Universidad Inca Garcilaso de la Vega

TESIS

“EVALUACIÓN CUANTITATIVA DE RIESGOS TECNOLÓGICOS DE CIBERSEGURIDAD EN UNA APLICACIÓN DE TRANSFERENCIAS DIGITALES EN UNA ENTIDAD FINANCIERA PERUANA, PERIODO 2021-2022”

PARA OPTAR EL TÍTULO DE

INGENIERO DE SISTEMAS Y CÓMPUTO

AUTOR

MANUEL MARTÍN PÉREZ CASTRO

ASESOR

MG. PAUL ALBERTO DÍAZ FLORES

LIMA, DICIEMBRE DE 2022

Visualizador de documentos

Turnitin Informe de Originalidad

Procesado el: 14-dic.-2022 9:30 a. m. -05
Identificador: 1981107707
Número de palabras: 11330
Entregado: 1

EVALUACIÓN CUANTITATIVA DE RIESGOS TECNOLÓGIC... Por Manuel Martín Pérez Castro

Índice de similitud	Similitud según fuente	
13%	Internet Sources:	13%
	Publicaciones:	0%
	Trabajos del estudiante:	6%

incluir citas | incluir bibliografía | excluir las coincidencias menores | modo: ver informe en vista quickview (vista clásica)

imprimir | actualizar | descargar

1% match (Internet desde 23-oct.-2022)
http://repositorio.uigv.edu.pe

1% match (Internet desde 16-abr.-2018)
http://repositorio.uigv.edu.pe

1% match (Internet desde 26-sept.-2022)
https://img1.wsimg.com/blobby/go/b653c9ee-535c-4528-a9c5-bb00166ad0dc/downloads/BID%20-%20OEA%20Reporte-Ciberseguridad-2020-riesgos-.pdf?ver=1601971104202

<1% match (Internet desde 14-nov.-2020)
http://repositorio.uigv.edu.pe

<1% match ()
De La Cruz Carrillo, Vanessa Carolina. "Evaluación del modelo de enseñanza blended learning y sus efectos en la calidadeducativa de la red de colegios innova schools en la sede San Miguel 2", Universidad Inca Garcilaso de la Vega, 2017

<1% match (Internet desde 08-abr.-2021)
http://repositorio.uigv.edu.pe

<1% match (Internet desde 16-nov.-2020)
http://repositorio.uigv.edu.pe

<1% match ()
Quichua Huayascachi, Catherine Noemí. "Grado de conocimiento del decreto legislativo N°1158 del cambio de denominación de la superintendencia nacional de aseguramiento en salud en los internos de la facultad de estomatología2018-II", 2018

<1% match (Internet desde 05-feb.-2022)
http://repositorio.uigv.edu.pe

<1% match (Internet desde 17-jul.-2021)
http://repositorio.uigv.edu.pe

<1% match (Internet desde 26-nov.-2020)
http://repositorio.uigv.edu.pe

<1% match ()
Cuba Padilla, Lourdes Ivonne. "Nivel de conocimiento de ética y deontología y su desarrollo en la práctica pre profesionalde los alumnos de internado en estomatología del hospital militar central", Universidad Inca Garcilaso de la Vega, 2018

<1% match ()
Vidal Navarrete, Jose Luis. "El uso de las nuevas tic's de la plataforma virtual y la retención de los alumnos de contabilidad a distancia de la Universidad Inca Garcilaso de la Vega", Universidad inca Garcilaso de la Vega, 2018

<1% match (Internet desde 01-nov.-2022)
https://repositorio.ucv.edu.pe/handle/20.500.12692/87129?show=full

<1% match (Internet desde 05-oct.-2022) https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/96925/Mallqui_MAJDM-SD.pdf?isAllowed=y&sequence=1

<1% match (Internet desde 13-may.-2022)
https://www.coursehero.com/file/p6ko1lp/cedimiento-que-permita-ayudar-a-los-usuarios-a-determinar-qu%C3%A9- tipo-de/

<1% match (trabajos de los estudiantes desde 14-oct.-2022)Clase:
CIENCIAS ADMINISTRATIVA
Ejercicio: TESIS ADMINISTRACIÓN
Nº del trabajo: 1925254812

<1% match (trabajos de los estudiantes desde 27-mar.-2019) Submitted to Universidad Inca Garcilaso de la Vega on 2019-03-27

<1% match (trabajos de los estudiantes desde 26-may.-2022) Submitted to Universidad Inca Garcilaso de la Vega on 2022-05-26

<1% match (Internet desde 14-nov.-2022)
https://repositorio.uchile.cl/bitstream/handle/2250/180169/Guia-de-implementacion-de-un-programa-de-gestion-de-riesgos-de-ciberseguridad-en-entidades-de-intermediacion-financiera.pdf?isAllowed=y&sequence=1

<1% match (Internet desde 01-ene.-2022)
https://repositorio.autonoma.edu.pe/bitstream/handle/20.500.13067/1529/Riojas%2c%20Adriana%20y%20Huisarayme%2c%20Favio.pdf isAllowed=y&sequence=1

DEDICATORIA

A Dios, por darme la salvación para concluir esta etapa,

a mi esposa Diana, por su ayuda y motivación incondicional,

a mis hijos Génesis & Ethan, por las fuerzas que me dan para siempre ser ejemplo y tener perseverancia.

AGRADECIMIENTOS

A Dios, por darme un día más de vida,

a mis padres Víctor y Jewel, por su apoyo y respaldo para terminar esta etapa universitaria.

LISTA DE FIGURAS

ÍNDICE

RESUMEN

La presente Tesis tuvo como objetivo analizar si una evaluación cuantitativa de riesgos tecnológicos de ciberseguridad ayudó en la toma de decisiones para la gestión del riesgo y de la ciberseguridad a una entidad financiera peruana, la cual dispone a sus clientes, una aplicación para que realicen transferencias digitales, pararealizar esto, se seleccionó el riesgo de “Actividades maliciosas por un usuario privilegiado”.

El método que se usó para la recolección de la información fue el uso de reuniones y entrevistas con los principales stakeholders de la entidad financiera, de modo que se identificaron las principales variables para desplegar la evaluación cuantitativa por medio de la metodología FAIR, dando como resultado, los valores de la ejecución del modelo matemático de Monte Carlo en su simulador web FAIR-U.

Las principales conclusiones que se obtuvieron de toda esta investigación fueron que una evaluación cuantitativa arroja más información probabilística para gestionar de una manera más eficiente los riesgos de ciberseguridad y los controles tecnológicos en comparación a una evaluación cualitativa.

Así mismo, se demostró de una manera más visual y gráfica la exposición monetaria a la cual está expuesta la entidad financiera, permitiendo a los usuarios finales tomar decisiones a corto, mediano y largo plazo para cerrar brechas de seguridad.

Palabras clave: evaluación cuantitativa, riesgos, ciberseguridad, FAIR.

ABSTRACT

The objective of this Thesis was to analyze if a quantitative evaluation of technological cybersecurity risks helped in decision-making for risk management and cybersecurity to a Peruvian financial institution, which provides its clients with an application for them to carry out digital transfers, to do this, the risk to “Malicious activities by a privileged user” was selected.

The method used to collect the information was the use of meetings and interviews with the main stakeholders of the financial institution, this way, the main variables were identified to deploy the quantitative evaluation through the FAIR methodology, resulting in, the values of the execution of the Monte Carlo mathematical model in its FAIR-U web simulator.

The main conclusions that were obtained from all this research were that a quantitative evaluation gives more probabilistic information to manage cybersecurity risks and technological controls in a more efficient way compared to a qualitative evaluation.

Likewise, it was demonstrated in a more visual and graphic monetary exposure, to which the financial institution is exposed allowing end users to make decisions in the short, medium and long term to close security gaps.

Keywords: quantitative evaluation, risks, cybersecurity, FAIR.

INTRODUCCIÓN

En la actualidad estamos viviendo en la tercera revolución industrial donde la informática y el uso de la tecnología de la información han ayudado a que las cosas vallan más rápidas y eficientes, además de esto, la aparición de la pandemia del Covid-19, ha acelerado la digitalización de varios procesos manuales y presenciales, alcanzando a todo tipo de empresa, desde la más pequeña hasta la más grande, incluyendo el sector financiero.

Si bien, la banca a nivel mundial ha sido beneficiada con toda esta aceleración tecnológica para llegar a sus clientes, esto también conllevó a un crecimiento en los delitos cibernéticos, colocando mayor atención en las aplicaciones que se utilizan para realizar trasferencias de dinero de manera digital.

Es en este contexto que la gestión oportuna de todo riesgo relacionado con delitos informáticos, brechas de seguridad, vulnerabilidades y ciberseguridad ha tomado mayor relevancia, al punto que se ha convertido en la principal arma de defensa de las entidades financieras para hacer frente a los nuevos retos digitales.

Conociendo esta necesidad, nos toca escoger la mejor metodología para evaluar de una manera eficiente todo lo que se viene por delante, es en este punto donde se desarrolla la presente investigación, retando a los modelos actuales para la gestión del riesgo, por medio de la ejecución de una evaluación cuantitativa bajo la metodología FAIR, de modo que terminó influenciado en la toma de decisiones de la entidad financiera para la gestión de sus riesgos de ciberseguridad y sus controles tecnológicos, esto debido a que se les presentó a los usuarios finales, la exposición monetaria actual a la cual están expuestos para el riesgo de “Actividades maliciosas por un usuario privilegiado” y la cantidad y periodicidad promedio de ataques probables a su aplicativo de transferencias digitales.

Una vez identificado el riesgo residual, se mostró por medio de la misma metodología, cuánto podrían invertir en implementar los planes de acción propuestos para mitigar el riesgo identificado y cuanto cerraría la brecha de seguridad actual.

Todos estos resultados se contrastaron con la ejecución de una evaluación cualitativa con la metodología de CVSS, para el mismo riesgo, dando como resultado, que la evaluación cuantitativa aporta más información numérica y estadística para la correcta toma de decisiones por parte de los usuarios finales de la entidad financiera.

A continuación, se detalla lo investigado en cada capítulo de la tesis:

CAPÍTULO I: FUNDAMENTOS TEÓRICOS DE LA INVESTIGACIÓN. En este capítulo se tocaron conceptos básicos como la importancia que tiene la ciberseguridad hoy en día, qué se considera una evaluación cuantitativa y los riesgos tecnológicos en la actualidad; además de esto, se exploraron las principales investigaciones relacionadas con esto temas, así como la explicación de los principales conceptos utilizados en esta Tesis.

CAPITULO II: EL PROBLEMA, OBJETIVOS, HIPOTESIS Y VARIABLES. En este capítulo, se detalló a profundidad cuál fue el principal problema que vamos a abordar por medio del desarrollo del objetivo principal, “Analizar si la evaluación cuantitativa de riesgos tecnológicos de ciberseguridad en una aplicación de trasferencias digitales influye en la toma de decisiones en una entidad financiera peruana en el periodo 2021-2022.”, terminando en la definición de las hipótesis a validadas más adelante.

CAPITULO III: MÉTODO, TÉNICA E INSTRUMENTOS. En este capítulo, se identificó el riesgo tecnológico que se utilizado para el desarrollo de la tesis basado en el OWASP Mobile Top 10, así mismo, se definió que la técnica de recolección de datos sería por medio de reuniones y entrevistas, de modo que finalmente, se procese toda la información en la web de FAIR-U.

CAPITULO IV: PRESENTACIÓN Y ANÁLISIS DE LOS RESULTADOS. En este capítulo, se ejecutaron tanto la evaluación cuantitativa como la cualitativa, con la metodología FAIR y CVSS correspondientemente, al finalizar esto, se contrastaron y validaron las hipótesis planteadas con los resultados finales.

CAPITULO V: CONCLUSIONES Y RECOMENDACIONES. En este capítulo, se concluyó que la evaluación cuantitativa con la metodología FAIR influenció y ayudó a la entidad financiera a tomar decisiones más precisas para mitigar el riesgo identificado en su aplicativo de trasferencias digitales, en comparación con la evaluación cualitativa con la metodología CVSS.

CAPITULO I: FUNDAMENTOS TEÓRICOS DE LA INVESTIGACIÓN

1.1. Marco Teórico

1.1.1. La importancia de la Ciberseguridad

Según (Kaspersky, 2020), el término de ciberseguridad se puede definir como las técnicas utilizadas para proteger los componentes y activos tecnológicos de una organización tales como computadoras, servidores, móviles y redes de ataques maliciosos, teniendo entre las categorías más comunes:

- La seguridad de red para la protección de la red informática de cara a intrusos internos o externos.

- La seguridad de la información para la privacidad de la información, cuidando la confidencialidad, integridad y disponibilidad.

- La continuidad del negocio de cara a la pronta respuesta ante incidentes de ciberseguridad, de modo que se pueda restaurar lo antes posible y de la manera más eficiencia el activo afectado.

- La seguridad de las aplicaciones dedicada a mantener seguro el software y hardware en todas sus etapas de despliegue.

En relación a la ciberseguridad en América Latina, según (Kaspersky, 2021), menciona que durante los primeros ocho meses del 2021 aumentaron en un 24% los ciberataques, teniendo como principal vector de ataque el home office y la piratería, llegando a generar un promedio de 35 ataques por segundo.

La investigación también reflejó una tendencia importante en relación al incremento de ataques cibernéticos en los países latinoamericanos en relación al año

anterior, en el top 5 lo está liderando Ecuador con un aumento del 75%, seguido por Perú con 71%, Panamá con 60%, Guatemala con 43% y Venezuela con 29%.

Dentro de los principales ataques realizados, se encuentra el robo de tarjetas de crédito por medio adware (códigos embebidos en archivos como PDF) y troyanos web, lo cual hace que se genere un código malicioso en las webs de un e-commerce o en la de un banco, de modo que roba la información cada vez que un usuario ingresa sus credenciales a estas páginas.

Otro ataque muy común en América Latina este 2021 es el Phishing, especialmente desde equipos móviles por medio de ataques de Smishing (ataques de ingeniería social por SMS) o del envío de URL Shortener (direcciones web acortadas), todo esto con la finalidad de robar datos personales y bancarios de las personas.

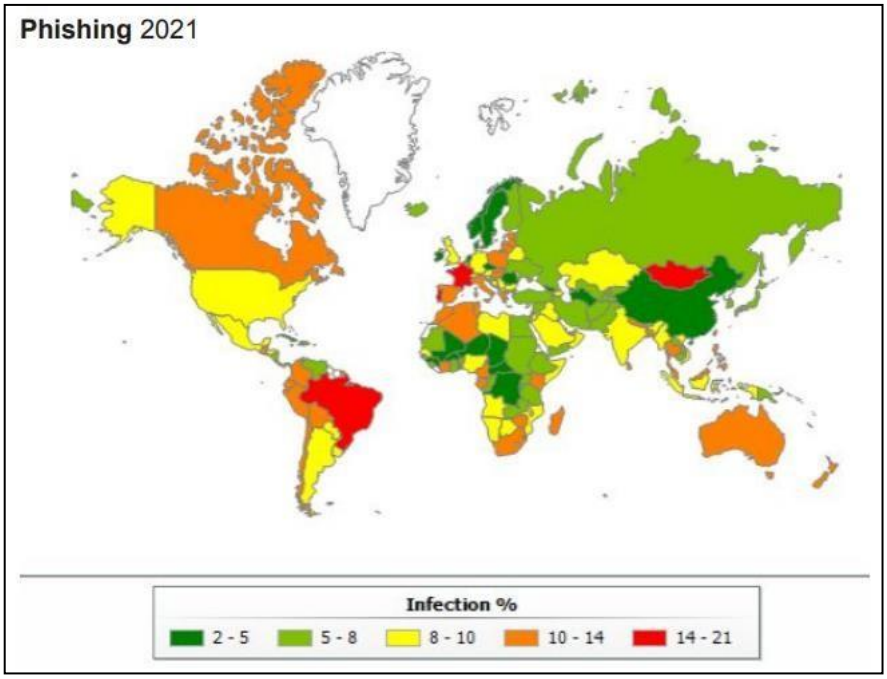


Figura 1. Incremento de Phishing en América Latina (Kaspersky, 2021)

1.1.2. ¿Qué es una Evaluación Cuantitativa?

De acuerdo con (Moral-Arce, 2014), comenta que una evaluación cuantitativa aplica métodos cuantitativos por medio de datos estadísticos hacia los objetivos que se desean estudiar, de modo que los instrumentos utilizados, sean independientes de sesgos del evaluador, dando como resultado la ayuda necesaria a los actores finales para tomar decisiones correctas.

Debido a que el resultado de la evaluación cuantitativa serán datos numéricos, se recomienda que la comunicación con los actores finales sea por medio de un modelo visual, utilizando marcos lógicos con formatos esquemáticos.

Continuando con la investigación de (Moral-Arce, 2014) mencionan que existen varios tipos de diseños diferenciados para realizar evaluaciones cuantitativas, motivo por el cual, es necesario seleccionar procedimientos que ayuden a los usuarios finales a determinar cuál es el mejor diseño con relación a la viabilidad y los costos relacionados, los distintos diseños posibles son (Moral-Arce, 2014, página 29)":

1. Diseño experimental. experimento aleatorio.
2. Diseño de regresión en discontinuidad.
3. Diseño de construcción de grupos de control para emparejamiento.
4. Diseño de series temporales.
5. Diseños de identificación y eliminación causal exhaustiva.
6. Diseño de opinión de expertos.
7. Diseño de opinión de informantes clave.

Debido a esta variedad, se establece el siguiente diagrama para diferenciar los distintos enfoques según la necesidad de los usuarios.

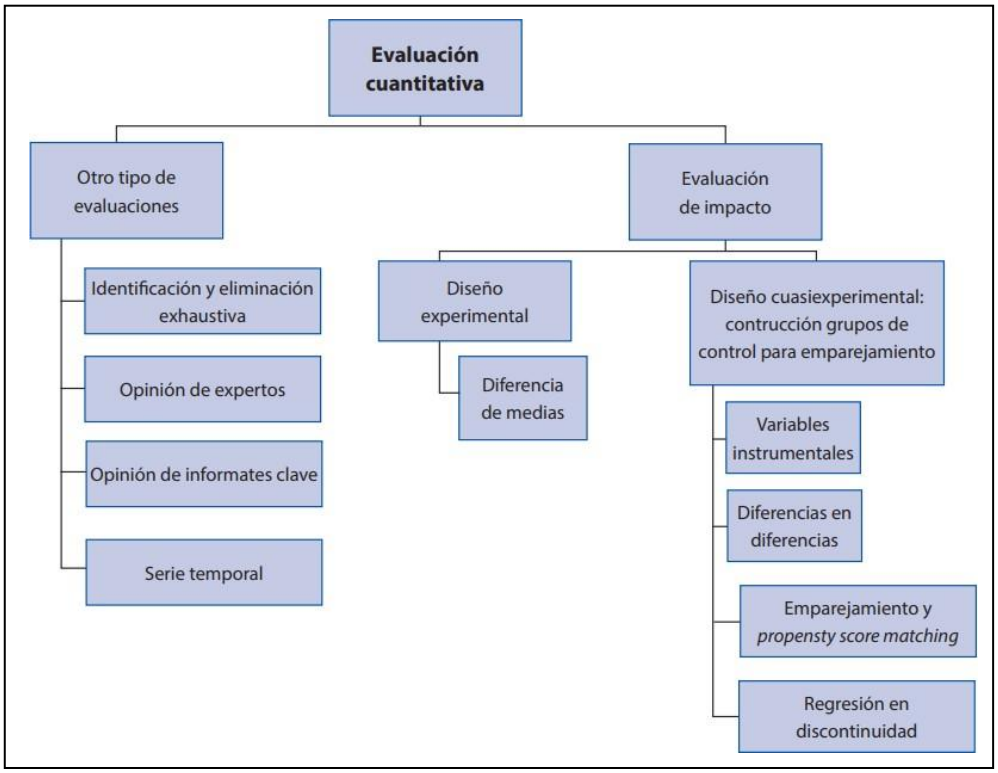


Figura 2. Diagrama de las diferentes evaluaciones cuantitativas (Moral-Arce, 2014)

1.1.3. Los riesgos tecnológicos en la actualidad

La correcta gestión de los riesgos tecnológicos ayuda a las empresas a tomar mejores decisiones en relación a su seguridad de la información, según (NCSC, 2019), menciona que la mayoría de organizaciones ya vienen evaluando y gestionando sus riesgos tecnológicos, sin embargo, en muchos de los casos, lo hacen sólo para cumplir con las obligaciones de los entes reguladores, demandas de cliente o por temas legales, lo cual puede llevar a tener prácticas débiles o una falsa sensación de seguridad, exponiendo a las organizaciones a problemas potenciales.

Como principal proceso para una correcta gestión de riegos tecnológicos es la integración con el enfoque organizacional, de modo que pueda apoyar a la organización a tener correctamente identificado las vulnerabilidades de ciberseguridad, sin bloquear las principales actividades del negocio ni generar un costo desproporcionado para la atención de los planes de acciones propuestos.

Sumado a esto, según (NCSC2, 2019), recomienda la implementación de líneas de defensas para proteger los activos más críticos, de modo que complemente a la gestión de los riesgos, al realizar esta buena práctica de seguridad, ayudará a reducir los incidentes más sensibles por medio de la ejecución de controles, estos a su vez validados por marcos como la ISO/IEC 27002 y la NIST.

Figura 3. 10 Steps to Cyber Security (NCSC2, 2019)

1.2. Investigaciones

En la investigación de (Gumucio, 2021), “Guía de implementación de un programa de gestión de riesgos Ciberseguridad en entidades de intermediación financiera”, tesis para el grado de Magister en la Universidad de Chile, menciona la importancia que tiene la transformación digital para las entidades financieras en el mundo de hoy, esto debido a que abre la posibilidad de estar más cerca de los clientes para ofrecer mayor cantidad de productos, sin embargo, el autor menciona que en Latinoamérica, no se tiene una legislación madura en relación a la Ciberseguridad,

por este motivo, realiza el trabajo de implementar una guía gerencial para la gestión de los riesgos de Ciberseguridad de forma integral, para esto, usa como base el marco NIST (National Institute of Standars and Technology) en conjunto con la medición de la CVSS (Common Vulnerability Scoring System), todo eso permite gestionar correctamente los riesgos de ciberseguridad, aspi como fortalecer el pilar digital en la organización.

Así mismo, en la investigación de (Vásquez, 2021), “Ciberseguridad basada en analítica para bases de datos Oracle”, tesis para Maestría en la Fundación Universitaria Konrad Lorenz de Bogotá, Colombia, menciona la problemática que se tiene en la creciente exposición de riesgos de seguridad en las organizaciones debido a la adquisición constante de nuevas tecnologías, lo cual produce una falta del seguimiento de las brechas de seguridad, por tal motivo, el trabajo realizado, busca clasificar los niveles de riesgo expuesto, así como la automatización de controles en bases de datos Oracle, para realizar esto, el autor se apoya en las mejores prácticas de seguridad para crear una línea base de modo que se sobre esta, se procesen todos los datos obtenido para que finalmente se crucen con la NVD (NationalVulnerability Database).

En la misma línea, la investigación de (Reinoso, 2017), “Análisis y evaluación de riesgos de seguridad informática a través del análisis de tráfico en redes de área local.”, trabajo de titulación en la Escuela Politécnica Nacional de Quito, Ecuador, identifica la necesidad de evaluar los riesgos de seguridad informática por medio del análisis del tráfico local de la red, para esto, desarrolló un modelo mezclando metodologías de riesgos (NIST SP800-30, OCTAVE y MAGERIT) con herramientas de sniffer de red (WIRESHARK, TCPDUMP y CAPSA PACKET SNIFFER) y formularios específicos creados para cada una de las seis fases del modelo propuesto, con lo cual se validó su eficacia al implementarlo en un caso de estudio en un sistema de TI de una institución pública del país.

En referencia al territorio nacional, tenemos la investigación de (Huaylla y Vargas, 2022), “Gestión de tecnologías de información y comunicación y los procesos de seguridad informática en el gobierno regional de Apurímac”, trabajo de titulación de la Universidad Tecnológica de los Andes de Abancay-Apurímac, donde utilizan el método probabilístico y aleatorio simple para la prueba del coeficiente de correlación “r” de Pearson (índice para medir el grado de relación de dos variables) entre lo concerniente a las tecnologías y la seguridad de información en el ente estatal, para esto, se tomaron en cuenta las variables de la infraestructura/arquitectura tecnológica, recursos humanos y los principales procesos de negocio, dando una respuesta positiva en relación a las definiciones de estrategias para enfrentar riesgos de seguridad que puedan impactar la confidencialidad, integridad y disponibilidad de los sistemas , así como el cumplimiento de políticas gubernamentales en relación a los sistemas de información.

En la investigación de (Manrique, 2022) “Modelo de ciberseguridad para mejorar la gestión de tecnología de la información de un Instituto Superior Tecnológico público”, trabajo para Maestría de la Universidad Cesar Vallejo en Lima-Perú, también analiza la importancia que tiene la gestión de la ciberseguridad en el proceso de transformación digital en una entidad estatal, proponiendo un enfoque cualitativo por medio de entrevistas semiestructuradas y análisis documental a tres expertos en ciberseguridad especializados en el sector de educación superior, para realizar esto, se basa en la Norma ISO/IEC27032, teniendo como finalidad la aplicabilidad de las buenas prácticas de la norma en lo relacionado a controles, políticas y mecanismos para mitigar riesgos de seguridad, cabe mencionar, que en la actualidad, los institutos públicos del Perú aún no realizan de manera integral este tipo de implementaciones.

Finalmente, en la investigación de (Cornejo y Lezama, 2022) “Propuesta de sistema de gestión de seguridad de la información para garantizar la seguridad de la información en la sub gerencia de tecnología de la información del Gobierno Regional de la Libertad”, trabajo para título profesional en la Universidad Cesar Vallejo en Trujillo-Perú, proponen mejorar el nivel de integridad de la información sobre el personal de tecnologías de información del Gobierno Regional por medio de la

implementación de las buenas prácticas de seguridad basados en la NTP-ISO/IEC 27001 y midiendo los resultados con la prueba de normalidad de Shapiro-Wilk (contraste de un conjunto de datos basados en un población normalmente distribuida), luego de sus investigación, se notó un aumento de más del 50% en relación a la seguridad de información.

1.3. Marco Conceptual

- Control de Acceso

Procedimientos y reglas que controlan los accesos a los sistemas de información, recursos tecnológicos e instalaciones físicas.

- Amenaza Persistente Avanzada (APT)

Ataque donde se tiene altos niveles de conocimiento en relación a los recursos tecnológicos, los cuales permiten crear ataques repentinos durante un periodo largo de tiempo y adaptar el ataque a los controles de defensa sin que el objetivo se dé cuenta.

- Adware

Código malicioso que muestra, reproduce o descarga anuncios sin el consentimiento del usuario, después de instalar o usar un software malicioso.

- Situación de alerta

Periodo de tiempo donde un procedimiento de emergencia supera el umbral de servicio donde la interrupción no se resuelve.

- Seguridad de la aplicación

Son todos los aspectos de seguridad que tiene la aplicación, teniendo como principales puntos la gestión de los roles, responsabilidades y pistas de auditoría.

- Activo

Componente o recurso tecnológico, tangible o intangible, de alto valor para la organización.

- Ataque

Método utilizado para entregar un exploit a un objetivo por medio de un vector de ataque.

- Vector de ataque

Ruta utilizada por un atacante para obtener acceso al objetivo (activo).

- Gestión del cambio

Enfoque holístico y proactivo para gestionar transiciones organizacionales de un estado a otro, considerando desarrollo de sistemas, stakeholders, políticas, procedimientos, recursos humanos, infraestructura, entre otros.

- Confidencialidad

Restringe los accesos a la divulgación de la información de modo que se proteja la privacidad.

- Control

Políticas, procedimientos, buenas prácticas, directrices o estructuras organizaciones que tienen como finalidad salvaguardar los activos de la organización.

- Marco de control

Conjunto de controles que facilitan el cumplimiento de la seguridad de los activos evitando de este modo pérdidas financieras.

- Ataque de denegación de servicio (DoS)

Ataque informático que tiene como finalidad detener por completo un servicio por medio de la saturación de solicitudes.

- Frecuencia

Medida de ocurrencia de eventos durante un periodo de tiempo en específico.

- Gobierno de TI

Visión de gobierno que tiene como finalidad asegurar la información y los componentes tecnológicos de la organización de modo que se respalden y protejan, cumpliendo la estrategia y objetivos empresariales.

- Hacker

Individuo que intenta obtener accesos no autorizados a los activos tecnológicos de la organización.

- Impacto

Magnitud de la pérdida económica resultante de un ataque exitoso.

- Incidente

Evento que no forma parte del servicio normal de la organización el cual puede causar una reducción o interrupción del servicio.

- Integridad

La capacidad para proteger el activo de la información en contra de una modificación o destrucción indebida.

- Atacante interno (insider)

Usuario autorizado para el uso de la aplicación o sistema informático que abusa de sus privilegios para el beneficio propio.

- Malware

Software malicioso que infecta sistemas informáticos sin el consentimiento del propietario, teniendo como único propósito infiltrar, dañar u obtener información sensible, por ejemplo, troyanos, spyware, adware, etc.

- Ataque de Man in the middle

Ataque informático donde el atacante intercepta la comunicación entre dos partes para luego reemplazar la trama de comunicación.

- Política

Documento formal realizado por la organización, el cual tiene como objetivo orientar la toma de decisiones presentes y futuras de modo que estén alineadas con la filosofía, objetivos y principios de la organización.

- Riesgo residual

Es el riesgo que se tiene con el despliegue de los controles actuales.

- Resiliencia

Capacidad que tiene un sistema para resistir fallas y/o ataques de modo que se recupere rápidamente de cualquier interrupción.

- Evaluación de riesgos

Proceso por el cual se estima la criticidad, planes de acción, controles, responsables, vector de ataque e impacto de los escenarios de riesgo.

- Aplicación de transferencias digitales

Es un software gestionado por una entidad financiera, pudiendo ser de desarrollo propio o tercero, el cual tiene como principal objetivo permitir a los clientes realizar transferencias digitales de dinero desde su celular entre cuentas del mismo banco o a terceras personas.

Cabe mencionar que el desarrollo y funciones que tiene este tipo de aplicaciones están constantemente reguladas por las entidades como la SBS, cumpliendo estándares internacionales como PCI.

- Apetito de riesgo

Es el umbral que tiene una organización para aceptar o no un riesgo.

- Concientización de seguridad

Medidas que realiza la organización para que los empleados que tiene accesos a información sensible entiendan los niveles apropiados de seguridad que deberán aplicar en su trabajo diario, así como las responsabilidades que tiene de cara a la seguridad de los activos.

- Incidente de seguridad

Serie de eventos inesperados que involucran uno o más ataques en uno o más activos tecnológicos.

- Sniffing

Ataque en el cual se interceptan o monitorean datos en tránsito.

- Ingeniería social

Ataque basado en engañar a usuarios por medio de la suplantación del sitio destino, tiene como finalidad revelar información sensible.

- Spyware

Software espía que tiene como finalidad rastrear las acciones que realiza un usuario en un dispositivo digital (como por ejemplo en una laptop, computadora o móvil) de modo que pase esta información a terceros, todo esto sin el consentimiento de las personas.

- Inyección SQL

Ataque en el cual se busca ingresar sentencias SQL a los sistemas, sin las validaciones adecuadas de seguridad, tiene como finalidad obtener información de repositorios de información como bases de datos de manera no previstas en el diseño original de la aplicación.

- Muestreo estadístico

Método que realiza cálculos matemáticos y probabilidades en base a una selección de una porción de una población, todo esto con la finalidad de tener inferencias sólidas y científicas de lo que se está evaluando.

- Amenaza

Cualquier causa potencial no deseada que puede resultar en daños en los activos de la organización.

- Vulnerabilidad

Una debilidad identificada en el diseño, despliegue, operación o control interno que podría desencadenar en una exposición del sistema a amenazas y futuros ataques.

- CVSS (Common Vulnerability Scoring System)

Es una metodología gratuita y libre que tiene como finalidad valorar la criticidad de las vulnerabilidades de seguridad de información y ciberseguridad en las plataformas tecnológicas, por medio de la asignación de puntajes (del 0 al 10) según la gravedad que tenga sobre los recursos impactados. La versión que se utilizará para esta investigación será la 3.1.

- Mapa de calor de riesgos

Es una herramienta tecnológica desarrollada por lo general en un Excel o en una plataforma especializada que tiene como principal objetivo dar conocimiento y entendimiento de los riesgos específicos que se están ejecutando, esto con la finalidad que se tenga bien identificado el perfil y apetito del riesgo de la organización.

Por lo general, se suele graficar por medio de una matriz bidimensional, considerando al eje X la probabilidad de ocurrencia del riesgo y el eje Y el impacto económico, así mismo, se suele determinar los niveles de riesgos por medio de colores, lo cual ayuda de manera visual identificar en que escenario se encuentra el riesgo.

- Actividades maliciosas

Se considera una actividad maliciosa a toda acción que ejecute un usuario interno o externo en la infraestructura y/o componentes tecnológicos de la organización, teniendo como finalidad impactar la confidencialidad, integridad o disponibilidad, del activo tecnológico o de la información, todo esto para tener beneficios económicos fraudulentos, cabe mencionar que estás acciones pueden ser de manera manual, semiautomatizadas o completamente automatizadas.

- Usuarios privilegiados

Todo usuario que tenga un perfil administrador y/o de gestor de un proceso, herramienta o componente tecnológico se considera como privilegiado, esto también conlleva a que la relación laboral con estos usuarios sea de suma confianza, debido a que tendrán accesos y permisos especializados, en mucho de los casos, afectando a toda la organización o a la herramienta bajo custodia.

- Líderes técnicos

Son todos los usuarios que tienen un perfil técnico y administren todo el ciclo de desarrollo de la aplicación, de modo que tienen la responsabilidad de todo lo que suceda en el componente tecnológico, también tienen pleno conocimiento de cada función y proceso a nivel front end, back end y middelware.

- Stakeholders

Es todo usuario que tiene interacción con la herramienta o componente tecnológico, tanto desde la parte funcional y comercial hasta la parte técnica y de soporte, estos usuarios son de suma importancia, debido a que tienen todo el conocimiento necesario para saber cuáles son los principales procesos, ayudándonos en un futuro, identificar el alcance que tiene la posible materialización de los riesgos a evaluar.

- Product Owner

Es el responsable y dueño principal de la herramienta o componente tecnológico, es el encargado de que todos los stakeholders interactúen de manera ordenada y organizada, de modo que la operativa no se vea impactada, además vela por las nuevas funciones a desarrollar validando que cumplan con las expectativas deseadas por la organización incluyendo la parte de seguridad de la información, ciberseguridad, presupuestos, indicadores, etc.

- FAIR (Factor Analysis of Information Risk)

Es una metodología cuantitativa basada en el ingreso de datos y la ejecución del modelo matemático de Monte Carlo, la cual tiene como principal objetivo,

gestionar los riesgos de ciberseguridad de cualquier organización de modo que se tengan los posibles costes económicos por eventos.

- Risklens

Es una empresa de Estados Unidos dedicada a ayudar e implementar soluciones de gestión de riesgos de ciberseguridad a distintas organizaciones por medio de su propio estándar FAIR.

- Fair-U

Es la plataforma web gratuita que dispone la empresa Risklens para ejecutar la metodología FAIR, en la cual se puede ingresar todos los parámetros necesarios para la correcta ejecución del modelo matemático de Monte Carlo, teniendo como finalidad mostrar los resultados de las pérdidas económicas estimadas.

- Frecuencia de Evento de Amenaza (TEF - Threat Event Frequency)

Se considera como el indicador de la frecuencia probable con el que un atacante intentará causar daño al activo tecnológico, en un tiempo determinado.

- Frecuencia de Evento de Pérdida (LEF – Loss Event Frequency)

Se considera como el indicador de la frecuencia probable con el que un atacante causará daño al activo tecnológico, en un tiempo determinado.

- Vulnerability (Eficiencia)

Se considerará como el indicador de eficiencia que tienen los controles tecnológicos de cara al riesgo, de modo que se identifica la eficiencia mínima, promedio y máxima de los mismos, esto será importante para analizar en dónde y que planes de acción se deberán implementar para mitigar el riesgo.

- Magnitud de pérdida

Es el total de pérdidas económicas estimadas promedio que podría suceder tras la materialización de un riesgo en el siguiente año, este valor es el resultante de la ejecución de la metodología FAIR, el cual no solo sirve para que la organización vea la exposición que tiene actualmente, sino que también ayuda a la gestión del riesgo de una manera mejor.

- Confidence (confianza)

Según la metodología de FAIR, la confidence o confianza, se refiere a la certeza que tiene el evaluador en referencia a la información recolectada para el ingreso inicial de los parámetros, la cual tiene tres niveles, bajo cuando se tiene poca certeza, medio cuando es regular la certeza y alto cuando es garantizada y fidedigna la información recolectada.

- Evasión (Categoría del control)

Es la primera categoría de controles tecnológicos que tiene la metodología FAIR antes que el atacante tenga acceso al activo, su finalidad es evitar que entren en contacto con los activos, por ejemplo, segmentación de redes, seguridad física, etc.

- Disuasión (Categoría del control)

Es la segunda categoría de controles tecnológicos que tiene la metodología FAIR una vez que el atacante ha establecido algún contacto con el activo, su finalidad es evitar que los atacantes ejecuten eventos de amenazas, por ejemplo, monitoreo de redes, cámaras de seguridad, enmascaramiento de datos, etc.

- Resistencia (Categoría del control)

Es la tercera categoría de controles tecnológicos que tiene la metodología FAIR una vez que el atacante a realizado algún ataque, su finalidad es evitar que los ataques se conviertan en eventos de pérdida, de modo que fortalezcan los activos, por ejemplo, autenticación, administración de accesos, parchados, etc.

- Respuesta (Categoría del control)

Es la cuarta categoría de controles tecnológicos que tiene la metodología FAIR una vez que el atacante logra su cometido, su finalidad es limitar la magnitud de la pérdida, por ejemplo, cifrado, destrucción de datos, etc.

- Productividad (Tipo de pérdida)

La productividad es el tipo de pérdida que está directamente relacionada con la el valor que deja de generar la organización por el bloqueo de un producto o servicio, por ejemplo, pérdidas por el corte de un sitio web minorista, falta de pagos de trabajadores por el bloqueo del sistema de planillas.

- Respuesta (Tipo de pérdida)

La respuesta es el tipo de pérdida que sufre la organización por gastos asociados con la gestión de la respuesta a raíz de un evento de pérdida, por ejemplo, revisiones forenses, notificaciones de incumplimiento, reposiciones, etc.

- Reemplazo (Tipo de pérdida)

El reemplazo es el tipo de pérdida relacionada con el gasto asociado con la sustitución o reparación de activos o personal involucrado o afectado en el ataque, por ejemplo, sustituir servidores, reemplazar personal, etc.

- Ventaja competitiva (Tipo de pérdida)

La ventaja competitiva es el tipo de pérdida relacionada con la pérdida por la obtención por parte de competidores de los secretos del negocio, planes de fusiones, adquisiciones o datos corporativos, por ejemplo, porción de participación de mercado, copia de productos o servicios nuevos, etc.

- Multas y sanciones (Tipo de pérdida)

Las multas y sanciones son el tipo de pérdidas relacionadas por acciones legales o regulatorias a través de acciones legales, penales o contractuales, por parte de clientes, usuarios, colaboradores y/o entes reguladores, por ejemplo, multas regulatorias, demandas, juicios, etc.

- Daños a la reputación (Tipo de pérdida)

Los daños a la reputación son pérdidas relacionadas con la percepción externa que tienen los clientes o demás actores del rubro de la organización en relación a los servicios brindados, desempeño o valores éticos, por ejemplo, aumentos pasivos, pérdida en la participación de mercado, etc.

- Pérdidas primarias

Se consideran pérdidas primarias a toda pérdida económica que sufra la organización que esté directamente relacionada con la materialización del riesgo evaluado, se considera dentro de este total cualquiera de los tipos de pérdidas que utiliza la metodología FAIR.

- Pérdidas secundarias

Se consideran pérdidas secundarias a toda pérdida económica que sufra la organización como daño colateral o de segundo grado relacionado con la materialización del riesgo evaluado, se considera dentro de este total cualquiera de los tipos de pérdidas que utiliza la metodología FAIR.

- Modelo Monte Carlo

Es un modelo matemático computarizado que hace miles de simulaciones mediante el reemplazo de un rango de valores en base a parámetros iniciales, de modo que calcula distintos resultados, una y otra vez, usando un grupo diferente de valores aleatorios.

Como principales ventajas ofrece resultados gráficos, análisis de sensibilidad, análisis de escenario y correlación de variables de entrada. (Montecarlo, 2019).

- Attack Vector (CVSS)

Es una métrica que identifica cómo se puede explotar la vulnerabilidad evaluada, de modo que muestra todas las posibles formas de ataques, entre las opciones que se pueden escoger, se tiene Network (N), Adjacent (A), Local (L) y Physical (P).

- Attack Complexity (CVSS)

Es una métrica que describe la complejidad para explotar las vulnerabilidades encontradas en el riesgo evaluado, entre las opciones que se pueden escoger, se tiene Low (L) y High (H),

- Privileges Required (CVSS)

Es una métrica que muestra el nivel de privilegios que deberá contar el atacante para materializar el ataque, entre las opciones que se pueden escoger, se tiene None (N), Low (L) y High (H).

- User Interaction (CVSS)

Es una métrica que muestra la interacción que necesita tener el atacante con el activo para materializa el ataque, entre las opciones que se pueden escoger, se tiene None (N) y Required (R).

- Scope (CVSS)

Es una métrica que muestra el impacto que sufre el objetivo una vez que ha sido atacado, entre las opciones que se pueden escoger, se tiene Unchanged (U) y Changed (C).

- Confidentiality (CVSS)

Es una métrica que valida cuánto fue el impacto del ataque en relación a la confidencialidad del activo, entre las opciones que se pueden escoger, se tiene None (N), Low (L) y High (H).

- Integrity (CVSS)

Es una métrica que valida cuánto fue el impacto del ataque en relación a la integridad del activo, entre las opciones que se pueden escoger, se tiene None (N), Low (L) y High (H).

- Availability (CVSS)

Es una métrica que valida cuánto fue el impacto del ataque en relación a la disponibilidad del activo, entre las opciones que se pueden escoger, se tiene None (N), Low (L) y High (H).

- SBS

Las siglas significan Superintendencia de Banca, Seguros y AFP, representan al ente regulador u organismo encargado de supervisar y regular todos los temas

relacionados con los sistemas financieros, de pensiones privadas, de seguros, de crédito, etc, así como de detectar y prevenir todo lo relacionado con financiamiento al terrorismo y el lavado de activos.

- OWASP Mobile Top 10

Las siglas significan Open Web Application Security Project y es una organización sin fines de lucro que tienen como principal función proporcionar apoyo e infraestructura para la solución de vulnerabilidades en el software; el “Mobile Top 10” hace referencia a los 10 principales riesgos de seguridad de información y ciberseguridad identificados en aplicaciones para equipos móviles, considerando por ejemplo, sistemas operativos como IOS y Android, además de identificar los principales riesgos, también explica cómo se podrían dar esas vulnerabilidades (vectores de ataques), sus criticidades y recomendaciones para tratar de mitigar estos riesgos.

CAPITULO II: EL PROBLEMA, OBJETIVOS, HIPÓTESIS Y VARIABLES

2.1. Planteamiento del problema

2.1.1. Descripción de la Realidad Problemática

La evaluación cuantitativa se puede definir como el proceso en el cual se analizan los datos de una investigación de modo que se transforman en inferencias numéricas confiables y válidas en relación a su contexto (Hernández, 2014), todo esto con la finalidad de ayudar a la toma de decisiones sobre lo evaluado. Su aplicabilidad es sobre casi cualquier contenido, como por ejemplo indicadores gerenciales, valores o intereses de personas, análisis económicos, cultivos de cosechas, entre otros.

Por otro lado, según la publicación de ISACA Journal, la autora del artículo (Ho, 2019) menciona que los riesgos tecnológicos de ciberseguridad deberían ser parte del marco de gestión de riesgos de la organización, quienes, apoyándose en los equipos de las tres líneas de defensa de seguridad, deberían proteger los principales activos de información, garantizando la confidencialidad, disponibilidad e integridad de los mismos.

Sumando a lo antes mencionado, el informe que realizó (IBM Security, 2021) sobre el costo de una brecha de seguridad de datos (donde se considera una brecha como un evento en el cual el nombre, historial médico o información bancaría de una persona, se ponen potencialmente en riesgo) valida un aumento del 10% en el costo total promedio de una brecha entre el año 2020 y 2021, llegando a un monto de USD 4,24 M. Dentro de las principales amenazas para la materialización de riesgos de seguridad se tienen malware, ransomware, ingeniería social, amenazas internar, ataques de denegación de servicios (DDoS) y amenazas persistentes avanzadas (APT).

En referencia a nuestra región, se tienen esfuerzos en conjunto con la Organización de Estados Americanos para formar un Modelo de Madurez de la

Capacidad de Ciberseguridad para las Naciones (CMM, por sus siglas en ingles), de modo que se puedan hacer frente de manera consolidada, estratégica y dinámica a los riesgos de ciberseguridad.

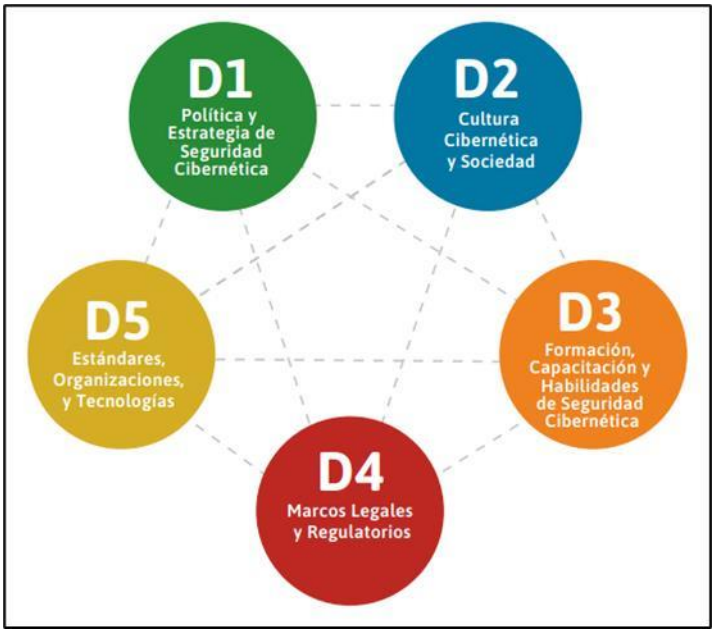


Figura 4. Las cinco dimensiones del CMM (OEA, 2021)

En temas relacionados con ciberseguridad, el Perú cuenta con la Ley N° 30618 en la cual define la seguridad digital como " la situación de confianza en el entorno digital, frente a las amenazas que afectan las capacidades nacionales, a través de la gestión de riesgos y la aplicación de medidas de ciberseguridad y las capacidades de ciberdefensa, alineada al logro de los objetivos del Estado" (Ley 30618, 2017), además del decreto supremo Nº 106-2017-PCM, donde se "aprueba el Reglamento para la Identificación, Evaluación y Gestión de Riesgos de los Activos Críticos Nacionales, que son recursos, infraestructuras y sistemas que son esenciales e imprescindibles para mantener y desarrollar las capacidades nacionales o que están destinados a cumplir dicho fin" (DS 106, 2017).

Así mismo, se cuenta con un Equipo de Respuesta a Incidentes en Seguridad Informática (CSIRT, por sus siglas en inglés) a nivel nacional, cuya misión principal

es la prevención, el tratamiento y la respuesta ante incidentes de ciberseguridad en las instituciones en el sector público, por medio de la elaboración de mecanismos, estrategias y prácticas para suplir las necesidades de ciberseguridad a nivel del Estado.

En el sector financiero peruano, la Superintendencia de Banca, Seguros y AFP, por medio de sus boletines semanales, identifica la necesidad de que las organizaciones desarrollen la "ciber-resiliencia" de modo que adquieran la capacidad de responder y recuperarse lo más rápido posible de los ataques de ciberseguridad (SBS, 2018), siendo el equipo de riesgos tecnológicos, los primeros en estar preparados, sin embargo, en este proceso, se identifica la gran dificultad que se tiene en cuantificar la pérdida económica relacionada con riesgos residuales y objetivos, para la toma de decisiones gerenciales respecto a los planes de acción que se implementarán.

Dentro de las principales causas por las que no se puede calcular de manera cuantitativa y eficiente los riesgos tecnológicos de ciberseguridad se debe al uso del modelo cualitativo del mapa de calor de riesgos clásico, la cantidad de variables a evaluar y la dificultad en el cálculo de las pérdidas proyectas, todo esto tiene como principal consecuencia, el invertir mayores recursos de la organización en la gestión de este tipo de riesgo, aumentando la inversión inicial así como la brecha de seguridad hasta la mitigación del mismo.

Para dar una respuesta a esta problemática, la presente tesis, propone el uso de la metodología FAIR (Factor Analysis of Information Risk) y su herramienta de cálculo matemático de pérdidas estimadas, para el cálculo cuantitativo de riesgos tecnológicos de ciberseguridad, de modo que se tenga una visión más clara de la exposición que tiene la organización frente a estos riesgos.

2.1.2. Antecedentes Teóricos

La ciberseguridad enmarca todo lineamiento o buena práctica para la protección de los componentes y activos tecnológicos de una organización, llevando la seguridad a las redes informáticas, gestión de la información, continuidad de negocio, aplicaciones, servidores, end points entre otros.

Entre los principales retos que tiene la ciberseguridad, se encuentra la mitigación de los ciberataques, los cuales han estado en aumento debido al incremento de la digitalización y la virtualización de servicios en las organizaciones, según una evaluación que hizo Kapersky el 2021 en América Latina, los ciberataques se aumentaron un 24% en referencia al año anterior, teniendo como en el segundo lugar a Perú.

La descarga de código malicioso y Phishing, lideran los ciberataques que han tenido mayor popularidad y éxito en este último tiempo, ambos enfocados al robo de datos personales y bancarios para terminar en transferencias no reconocidas de dinero a terceros.

Por otro lado, para definir una evaluación cuantitativa, se hará por medio del uso de datos estadísticos e información numérica, de modo que sea lo más objetivo posible, siendo totalmente independiente de los sesgos del evaluador y dando como resultado la información necesaria para tomar las mejores decisiones sobre lo evaluado, se recomienda presentar los resultados finales por medio de un modelo visual o esquemático para que todos los involucrados puedan comprenderlo de la mejor manera.

Finalmente, una correcta gestión de riesgos tecnológicos siempre ayudará a las organizaciones a tomar mejores decisiones en relación a los planes de acción, controles, alcance, criticidad y responsables de su seguridad de la información,

debido a que muchas veces, se toca estos temas sólo por cumplir requisitos mandatorios impuestos por los entes reguladores o actores finales, lo cual lleva a tener una falsa sensación de seguridad.

Para tener una gestión de riesgos tecnológicos eficiente, se tiene que integrar con el enfoque organizacional, de este modo, se tendrá claro las prioridades del negocio y se conocerá cuánto es el impacto de una inversión de recursos para la mitigación de los riesgos identificados, sin afectar otros procesos críticos.

Una buena práctica para alcanzar todos estos objetivos, es implementar y desplegar líneas de defensas para la protección de los activos más críticos de la organización, las cuales tienen como eje central la ejecución de controles de seguridad validados en marcos como la ISO/IEC 27002 y la NIST.

2.1.3. Definición del Problema

- General

¿Cómo la evaluación cuantitativa de riesgos tecnológicos de ciberseguridad en una aplicación de transferencias digitales influye en la toma de decisiones en una entidad financiera peruana en el periodo 2021-2022?

- Específicos

¿Cómo la evaluación cuantitativa de riesgos tecnológicos utilizando la metodología FAIR en una aplicación de transferencias digitales ayuda a la gestión de la ciberseguridad?

¿Cómo la evaluación cuantitativa de riesgos tecnológicos utilizando la metodología FAIR en una aplicación de transferencias digitales ayuda a la gestión de riesgos?

2.2. Finalidad y Objetivos de la Investigación

2.2.1. Finalidad

La siguiente investigación tiene como finalidad analizar la influencia que tiene la ejecución de una evaluación cuantitativa por medio de la metodología FAIR para gestionar correctamente los riesgos tecnológicos de ciberseguridad en una aplicación de trasferencias digitales en una entidad financiera peruana en el periodo 2021-2022.

2.2.2. Objetivo general y específicos

- General

Analizar si la evaluación cuantitativa de riesgos tecnológicos de ciberseguridad en una aplicación de trasferencias digitales influye en la toma de decisiones en una entidad financiera peruana en el periodo 2021-2022.

- Específicos

Determinar si la evaluación cuantitativa de riesgos tecnológicos utilizando la metodología FAIR en una aplicación de trasferencias digitales ayuda a la gestión de la ciberseguridad.

Determinar si la evaluación cuantitativa de riesgos tecnológicos utilizando la metodología FAIR en una aplicación de trasferencias digitales ayuda a la gestión de riesgos.

2.2.3. Delimitación del estudio

La investigación tiene como alcance analizar la influencia de las evaluaciones cuantitativas en relación a la gestión del riesgo de ciberseguridad en una aplicación de transferencias digitales en una entidad financiera peruana para el periodo 2021-2022.

Para la correcta ejecución de la metodología cuantitativa se necesitará tener conocimiento técnico y funcional en el desarrollo y arquitectura de software, seguridad de la información, entendimiento de FAIR y la creación de un usuario en la plataforma gratuita de FAIR-U.

2.2.4. Justificación e importancia del estudio

El principal activo de una entidad financiera es la información de sus clientes, motivo por el cual se debería tener un mayor cuidado en la seguridad y tratamiento de la misma, no solo para brindar un servicio eficiente a los clientes, sino también para cumplir con los lineamientos establecidos por las entidades regulatorias (SBS, INDECOPI, etc), el no tener una correcta seguridad en la información conllevaría a la entidad financiera tener pérdidas reputacionales, económicas, juicios, demandas y sanciones.

Una parte fundamental de la seguridad de la información es gestionar correctamente los riesgos de ciberseguridad identificados en sus procesos y herramientas tecnológicas, esto ayudará a la entidad financiera a definir, alcanzar y

mantener los umbrales apropiados de confidencialidad, disponibilidad e integridad, necesarios para operar de una manera eficiente.

Para tener una gestión más detallada sobre el verdadero alcance que tiene un riesgo de ciberseguridad, la metodología FAIR nos ayuda a tener una visión cuantitativa de las pérdidas anualizadas estimadas, para realizar esto, la metodología está basada en los siguientes puntos:

- Recopilación de información de los principales actores del negocio, procesos y herramientas.
- Identificación del riesgo (magnitud de la pérdida x frecuencia) relacionado al evento que se está evaluando.
- Ejecución de la simulación matemática (modelo de Monte Carlo) con una herramienta automatizada.
- Presentación de resultados a los foros de decisión.

2.3. Hipótesis y Variables

2.3.1. Hipótesis Principal y Especificaciones

- General

La evaluación cuantitativa de riesgos tecnológicos de ciberseguridad en una aplicación de trasferencias digitales influye en la toma de decisiones por parte de la entidad financiera peruana.

- Específicos

La evaluación cuantitativa de riesgos tecnológicos utilizando la metodología FAIR en una aplicación de transferencias digitales ayuda a la gestión de la ciberseguridad.

La evaluación cuantitativa de riesgos tecnológicos utilizando la metodología FAIR en una aplicación de transferencias digitales ayuda a la gestión del riesgo.

2.3.2. Variables e Indicadores

- Variables

La evaluación cuantitativa de riesgos tecnológicos de ciberseguridad influye en la toma de decisiones.

La evaluación cuantitativa de riesgos tecnológicos de ciberseguridad utilizando la metodología FAIR ayuda a la gestión de la ciberseguridad.

La evaluación cuantitativa de riesgos tecnológicos de ciberseguridad utilizando la metodología FAIR ayuda a la gestión del riesgo.

- Indicadores

  Evaluación cuantitativa

  Evaluación cualitativa

  Riesgos tecnológicos

  Gestión de riesgos

Ciberseguridad

Metodología FAIR

CAPITULO III: MÉTODO, TÉCNICA E INSTRUMENTOS

3.1. Población y muestra

Según el “Reporte de Ciberseguridad en las Aplicaciones Móviles de Home banking en Perú” DeepSecurity (2020), realizó un análisis pasivo en las aplicaciones móviles que ejecutan transferencias digitales de los 12 principales bancos del Perú, SBS (2020), tomando como referencia el OWASP mobile Top 10, dando como resultado la siguiente lista de riesgos:

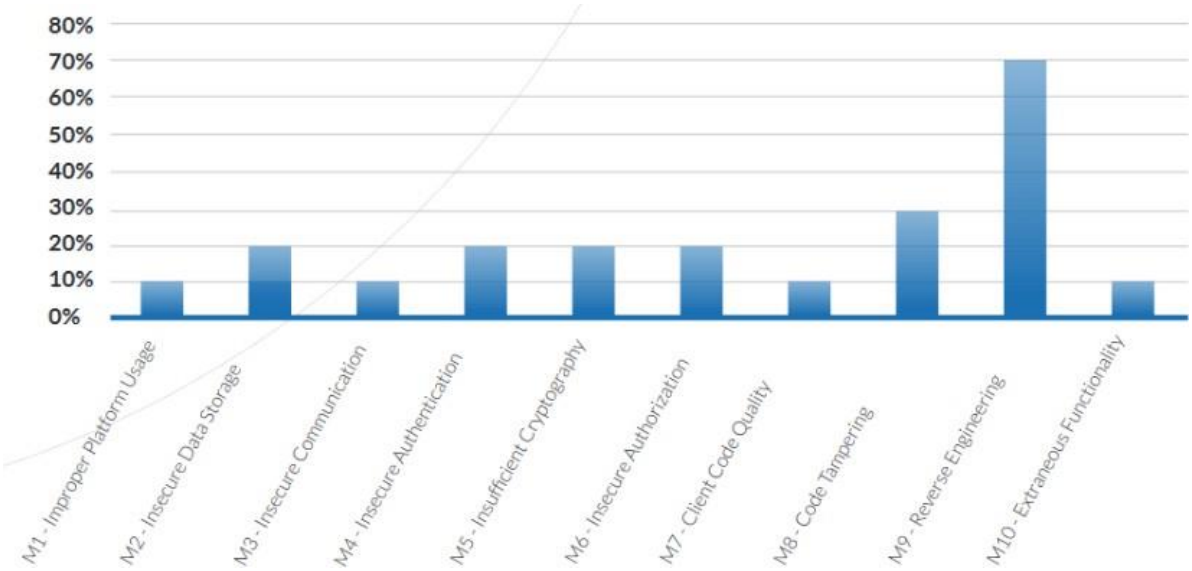


Figura 5. Listado de riesgos OWASP mobile Top 10. (DeepSecurity, 2020)

Considerando este listado de los principales diez riesgos, se tomará como muestra para el desarrollo de esta investigación el “M1 – Improper Platform Usage”, en el cual se detallará el riesgo de “Actividades maliciosas por un usuario privilegiado”.

3.2. Enfoque y Diseño

El enfoque que se eligió para esta investigación fue el cuantitativo, debido a que, a través de una medición numérica por medio de un modelo matemático, se probarán las hipótesis formuladas.

En relación al diseño escogido para esta investigación, será el experimental, debido a que se manipularán variables independientes para lograr cambios en las variables dependientes, por medio de la modificación de los parámetros ingresados.

3.3. Técnicas e instrumentos de Recolección de Datos

Para la recolección de los datos para la ejecución de la investigación, se usarán las entrevistas y reuniones con los principales stakeholders de la organización, de modo que se tenga claridad de punta a punta de todos los posibles vectores de ataques y del alcance de cada uno.

Cabe mencionar que para aprovechar al máximo el tiempo de las reuniones y entrevistas, el evaluador no solamente tiene que conocer la metodología de FAIR sino que también tendrá que tener un conocimiento previo de manera general del activo o proceso a evaluar, de modo que realice las preguntas indicadas según lo que ha identificado previamente.

3.4. Ética de la Investigación

La ética aplicada en esta investigación está basada en el respeto por las personas y organizaciones financieras que usaremos para la evaluación.

Así mismo, se estará guardando la confidencialidad de la información proporcionada, de modo que no se expongan datos como nombres del personal, arquitecturas de la infraestructura tecnológica, IPs, usuarios, contraseñas, etc.

3.5. Procesamiento de Datos

Para el procesamiento de los datos recopilados, se usará la web gratuita proporcionada por Risklens, FAIR-U (https://app.fairu.net/login), de modo que se ingrese la información según los pasos de la metodología de FAIR, para que finalmente, la misma herramienta ejecute el modelo matemático de Monte Carlo, brindando los resultados de la evaluación cuantitativa.

CAPITULO IV: PRESENTACIÓN Y ANÁLISIS DE LOS RESULTADOS

4.1. Presentación de Resultados

Para validar los objetivos planteados en esta investigación, se compararán dos tipos de evaluación de riesgos tecnológicos de ciberseguridad, una cuantitativa por medio de la metodología FAIR y la otra cualitativa por medio de la CVSS en apoyo con el mapa de calor de riesgos.

Como caso práctico, se evaluará el riesgo de ciberseguridad “Actividades maliciosas por un usuario privilegiado”, aplicado al App Móvil de una entidad financiera del Perú.

4.1.1. Evaluación Cuantitativa (FAIR)

Para la recolección de información de la evaluación cuantitativa se usará la plataforma tecnológica de FAIR-U creada por Risklens.

La evaluación comienza con las entrevistas a los actores principales del App Móvil, como líderes técnicos, owners, comercial, etc, esto con la finalidad de recolectar la mayor cantidad de información posible que sirva como insumo para los cálculos finales y el correcto modelamiento del riesgo.

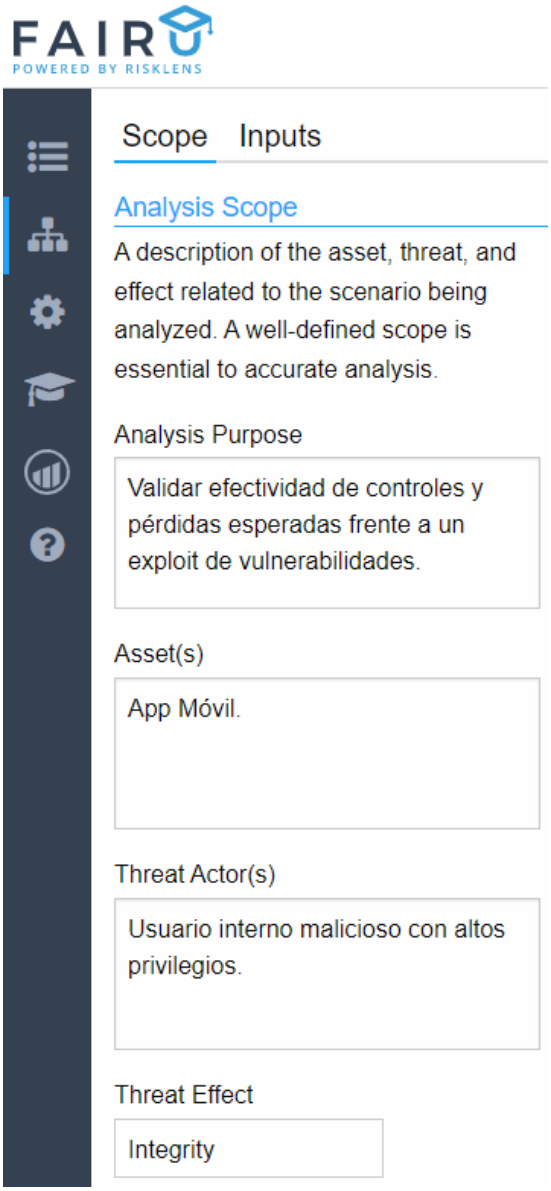


Figura 6. Definición del objetivo y alcance de la evaluación. Fuente, elaboración propia.

El objetivo de la evaluación es validar la efectividad de los controles que tiene actualmente la organización, para hacer frente a un exploit de vulnerabilidades por parte de un atacante interno malicioso con altos privilegios en el App Móvil, pudiendo afectar la integridad de la aplicación a nivel de código, infraestructura y/o datos, así como, determinar las posibles pérdidas esperadas.

Una vez modelado el riesgo a evaluar, se definirá límites mínimos, promedios y máximos para cada una de las variables que están pendientes, para comenzar, se debe precisar cuál es la Frecuencia de Evento de Amenaza (TEF), para el escenario que estamos evaluando, se tiene que definir la frecuencia probable con la que el usuario malicioso con altos privilegios ha intentado ejecutar los exploits de vulnerabilidades en el App Móvil de manera anualizada, quedando de la siguiente manera:

- El límite máximo del TEF será el tiempo máximo que el App Móvil está en producción, el cual es desde hace 5 años.

- El límite mínimo del TEF se tomará en conceso con todos los actores principales y será de 2 años, debido a que el último año no se tiene registro de este tipo de ataque, sin embargo, debido a que se tiene una brecha, se podría materializar el siguiente año.

- El límite promedio del TEF será la media de ambos límites, un posible ataque cada 3 años.

- La confianza será medio, debido a que los cálculos fueron apoyados en datos reales y acuerdos mutuos.

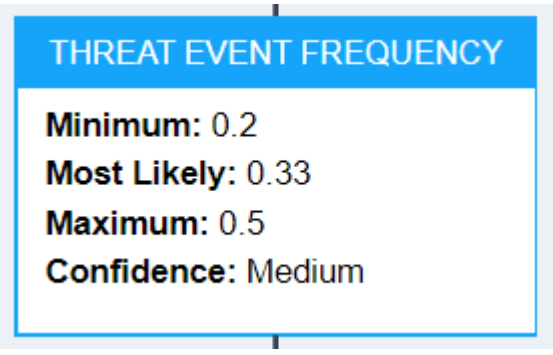


Figura 7. Definición del TEF. Fuente, elaboración propia.

Como siguiente paso se definirá la susceptibilidad (vulnerability) o eficacia que tienen los controles para detener este tipo de ataque, para esto se considerará los siguientes tipos de controles que podrían aplicar:

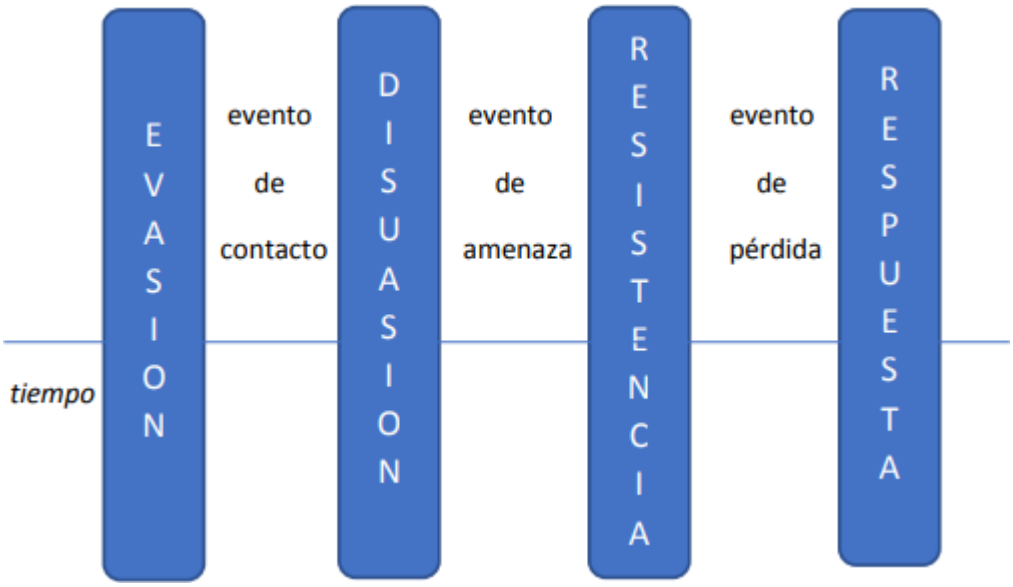


Figura 8. Tipos de controles. (RiskLens, 2021)

Los controles identificados con los usuarios principales son:

- Firewall de red (evasión).
- Monitoreo de Base de Datos con herramienta especializada (disuasión).
- Gestión de acceso por medio de matriz de roles (resistencia).

Teniendo claro cuáles son los controles de ciberseguridad, se podría definir que es poco probable que lo usuarios externos a la organización ejecuten algún ataque en las redes internas (control de evasión); sin embargo, por más que se tenga

identificado lo que hace el usuario (control de disuasión) por medio de los accesos que se les han brindado (control de resistencia) por sus funciones y rol, a la infraestructura del App Móvil, tiene total libertad para ejecutar cualquier tipo de exploit, debido a esto, la probabilidad de materialización quedaría de la siguiente forma:

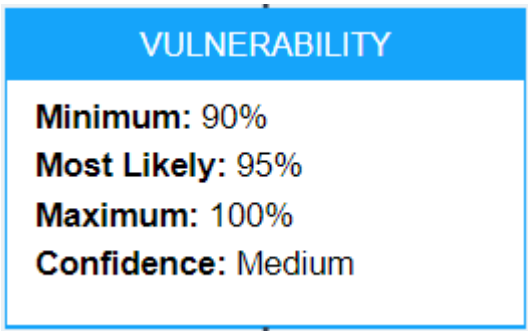


Figura 9. Definición de la susceptibilidad (riesgo residual). Fuente, elaboración propia.

Para el riesgo que se está evaluando, se tomará la siguiente información, considerando los tipos de pérdidas que corresponden al alcance:

Pérdida por Productividad:

Monto que se deja desembolsar por indisponibilidad del App Movil

- Mínimo: Ticket promedio x 8 horas (9am a 6pm de cualquier día) = $ 33,800
- Promedio: Promedio = $ 40,425
- Máximo: Ticket promedio x 7 horas (9am a 5pm de un viernes) + (hora pico de 5pm a 6pm de un viernes) = $ 50,825

Respuesta:

Revisión forense

- Mínimo = $ 9,500
- Promedio = $ 23,750
- Máximo = $ 37,500

Multas y Sanciones:

Multas relacionadas a fuga de información sensible por LPDP. (UIT: S/ 4,400)

- Mínimo = $ 11,000
- Promedio = $ 55,000
- Máximo = $ 110,000

Reemplazo:

Posible implicado en un evento, usuario privilegiado (insider)

- Mínimo = $105
- Promedio = $ 1,550

- Máximo = $ 3,125

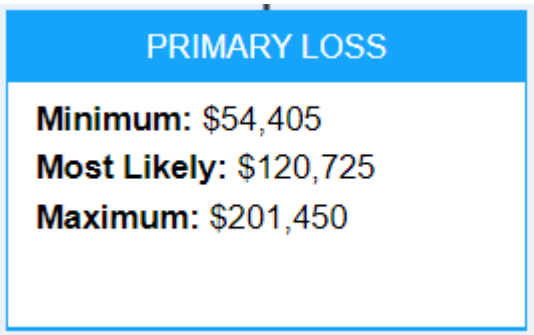


Figura 10. Sumatoria de posibles pérdidas. Fuente, elaboración propia.

Finalmente, una vez que se tiene identificada la frecuencia que tiene elatacante con los activos tecnológicos, la efectividad de los controles de ciberseguridad y las posibles pérdidas económicas, se ejecuta el modelo de Monte Carlo, el cual es un proceso matemático que corre miles de veces simulaciones con las variables previamente ingresadas, terminando con el siguiente resultado:

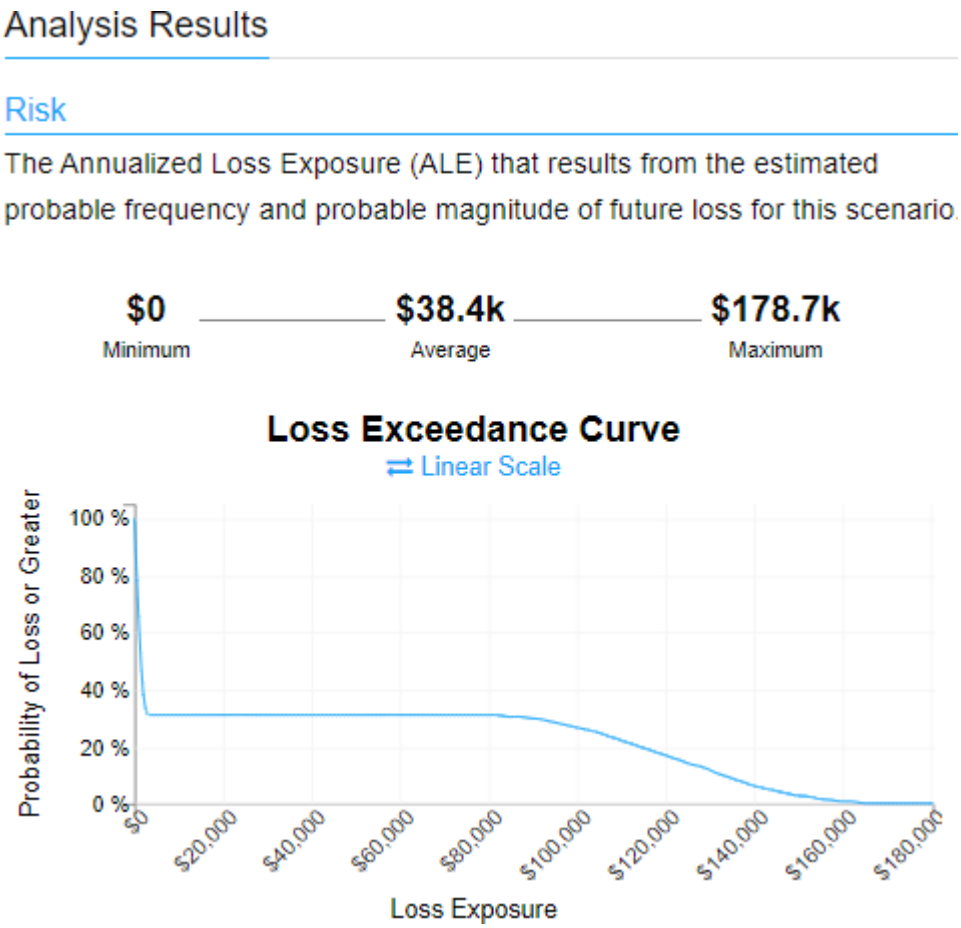


Figura 11. Pérdidas anualizadas (riesgo residual). Fuente, elaboración propia.

- Minimum = $0

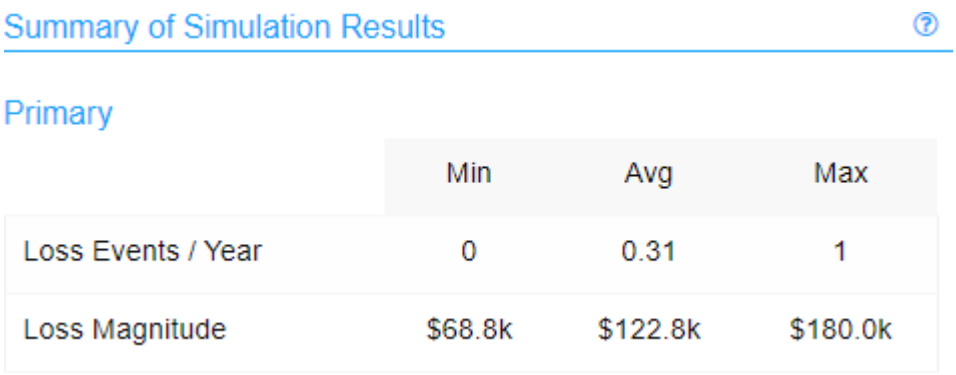
Se tiene una mínima probabilidad de que el siguiente año no se tenga ninguna pérdida relacionada al riesgo en evaluación.

- Average = $38.4k

Se tiene una gran probabilidad de sufrir un total de pérdidas (relacionadas al riesgo en evaluación) de $38,000 en el siguiente año.

- Maximum = $178.7k

En el peor escenario, se tiene una probabilidad de sufrir un total de pérdidas (relacionadas al riesgo en evaluación) de $178,700 en el siguiente año.



Summary of Simulation Results

Primary

	Min	Avg	Max
Loss Events / Year	0	0.31	1
Loss Magnitude	$68.8k	$122.8k	$180.0k

Figura 12. Pérdidas por eventos por año (riesgo residual). Fuente, elaboración propia.

Así mismo, se puede identificar, cuánto podría ser las pérdidas por eventos por cada año, teniendo los siguientes resultados:

- Mínimo

Se tiene una mínima probabilidad que se materialice algún evento (relacionadas al riesgo en evaluación) con un impacto de $68,800 en el siguiente año.

- Average

Se tiene una gran probabilidad de que se materialicen un evento cada tres eventos (relacionados al riesgo en evaluación), con una sumatoria de pérdida de $38,000.

- Maximum

En el peor escenario, se tiene una probabilidad que se materialice un solo evento (relacionadas al riesgo en evaluación) de $180,000 en el siguiente año.

Los resultados anteriormente presentados, pertenecen al riesgo residual que se tiene actualmente, sin embargo, para obtener el mayor provecho de ejecutar una metodología de riesgos cuantitativos, se tendrá que identificar el riesgo objetivo, para esto, se identificarán los planes de acción necesarios para mitigar el riesgo y acortar las posibles pérdidas identificadas.

Se considerarán los siguientes planes de acción:

- Gestión de aseguramiento de las líneas bases de los servidores.

- Alertamiento de configuraciones en los servidores.

Estos planes de acción, suman una efectividad del 80% y 90% en relación a la mitigación del riesgo, esto debido a que, los controles antes mencionados, se le suman la gestión de la línea base de los servidores, lo cual, limita el uso de aplicaciones o funciones poco seguras en la aplicación por parte de los usuarios administradores, además del alertamiento de configuraciones para cualquier acción sospechosa que se pueda realizar.

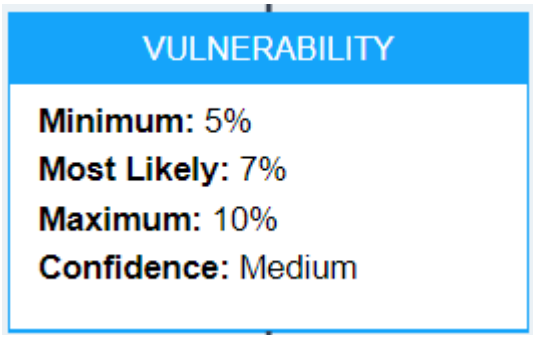


Figura 13. Definición de la susceptibilidad (riesgo objetivo). Fuente, elaboración propia.

Este ingreso de nuevos parámetros, modifica la exposición promedia anualizada del riesgo en $2,700.

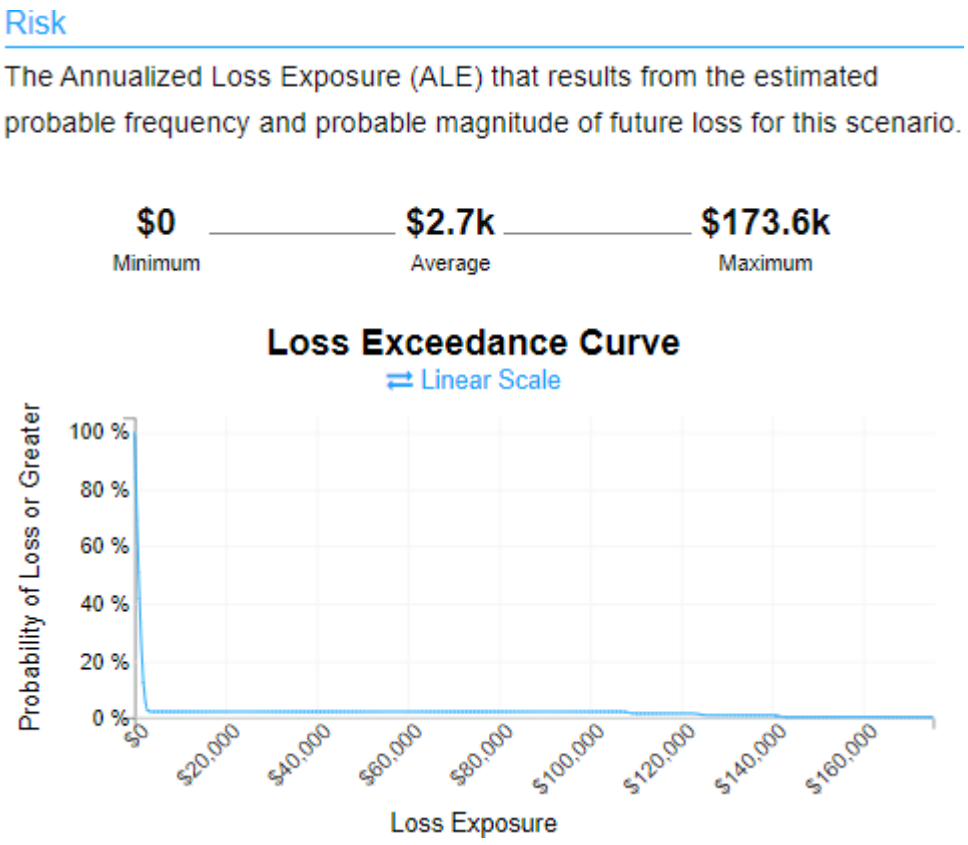
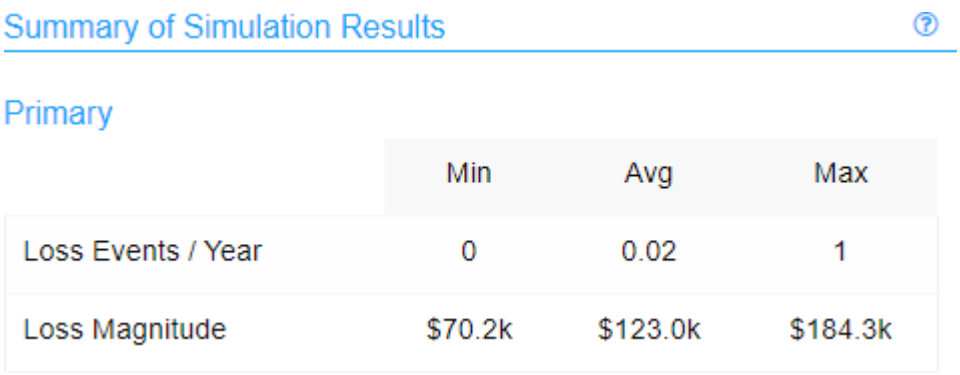


Figura 14. Pérdidas anualizadas (riesgo objetivo). Fuente, elaboración propia.

Así mismo, modifica el promedio de materialización del evento, de un posible evento cada tres años a un posible evento cada cincuenta años.



Summary of Simulation Results

Primary

	Min	Avg	Max
Loss Events / Year	0	0.02	1
Loss Magnitude	$70.2k	$123.0k	$184.3k

Figura 15. Pérdidas por eventos por año (riesgo objetivo). Fuente, elaboración propia.

4.1.2. Evaluación Cualitativa (CVSS)

Para la ejecución de la evaluación de riesgos de manera cualitativa, se tomará en cuenta la versión 3.1, la cual que se tomará de la siguiente fuente https://www.first.org/cvss/calculator/3.1.

Figura 16. Ejecución cualitativa en CVSS (riesgo residual). Fuente, elaboración propia.

Tomando en cuenta el mismo riesgo evaluado con la metodología cuantitativa (alcance, controles y planes de acción), se tienen los siguientes parámetros para materializar el riesgo:

- Attack Vector

El vector de ataque será adyacente, debido a que el atacante podrá realizar el ataque desde la red interna.

- Attack Complexity

La complejidad del ataque será Alto, debido a que se deberá tener conocimientos técnicos avanzados.

- Privileges Required

Los privilegios requeridos serán Altos, debido a que sólo usuarios privilegiados podrán tener acceso.

- User Interaction

La interacción del usuario será requerida, debido a que tendrá que ejecutar comandos, configuraciones o scripts.

- Scope

El objetivo o App Movil será cambiado, debido a que el atacante podrá agregar, modificar o eliminar datos, código o información.

- Confidentiality, Integrity, Availability

Todos los vectores de seguridad son impactados en sus más altos niveles.

La ejecución de la CVSS, dio como resultado que la criticidad del riesgo asociado es de un nivel “Alto 7.3”, lo cual lo ubica con una pérdida estimada entre $151,001 y $500,000 y una frecuencia de materialización entre una y dos veces al año, según el mapa de calor de riesgos.

Impacto(USD)					
307,500	61,500	102,500	307,500	615,000	> 3,000,000
250,000	50,000	83,333	250,000	500,000	3,000,000
113,500	22,700	37,833	113,500	227,000	1,362,000
12,500	2,500	4,167	12,500	25,000	150,000
3,125	625	1,042	3,125	6,250	37,500
Frecuencia Anual	Cada 5 años	Cada 3 años	Cada año	Cada 6 meses	Más de 2 veces al año

Crítico	501,000 - >3,000,000
Alto	151,001 - 500,000
Relevante	37,801 - 150,000
Moderado	12,501 - 37,800
Bajo	0 - 12,500

Figura 17. Mapa de calor de riesgos. Fuente, elaboración propia.

Se aplica los planes de acción identificados, los cuales impactan tanto a la confidencialidad, integridad y disponibilidad.

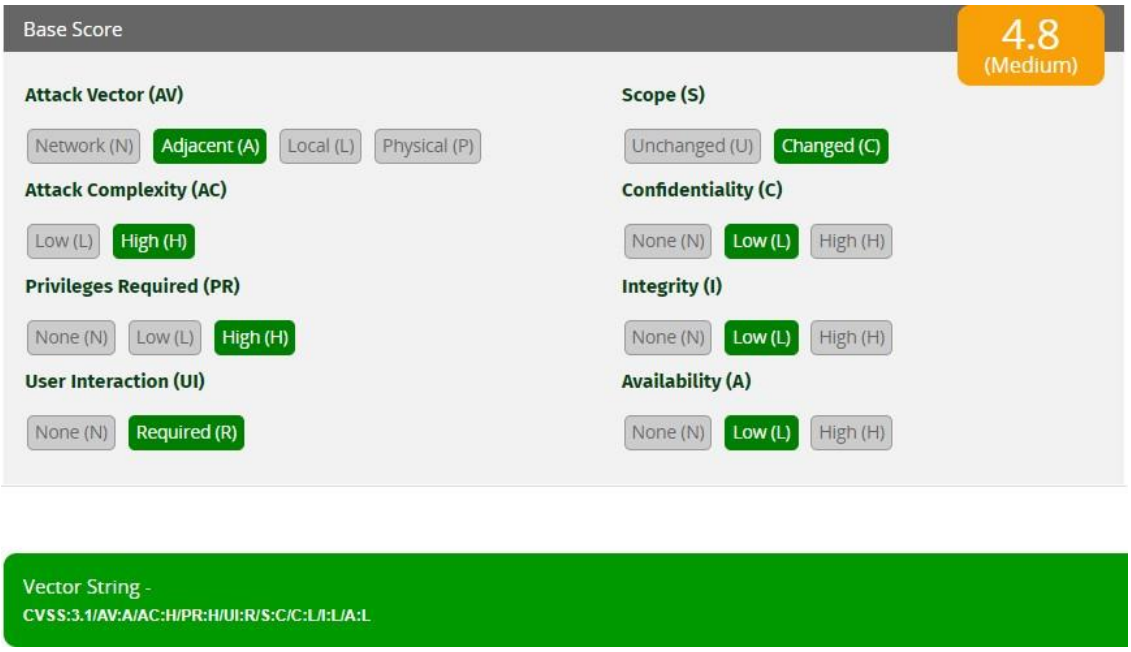


Figura 18. Ejecución cualitativa en CVSS (riesgo objetivo). Fuente, elaboración propia.

Los planes de acción implementados bajan la criticidad a “Medio 4.8”, lo cual lo coloca en la sección de Relevante con una pérdida estimada entre $37,801 y $150,000 y una frecuencia de materialización mayor a un año, según el mapa de calor de riesgos.

4.2. Contrastación de Hipótesis

La ejecución de la evaluación cuantitativa de riesgos tecnológicos de ciberseguridad, dio como resultado un enfoque más amplio de la magnitud que podría tener la materialización del riesgo y el impacto económico en la organización, esto debido a que se muestra el detalle de los posibles eventos y pérdidas económicas que se podrían tener el siguiente año, información valiosa para la organización para las tomas de decisiones gerenciales en relación a la exposición que se tiene al riesgo en la actualidad y si conviene implementar los planes de acciones recomendados.

Así mismo, se validó que la ciberseguridad se llegó a mejorar con la evaluación cuantitativa, debido a que se identificaron todos los puntos de compromiso dentro del vector de ataque relacionado al riesgo evaluado, así como los controles y planes de acción necesarios para mitigar el riesgo, todo esto, clasificado dentro de las cuatro categorías de eficiencia de control de ciberseguridad de la metodología FAIR (Evasión, Disuasión, Resistencia y Respuesta).

Por último, luego de que la evaluación cuantitativa con la metodología FAIR, identificó los posibles eventos y pérdidas económicas, así como los controles y planes de acción necesarios para mitigar el riesgo, se puede validar con esta información, que se está mejorando la gestión del riesgo, debido a que se sabe la frecuencia e impacto, además del costo para los próximos pasos a seguir, ayudando a la organización a tener mayor claridad en el seguimiento de cada acción a tomar, pudiendo responder no solamente al ataque mismo, si no ha entidades reguladores y clientes finales.

4.3. Discusión de Resultados

Evaluando el mismo riesgo de ciberseguridad con las evaluaciones cualitativa y cuantitativa, se pueden obtener los siguientes puntos:

	Evaluación cualitativa con la metodología CVSS	Evaluación cuantitativa con la metodología FAIR
Aporte a la organización	Se identificó la criticidad del riesgo al que están expuestos, sin embargo, la identificación de las pérdidas económicas, fueron a muy alto nivel, aterrizándolo en un rango bastante abierto, así como la aproximación de la periodicidad fue a juicio experto, sustentado en el mapa de calor de riesgos.	Se identificó la pérdida estimada mínima, promedio y máxima a la que están expuestos, así como, la probabilidad de materialización, todo esto basado en los parámetros ingresados inicialmente, ejecutados con el modelo matemático de Monte Carlo.
Identificación y uso de los controles de seguridad de la	La identificación de los controles actuales, sirvieron	La identificación de los controles actuales, sirvieron

información y ciberseguridad	para calcular la eficiencia que tienen, de modo que se seleccione alguna opción de la calculadora.	como parámetro inicial para el modelo matemático, el cual calculó el impacto en la pérdida estimada final.
Eficiencia de los planes de acción propuestos para mitigar el riesgo evaluado	La identificación de los planes de acción, sirvieron para que a juicio experto se seleccione alguna opción de la calculadora.	La identificación de los planes de acción, sirvieron para validar en que etapa del vector de ataque se podría fortalecer la tecnología y/o proceso, lo cual conllevaría a retar la eficiencia de los mismos, impactando directamente en el cálculo final del impacto promedio.
Aporte en la gestión de riesgos y toma de decisiones	Para la gestión del riesgo, se muestra la criticidad residual y objetiva a la que la organización está expuesta, sin embargo, los valores resultantes, se muestran en rangos abiertos, lo cual no permite, una toma correcta de	Para la gestión del riesgo, se muestra las pérdidas promedio estimadas, tanto para el riesgo residual como objetivo, lo cual le da más claridad a los usuarios finales para decidir invertir o no en la implementación de los planes de acción

	decisiones en relación a la inversión necesaria para mitigar elriesgo.	propuestos, en los tiempos estimados de la posible materialización.

CAPITULO V: CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusión

Al finalizar la siguiente investigación, se concluye que tanto la evaluación cuantitativa como la cualitativa, brindan como resultados, la exposición que tiene la organización en relación al riesgo evaluado, sin embargo, la que se realizó con la metodología de FAIR en contra parte de la realizada con la CVSS, muestra un mayor detalle, permitiendo medir el riesgo de una manera más precisa, lo cual facilita la comunicación y gestión de las pérdidas futuras.

Así mismo, se validó que en una evaluación cuantitativa con la metodología de FAIR, se mejora la ciberseguridad en la organización, esto debido a que se recorre de punta a punta los vectores de ataques, identificando la efectividad promedio de cada control tecnológico actual y la mejoría que sumaría los planes de acción recomendados.

Además de esto, la evaluación cuantitativa, al estar basada en su mayoría en datos y modelos matemáticos, quita de la ejecución de la gestión del riesgo, el sesgo que podría tener el evaluador en escoger información ambigua, lo que hace más fidedigno el resultado final, permitiendo a los usuarios finales, tomar decisiones más acertadas en relación a la inversión necesaria para mitigar el riesgo evaluado.

Por otro lado, es de suma importancia para que la evaluación cuantitativa por medio de la metodología de FAIR de resultados detallados, claros y precisos, que se recolecte la mayor cantidad de información por medio de las entrevistas personales con los stakeholders, de modo que cada parámetro ingresado tenga un sustento.

Finalmente, se podría continuar con la investigación, comparando la eficacia de la evaluación cuantitativa con la metodología FAIR con otras metodologías cualitativas, así como con otros riesgos de ciberseguridad enfocados a otros componentes y arquitecturas tecnológicas.

5.2. Recomendaciones

Se recomienda tener conocimientos robustos en relación a la metodología FAIR, de modo que todas las fases se puedan hacer de la mejor manera, desde la captura de parámetros iniciales, hasta la ejecución y presentación de resultados a los usuarios finales, lo cual permita a la organización entender y tomar las mejores decisiones en relación a la mitigación del riesgo.

Así mismo, se tiene que conocer muy bien el vector de ataque por el cual se podría materializar el riesgo, así como el proceso funcional y todos los componentes tecnológicos involucrados.

REFERENCIAS

SBS (2018). Boletín semanal 17 - 2018. https://www.sbs.gob.pe/Portals/0/jer/BOLETIN-SEMANAL/2018/BoletinSem17_2018.pdf

DS106 (2017). Gobierno del Perú. https://www.gob.pe/institucion/pcm/normas-legales/454348-106-2017-pcm

Ley 30618 (2017). Gobierno del Perú. https://www.gob.pe/institucion/dini/normas-legales/887205-30618

OEA (2021) OEA - Observatorio de Ciberseguridad. Riesgos, avances y el camino a seguir en américa latina y el caribe.

IBM Security (2021) IBM Security. Informe del costo de una brecha de seguridad de datos. https://www.ibm.com/mx-es/topics/cybersecurity

Hernández (2014). Metodología de la investigación. Roberto Hernández Sampieri; Carlos Fernández Collado; María del Pilar Baptista Lucio. Mexico. McGraw-Hill Interamericana.

Ho (2019) Amelia Ho. Roles de las tres líneas de defensa para la seguridad de la información y gobierno. ISACA Journal.

Gumucio (2021), Iván Miguel Braga Calderón. Tesis para Maestria. “Guía de implementación de un programa de gestión de riesgos Ciberseguridad en entidades de intermediación financiera”. Universidad de Chile.

Vásquez (2021), Rubio de Jesús Vásquez Bustamante. Tesis para Maestría. “Ciberseguridad basada en analítica para bases de datos Oracle”. Fundación Universitaria Konrad Lorenz de Bogotá, Colombia.

Reinoso (2017), Andrés Rodrigo Reinoso Córdova. Tesis de Titulación. “Análisis y evaluación de riesgos de seguridad informática a través del análisis de tráfico en redes de área local.”. Escuela Politécnica Nacional de Quito, Ecuador.

Huaylla y Vargas (2022), Alejandrina Huaylla Quispe y Marina Vargas Pancorbo. Tesis para Titulación. “Gestión de tecnologías de información y comunicación y los procesos de seguridad informática en el gobierno regional de Apurímac”, Universidad Tecnológica de los Andes de Abancay-Apurímac, Perú.

Manrique (2022). Victor Hugo Manrique Reyna. Tesis para Maestría. “Modelo de ciberseguridad para mejorar la gestión de tecnología de la información de un Instituto Superior Tecnológico público”. Universidad Cesar Vallejo. Lima-Perú.

Cornejo y Lezama (2022). Alex Jonatan Cornejo Miranda y Arturo Ramón Lezama Calvo. Tesis para Titulación. “Propuesta de sistema de gestión de seguridad de la información para garantizar la seguridad de la información en la sub gerencia de tecnología de la información del Gobierno Regional de la Libertad”. Universidad Cesar Vallejo. Trujillo-Perú.

ISACA (2020). ISACA Interactive Glossary & Term Translations. https://www.isaca.org/resources/glossary

Kaspersky (2020). ¿Qué es la ciberseguridad? https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

RiskLens(2021). Fundamentos FAIR. Libro realizado por RiskLens.

NCSC (2019). Risk management for cyber security. https://www.ncsc.gov.uk/collection/board-toolkit/risk-management-for-cyber-security

Kaspersky (2021). Ciberataques en América Latina crecen un 24% durante los primeros ocho meses de 2021. https://latam.kaspersky.com/blog/ciberataques-en-america-latina-crecen-un-24-durante-los-primeros-ocho-meses-de-2021/22718/

NCSC2 (2019). Implementing effective cyber security measures. https://www.ncsc.gov.uk/collection/board-toolkit/implementing-effective-cyber-security-measures

Moral-Arce (2014). Ignacio Moral-Arce. Elección del método de evaluación cuantitativa de una política pública

MonteCarlo (2019). En qué consiste el método de simulación de Monte Carlo. https://www.ealde.es/metodo-simulacion-monte-carlo/

SBS (2019). Ley general del sistema financiero peruano. https://www.sbs.gob.pe/Portals/0/jer/LEY_GENERAL_SISTEMA_FINANCIERO/20190201_Ley-26702.pdf

DeepSecurity (2020). Reporte de Ciberseguridad en las Aplicaciones Móviles de Home banking en Perú. https://www.deepsecurity.pe/reporte-de-ciberseguridad-en-las-aplicaciones-moviles-de-homebanking-en-peru

SBS (2020). Listado de Bancos. https://www.sbs.gob.pe/supervisados-y-registros/empresas-supervisadas/directorio-del-sistema-financiero/empresas-bancarias