UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE GUAYAQUIL

CARRERA DE INGENIERÍA DE SISTEMAS

METODOLOGÍA DE EVALUACIÓN DE ACTIVOS DE INFORMACIÓN EN ARQUITECTURAS DISTRIBUIDAS PARA EMPRESAS PÚBLICAS

Trabajo de titulación previo a la obtención del
Título de Ingeniero de Sistemas

AUTOR: KEVIN EDUARDO ORTIZ PAZMIÑO

TUTOR: MAXIMO GIOVANI TANDAZO ESPINOZA

Guayaquil – Ecuador

2022

CERTIFICADO DE RESPONSABILIDAD Y AUTORÍA DEL TRABAJO DE TITULACIÓN

Yo, Kevin Eduardo Ortiz Pazmiño con documento de identificación N° 0927233015 manifiesto que:

Soy el autor y responsable del presente trabajo; y, autorizo a que sin fines de lucro la Universidad Politécnica Salesiana pueda usar, difundir, reproducir o publicar de manera total o parcial el presente trabajo de titulación.

Guayaquil, 27 de octubre del año 2022

Atentamente,

_____

Kevin Eduardo Ortiz Pazmiño

0927233015

CERTIFICADO DE CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE TITULACIÓN A LA UNIVERSIDAD POLITÉCNICA SALESIANA

Yo, Kevin Eduardo Ortiz Pazmiño con documento de identificación No. 0927233015, expreso mi voluntad y por medio del presente documento cedo a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que soy autor(a) del Artículo Académico: "Metodología de evaluación de activos de información en arquitecturas distribuidas para empresas públicas", el cual ha sido desarrollado para optar por el título de: Ingeniero de Sistemas, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En concordancia con lo manifestado, suscribo este documento en el momento que hago la entrega del trabajo final en formato digital a la Biblioteca de la Universidad Politécnica Salesiana.

Guayaquil, 27 de octubre del año 2022

Atentamente,

Kevin Eduardo Ortiz Pazmiño
0927233015

CERTIFICADO DE DIRECCIÓN DEL TRABAJO DE TITULACIÓN

Yo, Maximo Giovani Tandazo Espinoza con documento de identificación N° xxxxxxxxxx, docente de la Universidad Politécnica Salesiana, declaro que bajo mi tutoría fue desarrollado el trabajo de titulación: METODOLOGÍA DE EVALUACIÓN DE ACTIVOS DE INFORMACIÓN EN ARQUITECTURAS DISTRIBUIDAS PARA EMPRESAS PÚBLICAS, realizado por Kevin Eduardo Ortiz Pazmiño con documento de identificación N° 0927233015, obteniendo como resultado final el trabajo de titulación bajo la opción Artículo Académico que cumple con todos los requisitos determinados por la Universidad Politécnica Salesiana.

Guayaquil, 27 de octubre del año 2022

Atentamente,

Maximo Giovani Tandazo Espinoza

DEDICATORIA

El presente trabajo investigativo lo dedicamos principalmente a Dios, por ser el inspirador y darnos fuerza para continuar en este proceso de obtener uno de los anhelos más deseados.

A mis padres, por su amor, trabajo y sacrificio en todos estos años, gracias a ustedes hemos logrado llegar hasta aquí y convertirnos en lo que somos. Ha sido el orgullo y el privilegio de ser su hijo, son los mejores padres.

A mis hermanas por estar siempre presentes, acompañándonos y por el apoyo moral, que nos brindaron a lo largo de esta etapa de nuestras vidas.

A todas las personas que nos han apoyado y han hecho que el trabajo se realice con éxito en especial a aquellos que nos abrieron las puertas y compartieron sus conocimientos….

AGRADECIMIENTO

No tengo palabras para expresar mi amor y mi gratitud por mi madre y padre, por su fe, su generosidad y su incansable ayuda en todo momento, gracias a ella he llegado a culminar un peldaño más de mi vida....

A mi tutor por el tiempo dedicado y los conocimientos brindados….

A todas las personas que me apoyaron e hicieron posible que este trabajo se realice con éxito....

Por último, pero no por eso menos importante a todos mis amigos que me apoyaron en todo momento y me dieron fuerzas para seguir adelante….

ABSTRACT

Se analizaron elementos de evaluación de riesgos y modelos de seguridad de la información que administran los activos. El problema es la falta de un mecanismo de gestión de la información en entornos distribuidos en el sector público. El objetivo principal es generar una metodología para incrementar el nivel de seguridad de la información sobre arquitectura distribuida para una Organización Pública del Ecuador. Se utilizaron el método deductivo y la investigación exploratoria para examinar la información de los artículos de referencia. Resultó lo siguiente: Prototipo de arquitectura distribuida, Algoritmo genérico para mitigar riesgos expresado en diagrama de flujo y Fórmula de probabilidad de ataque. Se concluyó que la propuesta generada es una alternativa para mantener la información de forma segura, con persistencia y disponibilidad.

Key words: Algoritmos de seguridad, Asegurar la información, Seguridad de la información, Arquitectura distribuida, Organización pública.

ÍNDICE DE CONTENIDO

1. INTRODUCCIÓN

En las arquitecturas distribuidas, los sistemas que gestionan la información están expuestos a amenazas; donde las redes, sistemas o información pueden ser víctimas de ataques generados por terceros. Los riesgos son inherentes a la información sensible que posee una organización pública (OP) o privada; en las empresas del sector público los riesgos, amenazas y vulnerabilidades ejecutadas sobre la información pueden derivar en costos económicos, sociales o políticos para el país; corromper la información puede tener impactos negativos para la OP y la sociedad.

Una arquitectura distribuida tiene recursos, nodos, procesos, clientes, servidores; además, a una variedad de estructuras de red, multicapas, software, hardware o varios tipos de procesamiento; las redes ayudan a gestionar la información de las empresas, que tienen usuarios dinámicos [1].

Los sistemas y redes tienen acceso a la información expuesta para ser utilizada por usuarios autorizados; el acceso no autorizado de personas o procesos internos o externos es latente.

Existen métodos para la evaluación de riesgos de seguridad de la información [2]. En las evaluaciones de riesgos se revisan los siguientes puntos: descripción de la criticidad de las vulnerabilidades, identificación de las vulnerabilidades y cuantificación del riesgo potencial [3].

Motivo: En Ecuador, desde febrero de 2019 existen 123 OP de diferentes tipos como: presidencia, secretarías, consejos, ministerios, institutos, agencias, empresas, banca, servicios, domicilios [4]; esta investigación plantea un mecanismo para aumentar el nivel de seguridad de la información en una OP.

¿Por qué es necesario definir una metodología para mejorar la seguridad de la información sobre arquitectura distribuida para una Organización Pública del Ecuador?

Mitigar los riesgos de seguridad de la información, ayudar a incrementar los mecanismos de protección adecuada, evitar el uso indebido de activos intangibles; dentro de una arquitectura distribuida para una OP de Ecuador.

El objetivo principal es generar una metodología para incrementar el nivel de seguridad de la información sobre arquitectura distribuida para una Organización Pública del Ecuador.

Los artículos relacionados con el tema de investigación son:

Distribuido o monolítico [1], Evaluación de riesgos de seguridad de la información: una comparación de métodos [2], Gráfico de ataque de flujo de exploración de riesgos para la evaluación de riesgos de seguridad [3], Estructura orgánica de Ecuador [4], Código de prácticas para la gestión eficaz de riesgos de seguridad de la información Uso de COBIT 5 [5], un método de evaluación de riesgos de seguridad de sitios web basado en el modelo I-BAG [6], un método mejorado de evaluación de riesgos de seguridad de la información para redes y computación cibernética-física-social [7], enfoque DSR para evaluación y reducción del riesgo de seguridad de la información en TELCO [8], Gestión del riesgo en un ecosistema en la nube [9], Mitigación del riesgo con ciberseguros [10], Modelo de análisis de riesgos de seguridad para sistemas de información [11], Análisis cuantitativo de riesgos en la gestión de la seguridad de la información [12] , Evaluación de riesgos de seguridad en sistemas de Internet de las cosas [13], ¿Cuál es su enfoque de riesgos de TI? [14].

Utilizamos el método deductivo y la investigación exploratoria para examinar la información de los artículos de referencia.

Los resultados son los siguientes: Prototipo de arquitectura distribuida, Algoritmo genérico para mitigar riesgos expresado en diagrama de flujo y Fórmula de probabilidad de ataque.

Se concluye que la propuesta generada es una alternativa para mantener la información de forma segura, con persistencia y disponible.

2. METODOLOGÍA

Se analiza elementos de evaluación de riesgos y modelos de seguridad de la información que administran los activos, posibles impactos y consecuencias del acceso no autorizado a los activos de la información. El problema es la falta de un mecanismo de gestión de la información en entornos distribuidos en el sector público.

En una primera instancia en Materiales, se revisaron ciertas investigaciones que analizan los riesgos de la seguridad de la información. En segunda instancia en Métodos se planteó: Alcance del modelo, Adoptar políticas de seguridad, Beneficios y Elementos de Evaluación.

2.1. Métodos de Recopilación de datos empleados

Se debe generar una metodología de evaluación de activos de información en arquitecturas distribuidas para empresas públicas, por lo cual se utilizó un algoritmo genérico para mitigar los riesgos expresados en un diagrama de flujo.

El autor propuso un modelo de comparación de riesgos en tres etapas: identificación, estimación y evaluación; definieron la estructura del proceso de gestión de riesgos y utilizan tareas como criterios de comparación; el modelo genera tres puntajes: el puntaje vertical obtiene la integridad total de los métodos, el puntaje horizontal obtiene la evaluación de riesgo particular, un puntaje final para determinar qué áreas se puede esperar mejorar; el autor identificó 26 tareas para comparar el informe de evaluación de riesgos, el mejor valor fue ISO27005 con 184 puntos [2]. Los autores propusieron un flujo de riesgos; aquí el modelo revisa las condiciones de la red, vulnerabilidades y escenario de ataque, luego genera un gráfico de ataques; basado en un algoritmo de flujo de riesgo máximo y un algoritmo de ruta factible, el modelo genera un diagrama de riesgo; el resultado son los riesgos potenciales y sus rutas críticas; la simulación se realizó en un modelo de red hipotético de 50 a 300 nodos y hasta 16.000 milisegundos; la complejidad de las rutas es de 94,25 unidades de diferencia, ambas tienden a aumentar [3]. Los autores propusieron un enfoque adaptativo y evolutivo a través de COBIT e ISO 27000 para controlar el riesgo de seguridad de la información; describen la implementación de actividades de alto y bajo nivel; consideran que el código de prácticas es eficaz y útil [5]. Para proteger la información de los sistemas web, los autores propusieron un modelo de cálculo de riesgo mejorado mediante el cálculo de la probabilidad condicional local de cada nodo; el modelo

genera el valor de riesgo del sitio web, consideran el modelo como factible y efectivo; en las pruebas el servidor de correo y base de datos tuvo la menor probabilidad de ataque promedio 0.5374% y 0.5891% respectivamente; y también obtuvieron el valor medio de riesgo más bajo 0,4497% y 0,4433% respectivamente; el servidor web obtuvo 0.8511% la mayor probabilidad de ataque promedio y 1.5419 unidades de valor de riesgo promedio [6]. Los autores propusieron un algoritmo mejorado para controlar la información y proteger la privacidad del usuario; el modelo utiliza una estructura de factores de riesgo en tres aspectos: activos, control del flujo de información y factores humanos; luego clasificados en nueve categorías; en las pruebas de valores de predicción compararon 4 algoritmos, el mayor porcentaje de error es 10.87% y el menor porcentaje de error es 1.25%; pero el primero tuvo el tiempo de CPU más corto con 51,3 segundos; el algoritmo necesita reducir su tiempo de ejecución [7]. Los autores diseñaron un modelo de reducción de riesgos de seguridad de la información para operadores de telecomunicaciones; para incorporar mecanismos de gobierno y gestión de tecnologías de la información utilizaron COBIT e ISO 270XX, para el modelo determinaron lineamientos, amenazas, vulnerabilidades y pesos [8]. Los autores propusieron un marco de gestión de riesgos para ser utilizado en la nube; el cual deriva en tres actividades: la evaluación de riesgos para identificar vulnerabilidades de la nube, tratamiento de riesgos para el diseño de políticas y planes, control de riesgos para el seguimiento de riesgos y eventos [9]. Para la evaluación de los riesgos de seguridad de la información, los autores propusieron una matriz de riesgos; la matriz obtiene la probabilidad y consecuencias, separa en riesgos aceptables e inaceptables, este modelo ayuda a tomar decisiones sobre inversiones en seguridad [10]. Los autores realizaron el análisis de riesgos de seguridad; el modelo consta de cuatro pasos: identificación y evaluación de activos, amenazas y vulnerabilidades, análisis de riesgos, mitigación de riesgos y estimación de daños; los resultados del modelo son cuantitativos basados en activos perdidos y probabilidades, además de entregar riesgos relevantes y residuales; probaron DoS, virus y cracking con probabilidades de 0,5, 0,7 y 0,4 respectivamente, donde el riesgo total para un escenario es de 42,3 unidades, el riesgo residual es de 14,7 unidades, la diferencia 27,6 se considera el beneficio [11]. El autor propuso un análisis de riesgo sobre tres alternativas; el primero aplica medidas de bajo costo y altos beneficios; el segundo es un enfoque para identificar y eliminar vulnerabilidades; el tercero utiliza escalas ordinales para las probabilidades de ocurrencia; el autor considera enfoques razonables y no excluyentes [12]. Los autores analizaron las razones por las que los enfoques de evaluación de riesgos son

inadecuados para IoT; las razones revisadas son: evaluaciones, los riesgos de las evaluaciones, los riesgos del conocimiento, los riesgos de los dispositivos e interfaces, los riesgos de ataques a los activos de información; proponen la actualización de la evaluación de riesgos [13]. Los autores revisaron un marco de gestión de riesgos cibernéticos que ofrece información de seguridad y amenazas en tiempo real y tiene buenas ventajas; también revisaron un indicador de riesgo de ciberseguridad que evalúa los sistemas de un entorno a través de factores con sus puntajes; en los puntajes probaron cinco sistemas, el punto más alto es 237 y el más bajo es 67, con esto determinan que el sistema con el puntaje más bajo debe proteger mejor sus activos [14].

2.2. Métodos y técnicas de Análisis de datos

Se utilizó el método deductivo y la investigación exploratoria para examinar la información de los artículos de referencia.

Se propuso una metodología para incrementar el nivel de seguridad de la información, para lo cual se consideraron los siguientes temas:

1.1.1. Alcance:

- Mitigar los riesgos de seguridad de la información
- arquitectura de 3 capas
- Arquitectura para una OP en Ecuador
- Se aplica arquitectura distribuida a la base de datos.

1.1.2. Adoptar políticas de:

- Antivirus
- Contraseñas
- Uso de activos
- Uso de Internet
- Correo

1.1.3. Beneficios:

Las ventajas [11] de la seguridad de la información para una OP:

- Servicio de información segura
- Protección de activos críticos: información
- Ayuda en la toma de decisiones
- Establecer políticas de seguridad de la información
- Proporcionar valiosos datos de análisis
- Independencia del tipo de organización

1.1.4. Elementos por evaluar:

Los elementos que deben ser evaluados, identificados o analizados son:

- Evaluar e identificar amenazas para determinar las causas
- Evaluar e identificar vulnerabilidades para determinar las probabilidades
- Evaluar e identificar los sitios de la arquitectura distribuida para determinar los accesos
- Analizar y evaluar los riesgos para determinar los efectos
- Obtener los activos de información para determinar el impacto

En la Figura 1 se dan los siguientes elementos como: Amenazas es la posibilidad de que ocurra un evento con los daños que puede causar un evento exitoso; Las vulnerabilidades son características del sistema con gran probabilidad de aplicar para sufrir el daño; Los sitios son los puntos de acceso físicos de la red y lógicos del sistema donde hay entradas a la información; El riesgo es la magnitud de los efectos aplicados a la información; Los activos de información son los datos, bases, sistemas y servicios de OP que pueden sufrir un fuerte impacto cuando se ejecuta un riesgo.

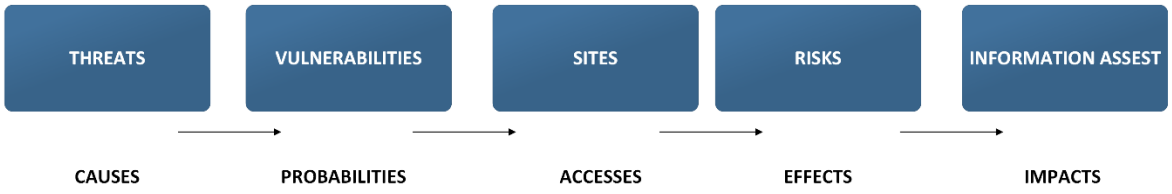

Figura 1. Elementos que impactan la información (Ortiz, 2022)

La Figura 1 muestra la secuencia de elementos a revisar para evitar acciones o fenómenos que alteren la información, piense en acciones que mitiguen las consecuencias de un mal impacto en los datos.

1.1.5. Evaluación de riesgos

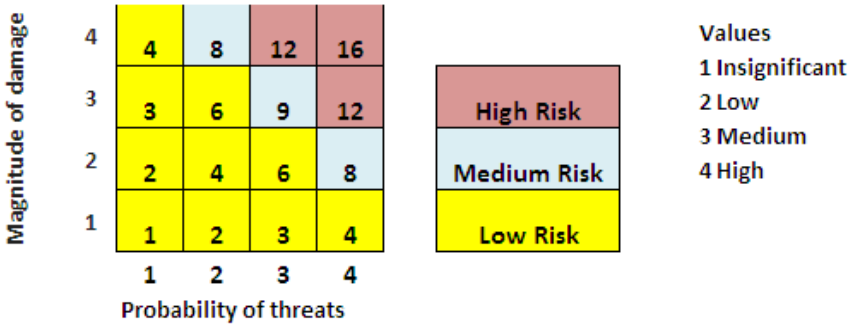

Figura 2. Grados de riesgo. (Ortiz, 2022)

La Figura 2 se utiliza para evaluar los riesgos, la probabilidad de amenazas y la magnitud del daño puede tener valores entre 1 (Insignificante) y 4 (Alto); para obtener el valor del riesgo se aplica la fórmula:

Riesgo = Probabilidad de amenaza * Magnitud del daño;

El resultado ubica el riesgo en uno de los rangos: Riesgo bajo está entre 1 y 6; El riesgo medio está entre 8 y 9; El riesgo alto está entre 12 y 16. Bajo se considera que el ataque está lejos, Medio se considera que el ataque sería a corto plazo, Alto se considera que el ataque no se puede prevenir.

3. RESULTADOS

Los resultados obtenidos en esta fase de investigación son:

- Prototipo de arquitectura distribuida
- Algoritmo genérico para mitigar los riesgos expresados en el diagrama de flujo
- Fórmula de probabilidad de ataque

2.1. Prototipo de arquitectura distribuida

En la Figura 3 se propone una arquitectura de 3 capas para una OP de Ecuador, la base de datos aplica arquitectura distribuida para garantizar una mejora en la gestión de la información.

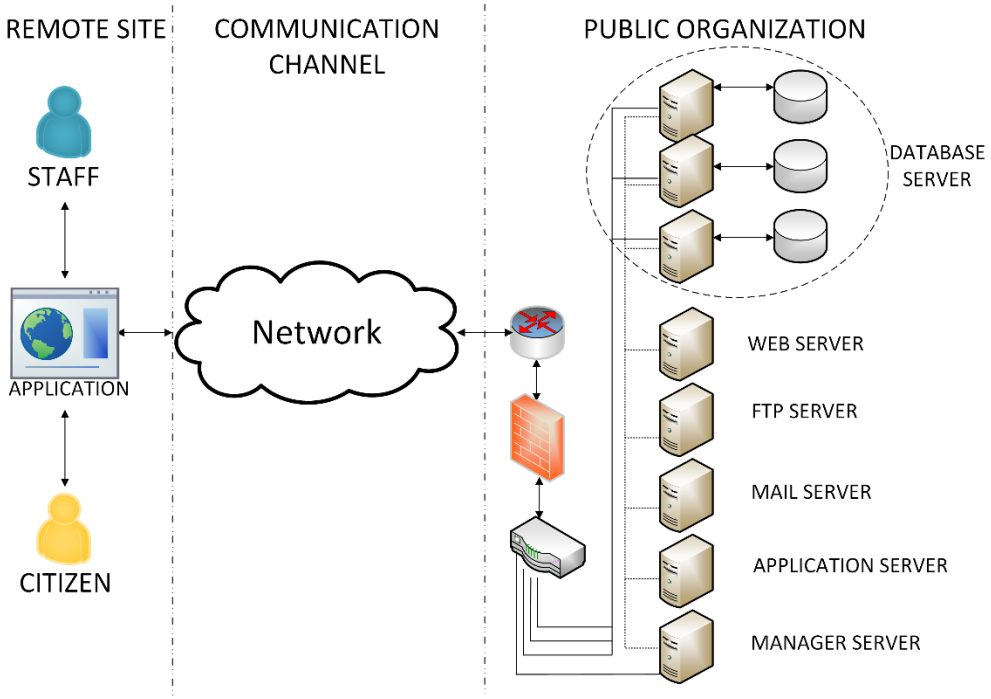

Figura 3. Arquitectura distribuida aplicada a base de datos. (Ortiz, 2022)

Figura 3, en la primera capa están los empleados públicos o ciudadanos que se conectan a través de una aplicación; en la segunda capa está el canal de comunicación es la red, celular, conexión inalámbrica. En la tercera capa está la red OP, tiene un enrutador, firewall, conmutador; el servidor administrador que administra la aplicación, el correo, el FTP, la web y la base de datos está conectado al conmutador. El concepto de arquitectura distribuida se

aplica a la gestión de datos para soportar concurrencia, escalabilidad, tolerancia a fallas y cierta flexibilidad.

2.2. Algoritmo genérico para mitigar los riesgos expresados en el diagrama de flujo

La metodología propuesta da como resultado un prototipo de algoritmo genérico sobre la secuencia de pasos que se deben seguir para mitigar los riesgos de seguridad de la información.

Al principio, se determinan y evalúan los Activos de Información de OP; identificar y evaluar las causas, probabilidades y accesos de OP que son los tres factores: amenazas, vulnerabilidades y sitios; esto nos ayuda a identificar y evaluar los posibles efectos para reducir, mitigar, controlar o monitorear los riesgos obtenidos; también sirve para planificar estrategias para asegurar la información.

El prototipo descrito en la Figura 4 se detalla de manera genérica para que funcione en una OP del Ecuador.

A continuación, los pasos del algoritmo:

Inicio

- Determinar los activos de información
- Evaluación
- Seleccione: Amenazas, Vulnerabilidades, Sitios
- Evaluar e identificar: Porcentaje de Amenaza, probabilidad y magnitud del daño
- Revisar los riesgos para poder asignar y evaluar el tipo de amenza
- Riesgo = Probabilidad de amenaza * magnitud del daño
- SI acepta el riesgo
- Entonces
    - Mitigar el riesgo
    - Monitorear el riesgo
- Caso contrario
    - Controlar el riesgo
- Final de condición

Fin

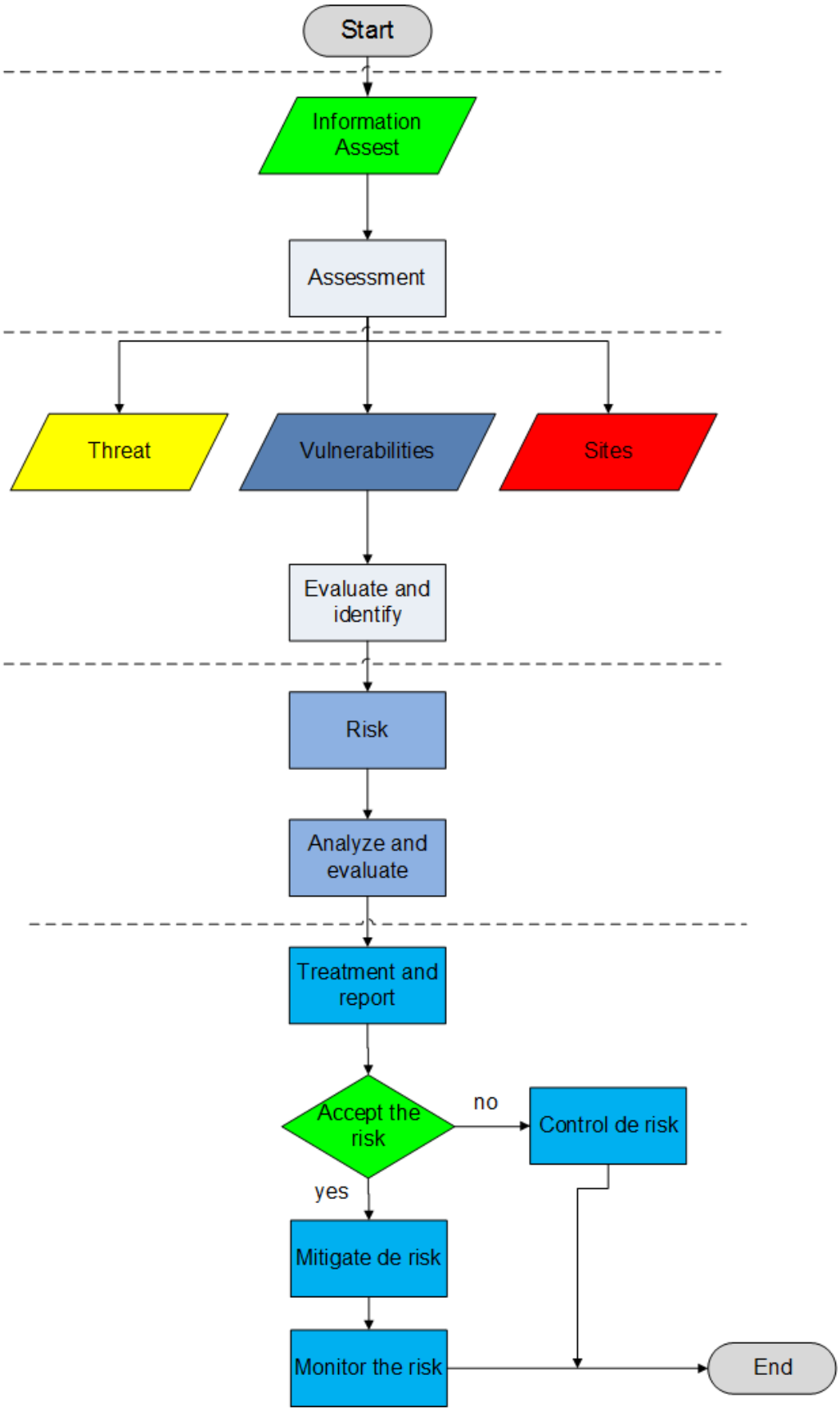

Figura 4. Elementos y actividades. (Ortiz, 2022)

El algoritmo propone; Primer nivel: tomar activos de información y valorarlos; Segundo nivel: Evaluar las amenazas, vulnerabilidades y sitios para determinar las causas, probabilidades y acceso en una OP; Tercer nivel: a partir del análisis de riesgo determinar los efectos para su evaluación; Cuarto nivel: Tratar los riesgos e informar, al decidir aceptar el riesgo se debe reducir y monitorear; de lo contrario solo controlarlo.

Caso Registro Civil del Ecuador:

Como ejemplo de dominio público y aplicación del algoritmo genérico se tomó el Registro Civil del Ecuador con una cantidad limitada de datos.

Primer nivel: se nombran cuatro activos

- Activos de información: Sitio Web, Servicios en Línea, Servicios Presenciales y Bases de Datos

Segundo nivel: se identificaron cuatro subelementos de cada elemento

- Amenazas: Falsificación de datos, Venta de información ciudadana, No encriptación de datos críticos, Falta de políticas
- Vulnerabilidades: Cambio de datos de ciudadanos, Robo de credenciales, Robo de identidad, Corrupción en servicios
- Sitios: Acceso Presencial o remoto, mala gestión de acceso, acceso no autorizado, puntos de acceso sin control; el Registro Civil cuenta con 221 puntos de atención a nivel nacional

La evaluación de riesgos ayuda a priorizar los riesgos para analizar las acciones a ejecutar; se valoró con 3 puntos a la Probabilidad de Amenazas

Los Activos de Información nombrados son de gran importancia; por lo que la Magnitud del Daño fue valorada con 4 puntos

Tercer nivel:

Los riesgos pueden afectar a la institución, aunque existan medidas; si el impacto es mayor al esperado, aumenta la probabilidad de afectación, se nombran tres riesgos:

- Modelo deficiente de la arquitectura del sistema
- Indisposición del sistema

- Información inconsistente

Con los riesgos identificados se evalúa la probabilidad del impacto, el personal que identifica los riesgos aplica su criterio de juicio experto

Se aplicó la fórmula de evaluación de riesgos:

Riesgo = Probabilidad de amenaza * Magnitud del daño;

El riesgo asociado a cada amenaza, vulnerabilidad o sitio da como resultado 12 puntos, que es riesgo alto

Se determinaron los siguientes impactos: Violación de datos, Pérdida o robo de datos, Actualizaciones no autorizadas, Infiltración del sistema, Fallas del sistema y La información se vuelve ilegítima

Cuarto nivel:

Mitigar el riesgo: está relacionado con la inversión de tiempo, personal y económica que la institución esté dispuesta a realizar; se nombran tres medidas:

- Evaluar el modelo de arquitectura para mejorar los accesos, procesos, funciones de la arquitectura global
- Preparar un sistema alternativo con su réplica sincronizada de la base de datos
- Las aplicaciones al sistema deben contar con el aval de un experto

Controlar el riesgo: analizar el correcto funcionamiento y aplicación de las medidas de protección y mejorar las deficiencias, registrar actividades, registrar eventos, dar seguimiento a las medidas; se nombran tres controles:

- Encontrar puntos arquitectónicos inaceptables y proponer mecanismos para su solución
- Determinar las condiciones y recursos necesarios para volver a instalar el sistema
- Identificar datos y procesos afectados, determinar cambios y aplicar

2.3. Fórmula de probabilidad de ataque

Se propone en la siguiente fórmula, para determinar la probabilidad de ataque:

$$PR = \frac{1}{(e-a)^{\frac{1}{2}}}$$

Variables:

e es el número de ejecuciones en un nodo

a es el número de acciones en un nodo

Para la presentación de la simulación el eje horizontal X es el tiempo de ejecución de 1 a 15 segundos; el eje vertical Y es el rango de acciones y ejecuciones; se genera un número aleatorio de acciones de usuario entre 1 y 10; se genera un número aleatorio de ejecuciones o instrucciones de usuario entre 1 y 10; el eje vertical Y secundario es para medir la probabilidad de ataque.

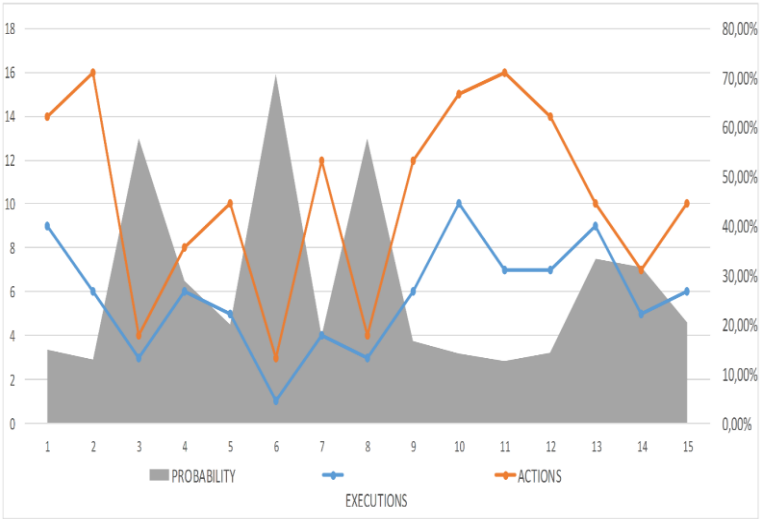

Figura 5. Simulación de probabilidad de ataque. (Ortiz, 2022)

En la primera simulación para cada nodo en 15 segundos. En el primer segundo la probabilidad es del 18%; en el duodécimo es del 17%; en el decimoquinto segundo es del

22%. La Figura 5 muestra que, entre más acciones o ejecuciones, la probabilidad es menor; hay una tendencia a la baja.

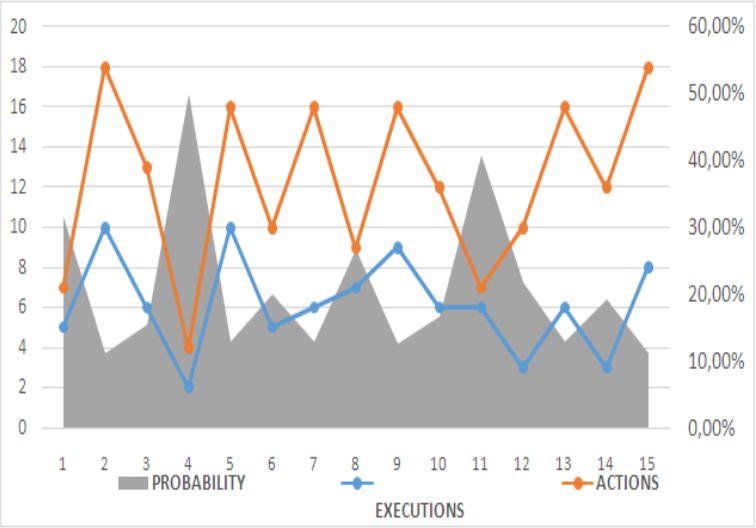

Figura 6. Second simulation of attack probability. (Ortiz, 2022)

En la segunda simulación para cada nodo en 15 segundos. En el primer segundo la probabilidad es del 31%; en el duodécimo es del 16%; en el decimoquinto segundo es del 11%. La Figura 6 muestra la tendencia de ataque a la baja.

Investigar	Mecanismo	Partes	Resultado
Nuestra propuesta	Algoritmo genérico	4 niveles	Riesgos puntuados
[2]	modelo de comparación	3 etapas	Puntuaciones
[3]	Flujo de riesgo	3 indicadores	Riesgos potenciales
[6]	modelo de probabilidad	1 cálculo	Valor del riesgo
[7]	Algoritmo mejorado	3 aspectos	Valores de predicción
[8]	Modelo de reducción de riesgos	3 pautas	Ponderaciones
[9]	Marco de riesgo	3 actividades	Gestión de riesgos
[10]	Matriz de riesgo	1 etapa	Probabilidad y consecuencias
[11]	Análisis de riesgo	4 pasos	Probabilidad
[14]	Marco de riesgo	1 etapa	Indicador de riesgo

Tabla 1. Comparaciones cualitativas de propuestas. (Ortiz, 2022)

En la Tabla 1 se presenta una comparación descriptiva de nuestra propuesta con las demás investigaciones revisadas, la propuesta es una alternativa para mitigar los riesgos y tomar decisiones para aumentar la seguridad.

4. DISCUSIÓN

El resultado obtenido como metodología para incrementar el nivel de seguridad de la información a través de un prototipo de arquitectura distribuida, algoritmo genérico y simulación depende mucho de la arquitectura de la OP y sus equipos.

La cantidad de amenazas, vulnerabilidades, sitios y riesgos depende de la cantidad de conexiones o nodos de la arquitectura distribuida.

El tamaño de la arquitectura influye en el número de accesos, lo que debe comprobarse al aplicar el algoritmo.

Se determina que para aplicar los algoritmos que protejan la información de las empresas públicas debe haber voluntad política y administrativa.

El algoritmo es independiente del número de capas que utiliza la arquitectura propuesta.

5. CONCLUSIÓN

Se concluyó que la propuesta generada es una alternativa para mantener la información de forma segura, con persistencia y disponible.

La metodología ayuda en los siguientes controles: acceso, contraseña, seguridad de internet, seguridad de aplicaciones, bases de datos y seguridad física; para garantizar la continuidad de la información.

El algoritmo fue simulado con datos de organización que utiliza bases de datos distribuidas, la simulación de la fórmula de probabilidad de ataque tiende a la baja.

Las estrategias que se tomen deben ser acordes a los riesgos obtenidos en la aplicación del algoritmo.

El acceso a información sensible influye en el costo económico, social o político, con impacto positivo o negativo en las autoridades de turno.

REFERENCIAS

[1] M. Mosleh, K. Dalili, and B. Heydari, “Distributed or Monolithic? A Computational Architecture Decision Framework,” IEEE Syst. J., vol. 12, no. 1, pp. 125–136, 2018.

[2] G. Wangen, “Information Security Risk Assessment: A Method Comparison,” Computer (Long. Beach. Calif)., vol. 50, no. 4, pp. 52–61, 2017.

[3] K. Zheng, B. Wu, F. Dai, and Y. Hu, “Exploring risk flow attack graph for security risk assessment,” IET Inf. Secur., vol. 9, no. 6, pp. 344–353, 2015.

[4] SENPLADES, “Estructura Organigrama,” Febrero, 2019. [Online]. Available: http://www.planificacion.gob.ec/wp-content/uploads/downloads/2019/03/SIE_OrganigramaFE_28022019-123.pdf.

[5] W. Al-Ahmad and B. Mohammed, “A code of practice for effective information security risk management using COBIT 5,” 2015 2nd Int. Conf. Inf. Secur. Cyber Forensics, InfoSec 2015, pp. 145–151, 2016.

[6] L. Liu, L. Liu, C. Huang, Z. Zhang, and Y. Fang, “A website security risk assessment method based on the I-BAG model,” China Commun., vol. 13, no. 5, pp. 172–181, 2016.

[7] S. Li, F. Bi, W. Chen, X. Miao, J. Liu, and C. Tang, “An improved information security risk assessments method for cyber-physical-social computing and networking,” IEEE Access, vol. 6, pp. 10311–10319, 2018.

[8] C. Montenegro, M. Murillo, F. Gallegos, and J. Albuja, “DSR Approach to Assessment and Reduction of Information Security Risk in TELCO,” IEEE Lat. Am. Trans., vol. 14, no. 5, pp. 2402–2410, 2016.

[9] M. Iorga and A. Karmel, “Managing Risk in a Cloud Ecosystem,” IEEE Cloud Comput., vol. 2, no. 6, pp. 51–57, 2015.

[10] P. H. Meland, I. A. Tondel, and B. Solhaug, “Mitigating risk with cyberinsurance,” IEEE Secur. Priv., vol. 13, no. 6, pp. 38–43, 2015.

[11] H. P. In, Y.-G. Kim, T. Lee, C.-J. Moon, Y. Jung, and I. Kim, “A Security Risk Analysis Model for Information Systems,” pp. 505–513, 2011.

[12] R. Oppliger, “Quantitative risk analysis in information security management: A modern fairy tale,” IEEE Secur. Priv., vol. 13, no. 6, pp. 18–21, 2015.

[13] J. R. C. Nurse, S. Creese, and D. De Roure, “Security Risk Assessment in Internet of Things Systems,” IT Prof., vol. 19, no. 5, pp. 20–26, 2017.

[14] L. Wilbanks, “Whats Your IT Risk Approach?,” IT Prof., vol. 20, no. 4, pp. 13–17, 2018.

[15] Zevallos, M. (2019) Modelo de gestión de riesgos de seguridad de la información: Una revisión del estado del arte. Revista Peruana de Computación y Sistemas, 2(2):43-60. http://dx.doi.org/10.15381/rpcs.v2i2.17103