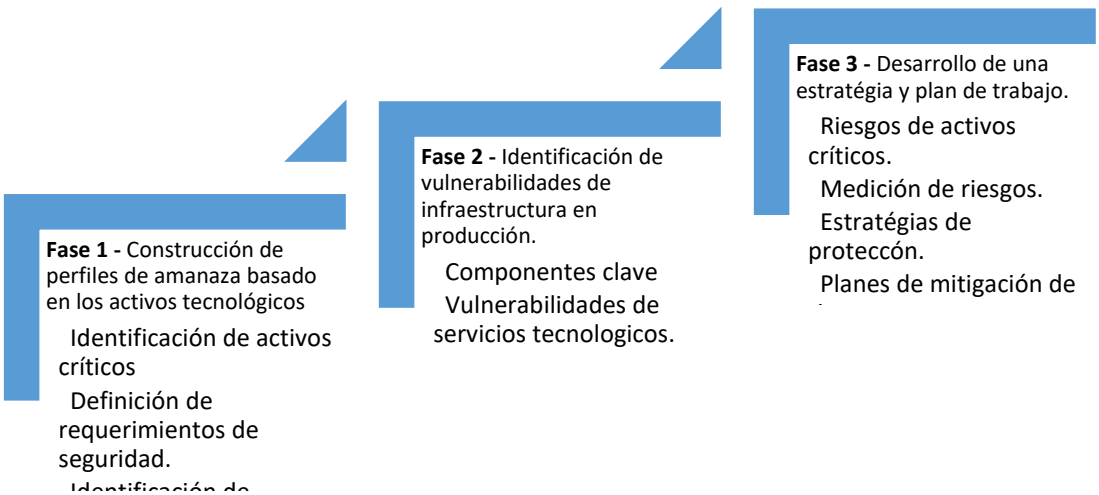
continua PHVA y la metodología Octave para disminuir, mitigar y manejar los riesgos a los que estos incidentes se encuentran asociados.

Vinculación con la sociedad y beneficiarios directos:

Durante el 2022 según lo indicado por la investigación realizada por la organización "Cloud Security Alliance" en (*Top Threats to Cloud Computing Pandemic Eleven | CSA*, s. f.) se evidenció un incremento en los incidentes de seguridad y una tendencia en cuanto se refiere a la adopción de normativas y esquemas de seguridad que permitan disponer de un procedimiento para el manejo y mitigación de riesgos. Este esquema de trabajo se encuentra definido mediante tres fases de operación siguiendo el metodología de Octave, como se muestra en la Figura 3:

Figura 2.

Fases y Procesos de la Metodología Octave



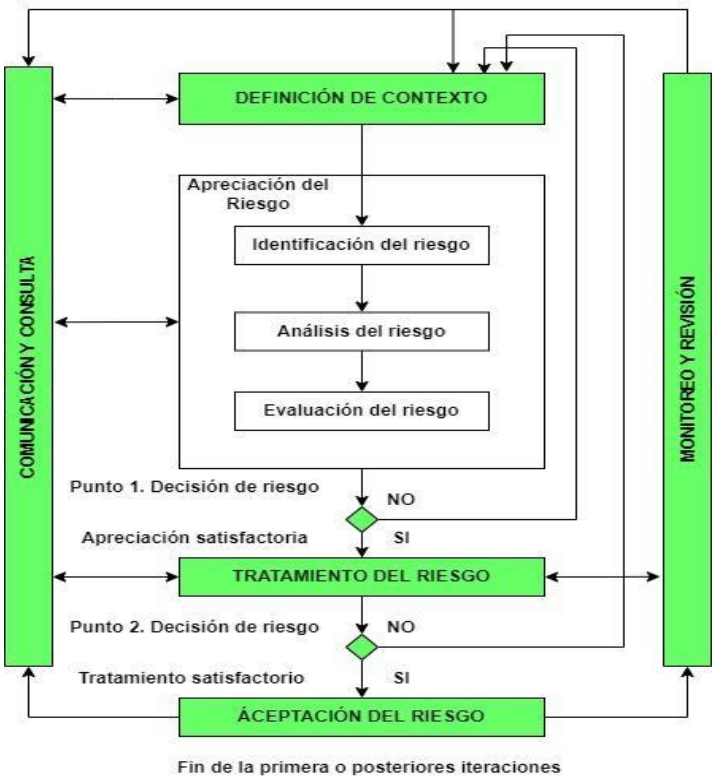
Nota. Fases de la metodología Octave. Adaptada de la metodología OCTAVE, Progressive Series of Workshops, 2007 (https://resources.sei.cmu.)

El desarrollo de un esquema de trabajo para el manejo de riesgos en un servicio IAAS, permitirá a diferentes tipos de empresas implementar dicho esquema y disponer de un proceso formal para el manejo de riesgos asociados con este tipo de servicios mediante un ciclo de mejora

continua, así como también disminuir el impacto a diferentes servicios corporativos que están alojados en esta infraestructura tecnológica. Este esquema de manejo de riesgos es una herramienta de estudio que permite a diferentes unidades tecnológicas de una compañía el poner en conocimiento a las alta gerencias respecto a las amenazas de seguridad a las cuales se enfrentan en la operación diaria, su impacto en servicios empresariales y el manejo correcto de estos riesgos de tal manera proveer de un proceso para el usuario final o un administrador para minimizarlos y mitigarlos.

Figura 3.

SGSI en ISO/IEC 27005:2011 y PHVA



Nota. Fases de la norma ISO 27005 empleando el ciclo PHVA. Adaptada de Norma ISO/IEC 27005:2011. 2011. (https://www.revistatonoetecsa.cu).

CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO

1.1. Contextualización general del estado del arte

En la actualidad se dispone de un sin número de diferentes tipos de normas, metodologías y estándares que permiten tener la gestión y un análisis de riesgos tecnológicos. Entre ellas tenemos las siguientes metodologías que se describen, a continuación:

Tabla 1.

Metodologías para la Gestión de Riesgos

Norma	Descripción	Año Publicación	País
Magerit v3	Metodología de análisis y gestión de riesgos	2012	España
Octave 2.0	Esquema de manejo de riesgos	2001	USA
CRAMM 5.0	Metodología de análisis de riesgos	1987	United Kingdom
COBIT 2019	Objetivos de control para tecnologías de la información	2019	
ISO 27005	Esquema de manejo de riesgos	2018	
ISO 31010	Esquema de manejo de riesgos	2019	
FAIR	Marco de Ciberseguridad	2005	USA
NIST	Marco de Ciberseguridad	2013	USA
ITIL 4	Conceptos y buenas prácticas.	2019	United Kingdom

Nota. Detalle de metodologías para la gestión de riesgos. Adaptada de la European Union Agency for cybersecurity, 2022 (https://www.sciencedirect.com/topics/computer-science/information-risk-management).

Para el desarrollo de esta investigación se analizaron tres metodologías enfocadas en el manejo y la gestión de riesgos de seguridad de la información considerando una infraestructura tipo IaaS que podrían implementarse y como resultado se establecerá una comparativa de las principales características relacionadas con una infraestructura en la nube.

Factor Analysis of Information Risk (FAIR)

Es una metodología que realiza un análisis factorial del riesgo a la que la información se encuentra expuesta, esta clasificación de factores contribuyen a la identificación de riesgos y su impacto entre sí. El principal objetivo es la definición de probabilidades precisas de la frecuencia y magnitud de los eventos en los cuales podría haber una afectación o pérdida de datos. Esta metodología es conocida como un marco de gestión de riesgos, fue desarrollado por Jack A. Jones y aporta a distintas empresas a entender, analizar y medir el riesgo de la información.

La metodología FAIR busca perfeccionar las metodologías tradicionales, tiene una licencia CC (Creative Commons) de la cual FAIR es su propietario y su uso para analizar el riesgo de una empresa o tercero con fines comerciales requiere una licencia RMI (Risk management Insight), apareció en el 2006 con su documento principal "An Introduction to Factor Analysis of Information Risk (FAIR)". Esta metodología contempla varios componentes que se encuentran en un escenario de riesgos, estos componentes tienen características (factores) que en combinación con otros impulsan el riesgo. El factor de riesgo inicialmente descompone el riesgo en sus partes fundamentales y como resultados se describe como los factores resultantes se combinan para impulsar el riesgo y establece una base para el resto del marco de trabajo FAIR.

- **Identificación de Activo Críticos**

El potencial de pérdida de un activo se deriva del valor que representa y/o de la responsabilidad que introduce en una organización. Por ejemplo, la información de los clientes proporciona valor por su papel en la generación de ingresos para una organización comercial. Esa misma información también puede suponer una responsabilidad para la organización si existe una obligación legal de protegerla o si los clientes esperan que la información sobre ellos esté debidamente protegida. FAIR define seis tipos de pérdidas:

- **Productividad.-** una reducción de la organización para producir efectivamente bienes o servicios con el fin de generar valor

- **Respuesta. -** los recursos gastados al actuar tras un evento adverso
- **Reemplazo.-** el gasto para sustituir/reparar un activo afectado
- **Multas y juicios (F/J).-** el coste del procedimiento legal global derivado del evento adverso
- **Ventaja competitiva (AC).-** oportunidades perdidas debido al incidente de seguridad
- **Reputación.-** pérdida de oportunidades o de ventas debido a la disminución de la imagen corporativa tras el suceso

FAIR categoriza el valor/responsabilidad de la siguiente manera:

- **Crítico.-** el efecto sobre la productividad de la organización
- **Coste.-** el coste desnudo del activo, el coste de reemplazar un activo comprometido
- **Sensibilidad.-** el coste asociado a la divulgación de la información, que se divide a su vez en:
    - **Vergüenza.-** la revelación declara el comportamiento inapropiado de la dirección de la empresa.
    - **Ventaja competitiva -** la pérdida de ventaja competitiva ligada a la revelación
    - **Legal/regulatorio -** el coste asociado a las posibles violaciones de la ley
    - **General -** otras pérdidas vinculadas a la sensibilidad de los datos

- **Identificación de Amenazas**

Los agentes de amenazas pueden agruparse por comunidades de amenazas, estos subconjuntos de la población global de agentes de amenazas comparten características clave. Las comunidades de amenazas deben definirse con precisión para poder evaluar eficazmente el efecto (magnitud de la pérdida). Estos agentes de amenaza pueden actuar de forma diferente sobre un activo:

- **Acceso -** leer los datos sin la debida autorización
- **Uso indebido.-** utilizar el activo sin autorización y o de forma diferente al uso previsto
- **Revelar.-** el agente permite que otras personas accedan a los datos
- **Modificar.-** cambiar el activo (modificación de los datos o de la configuración)
- **Denegar el acceso.-** el agente de la amenaza no permite que los usuarios legítimos previstos accedan al activo

Estas acciones pueden afectar a diferentes activos de distintas maneras: el efecto varía en relación con las características del activo y su uso. Algunos activos tienen una alta criticidad pero una baja sensibilidad, la denegación de acceso tiene un efecto mucho mayor que la divulgación en tales activos. Por otro lado un activo con datos altamente sensibles puede tener un efecto de baja productividad si no está disponible, pero un efecto embarazoso y legal si esos datos se divulgan, como por ejemplo, la disponibilidad de datos de salud de antiguos pacientes no afecta a la productividad de una organización sanitaria, pero su divulgación puede costar millones de dólares a la organización. Un mismo suceso puede afectar a diferentes activos, el robo de un computador portátil afecta a la disponibilidad del propio portátil, pero puede llevar a la potencial divulgación de la información almacenada en él. La combinación de las características de un activo y el tipo de acción contra ese activo que determina la naturaleza fundamental y el grado de pérdida. En la Tabla 2 se detallan las principales características de las metodologías analizadas:

Tabla 2.

Análisis Comparativo de Metodologías para Manejo de Riesgos

Metodología	Priorización	Costo/Beneficio	Cumplimiento	Flexibilidad	Analítica	Cuantitativa
FAIR	II	II		II	II	II

NIST		II
ISO		II
Octave	I	II

Nota. I – Cumple parcialmente el objetivo y II Cumple el objetivo. Adaptado de FAIR Institute, 2022. https://www.fairinstitute.org/what-is-fair

National Institute os Standards and Technology (NIST)

Anteriormente conocida como Oficina Nacional de Normas NBS (Nacional Bureau of Standards) es una administración tecnológica del departamento de comercio de Estados Unidos, su misión es promover la innovación y la competencia industrial mediante el desarrollo en avances en metrología, normas y tecnología para mejorar la estabilidad económica. Como parte de esta misión los especialistas continuamente refinan la ciencia (metrología), para obtener una ingeniería precisa y una manufacturación necesaria para el desarrollo de avances tecnológicos actuales. También están involucrados en el desarrollo de pruebas de cumplimiento orientados en el sector privado y gubernamental (White & Sjelin, 2022).

El marco de seguridad NIST permite disponer de una mejora en la seguridad cibernética de infraestructuras críticas, su orientación es facilitar a empresas de diferente tamaño a entender, gestionar y disminuir los riesgos, resguardar la red corporativa y la información almacenada. Como resultado se obtiene un lenguaje común considerando recomendaciones de mejores prácticas relacionadas con la seguridad de la información. El marco se adapta a empresas que tienen una dependencia tecnológica, ya sea que tengan un enfoque de seguridad de la información, sistemas de control físico, sistemas de control industrial o dispositivos electrónicos que dispongan de conectividad en una red (IoT). Este marco de trabajo tiene tres componentes:

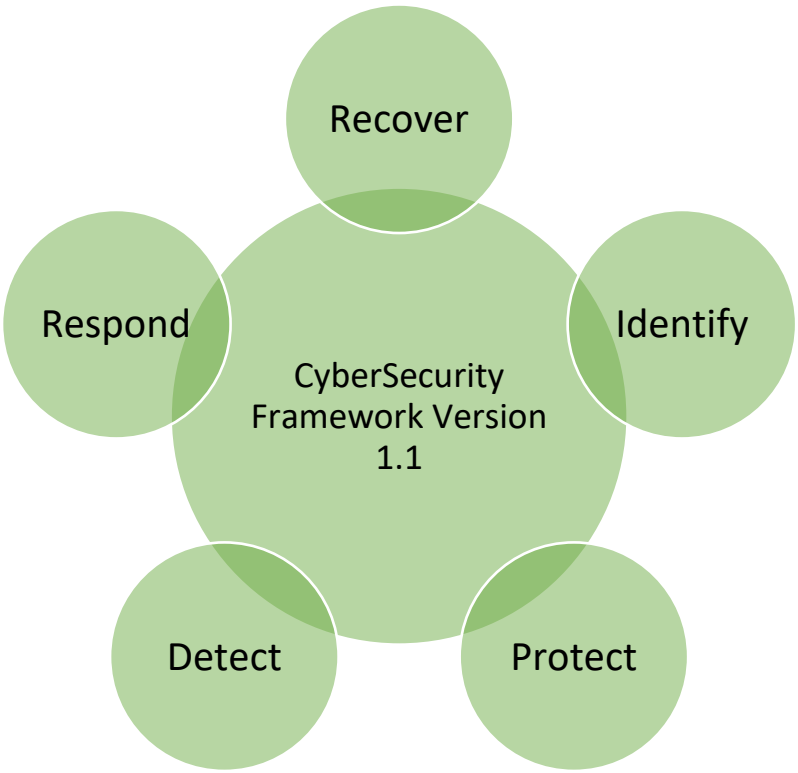
- Núcleo del marco
- Niveles de implementación
- Perfiles del marco

El Núcleo del Marco es una lista de actividades y funciones relacionados con la seguridad de la información, los resultados esperados, referencias informativas e infraestructura crítica. Este núcleo consta de cinco funcionalidades continuas y simultaneas

A continuación, la Figura 4 evidencia los procesos de este marco de trabajo:

Figura 4.

Funcionalidades del Marco NIST



Nota. Funciones que abarca la metodología NIST. Adaptada de NIST. 2022. (https://www.igi-global.com/chapter/the-nist-cybersecurity-framework/288672).

Estas funcionalidades brindan una visión estratégica de alto nivel respecto al ciclo de ejecución en el proceso de gestión de riesgos asociados con la seguridad de la información según lo indicado en el artículo (Villamizar, 2020) “Cada función está conformada por categorías, subcategorías y estas a su vez de normas y referencias a otros marcos de trabajo o estándares para utilizar sus conceptos en la definición de controles de seguridad informática”.

Tabla 4.

Categorías de las Funcionalidades NIST

Identificador único de función	Función	Identificador único de categoría	Categoría
ID	Identificar	ID. AM	Gestión de activos críticos
		ID. BE	Entorno Organizacional
		ID. GV	Gobierno
		ID. RA	Evaluación de riesgos
		ID. RM	Estrategia de gestión de riesgos
		ID. SC	Gestión del riesgo de la cadena de suministro
PR	Proteger	PR. AC	Gestión de identidad y control de acceso
		PR. AT	Conciencia y capacitación
		PR. DS	Seguridad de datos
		PR. IP	Procesos y procedimientos de protección de la información
		PR. MA	Mantenimiento
		PR. PT	Tecnología productora
DE	Detectar	DE. AE	Anomalías y eventos
		DE. CM	Vigilancia continua de seguridad
		DE. DP	Procesos de detección
RS	Responder	RS. RP	Comunicaciones
		RS. CO	Análisis
		RS. AN	Análisis
		RS. MI	Mitigación
		RS. IM	Mejoras
RC	Recuperar	RC. RP	Planificación de recuperación
		RC. IM	Mejoras

	RC.CO	Comunicaciones

Nota. Descripción de las categorías y funcionalidades de NIST. Adaptada de NIST. 2022. (https://www.igi-global.com/chapter/the-nist-cybersecurity-framework/288672).

En cuanto a las capas de implementación de NIST brindan un mecanismo de verificación y comprensión de las características de su enfoque para la gestión de riesgos, además de priorizar para alcanzar los objetivos propuestos para la seguridad de la información. Este marco considera cuatro niveles los mismos que se detallan en la Tabla 4, a continuación:

Tabla 5.

Niveles de Implementación para la Gestión de Riesgos

Parcial	Informado	Repetible	Adaptativo
No formalizado Reactivo	Procesos aprobados con aplicación parcial en la organización. Actividades de ciberseguridad basadas en objetivos de riesgo.	Procesos aprobados con aplicación total en la organización. Actividades de ciberseguridad actualizadas según las modificaciones en el perfil de riesgo	Mejora continua que incluye lecciones aprendidas e indicadores predictivos. La organización se adapta a un panorama cambiante de amenazas y tecnologías eficazmente.

Nota. Niveles de Implementación NIST. Adaptada de NIST. 2022. (https://www.igi-global.com/chapter/the-nist-cybersecurity-framework/288672).

Tabla 6.

Integración de la Gestión de Riesgos

Parcial	Informado	Repetible	Adaptativo
Conocimiento limitado sobre riesgos. Uso de la gestión del riesgo de forma irregular.	Conocimiento del riesgo de seguridad a en la organización. Se aplica la evaluación del riesgo pero NO es frecuente.	Definición e implementación de procedimientos y políticas. Se tiene un enfoque robusto para gestionar y monitorear el riesgo. Se dispone de personal calificado. El comité gerencial o la alta dirección socializa el	La gestión de riesgos es parte de la cultura organizacional. El riesgo es monitoreado como cualquier otro tipo de riesgo. Se tiene alineados los objetivos y riesgos de seguridad en la organización.

	estado de la seguridad de la información.	El presupuesto de la organización se basa en la comprensión del entorno de riesgo actual, el riesgo previsto y la tolerancia organizacional a dichos riesgos.

Nota. Niveles de Implementación NIST. Adaptada de NIST. 2022. (https://www.igi-global.com/chapter/the-nist-cybersecurity-framework/288672).

Tabla 7.

Participación Externa

Parcial	Informado	Repetible	Adaptativo
No hay colaboración con otras entidades. Se desconocen los riesgos,	La empresa colabora y recibe información de otras entidades, pero no comparte Es consciente de los riesgos, pero no actúa de forma consistente sobre estos.	La empresa recibe y comparte información con otras entidades. Es consciente de los riesgos y actúa de forma consistente sobre estos.	Utiliza información en tiempo real para comprender y actuar de forma coherente sobre los riesgos. Socializa de manera proactiva, mediante mecanismos formales e informales para mantener y desarrollar relaciones sólidas de la seguridad.

Nota. Niveles de Implementación NIST. Adaptada de NIST. 2022. (https://www.igi-global.com/chapter/the-nist-cybersecurity-framework/288672).

Como último componente se dispone del “Perfil”, el mismo que evidencia los resultados basados en las necesidades corporativas partiendo de las categorías y subcategorías del marco de trabajo. Este perfil define como la alineación base de prácticas, estándares y directrices con el núcleo del marco durante su implementación. Es una “fotografía” en tiempo real que evidencia el estado actual de la ciberseguridad en una empresa y permite diferenciar entre el estado actual y el estado deseado generando como resultado un plan de trabajo priorizado previo a la implementación. A continuación, se detallan los procesos a seguir para la implementación del marco de trabajo NIST:

- **Priorización y alcance:** Identificación de objetivos / misión corporativa y prioridades organizacionales a alto nivel.
- **Orientación:** Se identifican los sistemas, el enfoque de riesgo general, requisitos reglamentarios y los activos relevantes de mayor criticidad.
- **Perfil Actual:** Se define un perfil actual que evidencia que resultados de categorías y subcategorías del núcleo del marco se tienen en producción.
- **Evaluación de riesgos:** Se genera una evaluación orientada al proceso de gestión de riesgos o actividades previas a la evaluación. Se valida el entorno en producción para identificar la probabilidad de afectación de un evento de seguridad y el impacto en la empresa.
- **Perfil deseado:** Se crea un perfil objetivo basado en los resultados de la evaluación de las categorías y subcategorías. También se consideran las influencias y requisitos de todos los interesados.
- **Determinar, analizar y priorizar brechas:** Se compara el perfil actual (en producción) y el perfil deseado (objetivo) para identificar las inconsistencias y se crea un plan de trabajo priorizado para lograr el perfil deseado. Determinar los recursos de la evaluación para aportar en la toma de decisiones asociadas con la seguridad de estos activos, respaldar la gestión de riesgos y contar un proceso de mejora continua.
- **Implementar plan de acción:** Se determinan las acciones a tomar para remediar las brechas de seguridad, se optimizan los procesos de seguridad para alcanzar al perfil deseado. Para respaldar el plan de acción se identifica referencias adicionales sobre las categorías y subcategorías.

Estas normas pueden ser aplicadas en cualquier organización como guías de referencia o buenas prácticas bajo un esquema de trabajo estandarizado y normalizado, que como objetivo principal permitirá alcanzar los resultados esperados en cada aplicación. Sin embargo, ninguna de estas guías está orientada al manejo de riesgos de una infraestructura en la nube de tipo

IAAS, el uso e implementación de este tipo de esquemas cada vez se convierte en una tendencia global como una solución inteligente frente a las diferentes necesidades de almacenamiento y procesamiento a bajo costo, tan necesarios por las organizaciones para brindar sus servicios y almacenar su activo más preciado la información.

Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE)

Es una técnica para la valoración de riesgos desarrollada por Centro de Coordinación CERT en Carnegie Mellon University, como un grupo de herramientas, técnicas y métodos para la evaluación del riesgo que se enfoca en la seguridad de la información estratégica y su planificación, la misma que toma en cuenta la definición e identificación de los activos incluyendo: personas, componentes tecnológicos e información. En la siguiente tabla se detalla las publicaciones de la metodología en la línea de tiempo:

Tabla 8.

Línea de Tiempo OCTAVE

Fecha	Título de Publicación
Septiembre 1999	OCTAVE Marco de trabajo. Versión 1.0
Septiembre 2001	OCTAVE Marco de trabajo. Versión 2.0
Diciembre 2001	OCTAVE Criterios. Versión 2.0
Septiembre 2003	OCTAVE-S v0.9
Marzo 2005	OCTAVE-S v1.0
Junio 2007	Introducción de OCTAVE Allegro v1.0

Nota. Detalle de publicaciones del marco de trabajo OCTAVE. Adaptada de "Presentación de OCTAVE Allegro: Mejorando el Proceso de Evaluación de Riesgos de Seguridad de la Información de seguridad de la información". 2007 (https://resources.sei.cmu.edu).

Se enfoca en el riesgo organizacional y primordialmente en los aspectos asociados con la operación diaria y su objetivo principal abarca temas relacionados con la estrategia y la práctica; de igual manera proporciona una lineamiento base que es utilizado para enfocar la mitigación y

mejorar procedimientos ya definidos. Además equilibra los riesgos de la operación, las prácticas de seguridad y la tecnología en producción, lo que permite apoyar en la toma decisiones para la protección de la información y servicios corporativos considerando la confidencialidad, integridad y disponibilidad imprescindible en un cual empresa de servicios.

OCTAVE considera que el equipo de trabajo (personal) cumple un rol relevante en la misión organizacional e implementación del esquema propuesto por esto el equipo y quienes lo conforman son los participantes directos, pertenecientes a diferentes áreas y niveles jerárquicos los mismos que estan alineados en la identificación de activos relacionados con la información, destacar los de mayor relevancia y disponer de una estrategia para protegerlos. Como resultado se dispone de un equipo multinivel, conformado por los responsables del proyecto y el personal operativo durante el proceso de implementación.

Esta característica evidencia que los responsables del proyecto son los idóneos para identificar los servicios y que información es más crítica e importante en cada proceso además de conocer cómo se usa dicha información. El personal operativo que gestiona la infraestructura tecnológica, es quien está familiarizado con la configuración de los servicios tecnológicos y las vulnerabilidades de estos. Por otro lado los responsables de área conocen las capacidades y funciones de cada área a la que lideran, estas dos perspectivas proporcionan una vista panorámica de los riesgos de seguridad enfocados en los activos tecnológicos alojados en una infraestructura de tipo IAAS.

Las fases y procesos de esta metodología se adaptan a las necesidades específicas de una organización. Las tres metodologías de OCTAVE generadas por la entidad “Software Engineering Institute” (SEI) de la Universidad de Carnegie Mellon, se listan a continuación:

- OCTAVE. - Orientada para organizaciones a gran escala.
- OCTAVE-S.- Orientada para organizaciones en crecimiento.
- OCTAVE Allegro. – Enfocada en el manejo de riesgos considerando activos.

El siguiente listado detalla el esquema de códigos utilizados para estos elementos en las tablas a continuación:

- A - indica una entrada
- O - indica una salida
- F – indica la fase
- P – indica el proceso
- FX.AY - indica la actividad Y en la fase X
- R - indica un número de secuencia para una entrada o una salida (actividades)

Tabla 9.

Distribución de la metodología Octave

OCTAVE	OCTAVE-S	OCTAVE ALLEGRO
Fase1 – Proceso 1 - F1P1	Fase1 – Proceso 1 - F1P1	Fase1: Establecer dirección: Criterios de valoración de riesgos
Fase1 – Proceso 2 - F1P2		Fase1: Perfilar activos: Desarrollar perfiles de activos críticos.
Fase1 – Proceso 3 - F1P3		Fase1: Perfilar activos: Identificar recursos de información.
Fase1 – Proceso 4 - F1P4	Fase1 – Proceso 4 - F1P4	Fase2: Identificar amenazas: Áreas de interés para el análisis.
Fase2 – Proceso 5 - F1P5	Fase2 – Proceso 5 - F1P5	Fase2: Identificar amenazas: Escenarios de amenazas
Fase2 – Proceso 6 - F1P6		Fase3: Identificar y mitigar riesgos: Identificar riesgos
Fase3 – Proceso 7 - F1P7	Fase3 – Proceso 7 - F1P7	Fase3: Identificar y mitigar riesgos: Analizar riesgos
Fase3 – Proceso 8 - F1P8	Fase3 – Proceso 8 - F1P8	Fase3: Identificar y mitigar riesgos: Seleccionar enfoque de mitigación

Nota. Detalle de fases de aplicación de marco metodológico de OCTAVE. Adaptada del framework de trabajo de la metodología Octave. 2001 (https://resources.sei.cmu.edu). Y de la investigación "Modelo de Gestión de Riesgos IaaS". 2015 (*ESCUELA POLITÉCNICA NACIONAL*, s. f.)

La metodología OCTAVE, al conformarse como un conjunto de criterios mediante los cuales se desarrollan varias metodologías, se adapta perfectamente como parte del esquema de manejo de riesgos de una infraestructura como Servicios IaaS, mediante la integración con normas o mejores prácticas disponibles en el mercado.

Los criterios que conforman la metodología OCTAVE tienen un enfoque de evaluación de riesgos y dispone de los siguientes componentes para su representación; actividades, procesos, principios, atributos, entradas y las salidas.

Tabla 10.

Actividades de OCTAVE

Fase 1 (F1)	Fase 2 (F2)	Fase 3 (F3)
F1.A1 Identificar los activos	F2.A1 Seleccionar los componentes de la infraestructura para evaluar	F3.A1 Identificar los riesgos para los activos críticos
F1.A2 Identificar las prácticas actuales de seguridad	F2.A2 Ejecutar la evaluación de la vulnerabilidad (uso de herramientas)	F3.A2 Crear criterios de evaluación de riesgos
F1.A3 Identificar las Vulnerabilidades Organizacionales	F2.A3 Revisar las vulnerabilidades y resumir los resultados	F3.A3 Evaluar riesgos en activos críticos
F1.P4 Identificar los activos críticos		F3.A4 Definir una estrategia de protección
F1.A5 Describir los requisitos de seguridad de seguridad para los activos críticos		F3.A5 Crear planes de mitigación de riesgos
F1.A6 Crear perfiles de amenazas para Activos Críticos		F3.A6 Validar la estrategia de control y el plan de trabajo para la mitigación de riesgos
		F3.A7 Identificar los pasos a seguir

Nota. Actividades para la aplicación de la metodología OCTAVE. Elaboración propia.

Tabla 11.

Atributos y Principios de la Metodología Octave

Principio	Atributo
La metodología debe ser autodirigida	RA.1 Equipo de Análisis RA.2 Capacidades del equipo de análisis
Las medidas acorde a la necesidad	RA.3 Catálogo de prácticas RA.4 Perfil genérico de amenazas RA.5 Catálogo de vulnerabilidades
El proceso debe ser definido	RA.6 Actividades de evaluación definidas RA.7 Documentación de los resultados de evaluación RA.8 Alcance de la evaluación
El proceso debe ser continuo	RA.9 Próximos pasos RA.3 Catálogo de prácticas
El proceso seguido con visión de futuro	RA.10 Enfoque de riesgos
El proceso debe centrarse en un reducido número de riesgos críticos.	RA.8 Alcance de la evaluación RA.11 Actividades enfocadas
Gestión integrada	RA.12 Aspectos organizativos y tecnológicos RA.13 Participación de negocio y de áreas tecnológicas RA.14 Participación de la alta dirección
Comunicación abierta	RA.15 Enfoque colaborativo
Perspectiva global	RA.12 Aspectos organizativos y tecnológicos RA.13 Participación de negocio y de áreas tecnológicas
Equipo de trabajo	RA.1 Equipo de Análisis RA.2 Capacidades del equipo de análisis RA.13 Participación de negocio y de áreas tecnológicas RA.15 Enfoque colaborativo

Nota. Detalle de principios y atributos de la normativa Octave. Adaptada del framework de trabajo de la metodología Octave. 2001 (https://resources.sei.cmu.edu).

Estos principios son la base fundamental que brindan el tipo de la evaluación a realizar y definen la filosofía detrás del proceso y el enfoque de la evaluación, adicionalmente definen como base para el mismo. Esta metodología es autodirigida como parte de uno de los principios de OCTAVE, esta definición significa que los responsables por parte de la organización son los más importantes al dirigir la evaluación y participar en la toma de decisiones. Los requisitos para esta evaluación están incluidos en los atributos, entradas y salidas. Estos atributos hacen referencia a las cualidades distintivas o características de la evaluación, además corresponden a

los requisitos que definen el esquema del enfoque OCTAVE y brindan las directrices respecto a lo que se debe hacer para tener como resultado una evaluación satisfactoria desde la perspectiva del cumplimiento de requerimientos como de resultados del análisis. Como se puede evidenciar en la Tabla 8, los atributos son el resultado de los principios de la metodología OCTAVE. Uno de estos atributos es que un equipo interdisciplinario (equipo de análisis) conformado por personal responsable del proyecto este a la cabeza de la evaluación y el principio detrás de la creación de un equipo de análisis es que la metodología debe ser autodirigida. Las salidas son los resultados esperados en cada fase de evaluación aplicada, se definen también como los resultados que un equipo de análisis debe cumplir como objetivo durante cada fase. Existen varias actividades que producen las salidas de la metodología OCTAVE, por tal razón no se especifica un conjunto específico de actividades. En la Tabla 9 se evidencian los resultados de acuerdo con las tres fases de la metodología:

Tabla 12.

Faces y Salidas Octave

Fases (F)	Procesos (P)	Salidas (O)
F1. Visión Organizativa Identificar el conocimiento empresarial	P1. Identificar el conocimiento de la empresa P2. Identificar el conocimiento del área operativa P3. Identificar los conocimientos del personal. P4. Establecer requerimientos de seguridad	RO1.1 Lista priorizada de activos / servicios RO1.2 Requerimientos de seguridad para activos críticos. RO1.3 Amenazas para activos críticos. RO1.4 Prácticas de seguridad en producción RO1.5 Vulnerabilidades organizacionales de los servicios en producción.
F2. Visión Tecnológica Identificar el área operativa con el conocimiento	P5. Asignar los activos de alta prioridad en la infraestructura. P6. Realizar una evaluación de la vulnerabilidad de la infraestructura	RO2.1 Componentes clave RO2.2 Evaluación de Vulnerabilidades
F3. Estrategia y desarrollo del plan Identificar los conocimientos del personal	P7. Realizar un análisis de riesgos multidimensional. P8. Desarrollar una estrategia de protección.	RO3.1 Definición de riesgos para activos críticos RO3.2 Medidas y categorización de riesgo. RO3.3 Estrategias de Protección

	RO3.4 Planes de mitigación de riesgos

Nota. Detalle de faces, procesos y actividades de la metodología Octave. Adaptada del framework de trabajo de la metodología Octave. 2001 (https://resources.sei.cmu.edu).

De acuerdo con la Tabla 9, el proceso de evaluación contemplado por OCTAVE se divide en tres fases (F) y ocho procesos (P) y dieciséis actividades (A), que se describen a continuación:

Fase 1: Visión organizativa - Construcción de perfiles de amenaza (basados en activos)

El equipo de análisis determina lo que es importante para la organización (los activos relacionados con la información) y lo que se está haciendo actualmente para proteger esos activos. Posteriormente, el equipo selecciona aquellos activos que son más importantes para la organización (activos críticos) y sus requisitos de seguridad para cada uno. Así también se identifican las amenazas por cada activo identificado, dando como resultado un perfil amenaza para ese activo. Desde un punto de vista general esta fase es una evaluación organizativa.

- **Proceso 1 - Identificar conocimiento de la alta dirección:** Se identifican los activos importantes, amenazas percibidas, los requisitos de seguridad, las prácticas actuales de seguridad y vulnerabilidades de la organización desde la perspectiva de los altos directivos.
- **Proceso 2 – Identificar conocimiento de la dirección de áreas operativas:** Se identifican los activos importantes, amenazas percibidas, los requisitos de seguridad, las prácticas actuales de seguridad y vulnerabilidades de la organización desde la perspectiva de los administradores de las áreas operacionales.
- **Proceso 3 – Identificar conocimiento del personal de áreas operativas y de TI:** Se identifican los activos importantes, amenazas percibidas, los requisitos de seguridad, las prácticas actuales de seguridad y vulnerabilidades de la organización desde la perspectiva del personal de áreas operativas y de TI

- **Proceso 4 – Crear perfiles de amenazas:** El equipo de análisis evalúa la información de los procesos de 1 a 3, selecciona los activos críticos, refina los requisitos de seguridad asociados y se identifican las amenazas a esos activos para la creación de perfiles de amenaza.

Fase 2: Visión tecnológica - Identificación de la infraestructura de vulnerabilidades.

Esta es una evaluación de la infraestructura de información. El equipo de análisis examina e identifica vulnerabilidades y sus componentes tecnológicos relacionada con cada activo crítico, para posteriormente determinar la medida en que cada clase de componente es resistente a los ataques. Las vulnerabilidades de tecnología son las debilidades en los sistemas, dispositivos y componentes que pueden conducir directamente a la acción no autorizada

- **Proceso 5 – Identificar componentes clave:** El equipo de análisis identifica los sistemas de información y componentes tecnológicos claves para cada activo crítico. Los casos específicos se seleccionan para su evaluación.
- **Proceso 6 – Evaluar componentes seleccionados:** El equipo de análisis examina los principales sistemas y componentes tecnológicos vulnerables, para lo cual se utilizan herramientas de vulnerabilidad (software, listas de verificación, scripts). Los resultados se analizan y se resumen, de acuerdo con la importancia de los activos críticos y sus perfiles de amenaza.

Fase 3: Estrategia y desarrollo del plan de trabajo.

El equipo de trabajo analiza e identifica los riesgos de los activos críticos en la organización y toma decisiones respecto a qué hacer con ellos. Se genera una estrategia de control para la organización y procesos de mitigación frente a los riesgos de los activos críticos en base a un análisis del levantamiento de información inicial.

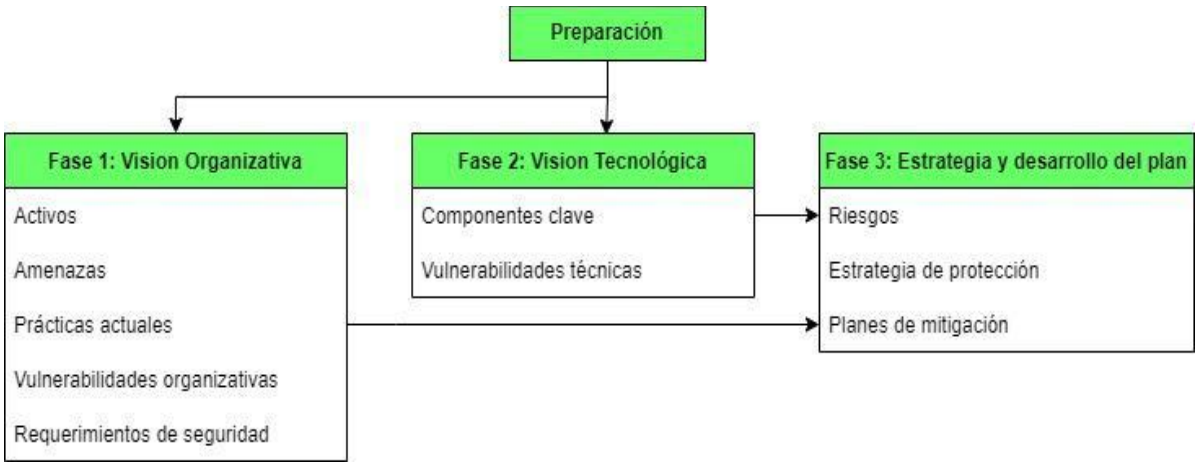
- **Proceso 7 – Análisis de riesgos:** El equipo de trabajo analiza e identifica el impacto de las amenazas sobre los activos críticos, define criterios de evaluación y evalúa el impacto

en base a estos criterios. Como resultado se obtiene un perfil de riesgo específico por cada activo crítico.

- **Proceso 8 – Diseño de estrategia de protección:** El equipo de trabajo analiza y define una estrategia de protección, además de un plan de mitigación en base al análisis del levantamiento de la información inicial. Los altos directivos revisan, modifican y aprueban la estrategia y los planes generados de este proceso.

Figura 5.

Resumen de las fases y procesos de la metodología Octave.



Nota. Detalle de las fases y procesos para la implementación de la metodología Octave. Adaptada del framework de trabajo de la metodología Octave. 2001 (https://resources.sei.cmu.edu).

Los responsables de tecnología deben definir los elementos importantes en sus servicios, los requisitos de seguridad, las amenazas, vulnerabilidades y riesgos de adoptar la computación en la nube, ya sea a través experiencias o casos de estudios publicados por líderes del mercado que impulsan la adopción de este tipos de tecnología. A esto se suma, el fácil acoplamiento a otras normas y estándares para crear nuevas metodologías de gestión de riesgos; equipo de análisis interdisciplinario de tres a cinco personas de la propia organización; se basa en los criterios del estándar con un enfoque en la práctica y evaluación de la seguridad basada en la información

del riesgo; apoyado en un catálogo de buenas prácticas, encuestas, hojas de cálculos para obtener y captar información; se centra en una técnica de análisis basada en la planificación de escenarios; incorpora el criterio de probabilidad en el análisis de riesgos; y lo más importante proporciona guías de implementación.

Ciclo de Mejora Continua PHVA (Plan, Do, Check, Act)

La normativa ISO 27005:2018 proporciona una guía para la gestión del riesgo de seguridad de la información en una organización, en apoyo a los requerimientos del sistema de gestión de seguridad definido en la norma ISO IEC 27001. Según lo indicado en la investigación "La metodología ISO 27005 utiliza un esquema PHVA" (Castro & Bayona, 2011), el mismo que se describe en el siguiente apartado:

PLANIFICAR: Se definen los objetivos y procedimientos en el proceso de gestión de riesgos tecnológicos. El objetivo de estas actividades corresponde a la planificación de la entrega de resultados acorde con los objetivos y las políticas de la organización. También se define el plan de comunicaciones, el análisis del contexto organizacional en producción y la definición del alcance en la gestión de riesgos.

HACER: Contempla la implementación y puesta en producción de controles, procedimientos y procesos (políticas definidas), también lo correspondiente al tratamiento y valoración de riesgos.

VERIFICAR: Medir y evaluar el desempeño de los procesos respecto a la política y los objetivos de seguridad propuestos. Así como socializar los resultados de la evaluación al personal asociado con la evaluación.

ACTUAR: Definir un esquema para el manejo de riesgos e implementar los cambios necesarios para la mejora continua de los procesos organizacionales. Como parte de las últimas

dos fases (verificar y actuar), se incluye el monitoreo y mejora continua, donde se validan los cambios y el cumplimiento de los indicadores establecidos desde la fase de planificación.

Tabla 13.

Modelo de Mejora Continua PHVA

<table>
<tr><th>PHVA</th><th colspan="3">ISO 27005</th></tr>
<tr><td rowspan="11">Planear</td><td colspan="3">Definir plan de gestión de riesgos</td></tr>
<tr><td colspan="3">Establecimiento del contenido</td></tr>
<tr><td colspan="2">Identificación del riesgo</td><td rowspan="3">Valoración del riesgo</td></tr>
<tr><td>Estimación del riesgo</td></tr>
<tr><td colspan="2">Evaluación del riesgo</td></tr>
<tr><td colspan="3">Desarrollar el plan de tratamiento del riesgo</td></tr>
<tr><td colspan="2">Aceptación del riesgo</td><td rowspan="5">Proceso de gestión del riesgo</td></tr>
<tr><td rowspan="2">Hacer</td><td colspan="2">Implementar el plan de tratamiento</td></tr>
<tr><td colspan="2">Implementar plan de comunicación del riesgo</td></tr>
<tr><td>Verificar</td><td colspan="2">Monitoreo y revisión del riesgo</td></tr>
<tr><td>Actuar</td><td colspan="2">Mantener y mejorar el proceso de gestión</td></tr>
</table>

Nota. Detalle del esquema de trabajo de la normativa ISO27005. Adaptada de Norma ISO/IEC 27005:2011. 2011. (https://www.revistatonoetecsa.cu).

Como resultado se obtiene la Tabla 11 que evidencia las principales características de las metodologías analizadas y en la cual sobresale la metodología OCTAVE con el mejor nivel de cumplimiento:

Tabla 14.

Análisis de Metodologías para gestión de riesgos

Características	FAIR	OCTAVE	NIST
Requiere de licencia	X		

Se aplica a un servicio IAAS	X	X	X
Se aplica a diferentes tamaños de empresa	X	X	X
Identifica los activos o servicios		X	
Identifica amenazas		X	
Identifica vulnerabilidades	X		X
Valora los activos o servicios		X	
Se adaptan a un ciclo de mejora continua	X	X	X
Determina el impacto	X	X	X
Determina el riesgo	X	X	X
Selección y recomendación de remediación		X	
Procesos por implementar	4	8	4
Determina la probabilidad	X	X	X
Establece un equipo de trabajo multidisciplinario		X	X

Nota. Análisis comparativo de metodologías de gestión de riesgo. Elaboración Propia.

1.2. Proceso investigativo metodológico

Enfoque de Investigación

La presente investigación sigue una metodología cualitativa con un enfoque bibliográfico, la cual empleará la técnica de la entrevista para el proceso de levantamiento de información.

Población y Muestra

Se utilizará un muestreo no probabilístico ya que se conformará grupos de trabajo con miembros de distintos niveles jerárquicos de acuerdo con el criterio del investigador. Estos equipos de trabajo estarán liderados por un responsable del área de tecnología y principalmente permitirán realizar el levantamiento de información de las prácticas de seguridad, identificación riesgos y servicios en producción por lo que es de gran importancia que los responsables de cada servicio sean incluidos como actores principales de esta actividad.

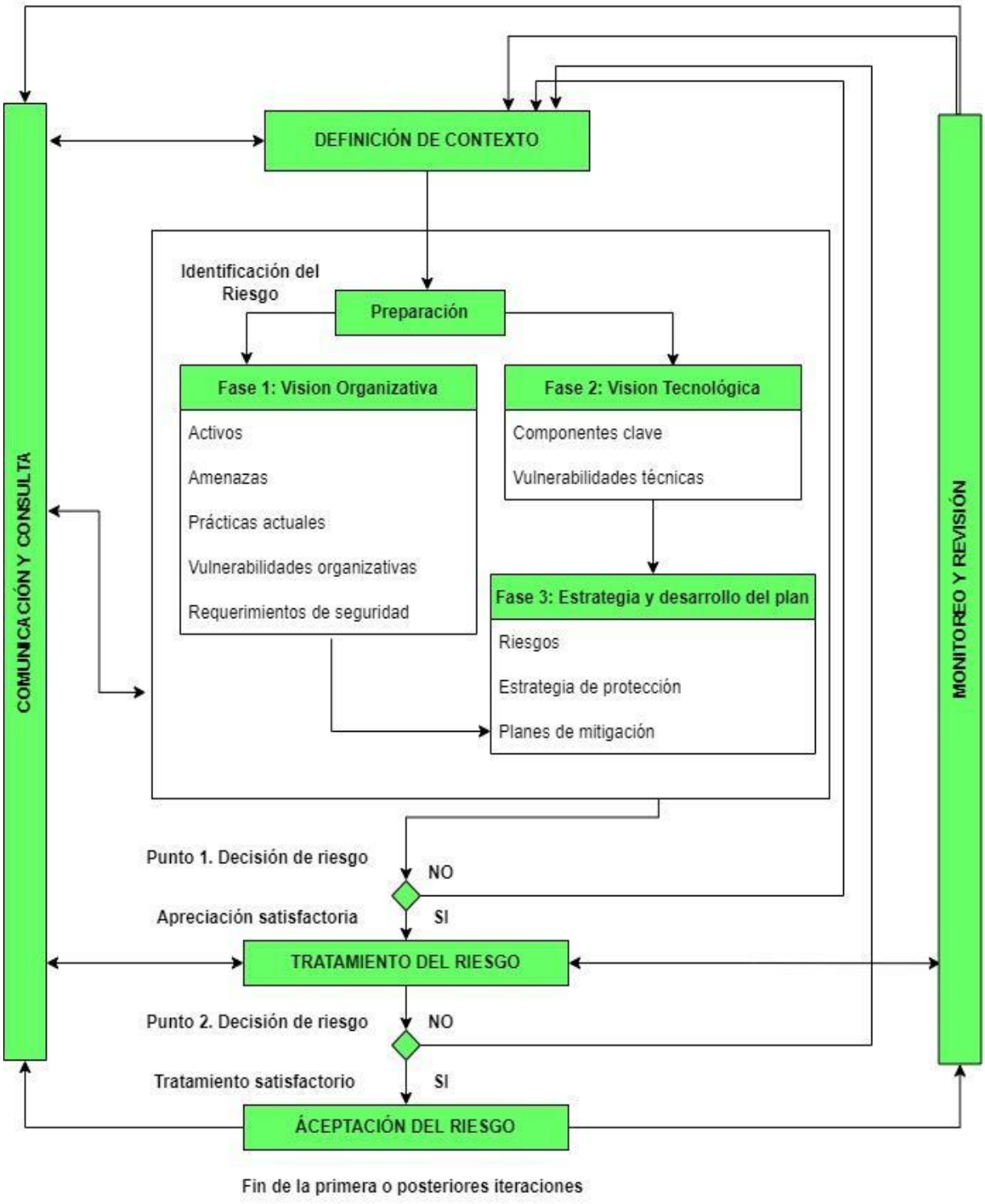
1.3. Análisis de resultados

Como parte de la adopción del esquema de manejo de riesgos mediante la metodología OCTAVE, se elabora de un perfil basado en los activos o servicios alojados en la infraestructura IaaS. Esto permitirá alinear los conocimientos organizacionales respecto a lo que se dispone en operación y está relacionado con los servicios internos y externos, así como también priorizar mediante un levantamiento de información los activos críticos en el cual se enfocara la evaluación. Así también se identifica las estrategias de seguridad que dispone la organización y como aplican en la operación diaria para evidenciar las vulnerabilidades, riesgos asociados, el impacto adverso que podría sufrir un servicio o activo específico. Como fase final de la metodología se dispone de un esquema de control y un plan de trabajo para la mitigación de riesgos asociados con los servicios y activos alojados en la infraestructura IaaS. Estas actividades de gestión de riesgos se encuentran encapsuladas en un ciclo de mejora continua que permite interacciones infinitas mediante cuatro procesos macro que aseguran la calidad del servicio, empezando por la planificación que brinda un enfoque de los resultados y el tiempo necesario para llegar a estos, la ejecución de actividades relacionadas al proceso de identificación, categorización de activos, vulnerabilidades, amenazas y definición estrategias de remediación, la verificación de efectividad en la implementación de controles, mitigación de riesgos y la revisión continua de mejoras en cada uno de los procesos para asegurar la disponibilidad, confidencialidad y la integridad de la información, servicios y activos alojados en la infraestructura IaaS.

En la Figura 6 se detalla el análisis de resultados posterior a la aplicación de la metodología Octave y la utilización de un ciclo de mejora continua PHVA.

Figura 6.

Esquema Propuesto para el de Manejo de Riesgos



Nota. Análisis de resultados posterior a la implementación de la metodología de Octave y la utilización de un ciclo de mejor continua PHVA. Elaboración propia.

Se obtiene una matriz resumen Tabla 15 con los activos y servicios de mayor relevancia, su criticidad y su estrategia para gestionar y mitigar los riesgos asociados a cada uno de los activos.

Tabla 15.

Estrategia de mitigación de riesgo

Priori dad	Activo	Indicador	Respo nsable	Amenazas	Seve ridad	Estrategia de Mitigación
1	Servicios Internos	Nivel de Seguridad. Disponibilidad del servicio. Criticidad. Soporte	R	Disposición de arquitectura en conexiones físicas y flujo de datos lógico que no correspondan al requerido para la operación de servicios	Alta	Notificar al administrador del servicio Configuración de ACLs en el servicio Ajustes en la definición de grupos de seguridad.
2	Servicios Externos	Nivel de Seguridad. Disponibilidad del servicio. Criticidad. Soporte.	R	Disposición de arquitectura en conexiones físicas y flujo de datos lógico que no correspondan al requerido para la operación de servicios.	Alta	Notificar al administrador del servicio Configuración de ACLs en el servicio. Ajustes en la definición de grupos de seguridad.

Nota. Estrategia de mitigación de riesgo. Elaboración propia.

El disponer de una esquema de gestión de riesgos permite a una organización mantener un mejor posicionamiento en el mercado tecnológico según el giro de negocios en el que se desarrolla y asegurar la calidad en sus servicios, dando a conocer la importancia que tiene la seguridad de la información en sus procesos corporativos.

CAPÍTULO II: PROPUESTA

1.1. Fundamentos teóricos aplicados

La propuesta en curso hace referencia al desarrollo de un esquema de manejo de riesgos sobre una infraestructura como servicios IAAS. Para lo cual se describen los conceptos teóricos de los componentes y aspectos principales relacionados con el tema de investigación:

Ciberseguridad

La ciberseguridad es denominada una práctica que permite proteger diferentes sistemas informáticos, redes y servicios de ataques digitales. Es común que estos ciberataques tengan como objetivo el acceder, modificar o eliminar información de una empresa o persona. A esto le sumamos la extorción a la que los usuarios y la afectación de un servicio tecnológico.

Según lo mencionado en la investigación "Ciberseguridad y robo de información: Una revisión sistemática de la literatura" por (Vilchez Villegas, 2022), es de gran importancia brindar educación sobre la ciberseguridad ya que hoy en día la tendencia del uso de la tecnología va en aumento al igual que los riesgos a los que un usuario se encuentra expuesto.

Seguridad de la información

Es el conjunto de medidas preventivas y reactivas (políticas y medidas) empleadas para resguardar y proteger la información de una empresa. La seguridad de la información es una pieza de gran valor que está relacionada con distintas operaciones de una empresa disminuyendo los riesgos a los cuales se encuentran expuestas.

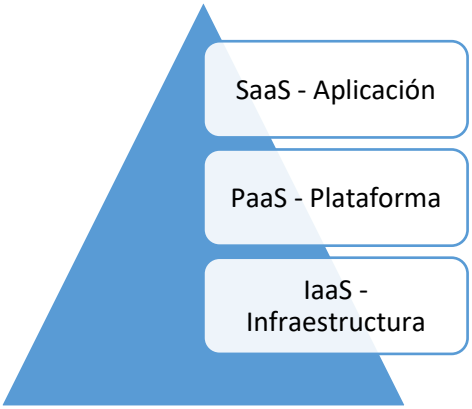
Como objetivos principales le corresponde el tratamiento de riesgos, analizarlos, prevenirlos y brindar opciones de solución. Según lo indicado por (Alomia & Montaño, s. f.), es importante ejecutar un seguimiento continuo de los diferentes procesos y procedimientos que se encuentren relacionados con la definición de un Sistema de gestión de seguridad de la información (SGSI).

Infraestructura como servicios "IAAS"

Un servicio en la nube tiene diferentes capas de operación, a continuación, en la Figura 7 se detalla la estructura del servicio cloud (nube):

Figura 7.

Capas de un servicio en la nube (cloud)



Nota. Capas de un servicios cloud. Adaptada del gráfico de los modelos de servicio cloud de Tsai, 2021. (https://repositorio.udesa.edu.ar).

- **Software como Servicio "SaaS":** Brinda una capa de software (aplicación) como servicio bajo demanda, además permite el acceso a varios usuarios de forma simultánea. El acceso a este tipo de servicio se realiza mediante un navegador web y no requiere de aplicaciones terceros.
- **Plataforma como servicio "PaaS":** Hace referencia a la capa intermedia de una arquitectura en la nube. Dispone de un entorno de desarrollo, un conjunto de complementos y servicios con los que aplicación es implementada en la plataforma. Algunos de estos complementos son conocidos como API (interfaz de programación de aplicaciones).
- **Infraestructura como servicio "IaaS":** Corresponde a la capa más baja de una arquitectura en la nube.
    - Soporta las capas IaaS y SaaS

- Permite la gestión de; servidores y estaciones de trabajo, repositorios de almacenamiento redundantes, características de cómputo que apoyan a las capas superiores y las aplicaciones alojadas en dicho servicio
- Proporciona capacidades particulares de la nube como escalabilidad y distribución de carga de trabajo entre servidores.

1.2. Descripción de la propuesta

El esquema de manejo de riesgos propuesto permitirá disponer de una metodología para la identificación de los diferentes riesgos a los cuales se encuentra expuesta una infraestructura como servicio en la nube, mediante la aplicación una serie de parámetros que persiguen como objetivo principal globalizar el compromiso corporativo con los principales actores y responsables del área tecnológica y jefaturas en diferentes niveles jerárquicos. Además de identificar de forma explícita los activos y servicios de mayor criticidad, conocer la metodología de trabajo en producción para la identificación y manejo de riesgos, definir un esquema base y como resultado un lineamiento que permitirá conocer en donde enfocar los esfuerzos cuando se conoce de un riesgo que podría tener un impacto negativo en la operación diaria y en el giro de negocios de la organización. Este esquema de trabajo también contempla un ciclo de mejora continua basado en evaluaciones constantes. Según lo indicado por (Quiroz Cuadros, 2019), " El ciclo de Deming PHVA (Planificar, Hacer, Actuar, Verificar), permite disponer de interacciones continuas sobre un proceso dado o toda la metodología de gestión de riesgos".

Acorde al esquema de trabajo propuesto este ciclo PHVA interviene una vez que los resultados generados en la identificación de riesgos de la metodología Octave sean obtenidos, para asegurar que la aplicación de esta metodología abarca la totalidad de los servicios corporativos, que los actores de cada proceso están alineados con sus debilidades y fortalezas tecnológicas, que la criticidad en cada servicio o activo se ajuste a las necesidades de la empresa y generando como resultado un esquema unificado que permitirá tener una identificación periódica de activos y servicios críticos, vulnerabilidades, amenazas y estrategias de gestión relacionados con una infraestructura como servicio alojado en la nube IAAS. Una vez que estas dos técnicas sean aplicadas en la evaluación, se dispondrá de indicadores que facilitaran el esquema de identificación, manejo y ciclo de mejora continua frente a los riesgos ante los cuales cualquier servicio tecnológico se encuentra expuesto hoy en día.

Metodología OCTAVE

Parte fundamental de la investigación e implementación de la metodología corresponde el identificar la información clave mediante el conocimiento del equipo de trabajo. Los niveles de implicancia en la estructura organizacional esta dado de la siguiente manera:

- **T (equipo de trabajo) — Grupo de análisis.:** Hace referencia al rol que se encarga de un análisis grupal y una definición de un tema específico.
- **J (jefatura del personal operativo) — Quién supervisa la administración del activo / servicio:** Hace referencia al rol que se encarga de la supervisión de la administración del activo / servicio.
- **R (responsable) — Quién está hace la evaluación:** Hace referencia al rol que se encarga de la actividad principal para completar la actividad y producir la salida esperada.
- **C (consultado – dueño / administrador del activo / servicio, usuario final) — Quién(es) proporciona entradas:** Este rol proporciona las entradas principales, corresponde al rol del responsable y de rendir cuentas, obtener información de otras unidades o también de interesados externos.

La siguiente tabla describe las fases en las que interviene el equipo de trabajo y los roles asociados a los miembros que lo conforman:

Tabla 16.

Roles y responsabilidades.

Fases de Identificación de Componentes	Responsables
Identificación de activos.	T
Identificación de amenazas, indicadores y estrategias de mitigación.	T
Identificación de componentes clave.	R

Definición de estrategia de control y plan de mitigación	JR
Definición de indicadores de cumplimiento	JR
Monitoreo y aplicación de ciclo de mejora continua	R, C

Nota. Roles y responsabilidades en la identificación de activos. Elaboración propia.

Atributos de la metodología OCTAVE

Los atributos son las características más relevantes de la evaluación. Describen los elementos base de una evaluación de riesgos, tanto desde el punto de vista del proceso como de la organización. La siguiente tabla muestra cómo se refleja cada atributo en el método OCTAVE.

Tabla 17.

Asignación de Atributos OCTAVE

Atributo	Aplicación del método OCTAVE
RA.1: Equipo de trabajo / análisis	Un equipo de trabajo interdisciplinario formado por miembros de las unidades de negocio y del área de tecnología de la información.
RA.2: Aumentar el análisis (habilidades del equipo de trabajo)	Se ofrece orientación sobre los tipos de competencias necesarias para llevar a cabo cada proceso. Si un equipo de análisis considera que no posee
RA.3: Catálogo de prácticas	Si un equipo de análisis considera que no posee los conocimientos y habilidades suficientes para llevar a cabo un proceso, debe incluir personal complementario que posea los conocimientos y habilidades requeridos para ese proceso.
RA.4: Perfil genérico de amenazas	El método OCTAVE requiere que las prácticas de seguridad organizacionales se evalúen con respecto a un catálogo de prácticas definido.
RA.5: Catálogo de vulnerabilidades	El método OCTAVE requiere que la infraestructura informática de la organización sea evaluada contra un catálogo definido de vulnerabilidades. El método requiere el uso de herramientas de análisis de vulnerabilidades.
RA.6: Actividades de evaluación definidas	Orientación para definir el alcance en la evaluación y seleccionar a los participantes, además de las directrices para llevar a cabo cada proceso. Hojas de trabajo y plantillas para registrar la información recopilada durante cada proceso Catálogos de información requerida por el proceso
RA.7: Resultados documentados de la evaluación	El método OCTAVE requiere que el equipo de trabajo documente los resultados de la evaluación.

RA.8: Límites de la evaluación	En las directrices previas a la guía de implementación de la metodología OCTAVE, se ofrecen recomendaciones para definir el alcance de la evaluación.
RA.9: Próximos pasos	La última actividad del Método OCTAVE requiere que los directivos definan acciones para implementar la estrategia de control y el plan de mitigación de riesgos para la organización. La actividad también requiere que los directivos asignen responsables de completar las acciones.
RA.10: Enfoque del riesgo	El método OCTAVE es una evaluación para la gestión de riesgos de seguridad.
RA.11: Actividades focalizadas	Cada proceso del Método OCTAVE se centra en identificar y analizar los problemas de seguridad de la información más importantes para la organización. Por ejemplo: ● En los "Procesos 1 a 3", los facilitadores centran las actividades utilizando los activos que los participantes consideran más importantes. ● En el "Proceso 4", el equipo de trabajo centra sus actividades de análisis utilizando los activos críticos que selecciona. ● En la "Fase 2", el equipo de trabajo limita la evaluación de vulnerabilidades de la infraestructura utilizando los activos críticos de la organización y las amenazas de esos activos. ● En la "Fase 3", el equipo de análisis establece las prioridades de los riesgos basándose en el impacto organizativo de los mismos.
RA.12: Cuestiones organizativas y tecnológicas	El método OCTAVE se centra en cuestiones tanto organizativas como tecnológicas. La primera fase es una evaluación organizativa en la que personas de toda la organización identifican activos y los clasifican. La segunda fase consiste en una evaluación de infraestructura de la tecnología de la información, que da lugar a la identificación de los problemas tecnológicos. Los datos organizativos y tecnológicos se analizan en la fase 3.
RA.13: Participación de las empresas y las tecnologías de la información	Un equipo de análisis interdisciplinario que incluye representantes de las áreas operativas y del departamento de tecnología de la información dirige la evaluación. En los procesos 1 a 3 participa personal de las unidades de negocio y del departamento de tecnologías de la información (incluida la representación de múltiples niveles organizativos) de la organización.
RA.14: Participación de la alta dirección	Los altos directivos deben participar en el Proceso 1, en el que los directivos aportan sus puntos de vista sobre los activos que son importantes para ellos y sobre el grado de protección de esos activos. Los altos directivos también participan en la tercera fase actividad 6 donde revisan, perfeccionan, aprueban el plan de trabajo a seguir y definen los siguientes pasos para aplicar la estrategia y los planes.
RA.15 Enfoque de colaboración	El método OCTAVE consiste en una serie progresiva de talleres. Cada taller requiere la interacción entre las personas que participan en él.

Nota. Definición de atributos a la metodología OCTAVE

Salidas de la Metodología OCTAVE

Los productos son los resultados necesarios para la evaluación, se definen los resultados que un equipo de trabajo debe alcanzar durante la evaluación. La siguiente tabla evidencia las secciones del método OCTAVE en las que se generan los resultados.

Tabla 18.

Salidas de la Metodología OCTAVE (Implementación)

Atributo	Aplicación del método OCTAVE
RO1.1: Activos críticos	Durante los "Procesos 1-3", todo el personal de la organización aporta sus puntos de vista sobre los activos que son importantes para realizar su trabajo. En el "Proceso 4", el equipo de trabajo selecciona los activos de mayor relevancia para la organización.
RO1.2: Requerimientos de seguridad para los activos críticos	Durante los "Procesos 1-3", todo el personal de la organización define los requerimientos de seguridad para los activos de mayor relevancia. El equipo de trabajo utiliza esta información durante el "Proceso 4" para describir los requerimientos de seguridad para los activos críticos de la organización.
RO1.3: Amenazas de los activos críticos	Durante los "Procesos 1-3", todo el personal de la organización identifica los escenarios que amenazan sus activos más importantes. Se consideran las áreas de críticas (relacionadas con los activos / servicios en IaaS) como entrada cuando se crea un perfil de amenaza por cada activo crítico durante el "Proceso 4".
RO1.4: Prácticas actuales de seguridad	Durante los "Procesos 1-3", todo el personal de la organización aporta sus puntos de vista sobre las prácticas de seguridad que se utilizan actualmente en la organización. Los participantes aportan con encuestas y hablan de los temas clave durante un debate posterior. Durante el "Proceso 8", el equipo de análisis consolida las prácticas de seguridad identificadas durante los tres primeros procesos.
RO1.5: Vulnerabilidades actuales de la organización	Durante los "Procesos 1-3", todo el personal de la organización aporta con sus puntos de vista sobre las prácticas ausentes o inadecuadas en la organización (vulnerabilidades organizativas). Éstas se identifican junto con las prácticas de seguridad mediante encuestas y debates posteriores. Durante el "Proceso 8", el equipo de análisis consolida las vulnerabilidades organizativas identificadas durante los tres primeros procesos.
RO2.1: Componentes clave	Durante el "Proceso 5", el equipo de trabajo identifica los activos clave de la infraestructura informática. Se utilizan los activos críticos y sus amenazas para enfocar la selección de componentes y posterior evaluar las vulnerabilidades tecnológicas.
RO2.2: Vulnerabilidades tecnológicas	Durante el "Proceso 6", el equipo de trabajo evalúa cada componente clave del "Proceso 5" utilizando herramientas de análisis de vulnerabilidades. El equipo interpreta los datos generados por las herramientas, identificando las debilidades tecnológicas (vulnerabilidades) presentes en cada componente.
RO3.1: Riesgos para los activos críticos	Durante el "Proceso 7", el equipo de trabajo identifica el impacto potencial en la organización para las amenazas a los activos críticos, lo que resulta en declaraciones explícitas de riesgo.
RO3.2: Medidas de riesgo	Durante el "Proceso 7", el equipo de trabajo evalúa el impacto de los riesgos acorde a una categorización de medidas cualitativas (bajo, medio,

	alto). El método OCTAVE considera opcional el uso de probabilidad en este proceso.
RO3.3: Estrategia de Protección	Durante el "Proceso 8", el equipo de análisis crea una estrategia de protección para mejorar la seguridad de la organización. El equipo basa la estrategia en la información organizativa y tecnológica que ha identificado a lo largo del Método OCTAVE.
RO3.4: Planes de Mitigación de Riesgos	Durante el "Proceso 8", el equipo de análisis crea planes de mitigación de riesgos, para reducir los riesgos de los activos más críticos de la organización. El equipo de equipo selecciona las acciones de mitigación basándose en la información organizativa y tecnológica que ha identificado a lo largo del proceso de evaluación.

Nota. Resultados de la aplicación de la metodología OCTAVE

Implementación de Fases y Actividades

- **Actividades de la fase 1 - Elaboración de perfiles de amenaza basados en activos.**

Como etapa inicial de la metodología se requiere que el personal relacionado con la infraestructura en evaluación (almacenamiento de información, servicios publicados, aplicativos internos, infraestructura en la nube) participen aportando con sus perspectivas únicas sobre los siguientes aspectos:

- Los activos asociados con la información que utilizan en sus trabajos.
- Las prácticas de seguridad que utiliza la organización.
- Qué vulnerabilidades organizativas están presentes en los activos que gestionan.

El equipo de trabajo consolida la información creando una visión global de la organización, de los activos asociados con la información, las prácticas de seguridad y las vulnerabilidades organizativas actuales. A continuación, se detallan sus principales actividades:

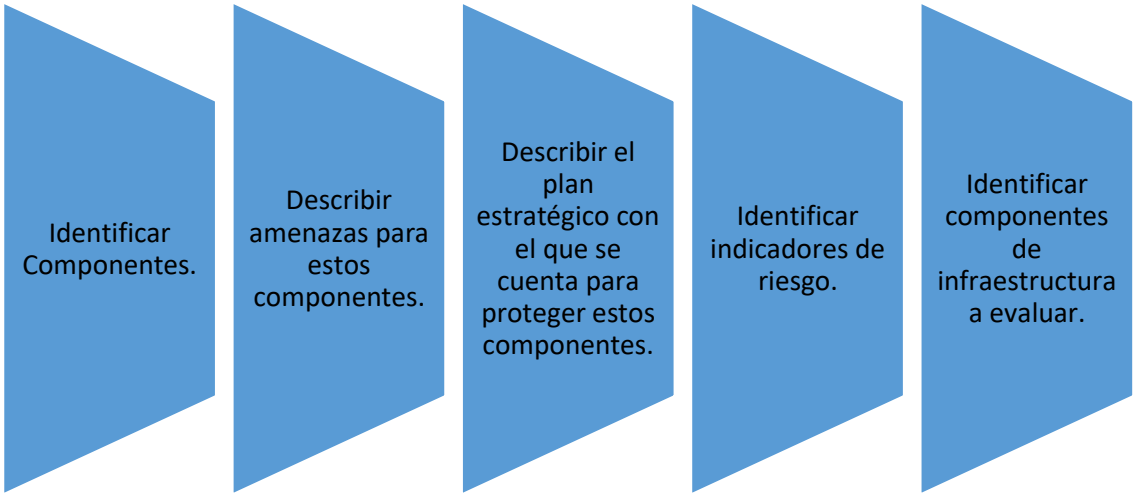
- Seleccionar los activos más importantes para cumplir la misión y los objetivos empresariales (activos críticos).
- Crear un conjunto de requerimientos de seguridad para cada activo crítico.

- Definir un perfil de amenaza para cada activo crítico que describe el universo de amenazas que se aplica a estos activos.

Según el modelo propuesto, consta de los siguientes procesos esquematizados en la siguiente figura, los mismos que permitirán asegurar que los componentes de la infraestructura y los riesgos relacionados con la implementación ya sea en la nube o en un centro de datos local no exceden la toleración de riesgo y que su impacto sea el menor posible para el desarrollo de un esquema de seguridad y manejo de riesgos.

Figura 8.

Identificación de Componentes de Infraestructura



Nota. Fase1 - Proceso de identificación de perfiles de amenaza. Elaboración propia

La fase 1 se compone de las siguientes seis actividades:

P1.1 Identificar los activos

Crear un listado de activos asociados con la información de la organización. Las siguientes preguntas clave deben ser respondidas durante esta actividad, estas se centran en la identificación de los activos importantes para cumplir la misión y los objetivos empresariales de la organización.

Preguntas clave para P1.1:

- ¿Cuáles son los activos importantes de la organización?
- ¿Existen otros activos que la organización deba proteger (por ejemplo, por ley o reglamento)?
- ¿Qué activos relacionados son importantes?
- ¿Qué activos son los más importantes? ¿Por qué?

El equipo de trabajo estará conformado por personal de diferentes áreas de la organización (por ejemplo, las áreas de negocio y de tecnología de la información) y de múltiples niveles organizativos (por ejemplo, la alta dirección, los responsables de área y el personal operativo), estos deben contribuir con sus perspectivas sobre los activos más relevantes empleados en la operación diaria. El equipo de trabajo consolida las perspectivas individuales, creando una visión global de la organización respecto a sus activos, la información y los servicios alojados de la infraestructura IaaS. El personal de toda la organización dependen de diferentes activos para realizar sus tareas, por lo que la identificación de estos tiene diferentes perspectivas acorde a las áreas involucradas. Antes de crear una perspectiva global de los activos de interés, hay que identificar las perspectivas individuales.

P1.2 Identificar las prácticas de seguridad actuales

Definir un listado de prácticas de seguridad empleadas por la organización (aplicadas en la operación). Las siguientes preguntas clave deben ser respondidas durante esta actividad, estas se centran en lo que el personal de la organización cree que hace para resguardar los activos de mayor importancia y que están relacionados con la información.

Preguntas clave para P1.2:

- ¿Qué está haciendo bien la organización con respecto a la protección de sus activos de mayor relevancia y que están relacionados con la información?
- ¿Existen políticas, procedimientos y prácticas específicas para los activos de mayor relevancia? ¿Cuáles son?

- ¿Es eficaz la estrategia de protección de la organización? ¿Por qué? ¿Por qué no?

Al responder a la primera pregunta clave, el personal debe considerar las prácticas de su organización en relación con un catálogo de prácticas ver Tabla 18 “RA.3 - Asignación de Atributos OCTAVE”. Esto permite valorar las prácticas de seguridad empleadas en la organización con respecto a una metodología conocida y aceptada en cuanto al cumplimiento de prácticas de seguridad.

P1.3 Identificar las vulnerabilidades actuales de la organización

Crear un listado de las vulnerabilidades presentes en la organización. Las siguientes preguntas clave deben ser respondidas durante esta actividad, estas se centran en lo que el personal de la organización cree que no está haciendo bien para resguardar los activos críticos de la organización en la operación diaria.

Preguntas clave para P1.3:

- ¿Qué es lo que la organización no está haciendo bien con respecto a la protección de los activos más importantes que están relacionados con la información?
- ¿Es eficaz la estrategia de seguridad de la organización? ¿Por qué? ¿Por qué no?

El equipo de trabajo consolida las perspectivas individuales de cada miembro, creando una visión de toda la organización respecto a las vulnerabilidades organizativas. Es importante solicitar las múltiples perspectivas sobre las vulnerabilidades organizativas con todo el personal, debido a que operan en diferentes áreas de la organización y suelen tener opiniones diferentes sobre lo que la organización está haciendo actualmente para proteger sus activos. Antes de que pueda crearse una perspectiva global de vulnerabilidades de la organización, deben identificarse las perspectivas individuales.

P1.4 Identificar Activos Críticos

Identificar los activos de mayor relevancia en la organización. Se debe responder a las siguientes preguntas clave, estas se centran en las violaciones de seguridad asociadas con los activos críticos en la organización. Cada pregunta se enmarca en torno a un resultado de amenaza específico.

Preguntas clave para P1.4:

- ¿Qué activos causarán un impacto adverso en la organización si son revelados a personas no autorizadas?
- ¿Qué activos causarán un impacto adverso en la organización si son modificados sin autorización? si se modifican sin autorización?
- ¿Qué activos causarán un impacto adverso en la organización si se pierden o se destruyen?
- ¿Qué activos causarán un impacto adverso en la organización si se interrumpe el acceso a ellos?

Seleccionar los activos críticos en la organización. El equipo de trabajo revisa inicialmente todos los activos asociados con la información que han sido identificados por los participantes de la organización. El número de activos críticos es reducido (a menudo no más de cinco).

P1.5 Describir los requerimientos de seguridad para los activos críticos

Describir los requerimientos de seguridad por cada activo crítico. Las siguientes preguntas clave deben ser respondidas durante esta actividad, estas se centran en las cualidades más importantes de los activos críticos definidos en la actividad P1.4.

Preguntas clave para P1.5:

- ¿El activo crítico es sensible? ¿Contiene información personal? ¿Debe ser inaccesible para cualquiera que no esté que no esté autorizado a verlo? Si la respuesta a alguna de estas preguntas es sí, ¿cuál es el requisito específico de confidencialidad?

- ¿Son importantes la autenticidad, la exactitud y la integridad del activo crítico? En caso afirmativo, ¿cuál es el requisito específico de integridad?
- ¿Es importante la accesibilidad del activo crítico? En caso afirmativo, ¿cuál es el requisito específico de disponibilidad?
- ¿Existen otros requisitos relacionados con la seguridad que sean importantes para el activo crítico? ¿Cuáles son?

Los requerimientos se describen desde una perspectiva organizacional, el equipo de trabajo crea un conjunto de requisitos de seguridad para cada activo crítico. Se considera la confidencialidad, integridad y disponibilidad de los activos. Para la identificación de los requerimientos de seguridad relacionados con una infraestructura sobre un servicio IAAS, se detallan los siguientes parámetros para el desarrollo de la evaluación:

Figura 9.

Requerimientos de Seguridad

Nota. Parámetros de evaluación de requerimientos de seguridad. Elaboración propia.

Como parte de la identificación de requerimientos de seguridad, también corresponde la identificación de los indicadores riesgo, amenazas y la definición de estrategias de mitigación de estos.

Tabla 19.

Identificación de Indicadores de Riesgo.

Indicadores	Amenazas	Estrategias de Control
Confidencialidad del servicio / activo.	Robo o divulgación de la información alojada en el servicio o activo	Controles en el perímetro de los servicios / activos.
Disponibilidad del servicio / activo.	Indisponibilidad del servicio o activo.	Monitoreo continuo con herramientas de terceros.
Integridad del servicio / activo.	Cambios no autorizados en la información que aloja el servicio o activo.	Revisiones de acceso y auditoría de usuarios.

Nota. Identificación de factores de riesgo. Elaboración propia.

P1.6 Crear Perfiles de amenaza para activos críticos

Identificar la gama de amenazas que podrían afectar a cada activo crítico. A continuación, se detallan las preguntas clave que deben ser respondidas durante el desarrollo de esta actividad, estas se centran en las amenazas de los activos críticos.

Preguntas clave para P1.6:

- ¿Para qué amenazas potenciales existe una posibilidad considerable de afectación en el activo crítico?
- ¿Para qué amenazas potenciales existe una posibilidad insignificante o ninguna de afectación en el activo crítico?

El equipo de análisis examina cada activo crítico en el contexto de las posibles amenazas en el perfil genérico de amenazas. A continuación, el equipo decide qué amenaza se aplica definiendo un perfil de amenaza único por cada activo. El perfil genérico de amenazas proporciona un rango de escenarios con amenazas comunes a considerar cuando se desarrolla un perfil de amenaza para un activo crítico. El equipo de análisis también tiene en cuenta las amenazas únicas que podrían no estar en el perfil genérico de amenazas.

Como parte de la identificación de amenazas se detallan los escenarios en los cuales se encuentra operando la infraestructura en la nube:

Tabla 20.

Perfiles de Amenaza.

Amenazas	Estrategia de Mitigación	Afectación de servicio	Criticidad
Robo o divulgación de la información alojada en el servicio o activo	Generación de ACLs para el consumo de servicios y conectividad destinados a los activos críticos.	SI	Alta
Indisponibilidad del servicio o activo.	Redundancia en la plataforma con tiempos mínimos de respuesta	NO	Baja
Cambios no autorizados en la información que aloja el servicio o activo.	Revisión de accesos autorizados y evaluaciones de seguridad al servicio o activo.	SI	Media

Nota. Identificación de amenazas en un servicio IAAS. Elaboración propia.

Para la clasificación de amenazas se ha definido un modelo basado en el tipo de afectación del servicio frente a las amenazas identificadas para el desarrollo del plan de implementación. La siguiente tabla detalla la definición de los niveles de amenazas:

Tabla 21.

Niveles de Severidad de Amenazas

Nivel de Amenaza	Afectación
Baja	Poca o ninguna afectación de servicios
Media	Afectación de servicio parcial, con tiempos altos de recuperación.
Alta	Afectación de servicio, con tiempos cortos de respuesta.

Nota. Definición de niveles de severidad de amenazas. Elaboración propia.

Fase 2 - Identificar las vulnerabilidades de la infraestructura IaaS

La segunda fase de OCTAVE requiere identificar las vulnerabilidades tecnológicas de la infraestructura IaaS. Abarca una evaluación que se centra en la infraestructura informática organizacional y los servicios que aloja. Durante esta fase el equipo de análisis y los miembros clave del área de tecnología de la información (TI) realizan las siguientes tareas:

- Seleccionan componentes específicos de la infraestructura para examinar las vulnerabilidades tecnológicas
- Seleccionan un enfoque para evaluar cada componente de la infraestructura
- Desarrollan un resumen de las vulnerabilidades tecnológicas que afectan a cada activo crítico
- Perfeccionan el perfil de amenaza de cada activo crítico basándose en la evaluación de los componentes clave de la infraestructura de ese activo.

La fase 2 de la metodología se compone de tres actividades que se describen a continuación:

P2.1 Seleccionar los componentes de la infraestructura a evaluar

Seleccionar los componentes alojados en la infraestructura IaaS para examinar las vulnerabilidades tecnológicas mediante una revisión por cada activo crítico y elegir un enfoque para la evaluación de vulnerabilidades. Al seleccionar los componentes y un enfoque, el equipo de análisis debe equilibrar la amplitud de la evaluación con el esfuerzo requerido para evaluar los componentes. Durante esta actividad se debe responder a las siguientes preguntas clave, estas se centran en la identificación de componentes típicos y en la selección de enfoques para evaluar dichos componentes.

Preguntas clave para P2.1:

- ¿Qué componente(s) específico(s) será(n) evaluado(s) para detectar vulnerabilidades tecnológicas?
    - ¿Es el componente de infraestructura típico de su clase?
    - ¿Qué grado de accesibilidad tiene el componente en la infraestructura IaaS? ¿Es propiedad de otra organización? ¿Es gestionado por un proveedor de servicios?

    - ¿Qué importancia tiene el componente para las operaciones de la empresa? ¿Se interrumpirán las operaciones empresariales cuando se evalúe el componente?
    - ¿Cuál es la justificación para seleccionar este componente o componentes específicos?
- ¿Qué enfoque se utilizará para evaluar cada componente seleccionado?
    - ¿Quién realizará la evaluación?
    - ¿Qué herramientas de evaluación de vulnerabilidades se utilizarán?
    - ¿Se necesitará un permiso especial o una programación para evaluar el componente?

Seleccionar componentes de infraestructura específicos para la evaluación. Para cada activo crítico el equipo de análisis y los miembros clave del personal de TI, revisan las amenazas que estan asociadas con el acceso a la red. Estas amenazas tienen un impacto directo sobre los activos críticos debido a la explotación deliberada de las vulnerabilidades tecnológicas o por acciones accidentales. Según las amenazas específicas de cada activo crítico, el equipo determina los componentes de la infraestructura que utilizan los usuarios legítimos para acceder a cada uno de ellos. También identifican los componentes que los actores de la amenaza podrían utilizar para acceder al activo crítico. Para las organizaciones con grandes infraestructuras informáticas, un primer paso opcional es identificar las clases clave de componentes de la infraestructura. A continuación, seleccionar los componentes individuales de cada clase clave para su evaluación, lo que hace que la evaluación de vulnerabilidades sea una actividad más manejable. Las siguientes preguntas podrían responderse durante esta actividad opcional, estas se centran en los componentes que forman parte o están relacionados con los activos críticos.

Preguntas clave opcionales para P2.1: Componentes en evaluación (clasificación de componentes clave)

- ¿Qué sistema(s) está(n) relacionado(s) directamente con el activo crítico? ¿En qué sistema(s) se almacena y procesa dicho activo?
    - ¿Cuáles son los tipos de componentes que forman parte del sistema en análisis? Considere los servidores, servicios, integraciones con terceros, networking, componentes de seguridad, servicios de almacenamiento y otros.
    - ¿Qué tipos de componentes están relacionados con el sistema de interés? ¿Cuáles son los tipos de hosts desde donde se accede legítimamente al sistema en evaluación? Considere las máquinas de escritorio (internos y externos), los ordenadores portátiles, los teléfonos celulares entre otros.
    - ¿Cómo podrían los actores de la amenaza acceder al sistema o sistemas? ¿A través de Internet? ¿A través de la red interna? ¿Redes externas compartidas? ¿Dispositivos inalámbricos? ¿Otros?
    - ¿Qué tipos de componentes podría utilizar un actor de la amenaza para acceder al sistema de interés? ¿Cuáles podrían servir como puntos de acceso intermedios? Considere el acceso mediante una cuenta de gestión y de red a los servidores, componentes de red, componentes de seguridad, ordenadores portátiles, dispositivos de almacenamiento y otros.

P2.2 Ejecutar las herramientas de evaluación de vulnerabilidades

Identificar las vulnerabilidades tecnológicas presentes en cada componente de infraestructura seleccionado y crear un resumen preliminar de las vulnerabilidades encontradas. Se debe responder a las siguientes preguntas clave, estas se centran en resumir las vulnerabilidades tecnológicas en función del momento en que deben abordarse.

Preguntas clave para P2.2:

- ¿Qué vulnerabilidades tecnológicas están presentes en cada componente de infraestructura IaaS evaluado?
- Para cada componente evaluado, ¿cuántas vulnerabilidades tecnológicas deben abordarse inmediatamente?
- Para cada componente evaluado, ¿cuántas vulnerabilidades tecnológicas deben abordarse en breve?
- Para cada componente evaluado, ¿cuántas vulnerabilidades tecnológicas pueden abordarse más tarde?

Para responder a la primera pregunta clave, el personal evalúa la infraestructura informática de la organización en relación con un catálogo de vulnerabilidades véase el "Atributo RA.5, Catálogo de Vulnerabilidades" criterios de OCTAVE. Esto permite a una organización evaluar su base tecnológica frente a las vulnerabilidades tecnológicas conocidas, proporcionando a la organización información sobre el grado de vulnerabilidad de su infraestructura informática. Las personas que dirigen esta actividad (miembros del equipo de análisis con experiencia en TI o personal complementario) emplean técnicas para el análisis de vulnerabilidades en cada componente alojado en la infraestructura IaaS. A continuación, este equipo revisa la información detallada sobre las vulnerabilidades reportadas por la(s) herramienta(s), interpretan los resultados y elaboran un resumen preliminar de las vulnerabilidades tecnológicas de cada componente clave.

P2.3 Revisar las vulnerabilidades y resumir los resultados

Desarrollar un resumen de las vulnerabilidades tecnológicas que afectan a cada activo crítico y perfeccionar el perfil de amenazas para cada uno basándose en la evaluación de los componentes clave de la infraestructura IaaS. Durante esta actividad se debe responder a las siguientes preguntas clave, estas se centran en el resumen de las vulnerabilidades y su efecto en la organización.

Preguntas clave para P2.3:

- ¿Hay cambios en el resumen de vulnerabilidades propuesto para cada activo crítico? ¿Cuáles son estos cambios?
- ¿Existen acciones o recomendaciones específicas para abordar las vulnerabilidades tecnológicas que afectan a cada activo crítico? ¿Cuáles son estas acciones o recomendaciones?
- ¿Existen vulnerabilidades tecnológicas asociadas a los componentes clave de la infraestructura IaaS que antes se creían insignificantes? ¿Cuáles son estas amenazas?

El personal que lleva a cabo la evaluación de vulnerabilidades (ya sean miembros del equipo de análisis con experiencia en tecnología de la información o personal complementario) revisan el resumen propuesto para cada activo crítico con el equipo de análisis, asegurándose de que todos los miembros del equipo de análisis entienden los resultados. Se pueden proponer e incorporar cambios en el resumen de ser necesario. Además, el equipo identifica y registra las acciones y recomendaciones específicas para abordar las vulnerabilidades tecnológicas. Por último, el equipo realiza un análisis de las deficiencias del perfil de amenaza por cada activo, optimizando el perfil de amenazas.

Actividades de la fase 3 - Desarrollo de la estrategia y planes de trabajo

Durante la tercera fase de la metodología OCTAVE, el equipo de análisis identifica los riesgos para los activos críticos de la organización y decide qué hacer con ellos. También analiza la información generada durante la evaluación y propone una estrategia de protección para la mejora de la organización y planes de mitigación de riesgos. Los altos directivos de la organización revisan la estrategia, los planes propuestos y los perfeccionan según convenga, basándose en los recursos y las limitaciones de la organización. A continuación, los altos directivos determinan los siguientes pasos necesarios para aplicar la estrategia de control y el plan de mitigación.

Durante la tercera fase el equipo de trabajo realiza las siguientes actividades:

- Identificar los riesgos por cada activo crítico
- Desarrollar prioridades basadas en la evaluación de los riesgos frente a los criterios de evaluación establecidos
- Desarrollar una propuesta de estrategia para el control y mejora de la seguridad organizacional
- Desarrollar una propuesta orientada a un plan de mitigación frente a los riesgos de los activos críticos

Los altos directivos realizan las siguientes actividades:

- Revisan y perfeccionan la estrategia de control propuesta
- Revisan y perfeccionan el plan de mitigación de riesgos propuesto
- Desarrollan los siguientes pasos necesarios para implementar la estrategia de control y el plan de mitigación.

La fase tres de la metodología se compone de las siete actividades siguientes:

P3.1 Identificar los riesgos para los activos críticos

Describir los impactos potenciales para la organización respecto a los posibles resultados de las amenazas en el perfil de cada activo crítico. Un objetivo opcional es reunir datos de probabilidad para las amenazas en el perfil de amenazas de cada activo crítico.

Las siguientes preguntas clave deben ser respondidas durante esta actividad, estas se centran en cómo las amenazas afectan a los objetivos de negocio y a la misión de la organización.

Preguntas clave para P3.1: Impacto

Por cada activo crítico basándose en los resultados de las amenazas

- ¿Cuál es la afectación potencial en la reputación organizacional?

- ¿Cuál es la afectación potencial en la confianza y credibilidad de sus clientes?
- ¿Cuál es la afectación potencial en la productividad de la organización?
- ¿Qué sanciones legales o multas podrían imponerse a la organización?
- ¿Cuál es la afectación financiera para la organización?

El equipo de trabajo revisa el perfil de las amenazas para cada activo crítico, en cada resultado (divulgación, modificación, pérdida/destrucción, interrupción) presente en el perfil, el equipo crea una descripción narrativa de los impactos potenciales para la organización. El uso de la probabilidad durante el análisis de riesgos es opcional. Si se utiliza la probabilidad entonces hay que responder las siguientes preguntas clave durante la actividad, estas se centran en los factores que contribuyen a determinar la probabilidad.

Preguntas clave opcionales para P3.1: Probabilidad

Para cada perfil de amenaza

- ¿Qué activos críticos son objetivos probables de actores de amenazas humanas?
- ¿Cuáles son los motivos, los medios y las oportunidades para cada actor humano amenazante que podría emplear el acceso corporativo para violar la seguridad del activo crítico?
- ¿Cuáles son los motivos, los medios y las oportunidades de cada actor humano amenazante que podría utilizar el acceso para violar la seguridad del activo?
- ¿Qué datos históricos están disponibles para las amenazas en el perfil de la amenaza?
- ¿Qué condiciones o circunstancias inusuales podrían afectar a la probabilidad de las amenazas? O afectar a la probabilidad de las amenazas en el perfil de amenaza?

P3.2 Crear criterios de evaluación de riesgos

Definir los criterios de evaluación del riesgo por el impacto de este, estableciendo un entendimiento común de las medidas cualitativas del impacto. Un objetivo opcional es definir

los criterios de evaluación del riesgo para la probabilidad, estableciendo un entendimiento común de las medidas cualitativas de la probabilidad. Las siguientes preguntas clave deben ser respondidas durante esta actividad. Las preguntas se centran en la definición de las medidas de impacto.

Preguntas clave para P3.2: Crear criterios de evaluación de riesgos (Impacto)

- ¿Cómo se define un impacto "alto" para la organización?
- ¿Cómo se define un impacto "medio" para la organización?
- ¿Cómo se define un impacto "bajo" para la organización?

El equipo de trabajo determina lo que constituye un impacto bajo, medio y alto para la organización considerando el impacto potencial en diferentes áreas. La aplicación de la probabilidad durante el análisis de riesgos es opcional.

Para la clasificación de riesgos, se ha definido un modelo basado en el tipo de afectación del servicio frente a los riesgos identificados para el desarrollo del plan de implementación. La siguiente tabla muestra el detalle de la definición de los niveles de amenazas:

Tabla 22.

Niveles de Severidad de Riesgos

Nivel de Riesgo	Afectación
Baja	No hay afectación de servicio.
Media	Existe afectación parcial sobre el servicio.
Alta	Existe afectación total sobre el servicio.

Nota. Definición de niveles de severidad de amenazas identificadas en la investigación.

Elaboración propia.

Al definir los criterios de revisión de probabilidad el equipo considera la información sobre el motivo, los medios y la oportunidad de los usuarios internos y externos que utilizan la red o una cuenta de gestión, cualquier dato histórico para todos los tipos de amenazas y cualquier condición actual inusual que pueda tener afectación. Si se utiliza la probabilidad hay que

responder a las siguientes preguntas clave durante clave, estas se centran en la definición de las medidas de probabilidad.

Preguntas clave opcionales para P3.2: Probabilidad

- ¿Cómo se define una probabilidad de ocurrencia "alta"?
- ¿Cómo se define una probabilidad de ocurrencia "media"?
- ¿Cómo se define una probabilidad de ocurrencia "baja"?

3.3 Evaluar los riesgos de los activos críticos

Establecer valores (alto, medio o bajo) para cada descripción de impacto, completando el perfil de riesgo por cada activo crítico. Un objetivo opcional es establecer valores de probabilidad (alta, media o baja) para cada amenaza. Las siguientes preguntas clave deben ser respondidas durante esta actividad. Las preguntas se centran en utilizar las medidas de impacto para determinar el valor de uno.

Preguntas clave para P3.3: Impacto

- Considerando los criterios de evaluación, ¿el impacto para la organización es "alto"?
- Considerando los criterios de evaluación, ¿el impacto para la organización es "medio"?
- Considerando los criterios de evaluación, ¿el impacto para la organización es "bajo"?

El equipo de análisis revisa cada descripción de impacto y la evalúa en función de los criterios de evaluación, asignando a la descripción del impacto un valor (alto, medio o bajo).

El uso de la probabilidad durante el análisis de riesgos es opcional. Si se utiliza el equipo de análisis revisa los datos de probabilidad para cada de cada amenaza y evalúa los datos en función de los criterios de evaluación de la probabilidad, asignando a la amenaza un valor de probabilidad (alta, media o baja). Cuando el equipo de análisis asigna un valor de impacto a cada descripción de impacto para un activo crítico y opcionalmente, un valor de probabilidad a cada

amenaza para el activo crítico, completa el perfil de riesgo para ese activo crítico. Si se utiliza la probabilidad, hay que responder a las siguientes preguntas clave, estas se centran en utilizar las medidas de probabilidad para determinar el valor de la probabilidad de cada amenaza.

Preguntas clave opcionales para P3.3: Probabilidad

Para cada amenaza en el perfil de amenazas:

- Considerando los criterios de evaluación, ¿la probabilidad de la amenaza es "alta"?
- Considerando los criterios de evaluación, ¿la probabilidad de la amenaza es "media"?
- Considerando los criterios de evaluación, ¿la probabilidad de la amenaza es "baja"?

P3.4 Crear una estrategia de protección

Crear una propuesta de estrategia de control organizacional, durante esta actividad se deben utilizar preguntas clave derivadas de las prácticas estratégicas del catálogo de prácticas. Las siguientes preguntas clave son ejemplos de preguntas relacionadas con las prácticas estratégicas de seguridad. Las preguntas se enfocan en el desarrollo de un conjunto de estrategias enmarcadas en el catálogo de prácticas.

Preguntas clave para P3.4:

- ¿Qué iniciativas de formación y educación podrían ayudar a la organización a mantener o mejorar sus prácticas de seguridad?
- ¿Qué se puede hacer para mejorar la forma en que las cuestiones de seguridad se integran con la estrategia empresarial de la organización?
- ¿Qué se puede hacer para garantizar que todos los miembros del personal comprendan sus funciones y responsabilidades en materia de seguridad?
- ¿Qué nivel de financiación es apropiado para apoyar las necesidades de seguridad de la organización?

- ¿Los procedimientos y políticas de la organización suficientes para cubrir las necesidades de seguridad? ¿Cómo podrían mejorarse?
- ¿Se dispone de políticas y procedimientos para resguardar la información cuando hay colaboración con organizaciones externas (por ejemplo, terceros, colaboradores, subcontratistas o socios)? ¿Qué puede hacer la organización para mejorar la forma en que protege la información cuando trabaja en colaboración con organizaciones externas?
- ¿Qué puede hacer la organización para mejorar la revisión de calidad y satisfacción en el cumplimiento de sus necesidades y requerimientos respecto a los servicios, mecanismos y tecnologías de seguridad subcontratados?
- ¿Cómo se puede garantizar que la organización ha definido y probado los planes de continuidad y de recuperación antes de un fallo? ¿Cómo se puede garantizar que los miembros del personal conocen y comprenden los planes de continuidad y recuperación en caso de catástrofe en un proceso o servicio tecnológico?

El equipo de análisis revisa las prácticas de seguridad utilizadas por la organización, las vulnerabilidades organizativas presentes en la organización y el perfil de riesgo por cada activo. También desarrolla una estrategia de protección considerando las áreas de prácticas estratégicas del catálogo de prácticas. El equipo busca estrategias que ayuden a la organización a mantener sus prácticas de seguridad actuales, a tratar sus vulnerabilidades organizativas y a abordar sus riesgos más prioritarios. A continuación, el equipo de análisis examina las principales áreas de prácticas operativas del catálogo y determina las estrategias adicionales que podrían permitir al personal de la organización comprender y desempeñar mejor sus responsabilidades de seguridad en de seguridad en esas áreas.

P3.5 Crear Planes de Mitigación de Riesgos

Crear propuestas de planes de mitigación para reducir los riesgos de los activos críticos. Las siguientes preguntas clave se debe responde para cada categoría de amenaza definida en el perfil de la amenazas, estas preguntas se centran en la capacidad de la organización para para reconocer, resistir y recuperarse de las amenazas a los activos críticos de la organización.

Preguntas clave para P3.5:

- ¿Cuáles son los riesgos de alta prioridad para el activo crítico? ¿Qué tipos de amenazas tendrán un mayor impacto en los objetivos empresariales y la misión de la organización?
- ¿Qué riesgos mitigará activamente la organización mediante la aplicación de acciones destinadas a contrarrestar el tipo de amenaza asociado? ¿Qué riesgos aceptará la organización y no tomará ninguna medida para abordarlos?
- ¿Qué medidas podrían adoptarse para ayudar a reconocer o detectar los tipos de amenazas a medida que se producen?
- ¿Qué medidas se podrían tomar para ayudar a resistir o evitar que se produzcan los tipos de amenaza?
- ¿Qué medidas podrían adoptarse para ayudar a recuperarse de los tipos de amenaza si se producen?
- ¿Qué otras medidas podrían adoptarse para hacer frente a estos tipos de amenazas?
- ¿Qué medidas podrían utilizarse para verificar que este plan de mitigación funciona y es eficaz?

El equipo de análisis revisa las prácticas de seguridad en producción, las vulnerabilidades organizativas presentes y el perfil de riesgos. Por cada activo crítico definido, el equipo determina los riesgos que la organización mitigará activamente mediante la aplicación de acciones destinadas a contrarrestar el tipo de amenaza asociada y los riesgos que la organización aceptará, y no tomará ninguna medida para abordarlos. También utiliza los valores de impacto

cuando determina si acepta o mitiga un riesgo. Si también se utiliza la probabilidad, los valores de probabilidad también se pueden tener en cuenta en la decisión. El equipo utiliza los valores de impacto para establecer las prioridades de mitigación.

Se centra en la mitigación de amenazas que tienen un impacto de mayor relevancia en el cumplimiento de la misión y los objetivos de la organización. Si también se utiliza la probabilidad en el análisis, los valores de probabilidad pueden aplicarse para refinar las prioridades establecidas utilizando el impacto.

Para la mitigación de riesgos se debe partir de un análisis del impacto que representa para el proyecto y posterior a esto se debe realizar un conjunto de actividades que permitan disponer la mitigación de estos riesgos. En la tabla a continuación, se muestran las amenazas y sus niveles de riesgo identificados dentro del proceso de desarrollo del plan de implementación. Los riesgos abarcan las dos opciones de infraestructura analizadas, así como también las estrategias de mitigación previstas:

Tabla 23.

Análisis de Riesgos.

Severidad	Activos	Vulnerabilidades	Amenazas	Estrategia de Mitigación
Alta	Robo o divulgación de la información alojada en el servicio o activo	Inexistencia de controles en el perímetro del servicio o activo.	Robo o divulgación de la información alojada en el servicio o activo	Generación de ACLs para el consumo de servicios y conectividad destinados a los activos críticos.
Baja	Indisponibilidad del servicio o activo.	Pocos recursos de cómputo en los servicios o activos.	Indisponibilidad del servicio o activo.	Redundancia en la plataforma con tiempos mínimos de respuesta
Media	Cambios no autorizados en la información que aloja el servicio o activo.	Inexistencia de registros que avalen la actividad de usuarios.	Cambios no autorizados en la información que aloja el servicio o activo.	Revisión de accesos autorizados y evaluaciones de seguridad al servicio o activo.

Nota. Análisis de riesgos. Elaboración propia.

P3.6 Revisar la estrategia de protección y los planes de mitigación de riesgos con la dirección

En conjunto con los altos directivos de la organización se debe validar la estrategia de protección y el plan definitivo para la mitigación de riesgos propuestos con el equipo de análisis y perfeccionarlo según corresponda. Las siguientes preguntas clave se centran en el contenido de la estrategia de control y el plan de mitigación de riesgos en relación con los recursos y las limitaciones de la organización.

Preguntas clave para P3.6:

- ¿Qué mejoras, modificaciones, adiciones o supresiones deben hacerse a la estrategia de protección?
- ¿Qué refinamientos, modificaciones, adiciones o supresiones deben hacerse a cada plan de mitigación de riesgos?

El equipo de análisis presenta una estrategia de control y el plan de mitigación de riesgos propuesto a la organización. Los altos directivos realizan ajustes, modificaciones, adiciones o supresiones a la estrategia y plan propuestos, teniendo en cuenta los recursos y limitaciones de la organización. El resultado es la versión final de la estrategia de control y el plan de mitigación de riesgos.

P3.7 Identificar los próximos pasos

Los altos directivos de la organización identifican los próximos pasos que se darán para implementar la estrategia de control y el plan de mitigación. Las siguientes preguntas clave deben ser respondidas durante esta actividad, estas se centran en el papel de la dirección para permitir la mejora continua de la seguridad en la organización.

Preguntas clave para P3. 7:

- ¿Qué hará la organización para aprovechar los resultados de esta evaluación?

- ¿Qué más hará la dirección para garantizar que la organización mejore su seguridad de la información?
- ¿Qué puede hacer la dirección para apoyar esta iniciativa de mejora de la seguridad?
- ¿Cuáles son los planes de la dirección para las actividades de evaluación de la seguridad en curso?

Se definen los próximos pasos para implementar la estrategia de control y el plan de mitigación. Los directivos determinan lo que la organización hará para implementar los resultados de la evaluación y determinan lo que los directivos harán para permitir la mejora de la seguridad en la organización. Los directivos también determinan si hay otras actividades de mejora de la seguridad que deban abordarse y determinan cómo abordará la organización las futuras evaluaciones. Elaborar un plan de mitigación de riesgos basado en el análisis de las actividades anteriores y considerando las matrices del Anexo 4 para el levantamiento de información.

Ciclo de Mejora Continua PHVA

"La implementación del ciclo PHVA es de gran utilidad para definir la estructura y ejecución de proyectos en el cual se requieran características como la calidad y la optimización en la productividad de diferentes niveles de la organización", según lo indicado por (Quiroz Cuadros, 2019).

Planear: Se realiza la evaluación de la mejor opción para la resolución del inconveniente o problema.

Paso 1: Definir, delimitar y analizar el problema (magnitud).

Mantener claro el enfoque del problema para entender de qué manera y donde se manifiesta, como se encuentra relacionado con la calidad, productividad e impacto en el servicio afectado. Así mismo es de gran importancia definir la frecuencia de ocurrencia y si existe un

impacto económico. Para lo cual se utilizan herramientas, como hojas de verificación, histogramas, diagrama de Pareto y entrevistas a los usuarios internos y externos de los servicios de la organización. Como resultado de este proceso se requiere definir y delimitar el problema. Como objetivo se tiene el alcanzar la mejora continua y una aproximación de los beneficios directos e inconvenientes a solventar.

Paso 2: Indagar las posibles causas

Es recomendable tomar como objetivo las causas de mayor probabilidad que estén asociadas con el origen al problema y no de sus consecuencias. También es importante evidenciar los cambios que puede tener el problema en su ejecución (activo, área, turno, horario) donde se identifican las falencias y en que procesos ocurren. Si hay una constante dificultad se recomienda observar el problema global y de tal manera no descartar alguna causa de este. Para este proceso es posible emplear un diagrama de Ishikawa o una lluvia de ideas.

Paso 3: Identificar la causa o factor de mayor relevancia.

Identificar las causas más importantes del problema, como están relacionadas para reconocer un comportamiento del problema central y su efecto. En este paso es posible utilizar un diagrama de dispersión, una hoja de verificación, un diagrama de Pareto, entre otros.

Paso 4: Considerar medidas para solventar las causas de mayor relevancia.

Disponer de soluciones con proyección a largo plazo en la resolución del problema (no temporales), esto permitirá disponer de un proceso de prevención a futuro. Estas soluciones deben ser evaluadas respecto a su utilidad, su objetivo, su alcance en la ejecución, el tiempo de ejecución, costos, responsables y su metodología para realizar una evaluación de las medidas establecidas y generar un plan de trabajo para su implementación.

Hacer: Se ejecutan las tareas de remediación.

Paso 5: Ejecutar las medidas de solución

Las medidas definidas en el plan de implementación de soluciones se deben realizar secuencialmente, además es importante involucrar al personal definido para la evaluación y alinearlos en cuanto a la importancia del problema y los objetivos requeridos como resultado.

Verificar: En esta etapa se realiza una validación de los resultados obtenidos en la remediación, su efectividad en el tiempo, valor o características similares.

Paso 6: Considerar medidas de solución para las causas de mayor relevancia

Las soluciones propuestas deben solventar la problemática de forma definitiva es decir a largo plazo. Estas soluciones deben ser cuestionadas respecto a su utilidad, su objetivo, su implementación y el tiempo de duración de cada una. Como herramienta en este paso es posible emplear técnicas estadísticas.

Actuar: En esta etapa se socializan las tareas a los procesos que estan relacionados y así prevenir nuevas incidencias de estos.

Paso 7: Preveer que el problema sea repetitivo

Como indicador del paso anterior se mide la eficiencia de las soluciones propuestas y en base a este dato se da lugar a la prevención del riesgo o problema a solventar. Es necesario estandarizar soluciones a los procedimientos, procesos, manuales o políticas internas, con el objetivo de que el proceso de aprendizaje/perfilamiento se vea reflejado en los procesos de la organización. También es importante comunicar y fundamentar las medidas de prevención, realizar capacitaciones al personal clave para su cumplimiento y seguimiento acorde a lo esperado.

Paso 8: Conclusiones de la evaluación

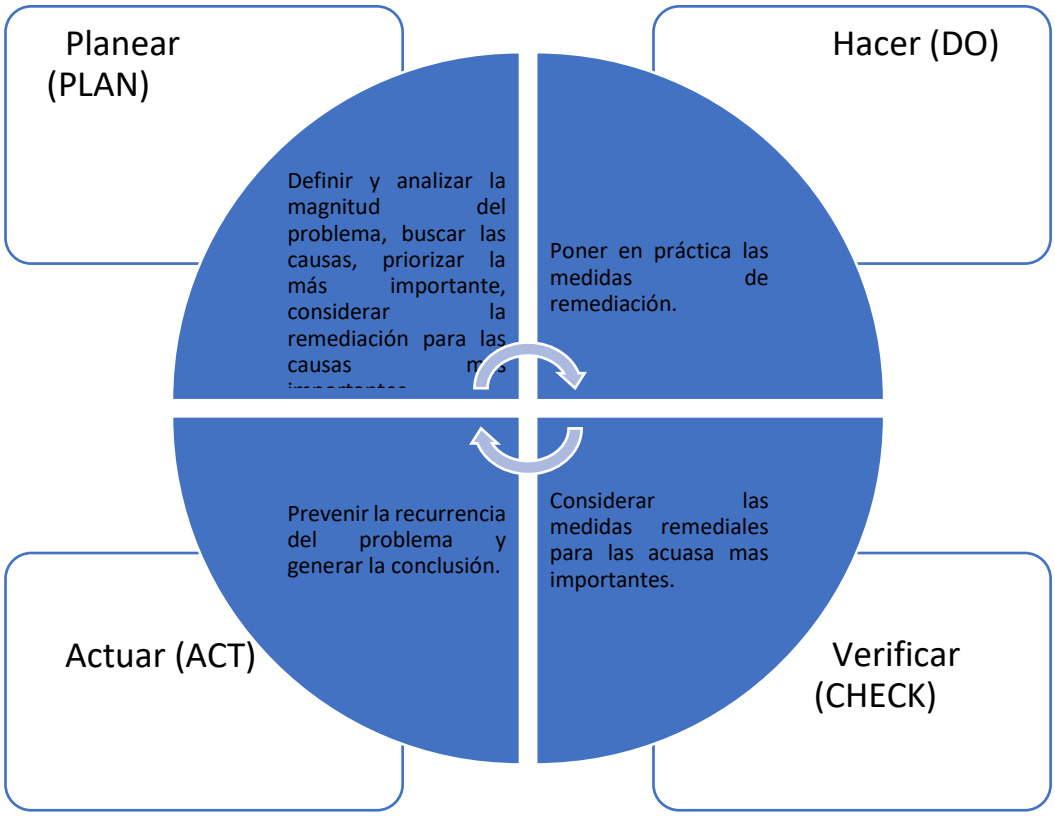
Es importante validar y documentar el procedimiento implementado, de tal manera planificar los pasos a seguir. Como herramientas en este paso se puede emplear una lista de observaciones que se mantienen posterior a la evaluación y recomendar opciones de

remediación. Los problemas de mayor relevancia son considerados para dar inicio al ciclo de mejora continua PHVA.

Es importante que los responsables de la evaluación apliquen este ciclo de mejora continua en la resolución de problemas tal como se observa en la Figura 10, a continuación:

Figura 10

Ciclo de Mejora Continua PHVA (Planificar, Hacer, Verificar y Actuar)



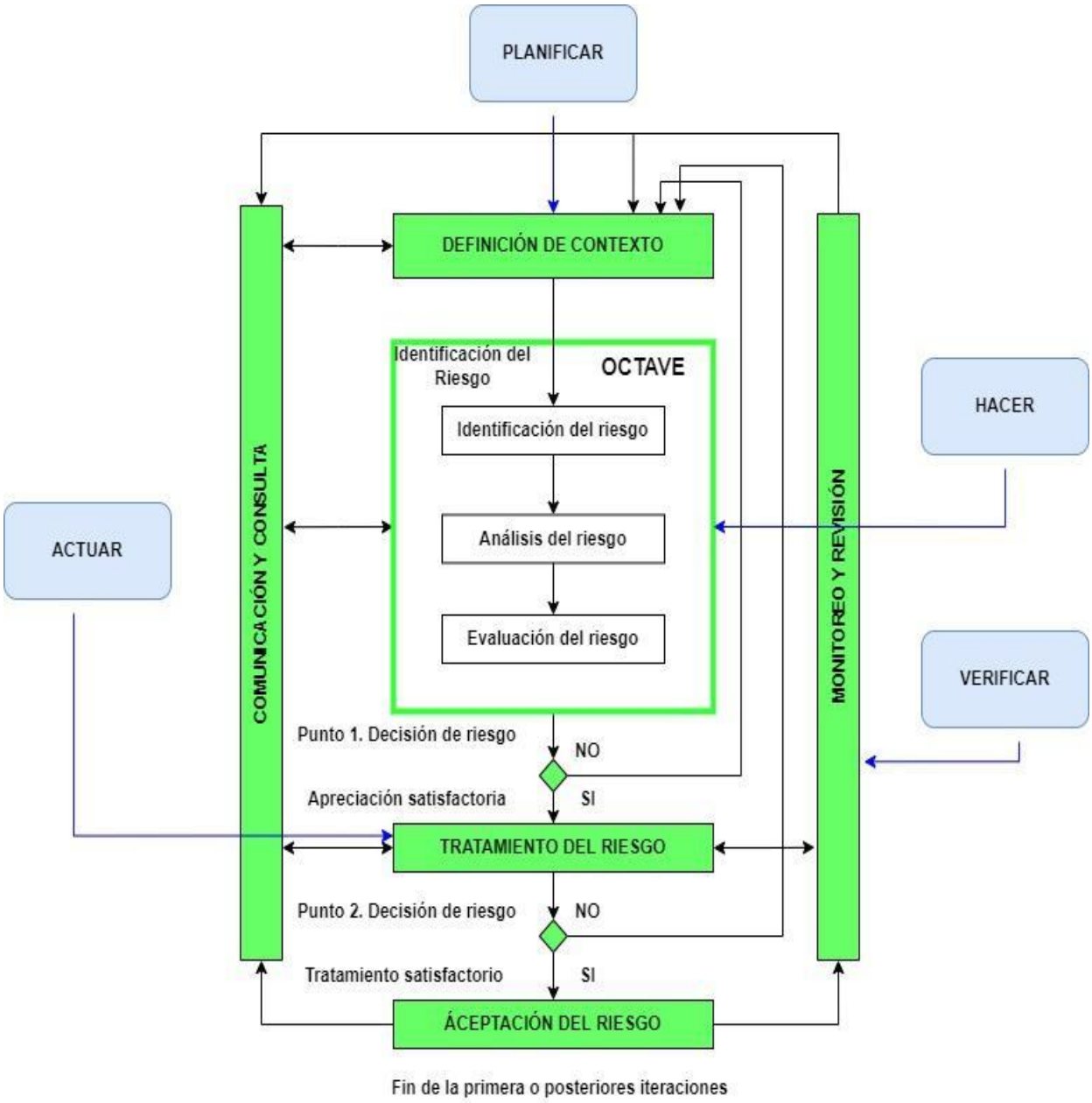
Nota. Ciclo de mejor continua PHVA. Auditoría propia.

El documentar las acciones realizadas permite obtener mejores resultados en los siguientes análisis.

a. Estructura general

Figura 11

Esquema de Manejo de Riesgos OCTAVE-PHVA



Nota. Arquitectura de manejo de riesgos propuesto mediante la identificación de riesgos con OCTAVE y el ciclo de Deming PHVA. Elaboración propia.

b. Explicación del aporte

Acorde a lo indicando en los apartados anteriores, se detalla la funcionalidad de la metodología de identificación de riesgos y el ciclo de mejora continua PHVA. Una correcta gestión de riesgos de seguridad de la información tiene un papel importante en una organización, su administración permite disponer de un enfoque de los procesos internos, el uso

correcto de los recursos tecnológicos, disminución de costos y el conocimiento general de la cultura enfocada sobre el control interno. Esta investigación permite disponer de un esquema de manejo de riesgos sustentado en la validación de las fuentes científicas y la aplicación de un análisis detallado para definir las etapas y variables de mayor uso en dichas investigaciones, adicionalmente se considera la experiencia práctica y criterios de especialistas que se desempeñan en el área de seguridad de la información.

Como resultado se propone un procedimiento metodológico para la identificación de riesgos, que cumple con la normativa legal del Ecuador, mediante diferentes instrumentos de medición que provee información relevante para la toma de decisiones, así como una evaluación el nivel de gestión de riesgos de una empresa.

c. Estrategias y/o técnicas

Describa las estrategias y/o técnicas que se emplearon en la construcción del producto. Según lo indicado en la investigación (Casas Anguita et al., 2003) las encuestas y la entrevista son ampliamente utilizada durante el proceso de desarrollo de una investigación, debido a que permite obtener y elaborar datos de forma rápida y eficaz. En el ámbito tecnológico el uso de encuestas es muy frecuente ya que permite disponer de un levantamiento de información detallado, esta técnica de investigación es aplicada a los involucrados en la misma y en ocasiones abarca diferentes niveles organizacionales para disponer de una visión general del estado actual del tema del que se requiere conocer. En el apartado de anexo se especifican los modelos de encuestas que permitirán realizar el levantamiento de información respecto a los diferentes servicios o activos, evidenciar el conocimiento de la población tecnológica, formalizar el lineamiento de seguridad base que se usa en el día a día y principalmente concientizar al área tecnológica y de las jefaturas involucradas del estado inicial y al que se desea llegar al implementar las herramientas descritas en esta investigación.

1.3. Matriz de articulación de la propuesta

En la presente matriz se sintetiza la articulación del producto realizado con los sustentos teóricos, metodológicos, estratégicos-técnicos y tecnológicos empleados.

Tabla 24.

Matriz de articulación

EJES O PARTES PRINCIPALES	SUSTENTO TEÓRICO	SUSTENTO METODOLÓGICO	ESTRATEGIAS / TÉCNICAS	DESCRIPCIÓN DE RESULTADOS	INSTRUMENTOS APLICADOS
Planificación de ejecución de evaluación de riesgos	Levantamiento de información con las áreas involucradas (entrevista y encuestas). Revisión de consideraciones en la aplicación de la metodología.	Fase de planificación. Inicio de ciclo de mejora continua PHVA. Identificación de vulnerabilidades organizacionales.	Revisión de entrevista y encuestas Revisión de inventario de servicios.	Cronograma de trabajo priorizando servicios, orden de ejecución de actividades, alcance, requerimientos, tiempos estimados por actividad.	Word, Excel
Identificación del riesgo	Análisis de tendencias sobre eventos de seguridad	Fase de ejecución Ejecución de análisis de vulnerabilidades sobre servicios críticos.	Revisión de levantamiento de información.	Reporte de vulnerabilidades en servicios bajo evaluación.	Word, Excel, Analizador de vulnerabilidades.

	según el cuadrante mágico de “Gartner”. Reportes de eventos de seguridad presentados en los servicios del servicio IAAS.			Reporte de eventos de seguridad en los servicios críticos.	
Análisis del riesgo	Revisión de reporte de análisis de vulnerabilidades. Revisión de controles recomendados por la CSA (Cloud Security Alliance)	Fase de ejecución Evaluación de vulnerabilidades reportadas.	Validación de remediaciones generadas en el análisis de vulnerabilidades.	Riesgos de seguridad y vulnerabilidades sobre los servicios a evaluar, categorizados según el giro de negocios de la empresa.	Word, Excel, Adobe PDF, Analizador de vulnerabilidades
Evaluación del riesgo	Revisión de reporte de análisis de riesgo. Revisión de procesos organizacionales.	Fase de ejecución Revisión de vulnerabilidades y resumen de resultados.	Valoración de riesgos y vulnerabilidades identificados con los responsables de área.	Evaluación de riesgos propuesto por los responsables de la evaluación.	Word, Excel, Adobe PDF

Tratamiento del riesgo	Revisión de matrices de evaluación de riesgo. Revisión de mejores prácticas de seguridad acorde a los servicios evaluados. Revisión de criterios de valoración de riesgos.	Fase de Verificación Validación de mejoras de seguridad y operación en servicios evaluados.	Aplicación de remediaciones en servicios evaluados.	Corrección de eventos de seguridad y vulnerabilidades identificadas. Generación de plan de mitigación de riesgos Generación de estrategia de protección.	Word, Excel, Adobe PDF	
Monitoreo y Revisión del riesgo	Revisión de informe de remediaciones aplicadas. Revisión de plan de mitigación de riesgos.	Fase de Verificación Revisión de efectividad en remediación aplicada.	Definición de indicadores y medición de resultados.	Informe de impacto posterior a la remediación.	Word, Excel, Adobe PDF	
Aceptación del riesgo	Revisión del informe de monitoreo y estabilización de servicios posterior a las remediaciones aplicadas.	Fase de ejecución Documentación de la evaluación realizada.	Levantamiento de información para desarrollo de memoria técnica.	Informe de evaluación realizada mediante la metodología de OCTAVE y cumplimiento del ciclo de mejora PHVA.	Word, Excel, Adobe PDF	

Comunicación y consulta	Resumen de actividades ejecutadas y resultados obtenidos. Reportes generados en cada fase de la metodología.	Fase de ejecución Socialización de evaluación realizada y resultados obtenidos a la organización.	Comunicados masivos. Campañas de correo informativas. Campañas de concientización.	Niveles de aceptación organizacional. Manejo de riesgos y disponibilidad de un ciclo de mejora continua.	Word, Excel, Adobe PDF, PowerPoint

Nota. Estructura del esquema de manejo de riesgos propuesto.

CONCLUSIONES

A partir de la revisión bibliográfica realizada la metodología Octave se adapta a una infraestructura en la "nube", así como también el ciclo de mejora continua PHVA (Planificar, Hacer, Verificar y Actuar), para disponer de un esquema de seguridad y manejo de riesgos que permita asegurar la información y servicios tecnológicos.

Se describe la aplicación del marco metodológico mediante el análisis de cada proceso que lo conforma y se define el lineamiento base de un esquema de manejo de riesgos basados en metodología Octave bajo un ciclo de mejora continua PHVA para una infraestructura en la nube IAAS (infraestructura como servicio).

Se detalla el diseño de un esquema de seguridad utilizando el ciclo de mejora continua PHVA y la metodología Octave para la definición de un proceso de manejo de riesgos y aseguramiento de la información que brinda integridad, disponibilidad y confidencialidad sobre los servicios alojados en una infraestructura en la nube.

Durante el desarrollo del esquema de manejo de riesgos se evidencia el nivel de criticidad y el impacto de estos incidentes en una infraestructura en la nube, mediante la aplicación del ciclo de mejora continua PHVA y la metodología Octave, para disminuir, mitigar y principalmente llevar un correcto manejo de los riesgos de seguridad.

Como parte de la aplicación de las fases de la metodología Octave se desarrolla la identificación de los servicios y activos de una infraestructura en la nube, permite alinear los conocimientos corporativos en distintos niveles jerárquicos, disponer de una revisión de los procesos internos para el manejo de servicios y el tratamiento de riesgos de seguridad de la información.

Posterior a la aplicación del esquema de manejo de riesgos se dispondrá de una estrategia que permitirá conocer a los responsables de cada área de la organización, el estado actual de seguridad en los distintos servicios y activos de una infraestructura en la nube, la criticidad de cada uno de estos, su impacto y disponer de un plan de mitigación que les permitirá asegurar la

integridad, disponibilidad y confidencialidad de los servicios institucionales alojados en una infraestructura IAAS.

La aplicación del ciclo de mejora continua PHVA permitirá disponer de un esquema de seguridad proactivo, mediante evaluaciones acorde a la necesidad de la organización ya sea a pequeña o gran escala, con el objetivo de disminuir el impacto frente a incidentes de seguridad y principalmente mitigar escenarios que tendrían una afectación de servicios.

RECOMENDACIONES

Establecer un esquema de seguimiento periódico a la metodología aplicada, a los servicios que se encuentran en producción y los que se espera disponer a corto y largo plazo en la organización bajo una plataforma como servicios en la nube, de tal forma contemplar los cambios requeridos en cada fase considerando los ajustes necesarios en cada evaluación y evaluación de resultados.

Involucrar a las jefaturas de área que intervienen en el proceso de aplicación del esquema de manejo de riesgos, para contar con retroalimentaciones que permitan optimizar las actividades establecidas en cada fase de la metodología a seguir con un enfoque organizacional. Esto permitirá alinear los conceptos y el esfuerzo que se requiere de cada participante en el proceso de evaluación y disponer de los resultados esperados.

El equipo de trabajo con el cual se llevará el esquema de manejo de riesgos y el ciclo de mejora continua debe estar principalmente liderado por el área tecnológica y los responsables de servicio, de tal manera conocer los detalles y consideraciones en la operación de estos servicios considerando las mejores prácticas de seguridad y lineamientos organizacionales.

Realizar la estandarización de los entregables que se manejarán durante la aplicación del esquema de manejo de riesgos, para asegurar que la información plasmada en los mismos abarque los principales aspectos y apoyen en la toma de decisiones en cuanto a la identificación de activos, el estado de seguridad actual y los resultados a obtener en cada uno de los procesos de la evaluación.

Definir un área o responsables del esquema de manejo de riesgos propuesto, que se encargue del proceso de evaluación, monitoreo, cumplimiento y mejora de este. El responsable del esquema de seguridad mediante indicadores de cumplimiento definirá el porcentaje de adopción de las remediaciones y socializar las observaciones o cambios en la evaluación y en el ciclo de mejora continua.

Como parte del proceso de aplicación del ciclo de mejora continua, es recomendable realizar una comparativa entre la metodología Octave que conforma el esquema de manejo de riesgos propuesto y metodologías similares que existen en el mercado, con el objetivo de evidenciar los posibles resultados posterior a la evaluación y optimizar el proceso empleado ya sea para minimizar el tiempo de ejecución de cada fase y asegurar la integridad, disponibilidad y confidencialidad de los servicios institucionales alojados en una infraestructura IAAS.

BIBLIOGRAFÍA

Agudelo, A. A. A. (2018). *MODELO DE SEGURIDAD PARA PLATAFORMAS IAAS DE LA EMPRESA VIRGIN MOBILE*. 95.

Alomia, G. A. R., & Montaño, A. F. T. (s. f.). *PLAN DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN FRENTE A LAS HISTORIAS CLÍNICAS POR LA IPS SALUD MAX S.A.S*. 50.

Ataques de ransomware aumentó 6% más en 2021. (2022, abril 13). *IT ahora*. https://itahora.com/2022/04/13/ataques-de-ransomware-aumento-6-mas-en-2021/

Bezanilla, I. A. F., Perellada, Ms. L. R. G., & Hernández, D. S. A. A. G. (2018). Gestión de riesgos técnicos en nubes privadas con soporte a la categoría de servicio IAAS. *Tono, Revista Técnica de la Empresa de Telecomunicaciones de Cuba S.A*, *14*(1), 32-42.

Casas Anguita, J., Repullo Labrador, J. R., & Donado Campos, J. (2003). La encuesta como técnica de investigación. Elaboración de cuestionarios y tratamiento estadístico de los datos (I). *Atención Primaria*, *31*(8), 527-538. https://doi.org/10.1016/S0212-6567(03)70728-8

Castro, A. R., & Bayona, Z. O. (2011). Gestión de Riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios. *Ingeniería*, *16*(2), 56-66.

de Caldas, F. J. (s. f.). *Technology risk management based on ISO 31000 and ISO 27005, and its contribution to business operation continuity*. *16*(2), 11.

Deepfakes, Cryptocurrency and Mobile Wallets: Cybercriminals Find New Opportunities in 2022. (2021, octubre 26). Check Point Software. https://blog.checkpoint.com/2021/10/26/deepfakes-cryptocurrency-and-mobile-wallets-cybercriminals-find-new-opportunities-in-2022/

ESCUELA POLITÉCNICA NACIONAL - PDF Free Download. (s. f.). Recuperado 5 de septiembre de 2022, de https://docplayer.es/56504800-Escuela-politecnica-nacional.html

Igual que los ataques, la seguridad tiene que evolucionar de manera constante. (2022, enero 18). CSO España. https://cso.computerworld.es/tendencias/igual-que-los-ataques-la-seguridad-tiene-que-evolucionar-de-manera-constante

Mateo, I. I. (2017). *0.3 TENDENCIAS DE SEGURIDAD Y VULNERABILIDADES EN SISTEMAS BASADOS EN LA NUBE*. *6*, 12.

Optimización de una IaaS en cloud computing haciendo uso de una nube privada. (s. f.). Recuperado 29 de abril de 2022, de https://190.116.48.43/handle/20.500.12866/1396

¿Qué ciberamenazas serán tendencia en 2022? - Red Seguridad. (2021, noviembre 3). Redseguridad. https://www.redseguridad.com/actualidad/informes-ciberseguridad/que-ciberamenazas-seran-tendencia-en-2022_20211103.html

Quiroz Cuadros, M. A. (2019). Implementación de la Metodología PHVA para incrementar la productividad en una empresa de servicios. *Repositorio de Tesis - UNMSM*. https://cybertesis.unmsm.edu.pe/handle/20.500.12672/10822

Top Threats to Cloud Computing: Egregious Eleven | CSA. (s. f.). Recuperado 10 de agosto de 2022, de https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-egregious-eleven/

Top Threats to Cloud Computing Pandemic Eleven | CSA. (s. f.). Recuperado 10 de agosto de 2022, de https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-pandemic-eleven/

Vilchez Villegas, J. C. (2022). *Ciberseguridad y robo de información: Una revisión sistemática de la literatura*. http://tesis.usat.edu.pe/handle/20.500.12423/4937

Villamizar, C. (2020, octubre 22). ¿Qué es NIST Cibersecurity Framework? *GlobalSuite Solutions*. https://www.globalsuitesolutions.com/es/que-es-nist-cibersecurity-framework/

ANEXOS

ANEXO 1

FORMATO DE ENTREVISTA

Esquema de Gestión de Riesgos Tecnológicos para Modelos de Servicio IAAS

Nombres y cargo de los participantes:

Nombre y Apellido	Cargo	Área	Conocimiento respecto al manejo de riesgos (SI - NO)

1- Defina los servicios tecnológicos de mayor criticidad alojados en el servicio IAAS y su afectación en caso de fallo por criticidad

Servicio	Disponibilidad de controles para el manejo de riesgos	Afectación (Ninguna, Parcial, Global)	Criticidad (Alta, Media, Baja)

2. ¿Cuál es el proveedor del servicio IAAS y que tipo de plan/contrato maneja?

……

……

……

……

……

3. ¿Dispone de una estrategia de mitigación de riesgos en producción?

SI ……. NO …….

Si la respuesta es SI, ¿Cuál?

……

……

……

……

……

4. ¿Dentro de servicio IAAS se dispone de herramientas de cumplimiento?

SI ……. NO …….

Si la respuesta es SI, ¿Cuál?

……

……

……

……

……

5. ¿Cuáles son las amenazas y vulnerabilidades de los servicios en producción que estan alojados sobre el servicio cloud?

SI ……. NO …….

Si la respuesta es SI, ¿Cuál?

……

……

……

……

……

6. ¿Se dispone de herramientas de análisis de vulnerabilidades para la evaluación del riesgo de los servicios alojados en el servicio IAAS?

SI ……. NO …….

Si la respuesta es SI, ¿Cuál

……
……
……
……

……

7. ¿Existe un área responsable de la gestión de riesgos?

SI ……. NO …….

Si la respuesta es SI, ¿Cuál?

……
……
……
……

……

8. ¿Se ha tenido una evaluación de riesgos previa sobre el servicio IAAS?

SI ……. NO …….

Si la respuesta es SI, ¿Cuál?

……
……
……
……

……

9. ¿Cómo se manejan los riesgos de los componentes alojados en el servicio IAAS?

SI ……. NO …….

Si la respuesta es SI, ¿Cuál?

……

……

……

……

……

10. ¿Cuáles son las áreas o departamentos asociados con los servicios alojados en el servicio IAAS?

SI ……. NO …….

Si la respuesta es SI, ¿Cuál?

……

……

……

……

……

11. Describa las dependencias de los servicios alojados en la infraestructura IAAS

……

……

……

……

……

12. Defina los indicadores que evidenciarán la aplicación y cumplimiento del esquema de manejo de riesgos (optimización de tiempos en un proceso específico, disminución de impacto frente a incidentes de seguridad, cumplimiento de normativa, mejor posicionamiento en el mercado, etc).

……

……

……

……

……

13. ¿Se dispone de un SGSI o políticas internas relacionadas con el manejo de riesgos de seguridad de la información para la IAAS?

SI ……. NO …….

Si la respuesta es SI, describa brevemente.

……
……
……
……

……

14. Siendo 1 el valor más bajo y 10 el más alto, especifique cuál es el nivel de conocimiento de los usuarios administradores respecto a la utilización de la seguridad de la información en los procesos del área en el que operan? Describa brevemente.

ALTO ……..

MEDIO ……..

NINGUNO ……..

15. ¿Se realizan programas de concientización respecto a la importancia de la seguridad de la información en la empresa?

SI ……. NO …….

Si la respuesta es SI, ¿Con que frecuencia se realiza? Y ¿Bajo qué lineamientos?

……
……
……
……

……

16. ¿Se dispone de un listado de las características contratadas en el servicio IAAS?

SI ……. NO …….

Si la respuesta es SI, detalle las características contratadas.

……

……

……

……

……

17. ¿Cuál es el objetivo para conseguir posterior a la aplicación de la metodología para manejo de riesgos propuesta?

……

……

……

……

……

18. ¿Se dispone de evaluaciones de riesgos en la empresa?

SI ……. NO …….

Si la respuesta es SI, detalle con qué frecuencia se realizan y quien lo realiza.

……

……

……

……

……

19. ¿Se lleva algún tipo de metodología de cumplimiento en la empresa que contemple los servicios alojado en el IAAS?

SI ……. NO …….

Si la respuesta es SI, detalle la metodología.

……

……

……

……

……
…

20. ¿Se tienen documentados los procesos en los que intervienen los servicios o activos alojados en el servicio IAAS?

SI ……. NO …….

Si la respuesta es SI, detalle los procedimientos documentados.

……
……
……
……

……

ANEXO 2

FORMATO DE ENCUESTA

Esquema de Gestión de Riesgos Tecnológicos para Modelos de Servicio IAAS

Nombres y apellidos:

Área:

Relación con el servicio a evaluar:

Fecha:

1. ¿Conoce de seguridad de la información y metodologías de gestión de riesgos?

○ Si

○ No

2. ¿Quién es responsable de la gestión del riesgo en el servicio que ud administra?

○ Operador TI

○ Administrador de infraestructura

○ Departamento de riesgos

Dueño o área responsable del servicio

3. ¿Los servicios que ud administra y que están alojados en el IAAS son críticos para el giro de negocios?

Si

No

¿Cuál es el porcentaje de afectación según su criterio? Defina una estimación del 0 al 10: ……

4. ¿Conoce ud del último análisis de vulnerabilidades realizado en el servicio IAAS?

Si

No

Desconozco

5. ¿Con que frecuencia se realiza una evaluación de riesgos en los servicios alojados en el IAAS?

Menos de 1 año

Más de 1 año

Desconozco

6. ¿Existe un lineamiento base respecto a un esquema de gestión de riesgos en la operación diaria que realiza?

Si

No

Desconozco

7. ¿Existe un lineamiento base respecto a un esquema de gestión de riesgos en la operación diaria que realiza?

- Si
- No
- Desconozco

8. ¿Emplea algún lineamiento de seguridad informática en las actividades que desarrolla en su cargo?

- Metodología
- Política Interna
- Ninguna

9. El servicio con que ud está relacionado está orienta a usuarios:

- Usuarios Internos
- Usuarios externos
- Usuarios Internos y Externos

10. ¿Conoce / Dispone de herramientas para la gestión de riesgos de seguridad de la información?

- Si
- No

Si la respuesta es sí, ¿Cuál es la herramienta? Liste las herramientas:

……

……

……

ANEXO 3

Matrices de Levantamiento de Información

Fase 1: Visión Organizativa - Identificar el conocimiento empresarial

N	Activo / Servicio	Tipo de servicio (Interno / Externo)	Dependencias	Áreas Involucradas	Estrategia de Seguridad	Amenazas	Vulnerabilidades	Crítico (Si/No)	Requerimientos de Seguridad
1	Portal de Correo	Externo	Si	TI	Antispam	Ataques informáticos	Falta de parches de seguridad.	SI	Disponibilidad
2	Storage de registros históricos	Interno	Si	TI, Desarrollo	Manejo de versionamiento	Robo o pérdida de información	Falencias en el proceso de acceso y asignación de permisos.	SI	Integridad, Confidencialidad
3	Servidor de Base de Datos	Interno	Si	Desarrollo, Infraestructura	Réplicas de seguridad incremental	Robo o pérdida de información	Falencias en el proceso de acceso y asignación de permisos.	SI	Integridad, Disponibilidad y Confidencialidad
4	Servidor Aplicativo Web	Externo	Si	Marketing, TI	Respaldos del activo	Indisponibilidad de servicios	Actualizaciones de sistema operativo inexistentes. Parchado de aplicativo web inexistente.	SI	Disponibilidad
5	Aplicación Web	Externo	No	Infraestructura, Desarrollo y TI	Alta disponibilidad	Indisponibilidad de servicios	Arquitectura de aplicativo web fuera de recomendaciones de desarrollo.	SI	Disponibilidad
6	Servidor de Intranet	Interno	No	Infraestructura, TI	Ninguna	Ataques informáticos	Actualizaciones de sistema operativo inexistentes.	No	Confidencialidad

7	Servidor de archivos	Interno	Si	Infraestructura, TI	Ninguna	Robo o pérdida de información	Actualizaciones de sistema operativo inexistentes.	No	Integridad, Confidencialidad
8	Servicio de DNS	Interno / Externo	Si	Infraestructura, TI	Ninguna	Indisponibilidad de servicios	Falencias en el proceso de acceso y asignación de permisos.	No	Disponibilidad
9	Servicio de respaldos	Interno	Si	Infraestructura, TI	Servicios de la plataforma IaaS	Robo o pérdida de información	Actualizaciones de sistema operativo inexistentes.	No	Integridad, Confidencialidad
10	VPNs Site to Site	Interno / Externo	No	Infraestructura, Desarrollo y TI	Redundancia con equipo perimetral en sitio	Indisponibilidad de servicios	Parchado de aplicativo web inexistente. Arquitectura de aplicativo web fuera de recomendaciones de desarrollo.	No	Disponibilidad

Fase 2: Estrategia y desarrollo del plan - Identificar los conocimientos del personal

N	Activo / Servicio Críticos	Afectación del Giro de Negocios (Si / No)	Tipo de Gestión (Interna o Externa)	Aplicación de Estrategia de Seguridad	Vulnerabilidades Reportadas	Vulnerabilidades Identificadas (https://www.incibe-cert.es/alerta-temprana/vulnerabilidades)
1	Portal de Correo	Si	Si	Si	Falta de parches de seguridad.	CVE-2022-36089, CVE-2022-33449, CVE-2021-36089, CVE-2022-36229.

2	Storage de registros históricos	Si	Si	Si	Falencias en el proceso de acceso y asignación de permisos.	CVE-2022-369987
3	Servidor de Base de Datos	Si	Si	Si	Falencias en el proceso de acceso y asignación de permisos.	CVE-2022-36089,CVE-2022-35589
4	Servidor Aplicativo Web	Si	Si	Si	Actualizaciones de sistema operativo inexistentes.	CVE-2022-36089, CVE-2020-312089, CVE-2021-332089, CVE-2021-456089, CVE-2020-312234
5	Aplicación Web	No	No	No	Parchado de aplicativo web inexistente. Arquitectura de aplicativo web fuera de recomendaciones de desarrollo.	CVE-2022-36089, CVE-2020-897654, CVE-2022-356089, CVE-2021-399089

Fase 3: Estrategia y desarrollo del plan - Identificar los conocimientos del personal

N	Activo / Servicio Críticos	Vulnerabilidades Identificadas (https://www.incibe-cert.es/alerta-temprana/vulnerabilidades)	Riesgos	Áreas de la Organización Afectadas	Estrategia Propuesta	Controles	Indicadores de Cumplimiento	Área Responsable del Cumplimiento	Plazo de implementación (corto, medio o largo plazo)

1	Portal de Correo	CVE-2022-36089, CVE-2022-33449, CVE-2021-36089, CVE-2022-36229.	- Plagio de cuenta de correo - Acceso a información confidencial - SPAM con el dominio corporativo	Toda la Organización	- Generación de ACLs para el acceso al servicio - Implementación de doble factor de autenticación - Implementación de política de contraseñas	- Controles de Firewall - Doble Factor de Autenticación - Política de Contraseñas	- Informes de Seguridad desde el equipo de perímetro - Informe de accesos	TI	Corto Plazo
2	Storage de registros históricos	CVE-2022-369987	- Robo de información - Afectación de servicios	TI	- Replicación de servicio de respaldos con mayor frecuencia.	- Servicio de replicación con distribución geográfica en tiempo real.	- Informes de tasa de transferencia de archivos de respaldo	TI	Mediano Plazo
3	Servidor de Base de Datos	CVE-2022-36089,CVE-2022-35589	- Daño o perdida de información - Afectación de servicios con dependencias.	TI	- Generación de ACLs para el acceso- Implementación de doble factor de autenticación - Implementación de procedimiento de acceso	- Controles de Firewall - Doble Factor de Autenticación - Procedimiento de acceso al Servidor de Base de Datos	- Informe de acceso - Informes de seguridad desde el equipo de perímetro	TI	Mediano Plazo

4	Servidor Aplicativo Web	CVE-2022-36089, CVE-2020-312089, CVE-2021-332089, CVE-2021-456089, CVE-2020-312234	- Afectación en la imagen de la organización. - Problemas de conectividad con servicios dependientes - Perdida de clientes potenciales.	Ventas, Marketing, TI	-Plan de trabajo para análisis de desempeño - Generación de ACLs para el acceso - Implementación de versionamiento mediante el servicio de la infraestructura IaaS	- Informe de desempeño - Controles de Firewall - Servicio de versionamiento IaaS	- Comparativo de los recursos de cómputo contratados vs el computo requerido y el porcentaje de ancho de banda atendido por el servidor.	TI	Corto Plazo
5	Aplicación Web	CVE-2022-36089, CVE-2020-897654, CVE-2022-356089, CVE-2021-399089	- Afectación en la imagen de la organización. - Perdida de la imagen y calidad de servicios con clientes ya posicionados.	Ventas, Marketing, TI	- Revisión periódica del estado de salud del activo. - Plan de trabajo para la revisión de Ingeniería de Software	- Informe de desempeño - Informe de Ingeniería de Software	- Número de visitas en el servicio web - Clientes registrados - Nuevas tendencias servicios y clientes - Posicionamiento corporativo en el mercado tecnológico	TI	Corto Plazo

ANEXO 4:

Criterios Octave (Catálogos de criticidad, entradas, salidas y formatos de ejemplo)

ANEXO 5: