**PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ**

**FACULTAD DE CIENCIAS E INGENIERÍA**

# GUÍA PARA EL ANÁLISIS DE RIESGOS DE CIBERSEGURIDAD Y PRIVACIDAD DE DATOS PARA EL ASEGURAMIENTO DEL CUMPLIMIENTO DE ENTIDADES BANCARIAS EN EL PERÚ, USANDO NIST CSF Y NIST SP 800-37

**Tesis para obtener el título profesional de Ingeniero Informático**

**AUTOR:**

Távara Dávila, Edinson Ramiro

**ASESOR:**

Huamán Monzón, Fernando Miguel

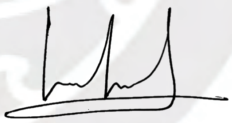
Lima, Noviembre, 2024

**Informe de Similitud**

Yo, **Fernando Miguel Huamán Monzón,** docente de la **Facultad de Ciencias e Ingeniería** de la Pontificia Universidad Católica del Perú, asesor de la tesis titulada **Guía para el análisis de riesgos de ciberseguridad y privacidad de datos para el aseguramiento del cumplimiento de entidades bancarias en el Perú, usando NIST CSF y NIST SP 800-37**, del autor **Tavara Davila, Edinson Ramiro**, dejo constancia de lo siguiente:

- El mencionado documento tiene un índice de puntuación de similitud de **18**%. Así lo consigna el reporte de similitud emitido por el software *Turnitin* el 27/11/2024.
- He revisado con detalle dicho reporte y la Tesis o Trabajo de Suficiencia Profesional, y no se advierte indicios de plagio.
- Las citas a otros autores y sus respectivas referencias cumplen con las pautas académicas.

Lima, viernes 29 de noviembre de 2024

| | |
|---|---|
| HUAMÁN MONZÓN, Fernando Miguel | |
| DNI: 70005931 | Firma  |
| ORCID: /0000-0003-1417-3466 | |

## Resumen

En la actualidad los avances tecnológicos y las amenazas cibernéticas para una entidad bancaria requieren un enfoque proactivo para identificar y gestionar los riesgos asociados a la seguridad de la información. De este modo debido a la creciente importancia en ciberseguridad y la privacidad de datos en el sector bancario es necesario gestionar adecuadamente los riesgos cibernéticos presentes en su actividad para lograr el cumplimiento normativo vigente. En este proceso se debe lograr identificar las obligaciones de cumplimiento, vulnerabilidades, amenazas y riesgos específicos en ciberseguridad y privacidad de datos en el sector bancario peruano. Así como de diseñar controles efectivos que ayuden a garantizar la seguridad de la información y lograr el cumplimiento normativo en las entidades bancarias.

El presente trabajo de fin de carrera realiza la investigación y análisis sobre las obligaciones de cumplimiento normativo entre los aspectos de ciberseguridad y privacidad de datos necesarios a cumplir por las entidades bancarias. Así como de los elementos específicos al abordar el diseño e implementación de estrategias como guías específicas para mantener la seguridad cibernética con el uso de los marcos de trabajo NIST CSF y NIST SP 800-37. El uso de estos marcos de trabajo permite abordar adecuadamente las vulnerabilidades y amenazas presentes en las obligaciones de cumplimiento bancaria en relación con el activo de información presente en una entidad bancaria. Así también al lograr gestionar y evaluar el conjunto de riesgos identificados sobre cada uno de los activos de información. Por último, al diseñar métodos de respuesta por medio de los controles de seguridad ante incidentes cibernéticos al evaluar los riesgos y controles diseñados para los activos de información.

## Dedicatoria y agradecimiento

Dedico este proyecto de fin de carrera a mi familia. A mis padres, Hilda y Edinson, por su apoyo incondicional y por abrirme todas las puertas necesarias para lograr mis objetivos. También a mi hermana Brenda por su constante apoyo y motivación.

Agradezco profundamente a mi asesor, Fernando Huamán Monzón, por su invaluable guía, dedicación y consejo a lo largo de todo el proceso de este proyecto, lo cual fue fundamental para alcanzar con éxito todos los objetivos propuestos.

# TABLA DE CONTENIDOS

# ÍNDICE DE TABLAS

# ÍNDICE DE FIGURAS

# Capítulo 1. Generalidades

## 1.1. Problemática

El presente capítulo desarrolla la problemática central del proyecto de fin de carrera relacionada con la guía para el análisis de riesgos de ciberseguridad y privacidad de datos para el aseguramiento del cumplimiento en las entidades bancarias del Perú. En particular, se desarrolla propiamente la descripción del problema y la situación actual en la que se encuentra el mismo. En este sentido, se ha realizado el esquema diseñado para el árbol de problemas, la descripción del árbol de problemas y la selección del problema para el presente proyecto, que en conjunto permiten una mejor comprensión de la situación actual y las posibles soluciones.

### 1.1.1. Árbol de problemas

La sección del árbol de problemas presenta los problemas identificados en la Tabla 1 para la problemática mediante la identificación y análisis del problema central relacionando las causas y efectos que lo implican.

Tabla 1 de problemas

*Árbol de problemas*

| | | | | |
|---|---|---|---|---|
| **Problemas Efectos** | Se generan sanciones por el incumplimiento de las obligaciones. | Los activos de información expuestos por las vulnerabilidades y amenazas no identificadas relacionadas a ciberseguridad y privacidad de datos. | Alta probabilidad de materialización de los riesgos de ciberseguridad y privacidad de datos generando un impacto negativo en las entidades bancarias. | No se generan los suficientes esfuerzos en diseño de controles para el tratamiento de riesgos en ciberseguridad y privacidad de datos para las entidades bancarias. |
| **Problema Central** | Inadecuada gestión de los riesgos de ciberseguridad y privacidad de datos como parte del aseguramiento de cumplimiento de las entidades bancarias del Perú. | | | |

| | | | | |
|---|---|---|---|---|
| **Problemas Causas** | Inadecuada identificación de las obligaciones de cumplimiento en las entidades bancarias. | Inadecuada identificación de las vulnerabilidades y amenazas de ciberseguridad y privacidad de datos en las entidades bancarias. | Inadecuada identificación de los riesgos en ciberseguridad y privacidad de datos en las entidades bancarias. | Limitado diseño de controles de ciberseguridad y privacidad de datos para abordar los riesgos identificados en las entidades bancarias. |

*Nota.* Esta tabla muestra el árbol de problemas desarrollado para describir de forma concisa la problemática.

### 1.1.2. Descripción

La tendencia actual en la actividad bancaria se ha desplazado de las operaciones de forma presencial hacia la banca por internet y la digitalización completa de los servicios por medio de mejoras en la accesibilidad y digitalización de los servicios (Malinka et al., 2022) ofrecidos por las entidades bancarias. De esta forma según SwissFinanceCouncil (apud Malinka et al., 2022) estima que en el año 2020 aproximadamente el 60% de las operaciones bancarias a nivel mundial se realizaron por medio de canales en línea o telefónico. En otras palabras, las entidades bancarias buscan facilitar el acceso de las personas a nuevos canales por medio de la digitalización de los servicios que se ofrecen. Aunque, para una institución bancaria esto significa una situación de retos en los aspectos de seguridad para la administración de los sistemas de información que actualmente se ofrecen.

Dado esto, los diversos servicios ofrecidos por una entidad bancaria tienen como objetivo ser fáciles de operar y accesibles de forma instantánea, aunque en algunos casos sólo representan una ilusión de seguridad (Wodo et al., 2021) y no aluden a sistemas realmente seguros. De esta forma Pham (apud Al-Alawi & Al-Bassam, 2019) menciona que el personal de la entidad bancaria puede no ser consciente de las consecuencias reales de sus acciones para mantener seguros los sistemas; así como si están siguiendo la normativa de cumplimento

establecido por las autoridades locales en forma de leyes y regulaciones para asegurar que se cumplen con los requisitos normativos en seguridad de los sistemas de información.

En esta medida, resguardar los activos de información dentro de la entidad bancaria debe representar el desarrollo de las actividades necesarias por medio del planteamiento de controles requeridos (Teodoro et al., 2015) y específicos para lograr los compromisos de cumplimiento en seguridad, con el fin de mantener los sistemas seguros frente a cualquier riesgo potencial derivado del uso malicioso o inadecuado sobre la información que resguarden. No obstante, para garantizar el cumplimiento de los requisitos legales por medio de las directrices internas en una entidad bancaria se revisan de forma manual y consume mucho tiempo dentro del ambiente de la entidad bancaria (Becker & Buchkremer, 2019). Por lo tanto, en el proceso es posible que las acciones de cumplimiento llevadas a cabo dentro de la entidad bancaria den lugar a errores inadvertidos, donde no se logren identificar adecuadamente los riesgos asociados de las obligaciones de cumplimiento relacionadas con los sistemas de información. Ante los posibles riesgos y el inadecuado diseño de medidas en una entidad bancaria en el Perú, en el año 2020 la Autoridad Nacional de Protección de Datos Personales (ANPD) para los sistemas en sus actividades de cumplimiento normativo recomienda que se deben adoptar medidas que garanticen la confidencialidad, integridad y disponibilidad de la información (ANPD, 2020b) para salvaguardarla.

Por consiguiente, a fin de proteger la integridad de los sistemas de información en una entidad bancaria, se evidencia que existen riesgos inherentes en las actividades que llevan a cabo los trabajadores en relación con los sistemas que en su labor administran para cumplir con las obligaciones de cumplimiento regulatorio. De este modo entre los riesgos en ciberseguridad relacionados con los sistemas pueden identificarse como, por ejemplo, a través del uso de *backdoors* en donde un atacante puede sortear el proceso normal de autorización debido a una configuración deficiente de los sistemas (Mahalle et al., 2018) y comprometa la

información confidencial de los clientes de la entidad bancaria que permita la realización de operaciones no autorizadas. También, con los incidentes de seguridad generados por brechas en el sistema, la manipulación inadecuada o el robo de los datos que generen la exposición de la información confidencial de los clientes (Mahalle et al., 2018). Estos incidentes de seguridad provocan que la información, como activo principal de los sistemas de información de la entidad bancaria, quede expuesta y se vulneren las normativas de cumplimiento vigentes en privacidad de datos requeridas para las operaciones realizadas por las entidades bancarias en su proceso de adhesión a las normativas vigentes.

Con el fin de que una organización bancaria abarque adecuadamente las obligaciones de cumplimiento en el Perú se presentan ciertas directivas y reglamentación derivadas de la Ley N.º 29733, Ley de Protección de Datos Personales. Estas directivas definen las actividades a realizar para el tratamiento adecuado de los datos personales, así como las medidas pertinentes a realizar para abordar situaciones inesperadas ante algún tipo de pérdida, alteración o brecha no autorizada de los datos personales. Las actividades para lograr el cumplimiento por la Ley N.º 29733, Ley de Protección de Datos Personales, representarían el conjunto de obligaciones en privacidad de datos de una entidad bancaria para el tratamiento de los datos de los clientes y trabajadores que realizan operaciones con la entidad. Así pues, la ley representa los derechos sobre la titularidad de los datos personales y sobre cómo el titular como objetivo del tratamiento a realizarse tiene derechos y obligaciones sobre el conjunto de datos recopilados al ser tratados. Además, la norma presenta los efectos del consentimiento informado que debe realizar la organización bancaria con el titular de los datos recopilados mediante la presentación de un anuncio claro y preciso que manifiesta la finalidad de la actividad de recopilación de los datos personales.

Adicionalmente, la reglamentación en ciberseguridad de los activos de información de las entidades bancarias en el Perú se realiza por medio de la normativa provista por la

Superintendencia de Banca y Seguros del Perú (SBS) para las entidades financieras entre las que se encuentra las entidades bancarias principalmente por medio de la Resolución S.B.S. N.º 504-2021 que presenta los procesos requeridos para lograr el cumplimiento de ciberseguridad en los sistemas de información internos. El proceso para lograr el cumplimiento en ciberseguridad define ciertas obligaciones como el control de accesos, la creación de un comité de riesgos, la implementación de un programa para la identificación de activos, el desarrollo de un análisis propio de las amenazas y vulnerabilidades asociadas a los activos que se controlan. Además, la norma presenta la necesidad de contar con políticas de seguridad que detallen cómo se tratará la gestión de riesgos en ciberseguridad con el objetivo de poder monitorear los riesgos asociados entre los servicios ofrecidos.

En consideración a los requisitos de cumplimiento que la entidad bancaria debe cumplir al realizar procesos de digitalización de las actividades internas y el uso de diversos sistemas de información para brindar los servicios, es necesario establecer procedimientos internos destinados a garantizar el cumplimiento. En el Perú ante la sofisticación, la frecuencia y persistencia de los riesgos cibernéticos (SBS, 2019) la SBS presenta como guía por medio de elementos específicos que al diseñar e implementar estrategias para la seguridad cibernética se pueden abordar las situaciones de cumplimiento, por ejemplo, al adoptar un marco de trabajo, definir métodos de respuesta ante incidentes, evaluar los riesgos y plantear controles (SBS, 2019). En otras palabras, los procesos internos de una entidad bancaria deben ser respaldados por controles individuales que, en conjunto, aseguren el cumplimiento regulatorio. Por lo tanto, resulta importante gestionar apropiadamente los sistemas de información y los datos personales de los clientes durante el procesamiento de la información para asegurar el cumplimiento derivado de los compromisos y acuerdos contractuales de la entidad bancaria con los usuarios de sus sistemas. Caso contrario, como ha ocurrido con una entidad bancaria en el Perú se

enfrentaría a un procedimiento administrativo sancionador por la violación de los sistemas de seguridad al permitir el acceso de terceros no autorizado (ANPD, 2019a).

En función de lo planteado debe ser prioridad para las entidades bancarias la protección de los sistemas de información porque contienen los recursos vitales (Addae et al., 2019) que necesita una entidad bancaria para realizar su operativa y, sobre todo, denota el valor de establecer una estrategia para los procesos de seguridad que permitan lograr el cumplimiento regulatorio. Por ejemplo, el estado peruano desde el Poder Ejecutivo presentó un proyecto de ley a fin de promover un marco legal para una adecuada gobernanza de los datos que controlan los sistemas de información del estado; con el objetivo de prevenir los riesgos en confidencialidad, integridad y disponibilidad de los sistemas (Ministerio de Justicia y Derechos Humanos, 2021) para garantizar la seguridad de los sistemas y la privacidad de los datos sensibles. Por esta razón las decisiones tomadas por la entidad bancaria para proteger los sistemas de información mediante la identificación de riesgos y el diseño de los controles permiten abordar las situaciones de cumplimiento en ciberseguridad y privacidad de datos que son requeridos por el ente regulatorio local.

En vista de ello, ante los riesgos inherentes de seguridad que presenta una organización bancaria resulta necesario desarrollar una guía para el análisis de los riesgos de ciberseguridad y privacidad de datos que permita lograr el cumplimiento de las obligaciones y compromisos locales. Por ese motivo, el análisis de riesgos debe incluir un conocimiento detallado de las vulnerabilidades de los sistemas de información, los cuáles pueden poner en riesgo la seguridad de la entidad bancaria. Así como, es necesario identificar las amenazas que pueden derivar en un ataque y comprometer la seguridad de los sistemas de la entidad bancaria. Considerando en todo momento que las entidades bancarias están expuestas a diversos tipos de ataques como de *ransomware*, *hacking*, robo de información, interrupción de los servicios internos y con los proveedores; así como de fraudes a las cuentas de sus clientes (SBS, 2022).

En definitiva, resulta conveniente identificar adecuadamente el conjunto de obligaciones locales de una institución bancaria para prevenir los riesgos derivados del uso no autorizado e inadecuado de los sistemas de información y conseguir el aseguramiento del cumplimiento regulatorio establecido para la ejecución adecuada de la operativa diaria de los controles diseñados para mantener seguros los sistemas. En consecuencia, es necesario abordar las situaciones de cumplimiento locales definiendo sus riesgos inherentes desde una perspectiva adecuada y el diseño de los controles que aseguren la continuidad de las operaciones internas de la entidad bancaria de forma segura e ininterrumpida. En este sentido, los servicios ofrecidos en ciberseguridad y privacidad de datos de los sistemas de información deben permanecer como prioridad absoluta en cuanto a la tolerancia a los riesgos (Mahalle et al., 2018).

### 1.1.3. Problema seleccionado

A partir de los problemas previamente expuestos es necesario llevar a cabo un análisis de los riesgos asociados a la ciberseguridad y privacidad de datos, como resultado de las obligaciones y compromisos necesarios para garantizar el cumplimiento de las normativas locales. Por consiguiente, el análisis de los riesgos permitirá identificar las vulnerabilidades y amenazas vinculadas a cada uno de los activos de información presentes en las obligaciones de cumplimiento en ciberseguridad y privacidad de datos de la entidad bancaria. En este proceso es esencial detectar las posibles amenazas y vulnerabilidades que puedan dar lugar a riesgos en los sistemas internos de la entidad bancaria, y puedan comprometer la seguridad de los sistemas internos de la entidad bancaria. Además, en respuesta a los riesgos asociados a la entidad bancaria resulta crucial establecer los controles de seguridad necesarios para poder mitigar los riesgos y garantizar el cumplimiento requerido en ciberseguridad y protección de datos personales. Por consiguiente, se considera como problema central la inadecuada gestión de los

riesgos de ciberseguridad y privacidad de datos en el aseguramiento del cumplimiento para las entidades bancarias en el Perú.

## 1.2. Objetivos

La sección de objetivos presentará el objetivo general, los objetivos específicos y los resultados esperados para cada objetivo específico.

### 1.2.1. Objetivo general

Elaborar una guía para el análisis de riesgos de ciberseguridad y privacidad de datos que asegure el cumplimiento de las entidades bancarias en el Perú, utilizando los marcos de trabajo NIST CSF y NIST SP 800-37.

### 1.2.2. Objetivos específicos

O1. Identificar el conjunto de obligaciones de cumplimiento en ciberseguridad y privacidad de datos para las entidades bancarias en el Perú.

O2. Identificar las vulnerabilidades inherentes y amenazas de ciberseguridad y privacidad de datos para las entidades bancarias.

O3. Identificar los riesgos de ciberseguridad y privacidad de datos para las entidades bancarias.

O4. Diseñar los controles en ciberseguridad y privacidad de datos como parte del proceso de cumplimiento de las entidades bancarias.

O5. Desarrollar una guía que integre los análisis y controles diseñados, asegurando su efectividad y aplicabilidad en las entidades bancarias en el Perú.

### 1.2.3. Resultados esperados

R1 para O1. Obligaciones de privacidad de datos para las entidades bancarias.

R2 para O1. Obligaciones de ciberseguridad para las entidades bancarias.

R1 para O2. Catálogo de vulnerabilidades de las obligaciones identificadas.

R2 para O2. Catálogo de amenazas de las obligaciones identificadas.

R1 para O3. Catálogo de riesgos de ciberseguridad y privacidad de datos.

R1 para O4. Diseño de controles para los riesgos de ciberseguridad y privacidad de datos identificados.

R1 para O5. Guía para el análisis de riesgos de ciberseguridad y privacidad de datos para el aseguramiento del cumplimiento de entidades bancarias en el Perú.

### 1.2.4. Mapeo de objetivos, resultados y medios de verificación

La selección de objetivos en relación con los resultados esperados se presenta en la Tabla 2, Tabla 3, Tabla 4, Tabla 5 y Tabla 6 para cada resultado esperado con el medio de verificación e indicador objetivamente verificable respectivo para comprobar que se alcanzaron los resultados deseados.

Tabla 2

*Resultados esperados con el medio de verificación e indicador del objetivo 1*

| **Objetivo 1:** Identificar el conjunto de obligaciones de cumplimiento en ciberseguridad y privacidad de datos para las entidades bancarias en el Perú. | | |
|---|---|---|
| **Resultado** | **Medio de verificación** | **Indicador objetivamente verificable** |
| Obligaciones de cumplimiento en privacidad de datos para las entidades bancarias. | Lista de obligaciones de cumplimiento en privacidad de datos. | Abarcar el 100% de obligaciones de cumplimiento de una entidad bancaria sobre privacidad de datos cubiertas y validado por un especialista de seguridad en el sector bancario. |
| Obligaciones de cumplimiento en ciberseguridad para las entidades bancarias. | Lista de obligaciones de cumplimiento en ciberseguridad. | Abarcar el 100% de obligaciones de cumplimiento de una entidad bancaria sobre ciberseguridad cubiertas y validado por un especialista de seguridad en el sector bancario. |

Tabla 3

*Resultados esperados con el medio de verificación e indicador del objetivo 2*

| **Objetivo 2:** Identificar las vulnerabilidades inherentes y amenazas de ciberseguridad y privacidad de datos para las entidades bancarias. | | |
|---|---|---|
| **Resultado** | **Medio de verificación** | **Indicador objetivamente verificable** |
| Catálogo de vulnerabilidades de las obligaciones identificadas. | Documento con las vulnerabilidades identificadas de las obligaciones. | Documento validado y aprobado al 100% por un especialista en seguridad de la información o privacidad de datos. |
| Catálogo de amenazas de las obligaciones identificadas. | Documento con las amenazas identificadas. | Documento validado y aprobado al 100% por un especialista en seguridad de la información o privacidad de datos. |

Tabla 4

*Resultados esperados con el medio de verificación e indicador del objetivo 3*

| **Objetivo 3:** Identificar los riesgos de ciberseguridad y privacidad de datos para las entidades bancarias. | | |
|---|---|---|
| **Resultado** | **Medio de verificación** | **Indicador objetivamente verificable** |
| Catálogo de riesgos de ciberseguridad y privacidad de datos. | Matriz de riesgos de ciberseguridad y privacidad de datos identificados. | Matriz de riesgos validado y aprobado al 100% por un especialista en seguridad de la información o privacidad de datos. |

Tabla 5

*Resultados esperados con el medio de verificación e indicador del objetivo 4*

| **Objetivo 4:** Diseñar los controles en ciberseguridad y privacidad de datos como parte del proceso de cumplimiento de las entidades bancarias. | | |
|---|---|---|
| **Resultado** | **Medio de verificación** | **Indicador objetivamente verificable** |
| Diseño de controles para los riesgos de ciberseguridad y privacidad de datos identificados. | Matriz del diseño de controles de seguridad para abordar los riesgos identificados de ciberseguridad y privacidad de datos. | Matriz del diseño de controles de seguridad validado y aprobado al 100% por un especialista en seguridad de la información o privacidad de datos. |

Tabla 6

*Resultados esperados con el medio de verificación e indicador del objetivo 5*

| **Objetivo 5:** Desarrollar una guía que integre los análisis y controles diseñados, asegurando su efectividad y aplicabilidad en las entidades bancarias en el Perú. | | |
|---|---|---|
| **Resultado** | **Medio de verificación** | **Indicador objetivamente verificable** |
| Guía para el análisis de riesgos de ciberseguridad y privacidad de datos para el aseguramiento del cumplimiento de entidades bancarias en el Perú. | Informe del diseño de controles para abordar los riesgos identificados de ciberseguridad y privacidad de datos. | Informe del diseño de controles validado y aprobado al 100% por un especialista en seguridad de la información o privacidad de datos. |

## 1.3. Herramientas, Métodos y Procedimientos

La presente sección presenta las herramientas, métodos y procedimientos que se emplean para obtener los resultados esperados de cada objetivo del proyecto de fin de carrera en la Tabla 7, Tabla 8, Tabla 9, Tabla 10 y Tabla 11.

Tabla 7

*Herramientas y métodos por usar en los resultados esperados del primer objetivo*

| **Objetivo 1:** Identificar el conjunto de obligaciones de cumplimiento en ciberseguridad y privacidad de datos para las entidades bancarias en el Perú. | |
|---|---|
| **Resultado esperado** | **Herramientas y métodos** |
| Obligaciones de privacidad de datos para las entidades bancarias. | - ISO 37301 cláusula 4.5 |
| Obligaciones de ciberseguridad para las entidades bancarias | - ISO 37301 cláusula 4.5 |

Tabla 8

*Herramientas y métodos por usar en los resultados esperados del segundo objetivo*

| **Objetivo 2:** Identificar las vulnerabilidades inherentes y amenazas de ciberseguridad y privacidad de datos para las entidades bancarias. | |
|---|---|
| **Resultado esperado** | **Herramientas y métodos** |
| Catálogo de vulnerabilidades de las obligaciones identificadas. | - ISO 27005<br>- NIST CSF<br>- NIST SP 800-37 Rev. 2 |
| Catálogo de amenazas de las obligaciones identificadas. | - ISO 27005<br>- NIST CSF<br>- NIST SP 800-37 Rev. 2 |

Tabla 9

*Herramientas y métodos por usar para el resultado esperado del tercer objetivo*

| **Objetivo 3:** Identificar los riesgos de ciberseguridad y privacidad de datos para las entidades bancarias. | |
|---|---|
| **Resultado esperado** | **Herramientas y métodos** |
| Catálogo de riesgos de ciberseguridad y privacidad de datos. | - NIST SP 800-30<br>- NIST CSF<br>- NIST SP 800-37 Rev. 2 |

Tabla 10

*Herramientas y métodos por usar para el resultado esperado del cuarto objetivo*

| **Objetivo 4:** Diseñar los controles en ciberseguridad y privacidad de datos como parte del proceso de cumplimiento de las entidades bancarias. | |
|---|---|
| **Resultado esperado** | **Herramientas y métodos** |
| Diseño de controles para los riesgos de ciberseguridad y privacidad de datos identificados. | - NIST CSF<br>- NIST SP 800-37 Rev. 2 |

Tabla 11

*Herramientas y métodos por usar para el resultado esperado del quinto objetivo*

| **Objetivo 5:** Desarrollar una guía que integre los análisis y controles diseñados, asegurando su efectividad y aplicabilidad en las entidades bancarias en el Perú. | |
|---|---|
| **Resultado esperado** | **Herramientas y métodos** |
| Guía para el análisis de riesgos de ciberseguridad y privacidad de datos para el aseguramiento del cumplimiento de entidades bancarias en el Perú. | - NIST CSF<br>- NIST SP 800-37 Rev. 2 |

### 1.3.1. International Organization for Standardization 37301

La *International Organization for Standardization* (ISO) 37301 presenta las directrices en forma de guía para que una organización pueda gestionar adecuadamente sus diversas situaciones de cumplimiento, en este caso será usado para una entidad bancaria. Si bien, es de conocimiento del autor del presente proyecto de fin de carrera que la ISO 37301 es utilizada en su conjunto para la implementación de un Sistema de Gestión de Cumplimiento, para el presente proyecto de fin de carrera se hará uso de la ISO 37301 específicamente la cláusula 4.5. al ser una buena referencia internacionalmente aceptada para la fase de identificación de obligaciones de cumplimiento que se requiere para este proyecto de fin de carrera. De este modo se hace uso de la herramienta en la cláusula 4.5 apartado a) que resalta los puntos en que las organizaciones deben identificar los compromisos de cumplimiento y como las diversas actividades cumplimiento deben estar relacionadas con sus actividades, productos y servicios (ISO, 2021) internos de tal forma que una vez identificados se puedan conocer las implicancias reales. Adicionalmente de la herramienta en la cláusula 4.5 apartado b) se presenta la necesidad de establecer ciertos mecanismos para la identificación de las leyes, regulación o situaciones de cumplimiento adquiridas o que tuvieron algún cambio (ISO, 2021) en el tiempo desde el momento desde su identificación. En conjunto las cláusulas mencionadas permiten evaluar las diversas obligaciones de cumplimiento ante algún cambio y, también, comprobar el cumplimiento con la regulación actual en ciberseguridad y privacidad de datos.

### 1.3.2. International Organization for Standardization 27005

La International Organization for Standardization (ISO) 27005 presenta los lineamientos para la identificación de riesgos dentro de una organización (ISO, 2018). En este sentido el documento se usa como guía para determinar las vulnerabilidades en una organización, en este caso será usado para una entidad bancaria, y como cada una de estas al ser explotadas por una amenaza ocasionan situaciones de riesgo. Con este fin la ISO se usa como referencia ante los principales ejemplos de vulnerabilidades y amenazas que se presentan en la herramienta para una organización, y se enfoca su uso para la situación particular de una entidad bancaria en base a las correspondientes obligaciones de cumplimiento. De esta manera, al utilizar la herramienta, se garantiza que las vulnerabilidades y amenazas que se identifiquen estén relacionadas a la situación de una entidad bancaria con las normas y regulaciones que rigen su funcionamiento.

### 1.3.3. NIST Special Publication 800-30

La NIST Special Publication (SP) 800-30 describe el proceso para la gestión y evaluación los riesgos (NIST, 2012). En esta evaluación, el documento como herramienta establece un marco de referencia para identificar y evaluar los riesgos por medio de una metodología de trabajo que permite relacionar la probabilidad de ocurrencia de un riesgo y su capacidad para que el riesgo genere un impacto adverso dentro de la entidad bancaria.

### 1.3.4. NIST Cybersecurity Framework 2.0

El marco de trabajo NIST Cybersecurity Framework (CSF) 2.0 se utiliza como guía para el desarrollo de las actividades en el análisis de riesgos, así como en la necesidad de la identificación de las vulnerabilidades y amenazas en una entidad bancaria entre sus diversas situaciones de cumplimiento al ser identificadas. Inicialmente el presente trabajo de fin de carrera comenzó utilizando la versión 1.1 del NIST CSF que presenta cinco funciones. Estas funciones se mantienen en la nueva versión del NIST CSF 2.0. Sin embargo, debido a la

actualización a la versión 2.0 del marco de trabajo se ha realizado un mapeo general de los cambios descritos por NIST para que el presente trabajo se alinee con las nuevas directrices, trabajando así en la versión del CSF 2.0 con seis funciones.

El NIST CSF 2.0 presenta las siguientes seis funciones definidas: gobernar, identificar, proteger, detectar, responder y recuperar (The NIST Cybersecurity Framework (CSF) 2.0 [CSF 2.0], 2024), Asimismo, se han introducidos cambios en la división de las categorías y subcategorías, complementando de forma más precisa el desarrollo de cada una de las funciones. El número de subcategorías en la versión del NIST CSF 2.0 está diseñado intencionalmente de forma no secuencial para que se entienda que algunas subcategorías fueron movidas entre la versión del CSF 1.1 y la 2.0 (CSF 2.0, 2024), permitiendo sobre estos cambios descritos desarrollar un análisis de riesgos adecuado con el planteamiento de controles efectivos para mitigar los riesgos.

### 1.3.5. NIST Special Publication 800-37

El marco de trabajo NIST Special Publication (SP) 800-37 presenta los lineamientos a desarrollar para el planteamiento correcto de controles en los sistemas de seguridad y de privacidad de datos dentro de una organización. El marco de trabajo usa el Risk Management Framework (RMF) el cual establece las estrategias necesarias para manejar riesgos ante situaciones de ciberseguridad y privacidad de datos no previstos (RMFISO, 2018). De esta forma, el RMF proveerá los lineamientos para la integración de los requerimientos y controles necesarios en ciberseguridad y privacidad en los procesos de arquitectura y sistemas de ingeniería de la organización (RMFISO, 2018) y poder categorizar de forma adecuada las situaciones de cumplimiento previamente identificadas. La formulación dependerá del conjunto de obligaciones identificadas mediante el uso de la ISO 37301 cláusula 4.5 y los niveles de cumplimiento interno de la entidad bancaria. Por lo tanto, se establece una estructura

definida para lograr los objetivos previstos por el marco de trabajo mediante las funciones de: preparar, categorizar, seleccionar, implementar, evaluar y autorizar (RMFISO, 2018).

# Capítulo 2. Marco Conceptual, Teórico y Regulatorio

El presente capítulo presentará el marco conceptual, teórico y regulatorio relacionado al tema de cumplimiento para las entidades bancarias en ciberseguridad y privacidad de datos para el proyecto final de carrera.

## 2.1. Marco Conceptual

La sección del marco conceptual desarrollará la definición de ciertos términos que serán usados en el presente documento.

### 2.1.1. Entidad financiera

La entidad financiera constituye la empresa que opera como intermediario financiero entre las personas y empresas que le entregan su dinero, y lo oferta a otras personas y empresas que lo necesitan (SBS, 2009). La entidad financiera divide sus operaciones entre las de intermediación directa para las entidades bancarias que reciben el dinero de las personas y usan ese dinero bajo diversas modalidades de crédito (SBS, 2009), y de intermediación indirecta para las entidades no bancarias que participan en la captación y canalización de los recursos financieros (SBS, 2009).

### 2.1.2. Entidad bancaria

La entidad bancaria es aquella empresa cuyo giro de negocio principal consiste en recibir el dinero de los clientes en forma de depósitos o bajo cualquier otra modalidad contractual; y utilizar el dinero de los depósitos, su propio capital y otras fuentes de financiación para conceder créditos (SBS, 2009).

### 2.1.3. Cumplimiento

El acto de demostrar la adhesión y habilidad que se cumplen los requisitos obligatorios por leyes y reglamentos, esto incluye los requisitos voluntarios derivados de las obligaciones contractuales y políticas internas (Information Systems Audit and Control Association [ISACA], apud en Al-Alawi & Al-Bassam, 2019). Por ejemplo, para la detección de una

actividad fraudulenta en una entidad bancaria se tienen que realizar operaciones de identificación y congelamiento de la operación conforme lo establece la regulación local para evitar situaciones ilegales como el lavado de dinero.

### 2.1.4. Privacidad de datos

Desarrollo de medidas concretas que garanticen el correcto manejo de la información personal dentro de una organización bajo un consentimiento informado (Conrad, 2019) en los lineamientos previamente acordados. Es decir, que el uso de la información personal relacionada con el sujeto objeto de los datos de la información privada, profesional o pública (Lakshmi et al., 2020) esté protegido.

### 2.1.5. Ciberseguridad

El proceso de proteger los sistemas de información mediante los procesos de prevención, detección y generar una respuesta a los ataques (Framework for Improving Critical Infrastructure Cybersecurity [FICIC], Version 1.1, 2018).

### 2.1.6. Vulnerabilidad

Debilidad en un sistema de información, en los procedimientos de seguridad del sistema, planteamiento o implementación de controles internos que podría ser explotados o provocados por una fuente de amenaza (RMFISO, 2018). Así como de fallos de seguridad del sistema de información (Kulik et al., 2022). Por ejemplo, cuando los sistemas no validan los datos de entrada dejando la posibilidad que se ejecute código malicioso.

### 2.1.7. Amenaza

La existencia de una circunstancia o evento con el potencial de afectar negativamente las operaciones de la organización, los activos de la organización, las personas, otras organizaciones o la Nación a través de un sistema mediante acceso no autorizado, destrucción, divulgación, modificación de información o denegación de servicios (RMFISO, 2018). Mediante el uso de una vulnerabilidad descubierta (Alsalamah, 2017) y que puede poner en

riesgo la seguridad de los sistemas de información. Por ejemplo, cuando se usa código malicioso en los sistemas de información expuestos y se logra robar información sensible.

### 2.1.8. Riesgo

Medida en la que una entidad se ve amenazada por una circunstancia o evento potencial relacionado a los impactos adversos que surgirían si acontece y la posibilidad que ocurran (FICIC, 2018). En particular cuando se conoce que existe cierta vulnerabilidad de que un agente externo ingrese al sistema, por lo que puede materializarse si no se realizan acciones pertinentes para evitar la amenaza.

### 2.1.9. Análisis de Riesgos

Es el proceso en el que se define el alcance, identifican y examinan las vulnerabilidades y amenazas que derivan en los riesgos. También, para determinar las posibles implicancias de la exposición y medir el impacto del riesgo identificado. En el proceso se determina el alcance como, por ejemplo, con la identificación de activos para comprender que ciertos sistemas como el de tarjetas de crédito si no siguen lineamientos de seguridad se encuentran expuestos a operaciones fraudulentas y que al no ser evaluadas correctamente la vulnerabilidad expuesta se puede concretar en la amenaza de la operación realizada de fraude.

### 2.1.10. Aseguramiento del cumplimiento

Descripción teórica sobre los procesos individuales a realizarse en la institución y cómo estos se llevarán a cabo mediante la ejecución diaria de los procesos dentro de la organización (Becker & Buchkremer, 2019). Así como, el desarrollo de la estrategia que se llevará a cabo para gestionar el cumplimiento de los procesos comerciales en la institución (Becker & Buchkremer, 2019).

## 2.2. Marco Teórico

La sección del marco teórico presentará los marcos y conceptos desarrollados para el presente trabajo de fin de carrera. En el proceso se abordan los marcos de trabajo NIST

Cybersecurity Framework (CSF) y NIST Special Publication (SP) 800-37 relacionados a los temas de ciberseguridad y privacidad de datos.

### 2.2.1. Marco de Trabajo NIST CSF 2.0

El marco de trabajo desarrollado para el NIST CSF 2.0 presenta los conceptos, guías y prácticas necesarias que manejan las organizaciones para el uso de herramientas requeridas para el desarrollo del marco de trabajo y abordar los riesgos en ciberseguridad (CSF 2.0, 2024). En el proceso de aplicación del marco de trabajo se definen los siguientes conceptos:

- El uso del CSF Core que concentra todas las actividades de ciberseguridad, categorías y subcategorías para gestionar los riesgos (CSF 2.0, 2024).
- Presentar un perfil definido de modo que se identifiquen los objetivos de ciberseguridad y las oportunidades de desarrollo (CSF 2.0, 2024).
- Desarrollar una perspectiva concreta sobre cómo abordar niveles de riesgos en ciberseguridad y los métodos efectivos de respuesta (CSF 2.0, 2024).

De este modo, se desprende la necesidad de un manejo adecuado de los niveles riesgos presentes en una organización; así como, poder desarrollar métodos de respuesta efectivos a los posibles riesgos derivados de las vulnerabilidades y amenazas. Por esta razón, es necesario definir una estrategia de gestión de riesgos eficaz que permita identificar, comunicar y ajustar situaciones de riesgos en ciberseguridad (CSF 2.0, 2024). a las necesidades de la organización. Así como, permitir manejar los riesgos identificados mediante el proceso de mitigar, transferir, evadir o aceptar los riesgos (CSF 2.0, 2024). Así mismo, en relación con el uso del CSF Core se tienen las siguientes funciones en específico:

- Gobernar (GV): Se plantea la estrategia de gestión de riesgos a nivel organizacional (CSF 2.0, 2024).

- Identificar (ID): Identificar los riesgos de ciberseguridad que tienen los sistemas, personas, activos y datos para priorizar adecuadamente la gestión de riesgos (CSF 2.0, 2024).
- Proteger (PR): Medidas de protección para la gestión de riesgos de los sistemas críticos (CSF 2.0, 2024).
- Detectar (DE): Detectan posibles ataques en eventos de ciberseguridad (CSF 2.0, 2024).
- Responder (RS): Actividades de respuesta a eventos de ciberseguridad (CSF 2.0, 2024).
- Recuperación (RC): Recuperar mediante un proceso planificado los servicios afectados por incidentes de ciberseguridad (CSF 2.0, 2024).

### 2.2.2. Desarrollo del marco de trabajo NIST SP 800-37 Rev. 2

El marco de trabajo NIST SP 800-37 Rev. 2 presenta la formulación del Risk Management Framework (RMF) para los lineamientos del desarrollo correcto de sistemas de seguridad y privacidad dentro de una organización (Risk management framework for information systems and organizations [RMFISO], 2018) ante riesgos de seguridad. El planteamiento correcto de los sistemas de seguridad dependerá del cumplimiento desarrollado de los lineamientos internos y los objetivos de la organización; así como, los definidos por el ente regulatorio local. Por esta razón, el RMF tiene como objetivo principal establecer estrategias para manejar los riesgos ante eventos de ciberseguridad y privacidad imprevistos, y poder responder (RMFISO, 2018) en concordancia a las necesidades planteadas por la organización.

De esta forma, el RMF proveerá los lineamientos para la integración de los requerimientos y controles necesarios en ciberseguridad y privacidad en los procesos de

arquitectura y sistemas de ingeniería de la organización (RMFISO, 2018). Por lo tanto, se establece una estructura definida para lograr los objetivos previstos por el marco de trabajo:

- Preparar la organización para establecer objetivos prioritarios (RMFISO, 2018).
- Categorizar los sistemas de información que procesan, almacenan y transmiten información (RMFISO, 2018).
- Seleccionar un conjunto de controles para los sistemas (RMFISO, 2018).
- Implementar los controles y describir cómo se emplean (RMFISO, 2018).
- Evaluar si los controles se implementan correctamente (RMFISO, 2018).
- Autorizar el uso de controles si el nivel de riesgo es aceptable (RMFISO, 2018).
- Monitorear los controles implementados y documentar los cambios efectuados (RMFISO, 2018).

Adicionalmente, los fundamentos de ciberseguridad para el RMF en NIST SP 800-37 se manifiestan desde el marco de trabajo NIST CSF (RMFISO, 2018) presentado en la sección 2.2.3 del presente documento de fin de carrera. Por lo que, el uso de los marcos de trabajo NIST SP 800-37 y NIST CSF se complementan en su desarrollo para el presente documento final de carrera.

## 2.3. Marco Regulatorio

La sección presentará el marco regulatorio relacionado al ámbito legal requerido en el proceso de cumplimiento para las entidades bancarias en el Perú sobre los asuntos de ciberseguridad y privacidad de datos.

### 2.3.1. Sobre Ciberseguridad

#### *2.3.1.1. Resolución SBS N.º 504-2021 Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad.*

El documento presenta la regulación desarrollada en el tema de ciberseguridad con el objetivo de establecer en forma de reglamento nacional los mejores estándares y prácticas desarrolladas internacionalmente para poder ser aplicadas a las empresas en el Perú (SBS, 2021). De tal forma que su desarrollo aborda la reglamentación para la gestión de los asuntos de ciberseguridad y sobre cómo se deben manejar los activos de información.

#### *2.3.1.2. Resolución SBS N.º 877-2020: Reglamento para la Gestión de la Continuidad del Negocio.*

El documento establece la reglamentación necesaria en la gestión requerida para la evaluación del análisis de los riesgos identificados dentro de una organización que permita asegurar la continuidad del negocio (SBS, 2020). De forma que, se desarrolle un análisis de riesgos para identificarlos y se pueda efectuar una evaluación sobre cómo prevenirlos para evitar la interrupción de la operativa de trabajo.

#### *2.3.1.3. Resolución SBS N.º 6523-2013 Reglamento de Tarjetas de Crédito y Débito.*

Establece los lineamientos en las normas y condiciones contractuales que deben las instituciones financieras lograr para cumplir con las condiciones necesarias de seguridad y evitar el uso fraudulento de las tarjetas de crédito y débito (SBS, 2013).

#### *2.3.1.4. Resolución SBS N.º 5570-2019 Modificatoria de la Resolución SBS N.º 6523-2013 Reglamento de Tarjetas de Crédito y Débito.*

Modifica el reglamento de la resolución SBS N.º 6523-2013 con el objetivo de reforzar las medidas de seguridad y los derechos de los ciudadanos al usar las tarjetas de crédito y débito de las entidades bancarias (SBS, 2019b).

### 2.3.2. Sobre Privacidad de datos

#### *2.3.2.1. Ley de Protección de Datos Personales - Ley N°29733.*

El documento establece los lineamientos requeridos por las organizaciones en relación con el cumplimiento de obligaciones sobre cómo se administran los datos personales. Los lineamientos desarrollan la obligación sobre los alcances para el tratamiento de la información derivados del manejo que le dan las instituciones privadas y públicas. Así como, los derechos y obligaciones que derivan sobre la titularidad de los datos del acreedor; el uso correcto de los bancos de información; y, también, sobre las infracciones derivadas de no cumplir con las obligaciones estipuladas (*Ley N° 29733. Ley de Protección de Datos Personales*, 2011). Por último, consigna que la Autoridad Nacional de Protección de Datos Personales (ANPD) como el órgano competente de realizar las acciones necesarias para supervisar el cumplimiento requerido por ley.

#### *2.3.2.2. Reglamento de la Ley de Protección de Datos Personales-Decreto Supremo N.º 003-2013-JUS.*

El documento desarrolla en forma de reglamento la Ley N.º 29733, Ley de Protección de Datos Personales, para garantizar el cumplimiento de las medidas definidas en la ley. Por consiguiente, el reglamento presenta las consignas requeridas en protección de datos personales para lograr el cumplimiento, por ejemplo, mediante el consentimiento informado del tratamiento de la información al solicitarlos, los alcances del uso de los bancos de información y las disposiciones generales sobre los derechos de los titulares de los datos personales (Autoridad Nacional de Protección de Datos Personales, 2013).

#### *2.3.2.3. Directiva de Seguridad - Resolución Directoral N.º 019-2013-JUS/DGPDP.*

Normativa que aprueba las obligaciones de cumplimiento para la reglamentación de la Ley N.º 29733, Ley de Protección de Datos Personales, y el reglamento que deriva de la ley con el Decreto Supremo N.º 003-2013-JUS (Ministerio de Justicia y Derechos Humanos [MINJUSDH], 2013).

#### *2.3.2.4. Directiva para el Tratamiento de Datos Personales mediante Sistemas de Videovigilancia - Resolución Directoral N.º 02-2020-JUS/DGTAIPD.*

Medida sobre la cuál la Autoridad Nacional de Protección de Datos Personales presenta la directiva para las obligaciones sobre el tratamiento de datos personales en los sistemas de videovigilancia aplicado para la Ley N.º 29733, Ley de Protección de Datos Personales (MINJUSDH, 2020).

#### *2.3.2.5. Guía práctica para la observancia del "Deber de Informar".*

Guía con descripción didáctica de cómo cumplir con el derecho de información personal (Autoridad Nacional de Protección de Datos Personales, 2019b). Documento desarrollado con el objetivo de poder abordar los incisos de la Ley N.º 29733, Ley de Protección de Datos Personales, para que las organizaciones puedan ser orientadas de una forma más práctica sobre el cumplimiento de la ley.

# Capítulo 3. Estado del Arte

## 3.1. Introducción

El presente capítulo comprenderá el estado del arte relacionado a la revisión sistemática de uso de herramientas de revisión de la literatura existente en el proceso de investigación relacionado al tema de ciberseguridad y privacidad de datos para el cumplimiento de las entidades bancarias.

## 3.2. Objetivos de Revisión

Se realizará la revisión sistemática de estudios sobre los riesgos que comprende los temas de ciberseguridad y privacidad de datos para las medidas de cumplimiento en las entidades bancarias. Así mismo, el tipo de investigación para los objetivos de revisión se realizará de forma empírica porque es necesario conocer diversos marcos y medidas formuladas para el tema planteado. El proceso de revisión del estado del arte se encontrará guiado por la metodología de trabajo por etapas propuesta por (Kitchenham & Charters, 2007) mediante el planeamiento, revisión y el posterior reporte de los resultados encontrados.

## 3.3. Preguntas de Revisión

Como medida para estructurar el planteamiento inicial se presentará un conjunto de preguntas para el proceso de revisión. Para la formulación de cada una de las preguntas relacionadas al tema del trabajo de fin de carrera se elaboró la Tabla 12; la tabla considera el uso de los criterios PICOC (Petticrew & Roberts, 2006).

Tabla 12

*Criterios generales PICOC*

| Criterio | Descripción |
|---|---|
| Población | Las entidades bancarias. |
| Intervención | Análisis de riesgos para el cumplimiento de ciberseguridad y privacidad de datos. |
| Comparación | (No aplica) |
| Resultados | La revisión sistemática de artículos e investigaciones sobre los riesgos de ciberseguridad y privacidad de datos para el cumplimiento de las entidades bancarias. |
| Contexto | Análisis de riesgos de ciberseguridad y privacidad de datos en entidades bancarias. |

*Nota.* Esta tabla muestra los criterios generales aplicados en el estado del arte para la pregunta de revisión.

De este modo, a partir de los resultados de la tabla 12 se plantean las siguientes preguntas de revisión:

- P1. ¿Cuáles son las principales obligaciones de cumplimiento de las entidades bancarias sobre ciberseguridad y privacidad de datos?
- P2. ¿Cómo se abordan los riesgos de ciberseguridad y privacidad de datos en las entidades bancarias?
- P2.1. ¿Qué marcos de trabajo internacionales se utilizan para la gestión de riesgos de ciberseguridad y privacidad de datos?
- P3. ¿Cuáles son los principales riesgos de ciberseguridad en entidades bancarias?
- P4. ¿Cuáles son los principales riesgos de privacidad de datos en entidades bancarias?

Las preguntas de revisión planteadas serán respondidas mediante la búsqueda de estudios en ciertas bases de datos con el uso de una estrategia de búsqueda a definir.

## 3.4. Estrategia de Búsqueda

La estrategia de búsqueda a seguir plantea la identificación y selección de documentos que estén relacionados al estado actual de la situación planteada para el proyecto de fin de carrera. En el proceso se seleccionarán diversos trabajos publicados en revistas científicas almacenadas en repositorios de bases de datos; por medio de la combinación de diversas palabras, uso de sinónimos, identificación de palabras clave y posterior selección de trabajos académicos relacionados a la investigación.

### 3.4.1. Motores de búsqueda a usar

Para la elección de los motores de búsqueda se selecciona un subconjunto de tres bases de datos como medio para optar por la documentación necesaria durante el proceso de revisión sistemática. Las bases de datos elegidas están entre las proporcionadas por la Pontificia Universidad Católica del Perú (PUCP) y son las siguientes:

- Scopus (https://www.scopus.com)
- IEEE Explorer (https://ieeexplore.ieee.org)
- ACM Digital Library (https://dl.acm.org)

### 3.4.2. Cadenas de búsqueda a usar

A partir del primer modelo PICOC plantado en la Tabla 12 se tomaron en cuenta la selección de algunos términos como palabras clave para la presentación se elaboró la tabla 13.

Tabla 13

*Palabras clave por criterio PICOC*

| Criterio | Descripción |
|---|---|
| Población | Entidades bancarias |
| Intervención | Riesgos, cumplimiento, ciberseguridad, privacidad de datos |
| Comparación | (No aplica) |
| Resultados | Riesgos, ciberseguridad, privacidad de datos, cumplimiento, entidades bancarias |
| Contexto | Ciberseguridad, privacidad de datos, entidades bancarias |

Adicionalmente, un factor a tomar en cuenta para el análisis de los riesgos está en que el NIST Cybersecurity Framework 2.0 al considerar durante el proceso de identificación las vulnerabilidades y amenazas para determinar el riesgo (CSF 2.0, 2024). Por ello, se usan ambos términos en las cadenas de búsqueda. Por consiguiente, las cadenas de búsqueda a usar en las bases de datos seleccionadas serán una traducción al inglés de los términos planteados en la Tabla 13: *risk, vulnerabilities, threats, cybersecurity, da*ta privacy, *data protection, bank entities, banking, compliance* y *compliant*.

### 3.4.3. Documentos encontrados

La cadena de búsqueda principal que será utilizada dentro de las cadenas de búsqueda para cada base de datos está definida por: "Riesgos, vulnerabilidades y amenazas de ciberseguridad y privacidad de datos en el cumplimiento de las entidades bancarias". Por lo tanto, en el proceso de búsqueda y selección de información dentro de los motores de búsqueda para la obtención de resultados específicos de los estudios relacionados se elaboró en el Anexo B sección 1 la Tabla 33 en donde se presenta la cantidad de resultados encontrados y estudios seleccionados.

### 3.4.4. Criterios de inclusión/exclusión

Dentro del conjunto de criterios de inclusión y exclusión definidos en el proceso de revisión sistemática se elabora la Tabla 14.

Tabla 14

*Criterios de inclusión y exclusión*

| Criterios de inclusión | Criterios de exclusión |
|---|---|
| Estudios relacionados al tema de cumplimiento en las entidades bancarias. | Estudios con fecha de publicación mayor a los 10 años. |
| Estudios relacionados al tema de privacidad de datos. | Estudios científicos que no hayan sido revisados por pares. |
| Estudios relacionados al tema de ciberseguridad. | Estudios redactados en idiomas diferentes al español o inglés. |

| | |
|---|---|
| Artículos de conferencias relacionados al tema de cumplimiento en las entidades bancarias. | |
| Artículos de conferencias relacionados al tema de privacidad de datos. | |
| Artículos de conferencias relacionados al tema de ciberseguridad. | |

Asimismo, en relación con las cadenas de búsqueda presentadas para ser usadas en cada motor búsqueda en el Anexo B sección 1 Tabla 33 y, también, de la tabla 14 considerando los diversos criterios de búsqueda de inclusión y exclusión se elaboran tres cadenas de búsqueda resultantes y específicas para cada motor de búsqueda en el Anexo B sección 2.

### 3.5. Formulario de Extracción de Datos

Conforme se realiza la recopilación de los documentos de estudio mediante el uso de las cadenas de búsqueda, los criterios de inclusión y exclusión se presentan en la Tabla 15 el diseño elaborado del formulario de extracción.

Tabla 15 Formulario de extracción de datos

*Formulario de extracción de datos*

| Campo del formulario de extracción | Descripción del campo | Indicador de pregunta |
|---|---|---|
| Id | Identificador número que será asignado para identificar el estudio. | General |
| Título | Título del documento de estudio. | General |
| Autor | Autor del documento de estudio. | General |
| Año de publicación | Año de publicación del documento de estudio. | General |
| Tipo de documento | Tipo de documento de estudio. | General |
| País | El país objetivo del documento de estudio. | General |
| Idioma | El idioma original en que se redactó el documento de estudio. | General |
| Base de datos | Base de datos en donde se encuentra el documento de estudio. | General |
| Digital Object Identifier (DOI) | Identificador único de la publicación del estudio. | General |
| Principales obligaciones de compliance de las entidades bancarias sobre ciberseguridad | Descripción sobre las principales obligaciones de compliance de las entidades bancarias sobre ciberseguridad en el estudio. | P1 |

| Campo del formulario de extracción | Descripción del campo | Indicador de pregunta |
|---|---|---|
| Principales obligaciones de compliance de las entidades bancarias sobre privacidad de datos | Descripción sobre las principales obligaciones de compliance de las entidades bancarias sobre privacidad de datos en el estudio. | P1 |
| Cómo se abordan los riesgos de ciberseguridad en las entidades bancarias | Descripción sobre cómo se abordan los riesgos de ciberseguridad en las entidades bancarias en el estudio. | P2 |
| Cómo se abordan los riesgos de privacidad de datos en las entidades bancarias | Descripción sobre cómo se abordan los riesgos de privacidad de datos en las entidades bancarias en el estudio. | P2 |
| Marcos de trabajo utilizados | Descripción sobre los marcos usados para el estudio. | P2.1 |
| Principales riesgos de ciberseguridad en entidades bancarias | Descripción de los principales riesgos de ciberseguridad en entidades bancarias en el estudio. | P3 |
| Principales riesgos de privacidad de datos en entidades bancarias | Descripción de los principales riesgos de privacidad de datos en entidades bancarias en el estudio. | P4 |

*Nota.* Esta tabla muestra el formato usado en el formulario de extracción en el proceso de recopilación de las fuentes para el estado del arte.

Así mismo, en el Anexo B sección 3 la Tabla 34 contiene los artículos seleccionados en el proceso de búsqueda catalogados mediante el ID del estudio analizado. Adicionalmente, el formulario de extracción desarrollado para los artículos seleccionados en la revisión se presenta en el Anexo B sección 4.

## 3.6. Resultados de la Revisión

### 3.6.1. Respuestas a la pregunta P1.

Con respecto a la primera pregunta de investigación planteada, ¿cuáles son las principales obligaciones de cumplimiento de las entidades bancarias sobre ciberseguridad y privacidad de datos?

Las entidades bancarias tienen la obligación de identificar y reportar los posibles intentos de explotar la red de estas organizaciones, las cuales son complejas y procesan un gran volumen de transacciones de datos personales y financieros en nombre de sus clientes (Scott, 2021). Por lo tanto, los procesos relacionados con la ciberseguridad y la privacidad de los datos

dentro de la red interna de una institución bancaria pueden generar cierto nivel de riesgo que no se identifica en los sistemas. La gestión de riesgos llevada a cabo por la entidad bancaria deberá encontrar un balance entre satisfacer los requisitos impuestos por las leyes locales, los reguladores y, también, evitar que los ciberdelincuentes obtengan accesos a los equipos y datos privados (Alsalamah, 2017) de los clientes que usan los sistemas de información que ofrece la entidad bancaria.

De este modo, la gestión de la ciberseguridad que realice una institución bancaria definirá ciertos niveles de riesgo con el objetivo de satisfacer los requisitos de complimiento durante el desarrollo de las operaciones. El conjunto de decisiones que se tomen para conocer si se cubren los compromisos de ciberseguridad en todos los niveles dependerá de las decisiones que se tomen desde la alta dirección (Al-Alawi & Al-Bassam, 2019). Por lo que, cuando se requiere implementar procesos seguros en los diversos sistemas de información de la institución bancaria la actividad de cumplimiento dependerá principalmente de las decisiones que tome la gerencia de la entidad, y cómo estas se transmitan en temas de cumplimiento hacia los trabajadores de la entidad bancaria. Es decir, que un factor concerniente dependerá de la voluntad y actitud de los trabajadores de los cuales se espera que cumplan con las reglas de seguridad provistas por la institución misma y los reguladores, provista mediante el Compliance, Safety y Accountability (CSA) (Al-Alawi & Al-Bassam, 2019) en forma de cumplimiento.

Adicionalmente, el tratamiento de los datos que realizan los trabajadores de la entidad bancaria con respecto a la información provista por los clientes requiere de un manejo adecuado de los sistemas de información para garantizar una gobernanza correcta de los sistemas y de los datos que contienen. Por esta razón, para el caso de Know Your Customer (KYC) se deben codificar contratos inteligentes y algoritmos para gestionar de forma anónima la identidad de los clientes con respecto a las transacciones y pagos relacionados dentro del sistema de

información de la entidad (Zetzsche et al., 2022), de manera que se cumpla con la regulación local en privacidad y protección de los datos en toda la red interna como forma cumplimiento.

Desde una perspectiva más general los datos recolectados de los clientes a lo largo del tiempo y la forma en que son usados dentro de los sistemas de información de la entidad bancaria dependen del manejo adecuado de los sistemas internos bajo procesos de seguridad definidos. De hecho, en general se presenta mediante contratos establecidos bajo ciertos requisitos comerciales acordados entre el cliente y la institución bancaria para el establecimiento de políticas de seguridad (Mahalle et al., 2018) que tienen por obligación proteger la información recolectada de los clientes. Consecuentemente, el tratamiento de la información se define con anterioridad y la institución tiene la obligación de cumplir con los estipulado en el contrato por el tiempo acordado previamente.

En relación con la idea anterior para el cumplimiento los contratos al seguir los lineamientos estipulados en los contratos y con base en el conjunto de datos personales a asegurar estos son considerados como forma de cumplimiento de *Personally Identifiable Information* (PII) y refieren a todos los datos que posiblemente permitan identificar al usuario específico (Lakshmi et al., 2020) que los generó y de donde provienen. De esta forma el trabajo realizado sobre los datos personal, también, comprenderá los procesos sobre cómo se almacena, procesa y archiva (Lakshmi et al., 2020). También, el proceso de cumplimiento de lo estipulado en los contratos estará relacionado a cómo se implementan los procesos de seguridad dentro de la institución bancaria. Esto último, se complementa con lo referido por General Data Protection Regulation (GDPR) que especifica que el controlador de los datos debe considerar la seguridad y exposición generada cuando se diseñan los procesos (Conrad, 2019) de seguridad para los datos personales.

De esta forma, considerando las principales obligaciones para una entidad bancaria encontrados en la revisión sistemática para la investigación y clasificando su uso entre

ciberseguridad y privacidad de datos se elaboró la Tabla 16 dependiendo del tipo de uso al que se hace referencia cuando se refieren a sus principales obligaciones de cumplimiento.

Tabla 16

*Principales obligaciones de cumplimiento encontradas*

| Tipo de uso | Principales obligaciones de cumplimiento | Artículos relacionados |
|---|---|---|
| Ciberseguridad y privacidad de datos | Society for Worldwide Interbank Financial Telecommunication (SWIFT) | E4, E8, E10, E12, E17 |
| | Know Your Customer (KYC) | E4, E7, E8, E12 |
| | Anti-Money Laundering (AML) | E1, E4, E7, E8 |
| | Risk Assessment | E5, E10, E19 |
| | Payment Card Industry Data Security Standard (PCI DSS) | E2, E12, E19 |
| | Payment Services Directive (PSD2) | E3, E12 |
| | Monetary Authority of Singapore (MAS) | E2 |
| | Committee on Payments and Market Infrastructures (CPMI) | E4 |
| | Federal Trade Commission (FTC) | E10 |
| Privacidad de datos | General Data Protection Regulation (GDPR) | E3, E4, E7, E9, E16, E19, E20 |
| | Personal Data Protection Commission Singapore (PDPC) | E2 |
| | California Consumer Privacy Act (CCPA) | E16 |
| Ciberseguridad | Counter-Terrorism Financing (CTF) | E1, E4 |
| | Strong Customer Authentication (SCA) compliant | E3, E12 |
| | Compliance, Safety, Accountability (CSA) compliance | E2 |
| | Cyber Security Agency of Singapore (CSA) | E2 |
| | Financial Action Task Force (FATF) | E7 |

*Nota.* Esta tabla muestra las principales obligaciones de cumplimiento encontrados en la revisión sistemática de la literatura catalogadas en las áreas de ciberseguridad o privacidad de datos según lo recopilado de cada artículo.

### 3.6.2. Respuestas a la pregunta P2.

Para la segunda pregunta de investigación, ¿cómo se abordan los riesgos de ciberseguridad y privacidad de datos en las entidades bancarias?

A partir del conjunto de obligaciones presentadas para una entidad bancaria como respuesta a la pregunta P1 en el punto 3.6.1 del presente documento, las entidades bancarias tienen como objetivo asegurar el cumplimiento necesario en relación con las actividades que

realizan referente a los clientes, proveedores y entes reguladores. Sobre estas obligaciones, ciertas como la Know Your Customer (KYC), mencionan que los riesgos relacionados a los datos personales en privacidad de datos se abordan a partir de la identificación y verificación de la información de los clientes mediante el control continuo de la información personal (Pocher & Veneris, 2022) que les fue proporcionada a las entidades bancarias. En tal sentido, según el compliance para el General Data Protection Regulation (GDPR) el ente o persona que controla y procesa los datos debe interactuar con estos sólo cuando sea necesario, mantener la actividad de procesamiento en registros, usar sistemas locales para la encriptación y desencriptación (Lakshmi et al., 2020) de forma que los controles respectivos de seguridad para la privacidad de datos estén alineados con las obligaciones de cumplimiento de la entidad regulatoria local.

De esta forma, los controles de seguridad deben formar parte de la infraestructura de la institución bancaria; se explica, por ejemplo, que usar sistemas de certificados digitales, *tokens* de contraseñas de un solo uso, políticas de seguridad en navegadores y el monitoreo de transacciones (Mahalle et al., 2018) son medidas de seguridad necesarias dentro de la organización bancaria. Es decir, establecer controles internos que provean un nivel adecuado en ciberseguridad ante los ataques informáticos que puedan ocurrir en los sistemas de información de la institución bancaria. Así tenemos, que en ocasiones se requiere de departamentos de auditoría interno, equipos de controles de cumplimiento y de aseguramiento (Al Batayneh et al., 2021) para la conformidad en el diseño de los controles establecidos.

Por otro lado, se encuentran los accesos que puedan ocurrir físicamente por un agente externo; en tal sentido, se menciona que los sistemas de seguridad deben incluir controles de acceso físicos y estar protegidos contra el daño que su acceso pueda ocasionar (Mahalle et al., 2018). Asimismo, el acceso inopinado a los sistemas con los que trabaja la institución bancaria debe generar una respuesta definida a los riesgos derivados; en donde, como se observa en la

Figura 1 se identifiquen proactivamente las vulnerabilidades en base a los niveles de riesgos encontrados mediante procesos de auditorías internas, revisión de los registros internos, comunicación objetiva y entrenamiento del personal (Pocher & Veneris, 2022), entre otros.

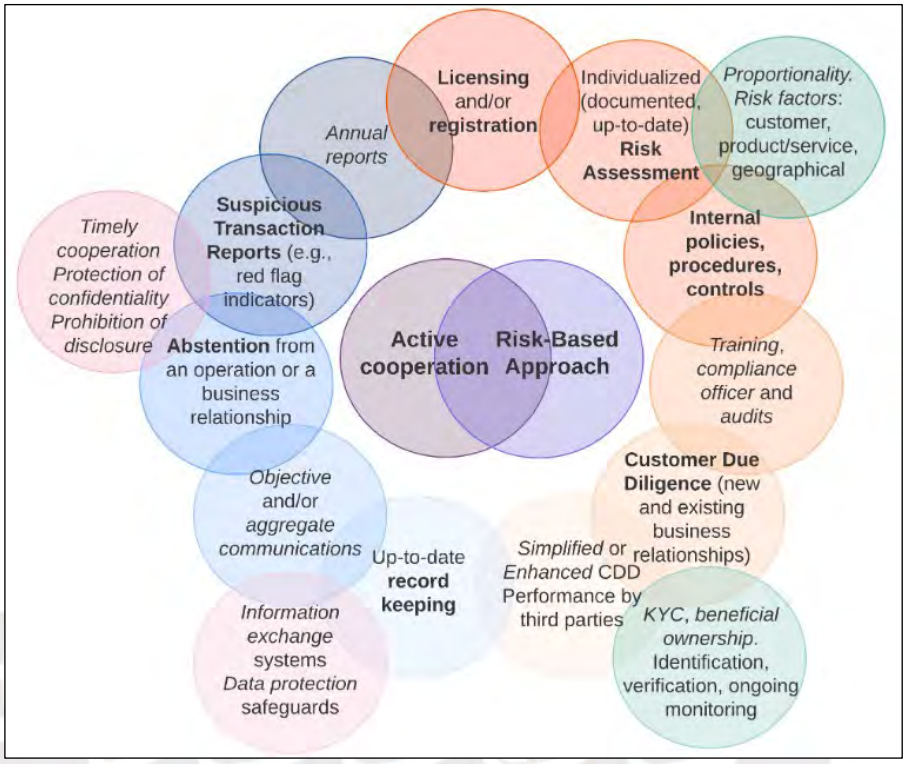



*Figura 1*. Cómo se bordan las obligaciones relacionadas en AML

*Nota*. *Figura tomada de* (Pocher & Veneris, 2022). *El gráfico* representa las situaciones sobre cómo se abordan los riesgos bajo el modelo de compliance desarrollado para AML.

Adicionalmente, con respecto a la segunda pregunta de investigación planteada subyace una pregunta adicional sobre la misma, ¿Qué marcos de trabajo internacionales se utilizan para la gestión de riesgos de ciberseguridad y privacidad de datos? En este sentido en el proceso de recopilación de información para determinar cómo se abordan los riesgos y representan las mejores prácticas internacionales en ciberseguridad y privacidad de datos en las entidades bancarias se presenta en la Tabla 17 los resultados obtenidos de la investigación durante el proceso de revisión sistemática.

Tabla 17

*Marcos de trabajos relacionados a los estudios*

| Marcos de trabajo utilizados | Artículos relacionados |
|---|---|
| National Institute of Standards and Technology (NIST): Cybersecurity Framework (CSF), 800-30, 800-53, 800-63 | E2, E3, E10, E11, E12, E15, E17 |
| General Data Protection Regulation (GDPR) | E3, E4, E7, E9, E16, E19, E20 |
| Information Systems Audit and Control Association (ISACA) | E5, E19 |
| International Organization for Standardization (ISO) 27002 y 27014 | E8, E19 |
| Control Objectives for Information and related Technology (CobiT) | E18, E19 |
| Red Teaming, Threat Intelligence-based Ethical Red Teaming (TIBER-EU) | E1 |
| Application Security Verification Standard (ASVS) open platform framework | E2 |
| Australian data protection framework | E4 |
| Anti-Money Laundering (AML) framework | E7 |
| Global Technology Audit Guide (GTAG) | E19 |
| Corporate Information Security Working Group (CISWG) | E19 |
| Information Security Governance Framework (ISGF) | E19 |
| Corporate Governance Task Force (CGTF) | E19 |
| FFIEC: The “Cybersecurity Assessment Tool” | E19 |

*Nota.* Esta tabla muestra los principales marcos de trabajo encontrados en la revisión sistemática desarrollada. Por consiguiente, se observa que los dos principales marcos de trabajo encontrados en la revisión sistemática son GDPR y NIST.

### 3.6.3. Respuestas a la pregunta P3.

Con respecto a la tercera pregunta de investigación, ¿cuáles son los principales riesgos de ciberseguridad en entidades bancarias?

Entre los principales riesgos en ciberseguridad de una entidad bancaria se comprende la actividad y los errores de los empleados durante la actividad laboral; dado a que, como Palmer (apud Al-Alawi & Al-Bassam, 2019) menciona que en el cumplimiento de sus funciones se pueden generar brechas de seguridad por el manejo inadecuado de los sistemas a causa de la falta de conocimiento y del entrenamiento correcto en sus funciones. Dicho de otra forma, al diseñar los sistemas de información se debe tomar en cuenta el factor humano durante la operativa de su actividad diaria; debido a que acciones o actividades no previstas durante la

definición de los controles pueden ocasionar fallas de seguridad y comprometer la realización de los controles de seguridad.

Por otro lado, los riesgos en ciberseguridad no se centran sólo en la actividad que realizan los empleados dentro de la entidad bancaria. Dado a que, se encuentran expuestos a técnicas o métodos de ingeniería social como *vishing* o *phishing* que tienen el objetivo de invadir, dañar o deshabilitar los sistemas de información de la organización bancaria (Ashiku & Dagli, 2019); métodos que al obtener información confidencial de los empleados de la entidad bancaria como, por ejemplo, al obtener las credenciales de seguridad por medio del engaño comprometería la seguridad de los sistemas al permitir el acceso no autorizado. También, se presentan factores de riesgos como la falta de compromiso y apoyo desde la alta dirección en la falta de presupuesto, ausencia de cumplimiento en ciberseguridad, y carencia de cultura organizacional de ciberseguridad (Al-Alawi & Al-Bassam, 2019) se identificaron como riesgos relevantes en el área ciberseguridad. Dicho esto, los tipos de riesgos a los que está expuesto una institución bancaria se pueden identificar como internos o externos (Ashiku & Dagli, 2019), y se desarrollan en la Tabla 18 mediante las categorías correspondientes.

Tabla 18

*Categoría y descripción corta de un ciberataque*

| Categoría | Descripción corta |
|---|---|
| *Malware* | *Software* malicioso que infecta los sistemas para robar información. |
| *Social Engineering* | Manipulación psicológica que permite el acceso a información confidencial. |
| *Password Attacks* | Herramientas y técnicas que se usan para descifrar contraseñas para obtener el acceso a la red. |
| *Distributed Denial of Service* (DDoS) | Intento de interrumpir los recursos de la red mediante el agotamiento de los recursos provistos para la red interna generado por un gran flujo de información. |
| *Man in the middle attack* (MitM) | De forma secreta se toma el control de una sesión alterando la información de la conexión de las partes imitando la comunicación legítima. |
| *Drive by Downloads* | Descargas automáticas de código malicioso que coinciden con las vulnerabilidades y fallas de los sistemas. |

| Categoría | Descripción corta |
|---|---|
| *Sniffers* | Herramienta de software que monitorea en tiempo real el flujo de datos a través de la red. |
| *Malicious Insiders* | Amenaza interna de un empleado de tomar represalias contra un empleador mediante el uso malicioso de los sistemas. |
| *Trap Doors* | Punto de entrada secreto a la aplicación o al sistema operativo con el fin de depurar, probar y evitar los controles de seguridad. |
| *Negligent Employee* | Oportunidad involuntaria que brindan los empleados a los *hackers* para aprovechar el acceso no autorizado a la red. |

*Nota.* Esta tabla muestra las categorías y descripciones pertinentes sobre riesgos de ciberseguridad. Adaptado de: (Ashiku & Dagli, 2019).

### 3.6.4. Respuestas a la pregunta P4.

Con respecto a la cuarta pregunta de investigación, ¿cuáles son los principales riesgos de privacidad de datos en entidades bancarias?

Los principales riesgos de privacidad de datos están relacionados al trabajo que realizan los empleados de la entidad bancaria con la información confidencial de los clientes y sobre cómo se diseñan los sistemas de información en la entidad bancaria. En primer lugar, se debe lograr mantener el anonimato de la identidad de las personas involucradas durante las operaciones financieras realizadas (Pocher & Veneris, 2022). Por esta razón, se sopesa que la información de las actividades que realizan los clientes de la entidad bancaria del ámbito particular es privada y se debe tener un mayor cuidado en la utilización. Por lo tanto, la información particular de los clientes de la entidad bancaria debe conservar el anonimato en el transcurso de las operaciones en la que se realice el tratamiento de la información personal, y que conforme a los resultados generados del uso de los datos personales se tendrá una revisión de los resultados por medio de los procesos de control en auditorías internas.

En caso contrario, la entidad bancaria de no seguir controles de seguridad en privacidad de datos puede ocasionar consecuencias imprevistas en los modelos de privacidad establecidos de forma interna. Por ejemplo, puede ocasionar que se revele la información personal detallada de los clientes patentizando sus nombres, números de cuenta o tarjeta de crédito; ocasionando la pérdida y el robo de la información de los clientes generando posibles sanciones financieras

(Mahalle et al., 2018) por parte de las entidades reguladoras locales. En estos casos, algunos riesgos emanan de la negligencia por parte de los empleados al realizar sus funciones (Addae et al., 2019). Así también, mediante la manipulación inadecuada de los sistemas de información o el desafortunado diseño puede generar brechas de seguridad que ocasionan el robo de los datos personales de los clientes. En concreto, bajo procesos de ingeniería social en donde mediante el engaño, el cliente es llevado a introducir sus credenciales o transmitir su información personal por medio de artimañas como el phishing o vishing (Mahalle et al., 2018).

## 3.7. Conclusiones

Dentro del conjunto de estudios analizados en el proceso de revisión sistemática se identificaron las principales obligaciones de cumplimiento de las entidades bancarias mediante el desarrollo de las actividades requeridas a seguir para lograr el cumplimiento local en ciberseguridad y privacidad de datos para abordar los riesgos derivados de los sistemas internos. A partir de esto, se determina que el cumplimento a desarrollarse debe darse bajo los compromisos provistos por la entidad bancaria mediante los contratos de servicios que abarquen la actividad a realizarse con los datos personales de los clientes y que cumplan con lo estipulado por la entidad regulatoria local. En cualquier caso, las actividades a ser realizadas deben estar definidas por los contratos de servicios que deben representarse internamente con la aplicación de controles internos de seguridad que desarrollen el conjunto de actividades a realizar, las medidas preventivas y los métodos de respuesta ante alguna intromisión en los sistemas de la organización bancaria.

Por lo que los activos de información que controle una entidad bancaria requieren de las medidas de control preventivas en ciberseguridad necesarias para mitigar los riesgos. Estas medidas preventivas deben haber sido contempladas durante el diseño de los controles para los sistemas de seguridad internos. Por lo tanto, mediante la revisión de la aplicación concurrente

de los controles internos para los sistemas de seguridad se pueden prevenir errores humanos derivados de la inadecuada manipulación interna o externa de los activos de información. Así también al establecer acciones de remediación ante situaciones que amenacen la seguridad de los sistemas de información en el caso que, por ejemplo, ocurra el robo de las credenciales personales de los empleados o clientes.

Por lo tanto, se deriva que el cumplimiento en privacidad de datos representa la correcta manipulación de los datos personales de los clientes y trabajadores de la institución bancaria. En este sentido los riesgos de exponer los datos personales se logran mitigar al cumplir con los lineamientos establecidos en los controles internos y los contratos de servicios previamente definidos con los clientes para el manejo de los datos personales. Por esta razón dentro de la entidad bancaria se deben generar los esfuerzos necesarios en seguridad por medio de la capacitación continua sobre los métodos adecuados para el tratamiento de los datos personales para evitar posibles brechas de seguridad que expongan los datos personales de los clientes.

Por último, en los diversos artículos identificados en la revisión sistemática para el estado del arte del proyecto de fin de carrera se observa a nivel global la existencia del uso de diversos marcos de trabajos y el formato de su aplicación realizado para lograr los objetivos previstos en la regulación local. Por el contrario, en el contexto peruano no se encontraron artículos que hagan referencia a los marcos de trabajo identificados ni que proporcionen alguna orientación o guía específica para lograr el cumplimiento de la regulación local en ciberseguridad y privacidad de datos. Tampoco se encontraron estudio que detallen los tipos de riesgos a los que se exponen las entidades bancarias en temas de ciberseguridad y privacidad de datos, ni sobre los marcos de trabajo que podrían desarrollar para su aplicación. Por esta razón, para el estado del arte desarrollado se destaca la importancia de definir el presente tema de investigación.

# Capítulo 4. Identificar el conjunto de obligaciones de cumplimiento en ciberseguridad y privacidad de datos para las entidades bancarias en el Perú

## 4.1. Introducción

En el presente capítulo se presentan los resultados obtenidos desde el primer objetivo planteado para el proyecto de fin de carrera. Este punto tiene como objetivo identificar las obligaciones de cumplimiento en ciberseguridad y privacidad de datos que aplican para las entidades bancarias en el Perú. Inicialmente se presenta el conjunto de documentos identificados en el marco regulatorio, y cómo estos documentos están relacionados al ámbito legal requerido para el proceso de cumplimiento a seguir por las entidades bancarias en el Perú en cuanto a ciberseguridad y privacidad de datos se refiere. Sobre esto último se usa como guía de referencia el estándar de la ISO 373001, específicamente la cláusula 4.5, para discernir entre las obligaciones de cumplimiento vigentes que son aplicables a las entidades bancarias en el Perú.

## 4.2. Resultados alcanzados

Inicialmente se presenta un diagrama de flujo, representado en la Figura 2, que ilustra de forma clara y ordenada los pasos a seguir para lograr los resultados alcanzados en el presente capítulo al identificar las obligaciones de cumplimiento en ciberseguridad y privacidad de datos para las entidades bancarias en el Perú. A través de este diagrama se observa la forma secuencial y lógica utilizada para lograr los objetivos planteados, proporcionando una guía visual para facilitar la comprensión de la explicación del proceso abordado. Para obtener una explicación detallada de cada componente del diagrama de flujo presentado en la Figura 2, el cuál condujo a los resultados alcanzados del presente capítulo se encuentra en la Tabla 35 Anexo D.

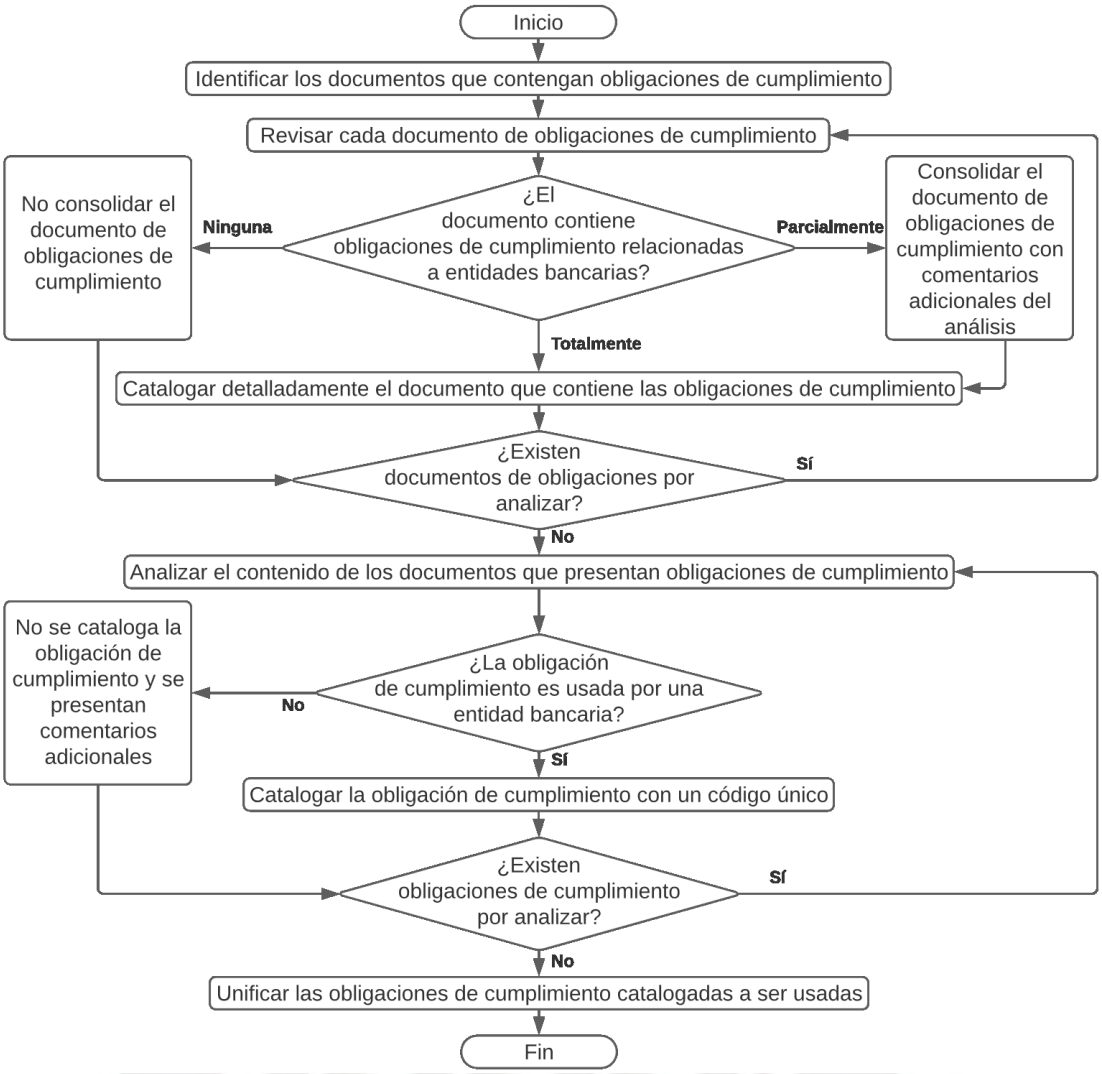



*Figura 2.* Diagrama de flujo al identificar las obligaciones de cumplimiento

*Nota. Elaboración propia.*

En primer lugar, sobre el conjunto de documentos a identificar inicialmente en relación con el marco regulatorio actual se realizó la revisión de cada uno de los documentos en cuanto al ámbito legal para las leyes, reglamentación planteada por las entidades peruanas e información complementaria adicional que esté relacionado a la actividad que realiza una entidad bancaria. En base a la información identificada de los documentos de obligaciones se realiza la unificación de los hallazgos en un documento que contiene cada una de las obligaciones de cumplimiento en ciberseguridad y privacidad de los datos para las entidades bancarias.

En segundo lugar, en el proceso de unificación de los documentos de obligaciones se categoriza cada documento por su obligación de cumplimiento con la asignación de un código de identificación, el nombre del documento, la descripción detallada de su contenido, fecha de publicación, enlace del documento y comentarios adicionales para los casos que no contengan obligaciones de cumplimiento adicionales para una entidad bancaria, pero que son considerados relevantes como información complementaria para lograr el cumplimiento. A continuación, en la Tabla 19, se presenta un extracto de uno de los documentos de cumplimiento.

Tabla 19

*Extracto de un documento de cumplimiento*

| Tipo | Detalle |
|---|---|
| Código del documento | D7 |
| Nombre del documento | Directiva de Seguridad - Resolución Directoral N.º 019-2013-JUS/DGPDP. |
| Descripción del documento | Normativa que presenta de forma informativa una forma de aplicar las obligaciones de cumplimiento en la reglamentación de la Ley N.º 29733, Ley de Protección de Datos Personales. |
| Fecha de publicación | 1 noviembre 2013 |
| Tipo de obligación de cumplimiento | Privacidad de datos |
| Enlace del documento | https://www.minjus.gob.pe/wp-content/uploads/2013/10/RD-Directiva-de-Seguridad.pdf https://cdn.www.gob.pe/uploads/document/file/1401560/Directiva%20de%20seguridad.pdf |
| Si presente en "Obligaciones de cumplimiento" | No |
| Comentario adicional | Herramienta de privacidad de datos complementaria que hace uso en su aplicación de otras leyes y reglamentos. |

*Nota.* Elaboración propia.

En tercer lugar, se procede a consolidar la información de cumplimiento en un documento. Esto se realiza a través de la categorización de cada obligación de cumplimiento que se identifica por medio de su código de documento referido, el capítulo señalado dentro del documento de obligaciones, el artículo del documento de cumplimiento que puede estar

presente entre los diversos capítulos, el área indicativo del nombre del artículo del cuál se hace referencia, el detalle de la obligación extraída del documento de obligaciones y, en caso de ser necesario, comentarios adicionales del análisis en cada una de las obligaciones de cumplimiento, especialmente en aquellos casos en los que la obligación de cumplimiento no aborde activos de información relacionados a la operativa de la entidad bancaria. A continuación, se presenta en la Tabla 20 un extracto de una de las obligaciones de cumplimiento.

Tabla 20

*Extracto de una obligación de cumplimiento*

| **Columna** | **Detalle** |
|---|---|
| Código del documento | D1 |
| Capítulo del documento | Disposiciones generales |
| Artículo del documento | 2 |
| Área indicativa del nombre del artículo | Definiciones |
| Detalle de la obligación de cumplimiento | (Sección con las definiciones establecidas en esta normativa: activo de información, amenaza, autenticación, canal digital, ciberseguridad, credencial, directorio, entidad, evento, factores de autenticación de usuario, identidad, incidente, información, interfaz de programación de aplicaciones, servicios en nube, reglamento, reglamento de Gobierno corporativo y de la Gestión Integral de Riesgos, reglamento para la Gestión de Riesgo Operacional, superintendencia, procesamiento de datos, usuario y vulnerabilidad). |
| Comentario adicional sobre la obligación de cumplimiento | Artículo que establece la definición sobre términos y objetivos específicos de la ley, norma o reglamento. |
| Si obligación primaria | No |
| Obligación de Cumplimiento | - |

*Nota*. Elaboración propia.

Adicionalmente, durante el proceso de identificación de las obligaciones de cumplimiento se consideran las diversas situaciones de cumplimiento de ámbito general aplicables a todas las empresas o instituciones en el Perú. Por lo tanto, es importante discernir entre las aplicaciones de cada obligación de cumplimiento, y los ámbitos de aplicación en los

que se aplican. De esta forma con el uso de los comentarios sobre cada obligación de cumplimiento se incorporan criterios secundarios para la identificación de las obligaciones de cumplimiento como, por ejemplo, para normas de alance general, disposiciones generales o definición de los términos de la norma. En situaciones de ámbito general que no especifiquen activos de información, estas obligaciones no pueden utilizarse en la guía para el análisis de riesgo. En este sentido, para este punto en los resultados alcanzados se optó por utilizar el color rojo para identificar rápidamente las obligaciones de cumplimiento que presentan criterios secundarios, mientras que el color verde para catalogar las obligaciones con un código único para su posterior identificación.

Por último, el documento consolidado para verificar el presente resultado esperado en donde se identificaron 189 obligaciones de cumplimiento en ciberseguridad y privacidad de datos para las entidades bancarias en el Perú se encuentra en el Anexo D sección 2. También, al abarcar el 100% de las obligaciones de cumplimiento en privacidad de datos y ciberseguridad de una entidad bancaria se alcanzan los indicadores objetivamente verificables al ser validado y aprobado por un especialista en seguridad de la información y privacidad de datos, el acta de validación se ubica en el Anexo D sección 3.

### 4.2.1. R1 para O1. Obligaciones de ciberseguridad para las entidades bancarias.

El proceso de búsqueda utilizado para identificar los documentos pertinentes en relación con las obligaciones de cumplimiento en ciberseguridad para las entidades bancarias se realiza por medio de la revisión exhaustiva de la legislación entre las resoluciones y normativas vigentes que refieren directamente al tema de ciberseguridad y su relación con las instituciones de control financiero en el Perú. De tal forma que se accedió a los diversos documentos que son de acceso gratuito publicados de la SBS sobre el campo de ciberseguridad para el control de las entidades financieras peruanas. Entre los documentos de obligaciones identificados se revisaron las fechas de publicación y se consultaron las fuentes más

actualizadas para confirmar la validez de los documentos identificados. Sobre los documentos analizados para las obligaciones de cumplimiento en el tema de ciberseguridad se tienen los siguientes:

- Resolución SBS N.º 504-2021 Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad: El documento presenta la regulación desarrollada en el tema de ciberseguridad con el objetivo de establecer en forma de reglamento nacional los mejores estándares y las mejores prácticas internacionales a ser aplicadas a las empresas en el Perú.
- Resolución SBS N.º 877-2020: Reglamento para la Gestión de la Continuidad del Negocio: El documento establece la reglamentación para la evaluación riesgos identificados dentro de una organización que permitan asegurar la continuidad del negocio evitando la interrupción de la operativa interna de trabajo.
- Resolución SBS N.º 6523-2013 Reglamento de Tarjetas de Crédito y Débito: Establece los lineamientos, normas y condiciones contractuales que deben establecer las instituciones financieras al ofrecer tarjetas de crédito y débito.
- Resolución SBS N.º 5570-2019 Modificatoria de la Resolución SBS N.º 6523-2013: Modifica el reglamento de la resolución SBS N.º 6523-2013 con el objetivo de reforzar las medidas de seguridad y los derechos de los ciudadanos al usar las tarjetas de crédito y débito de las entidades bancarias.

En conjunto los documentos contienen la regulación sobre ciberseguridad para las entidades bancarias en el Perú. Estos documentos están basados en estándares internacionales y reflejan las mejores prácticas en el campo. También se regula la gestión de archivos de información para asegurar la continuidad del negocio y prevenir las interrupciones inesperadas en la operativa de trabajo interna para la entidad bancaria. Además, se establecen los lineamientos a seguir mediante las normas y reglamentación necesaria que las entidades

bancarias deben seguir para asegurar el uso seguro y no fraudulento de todos los activos internos de la entidad bancaria.

#### 4.2.2. R2 para O1. Obligaciones de privacidad de datos para las entidades bancarias.

El proceso mediante el cual se ha identificado y recopilado los documentos pertinentes de las obligaciones de cumplimiento en privacidad de datos para las entidades bancarias se realiza por medio de la revisión exhaustiva de la legislación con las leyes elaboradas en el Congreso de la República del Perú sobre el tema de privacidad de datos. También con la reglamentación elaborada de la ley por la Autoridad Nacional de Protección de Datos Personales (ANPD) encargada de supervisar el cumplimiento de la normativa en privacidad de datos. Sobre los recursos identificados que proporcionan las mejores prácticas y estándares se realiza el análisis específico para las entidades bancarias. De los documentos considerados para las obligaciones de cumplimiento en privacidad de datos se obtienen los siguientes:

- Ley de Protección de Datos Personales - Ley N°29733: El documento establece los lineamientos requeridos por las organizaciones en relación con el cumplimiento de obligaciones sobre cómo se administran los datos personales. Los lineamientos desarrollan las obligaciones sobre los alcances para el tratamiento de la información derivados del manejo que le dan las instituciones privadas y públicas. Así como, los derechos y obligaciones que derivan sobre la titularidad de los datos del acreedor; el uso correcto de los bancos de información; y, también, sobre las infracciones derivadas de no cumplir con las obligaciones estipuladas.
- Reglamento de la Ley de Protección de Datos Personales-Decreto Supremo N.º 003-2013-JUS: El documento desarrolla la reglamentación de la Ley N.º 29733, Ley de Protección de Datos Personales, para garantizar el cumplimiento de las medidas definidas en la ley y que deben seguir las empresas en el Perú.

- Directiva de Seguridad - Resolución Directoral N.º 019-2013-JUS/DGPDP: Normativa que presenta de forma informativa la necesidad de aplicar las obligaciones de cumplimiento en la reglamentación de la Ley N.º 29733, Ley de Protección de Datos Personales.
- Directiva para el Tratamiento de Datos Personales mediante Sistemas de Videovigilancia - Resolución Directoral N.º 02-2020-JUS/DGTAIPD: Medida sobre la cual la Autoridad Nacional de Protección de Datos Personales (ANPD) presenta directivas para el tratamiento de datos personales en los sistemas de videovigilancia presentados por la Ley N.º 29733, Ley de Protección de Datos Personales.
- Guía práctica para la observancia del "Deber de Informar": Guía complementaria desarrollada por la ANPD con el objetivo abordar los incisos de la Ley N.º 29733, Ley de Protección de Datos Personales, orientado de una forma más práctica.

### 4.3. Discusión

En el proceso de identificación de las obligaciones de cumplimiento realizado se hace uso de la herramienta ISO 37301 cláusula 4.5. dado a que atiende la necesidad de que las obligaciones de cumplimiento puedan variar en su tamaño, complejidad y estructura; así como que las obligaciones a identificar pueden estar relacionadas a las leyes, regulaciones y reglas de guía complementarias necesarias a cumplir por las entidades bancarias. Además, en el proceso de integración de la documentación identificada con el uso de la herramienta para este objetivo se logra el mantenimiento adecuado de los cambios generados a través del tiempo con las obligaciones de cumplimiento. De esta forma es posible actualizar las obligaciones de cumplimiento antiguas para que se ajusten a la normativa de cumplimiento vigente de la entidad bancaria. Por lo general la generación de documentos adicionales se realiza por medio de directivas emitidas por los entes reguladores locales en el Perú.

En conjunto los documentos de obligaciones de ciberseguridad y privacidad de datos permiten establecer los lineamientos adecuados para lograr el cumplimiento de las obligaciones legales al realizar la administración de los datos personales en los sistemas internos por parte de instituciones privadas y públicas. Así también permite plantear mejoras en los lineamientos internos para asegurar el debido respeto por los derechos y obligaciones de los titulares de datos personales, esto por medio del uso correcto de los bancos de información para evitar infracciones por incumplimiento. Por esta razón, se representa en la Figura 3 la importancia de comprender la relevancia de la relación que existe entre los aspectos de ciberseguridad y privacidad de datos al estar interrelacionados los diversos incidentes que puedan generarse.

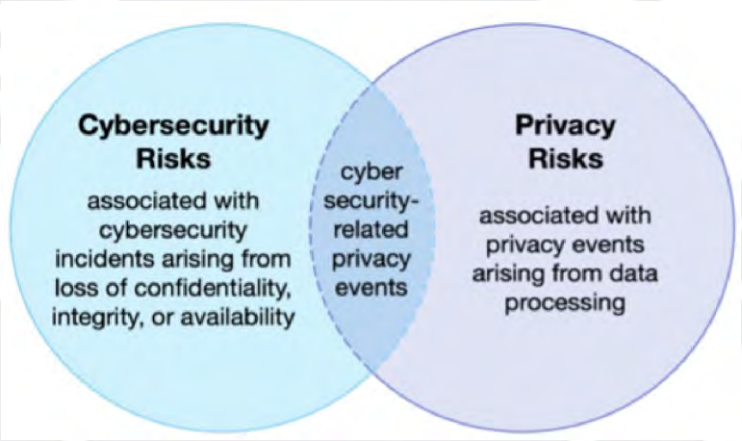



*Figura 3 Relación entre eventos de riesgos de ciberseguridad y privacidad de datos*

*Nota. Figura tomada de (CSF 2.0, 2024). El gráfico muestra un diagrama de Venn que ilustra la relación entre eventos de riesgos de ciberseguridad y privacidad de datos*.

Por último, es importante destacar que la Ley N.º 29733, Ley de Protección de Datos Personales, reglamenta a la ANPD a supervisar el cumplimiento correcto de la ley. De esta forma, la ANPD puede elaborar documentación complementaria adicional necesaria en privacidad de datos como, por ejemplo, la “Directiva de Seguridad - Resolución Directoral N.º 019-2013-JUS/DGPDP” y “Guía práctica para la observancia del Deber de Informar"; que al ser herramientas adicionales en el tema de privacidad de los datos las entidades bancarias pueden hacer de su uso por medio de la aplicación de la ley directamente en su operativa

interna. Por lo tanto, aunque ambos documentos mencionados no presentan obligaciones de cumplimiento adicionales se pueden usar por las entidades bancarias de forma complementaria para el desarrollo de las actividades necesarias en el proceso cumplimiento de sus obligaciones legales.

# Capítulo 5. Identificar las vulnerabilidades inherentes y amenazas de ciberseguridad y privacidad de datos para las entidades bancarias

## 5.1. Introducción

En el presente capítulo se presenta los resultados obtenidos desde el segundo objetivo planteado para el proyecto de fin de carrera. Este punto tiene como objetivo identificar las vulnerabilidades inherentes y amenazas de ciberseguridad y privacidad de datos para las entidades bancarias en el Perú usando como entrada las obligaciones de cumplimiento identificadas en el capítulo 4 del presente documento. Inicialmente se explica el proceso seguido para la identificación de los activos de información y sus correspondientes obligaciones de cumplimiento. Posteriormente se analizan las implicancias de las obligaciones de cumplimiento sobre cada uno de los activos de información por medio de la identificación de las vulnerabilidades y amenazas respectivas a los activos.

## 5.2. Resultados alcanzados

Inicialmente se presenta un diagrama de flujo, representado en la Figura 4, que permite visualizar de forma clara y organizada los pasos seguidos para alcanzar los resultados en la identificación de las vulnerabilidades inherentes y amenazas de ciberseguridad y privacidad de datos para las entidades bancarias en el Perú. A través de este diagrama se observa la forma secuencial y lógica que guía la consecución de los objetivos planteados, proporcionando una guía visual para facilitar la comprensión de la explicación del proceso abordado. Los detalles completos de cada componente del diagrama de flujo presentado en la Figura 4 para alcanzar los resultados obtenidos en el presente capítulo se encuentra en la Tabla 36 Anexo E.

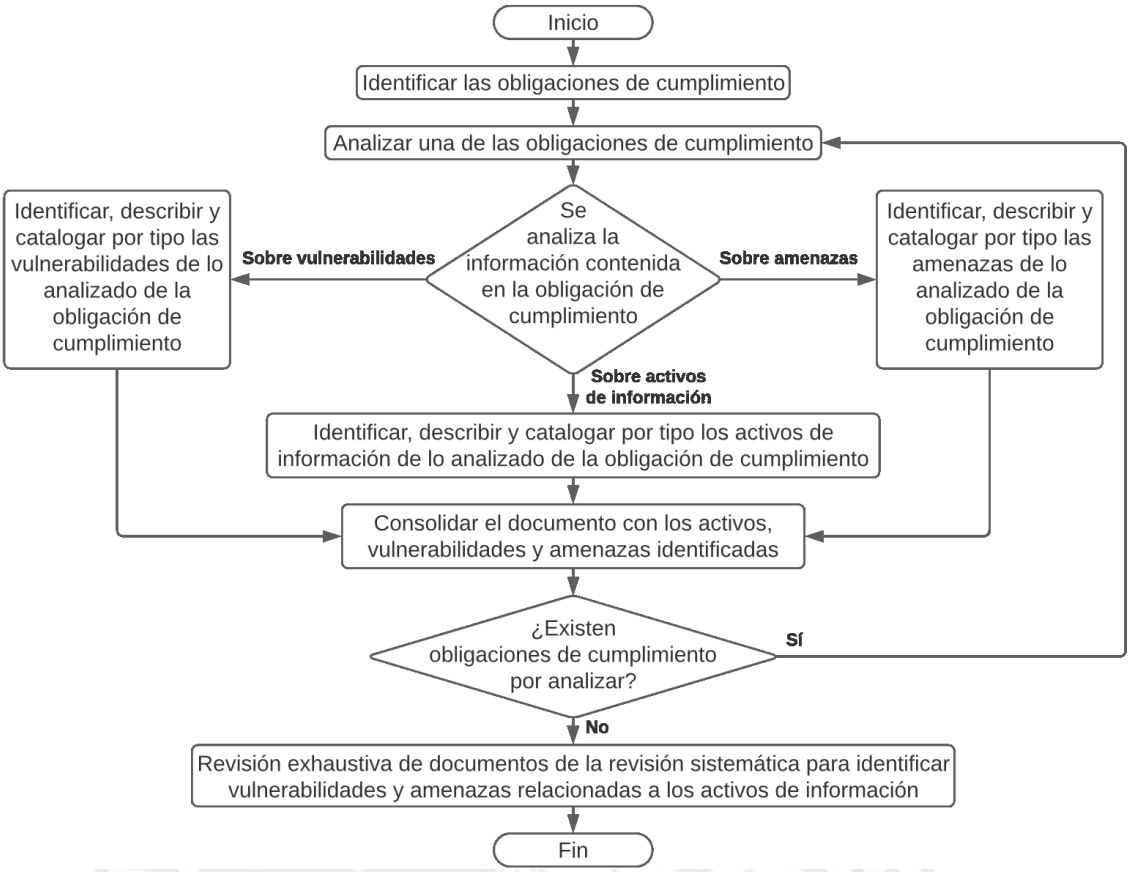



*Figura 4.* Diagrama de flujo al identificar las vulnerabilidades y amenazas

*Nota. Elaboración propia.*

En el proceso de identificación de las vulnerabilidades y amenazas primero se realiza la descomposición de cada una de las obligaciones de cumplimiento identificadas en el primer objetivo del proyecto de fin de carrera usando cada una de las obligaciones como entrada para el análisis de riesgo en ciberseguridad y privacidad de los datos a efectuar para las entidades bancarias. De forma que para cada obligación de cumplimiento se extrae el activo de información que lo representa, categorizando cada uno estos y relacionándolo al tipo de actividad principal efectuada dentro de una entidad bancaria.

De esta forma en el transcurso de la categorización de cada activo de información se agrupan entre sí los activos de información por medio de su afinidad más cercana llevada a cabo entre los principales departamentos de una entidad bancaria, por ejemplo, con los bancos de datos, alta dirección, recursos humanos, operaciones, banca comercial, etc. De este modo el

conjunto de obligaciones de cumplimiento se puede relacionar a un activo previamente identificado. En conjunto, se han identificado 12 tipos de activos de información que resultan aplicables a una entidad bancaria entre sus diversas obligaciones de cumplimiento. También, cada activo de información está acompañado por una descripción específica de la actividad que efectúa, esta descripción tiene el objetivo de poder ser usado por los varios niveles de organización, departamentos y segmentos de entidades bancarias para ser aplicado a sus contextos específicos. Finalmente, es relevante señalar que en total fueron identificados y evaluados 65 activos de información. A continuación, se muestra en la Tabla 21 la descripción sobre los campos usados en la columna de la Tabla 22 para un extracto para un activo de información identificado.

Tabla 21

*Descripción de columnas activo de información y obligaciones de cumplimiento*

| Nombre de columna | Descripción de la columna |
|---|---|
| N° | El número que indica el activo de información. |
| Tipo | El tipo de activo de información.<br>Se tiene contemplado los siguientes tipos de activo de información:<br>- Banco de datos<br>- Manual y formulario<br>- Alta dirección<br>- Cloud<br>- Puntos físicos de pago y recojo de dinero<br>- Entidades públicas (reportes y registros)<br>- RRHH<br>- Productos<br>- Operaciones<br>- Banca comercial<br>- Riesgos<br>- Seguridad |
| Activo de información | El nombre del activo de información. |
| Descripción del activo de información | Presenta una descripción concreta de la actividad que desarrolla el activo de información. |
| Obligación de cumplimiento | Presenta una lista de las obligaciones de cumplimiento relacionadas directamente con la actividad que desarrolla el activo de información. |

*Nota*. Elaboración propia.

Tabla 22

*Extracto de un activo de información y obligaciones de cumplimiento*

| Nombre de columna | Descripción |
|---|---|
| N° | 4 |
| Tipo | Manual y formulario |
| Activo de información | Manual sobre el reglamento de conducta interno de empleados de la entidad bancaria (físico y electrónico) |
| Descripción del activo de información | El manual sobre el reglamento de conducta interno de empleados de una entidad bancaria es un documento que establece las normas de conducta para los empleados de la entidad. Este documento incluye información sobre la misión, visión, valores y políticas de la entidad bancaria, así como las expectativas en cuanto a la integridad, ética, comunicación y responsabilidad profesional de los empleados. Además, puede cubrir temas relacionados a la protección de la información confidencial y la resolución de conflictos. |
| Obligación de cumplimiento | OBL01-C, OBL02-C, OBL03-C, OBL04-C, OBL05-C, OBL06-C, OBL07-C, OBL08-C<br>OBL18-C, OBL19-C, OBL20-C, OBL21-C<br>OBL31-C<br>OBL84-P, OBL114-P, OBL115-P, OBL116-P, OBL117-P<br>OBL151-P, OBL152-P, OBL153-P, OBL154-P |

*Nota*. Elaboración propia.

Para la identificación de las vulnerabilidades y amenazas el proceso realizado utiliza la descripción de las obligaciones de cumplimiento en la normativa identificada como, por ejemplo, de no utilizar los datos personales para fines distintos a los previamente autorizados. En el caso específico de esta norma para los bancos de datos establece una obligación de cumplimiento que garantiza la confidencialidad y la protección de los datos personales. Sin embargo, si la norma se ve comprometida proporciona la base para poder identificar las amenazas y vulnerabilidades para el entorno operativo de la entidad bancaria en circunstancias relacionadas con el uso extralaboral de la información personal. Adicionalmente, la información de los documentos identificados en la revisión sistemática se toma como referencia para la identificación de las vulnerabilidades y amenazas asociadas a los activos de

información. A continuación, en la Tabla 23, se presenta la descripción sobre los campos usados en las columnas de la Tabla 24 que contiene un extracto de las vulnerabilidades y amenazas identificadas para un activo de información.

Tabla 23

*Descripción de columnas en vulnerabilidades y amenazas*

| **Nombre de columna** | **Descripción de la columna** |
|---|---|
| N° | El número que identifica el activo de información. |
| Tipo | El tipo de activo de información. |
| Activo de información | El nombre del activo de información. |
| Tipo vulnerabilidad | Indica el tipo de vulnerabilidad que afecta al activo de información.<br>Se tiene contemplado los siguientes tipos de vulnerabilidad:<br>- Hardware<br>- Software<br>- Personal<br>- Organización<br>- Ubicación<br>- Documentos<br>- Servicios |
| Descripción de vulnerabilidad | Proporciona la descripción del tipo de vulnerabilidad relacionada con el activo de información.<br><br>Pueden ser utilizadas por las entidades bancarias como punto de partida con la adecuada adaptación a sus vulnerabilidades para ajustarse a cualquier condición específica. |
| Tipo amenaza | Indica el tipo de amenaza que afecta al activo de información.<br>Se tiene contemplado los siguientes tipos de amenaza:<br>- Sobre la información<br>- Software<br>- Activos físicos en equipos<br>- Personal<br>- Ubicación física (ambiental)<br>- Servicios<br>- Cibernéticas<br>- Activos físicos (documentos) |
| Descripción de amenazas | Proporciona la descripción del tipo de amenaza relacionada con el activo de información.<br><br>Pueden ser utilizadas por las entidades bancarias como punto de partida con la adecuada adaptación a sus amenazas para ajustarse a cualquier condición específica. |

| Nombre de columna | Descripción de la columna |
|---|---|
| Documentos relacionados de la Revisión Sistemática | Documentos relacionados del formulario de extracción que complementa la identificación de los activos de información, vulnerabilidades y amenazas. |

*Nota*. Elaboración propia.

Tabla 24

*Extracto vulnerabilidades y amenazas de un activo de información*

| Nombre de columna | Contenido |
|---|---|
| N° | 1 |
| Tipo | Banco de datos |
| Activo de información | Banco de datos de la actividad financiera de los clientes naturales y jurídicos de la entidad bancaria |
| Tipo vulnerabilidad | Hardware<br>Ubicación<br>Organización |
| Descripción de vulnerabilidad | Hardware<br>- Mantenimiento insuficiente / instalación fallida de medios de almacenamiento<br>- Falta de esquema de reemplazo periódicos<br>- Almacenamiento no protegido<br>- Falta de cuidado al descartarlo.<br>- Copia no controlada<br>- Arquitectura de red insegura.<br>- Falta de protección física del edificio, puertas y ventanas<br>- Falta de conciencia de seguridad<br>- Trabajo no supervisado del personal externo o de limpieza<br>Ubicación<br>- Red inestable de energía eléctrica en el edificio<br>- Ubicaciones en un área susceptible a las inundaciones<br>- Red inestable de energía eléctrica en el edificio<br>- Falta de protección física del edificio, puertas y ventanas<br>Organización<br>- Falta de procedimientos de registro y cancelación del registro |
| Tipo amenaza | Amenazas de información<br>Activos físicos en equipos<br>Cibernéticas |
| Descripción de amenazas | Amenazas de información<br>- Acceso no autorizado a la información<br>- Modificación no autorizada de la información<br>- Eliminación no autorizada de la información<br>- Robo de activos contenedores de información<br>- Inadecuada eliminación de activos contenedores de información |

| Nombre de columna | Contenido |
|---|---|
| | - Corrupción de datos por error de procesamiento<br>- Uso extralaboral de la información<br>- Virus informáticos que alteran o eliminan la información<br>- Fuga de Información<br>Activos físicos en equipos<br>- Corto circuito<br>- Filtraciones de agua o polvo<br>- Incumplimiento del plan de mantenimiento<br>- Uso inadecuado de los equipos<br>- Desconfiguración del equipo<br>- Obsolescencia de los componentes del equipo<br>Cibernéticas<br>- Ransomware<br>- Phishing<br>- Ingeniería Social<br>- Amenaza interna<br>- Pérdida de información<br>- Robo de información<br>- Ataques de día cero<br>- Indisponibilidad<br>- Malware |
| Documentos relacionados de la Revisión Sistemática | - E9: Analysis of General Data Protection Regulation Compliance Requirements and Mobile Banking Application Security Challenges<br>- E10: Security Risk Management in Online System<br>- E11: Data Privacy and System Security for Banking and Financial Services Industry based on Cloud Computing Infrastructure<br>- E13: Factors Influencing Information Security Policy Compliance Behavior<br>- E14: Cybersecurity as a Centralized Directed System of Systems Using SoS Explorer as a Tool<br>- E16: Protecting personal information and data privacy: what students need to know<br>- E17: A Survey of Practical Formal Methods for Security<br>- E18: Information Integrity: Are We There Yet?<br>- E21: Abuse Reporting and the Fight Against Cybercrime" |

*Nota*. Elaboración propia.

Con el fin de obtener una comprensión más clara de las vulnerabilidades y amenazas asociadas con cada activo de información de una entidad bancaria se desarrolla el documento ubicado en el Anexo E sección 2 para verificar el presente resultado esperado al identificar las vulnerabilidades inherentes y amenazas de ciberseguridad y privacidad de datos para las entidades bancarias en el Perú. También, el indicador objetivamente verificable se alcanzó con

el documento validado y aprobado al 100% por un especialista en seguridad de la información y privacidad de datos, el acta de validación de la revisión y aprobación del especialista se encuentra en el Anexo E sección 3. En el transcurso de la revisión con el especialista se tuvo en consideración los comentarios realizados con respecto a las vulnerabilidades y amenazas específicas de los activos de información que generalmente suele estar relacionadas a los bancos de datos y sistemas operacionales para el manejo de las transacciones.

### 5.2.1. R1 para O2. Catálogo de vulnerabilidades de las obligaciones identificadas.

Durante el proceso de categorización de los activos de información para cada una de las obligaciones de cumplimiento se extraen los puntos relacionados a una posible afectación en forma de debilidad o procedimiento de seguridad del sistema de información que podrían ser explotados por una fuente de amenaza interna o externa a la entidad bancaria. El formato utilizado como guía durante la categorización de los diversos tipos de vulnerabilidades identificadas para su planteamiento en el desarrollo del proyecto se complementa con el uso de la herramienta de ISO 27005. De tal forma para el presente resultado esperado con el uso de la herramienta se categorizan las vulnerabilidades identificadas. Como resultado de lo planteado se muestra en la Tabla 24 las vulnerabilidades identificadas para un activo de información.

### 5.2.2. R2 para O2. Catálogo de amenazas de las obligaciones identificadas.

Así también en el proceso de categorización de los activos de información con el uso de las obligaciones de cumplimiento se extraen las circunstancias o eventos con el potencial de afectar negativamente las operaciones internas de la entidad bancaria al usar los activos de información. Como referencia a seguir en el planteamiento se usa la ISO 27005 que representa circunstancias de amenazas generales aplicables a una organización, por ejemplo, accesos no autorizados, falta de cuidado al descartar los activos, modificación de la información, denegación de servicios, etc. (ISO, 2018). De modo similar a la operativa para el catálogo de

vulnerabilidades se realiza la identificación y categorización de las amenazas utilizando la herramienta ISO 27005 como guía. Como resultado de lo planteado se muestra en la Tabla 24 las amenazas identificadas para un activo de información.

## 5.3. Discusión

En el transcurso del análisis realizado para cada una de las obligaciones de cumplimiento se observa que los activos de información identificados y categorizados suelen repetirse entre las diversas obligaciones de cumplimiento. De igual forma una obligación de cumplimiento puede estar relacionada a uno o más activos de información dentro de una entidad bancaria. También, se observa que las vulnerabilidades y amenazas identificadas pueden estar relacionadas entre sí y su categorización dependerá del contexto específico interno al que aplique.

Además, al analizar las vulnerabilidades y amenazas relacionadas con los activos de información se denota que muchas de ellas están interconectadas entre sí. Esto significa que, aunque cada obligación de cumplimiento tenga requisitos específicos, la protección y gestión de los activos de información debe ser un tema transversal y crítica que se extienda a través de múltiples áreas en la entidad bancaria. En consecuencia, la comprensión de los activos de información, así como de las vulnerabilidades y las amenazas debe ser fundamental para cualquier entidad bancaria independientemente de su tamaño y complejidad a la que aplique.

Adicionalmente se destaca la importancia de la identificación de vulnerabilidades y amenazas al constituir un paso crítico en el análisis de riesgos en ciberseguridad y privacidad de datos para las entidades bancarias. Este aspecto descrito permite que en el proceso del análisis de los riesgos del presente capítulo permita plantear las medidas preventivas posteriores basadas en la identificación y categorización de los activos, vulnerabilidades y amenazas. Estas medidas tienen como objetivo ayudar a garantizar la seguridad y protección de la información crítica de la entidad bancaria como de sus clientes.

# Capítulo 6. Identificar los riesgos de ciberseguridad y privacidad de datos para las entidades bancarias

## 6.1. Introducción

En este capítulo se presenta los resultados obtenidos desde el tercer objetivo planteado para el proyecto de fin de carrera que consiste en identificar los riesgos de ciberseguridad y privacidad de datos aplicables a las entidades bancarias en Perú. En primer lugar, se seleccionan las principales vulnerabilidades y amenazas que afectan a cada uno de los activos de información. Posteriormente para cada una de las vulnerabilidades y amenazas seleccionadas de los activos se formulan los criterios de medición del nivel del riesgo identificado. De esta manera, se logra la evaluación completa y detallada de los riesgos asociados en ciberseguridad y privacidad de los datos en el contexto bancario en el Perú.

## 6.2. Resultados alcanzados

### 6.2.1. R1 para O3. Catálogo de riesgos de ciberseguridad y privacidad de datos.

Inicialmente se presenta un diagrama de flujo, representado en la Figura 5, que permite visualizar de forma clara y ordenada los pasos seguidos para desarrollar los resultados alcanzados al identificar los riesgos de ciberseguridad y privacidad de datos para las entidades bancarias en el Perú. A través de este diagrama se observa la forma secuencial y lógica utilizada para lograr los objetivos planteados, proporcionando una guía visual para facilitar la comprensión de la explicación del proceso abordado. La explicación detallada de cada una de las partes del diagrama de flujo presentado en la Figura 5 para alcanzar los resultados obtenidos en el presente capítulo se encuentra en la Tabla 37 Anexo F.

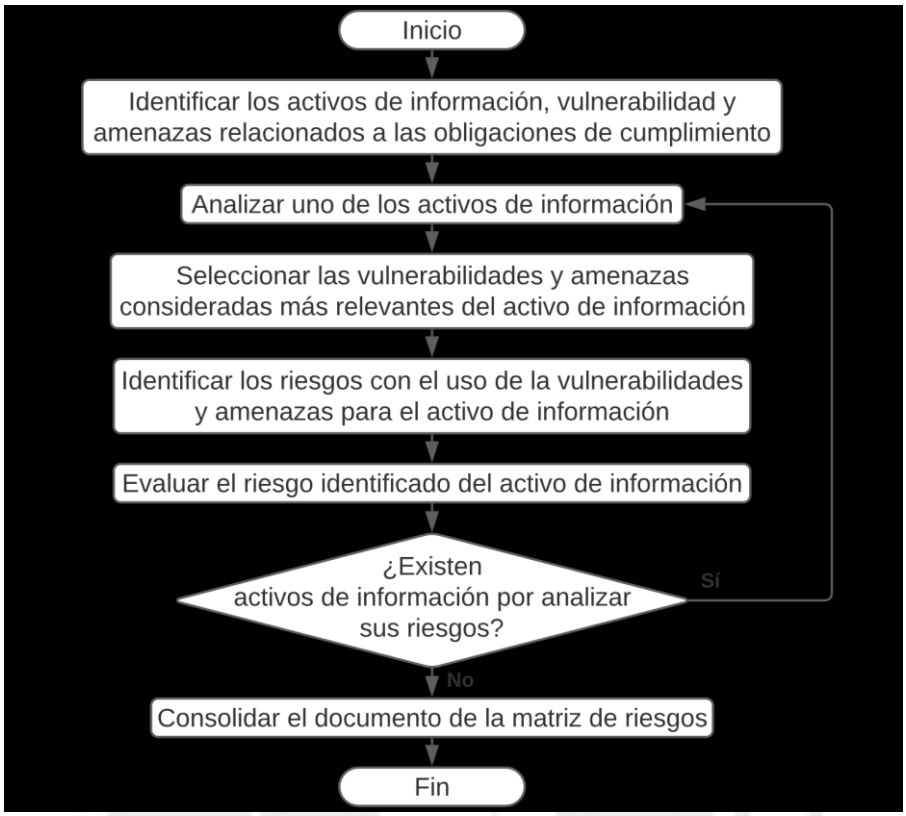



*Figura 5.* Diagrama de flujo al crear la matriz de riesgos

*Nota. Elaboración propia.*

En primer lugar, para el proceso de identificación de los riesgos de ciberseguridad y privacidad de datos se emplean los activos de información identificados previamente en el capítulo 5 para el segundo objetivo del proyecto de fin de carrera. De esta forma para cada uno de los activos de información se seleccionan las vulnerabilidades y amenazas más relevantes en función del desarrollo de su operativa principal identificada descrita del activo de información. En efecto la selección de las principales vulnerabilidades y amenazas respectivas del activo de información se fundamenta en los criterios profesionales cualificados al considerar el daño potencial que pueda ocasionar en el activo.

Posteriormente la identificación del riesgo se genera por medio de la unión de la vulnerabilidad y amenaza del activo de información, a través del empleo del término “ocasiona o genera”. Este punto resulta en la identificación de los cinco principales riesgos asociados a

cada uno de los activos de información como se observa en la Tabla 25 un extracto para la matriz de riesgos de un activo de información.

Tabla 25

*Extracto de la matriz de riesgos para un activo de información*

| N° | Tipo | Activo de información | Vulnerabilidad | Amenaza | Riesgo |
|---|---|---|---|---|---|
| 1 | Banco de datos | Banco de datos de la actividad financiera de los clientes naturales y jurídicos de la entidad bancaria | Falta de esquema de reemplazo periódicos | Indisponibilidad | Falta de esquema de reemplazo periódicos ocasiona o genera indisponibilidad. |
| | | | Almacenamiento no protegido | Robo de activos contenedores de información | Almacenamiento no protegido ocasiona o genera robo de activos contenedores de información. |
| | | | Falta de procedimientos de registro y cancelación del registro | Acceso no autorizado a la información | Falta de procedimientos de registro y cancelación del registro ocasiona o genera acceso no autorizado a la información. |
| | | | Falta de conciencia de seguridad | Modificación no autorizada de la información | Falta de conciencia de seguridad ocasiona o genera modificación no autorizada de la información. |
| | | | Falta de cuidado al descartarlo | Uso extralaboral de la información | Falta de cuidado al descartarlo ocasiona o genera uso extralaboral de la información. |

*Nota.* Elaboración propia.

En segundo lugar, se requiere evaluar cada riesgo identificado y para lograrlo se hace uso como guía de la herramienta de NIST SP 800-30. La metodología de trabajo de la herramienta considera la evaluación de los riesgos identificados por medio de escalas de evaluación para la probabilidad de ocurrencia y del impacto ocasionado. En las escalas de evaluación de la herramienta se adaptaron en conjunto las Tablas G-2, G-3, G-4 y G-5 en el

documento del resultado alcanzado para medir la probabilidad de ocurrencia del riesgo, la probabilidad que produzca impactos adversos y la probabilidad general que el evento no deseado ocurra (NIST, 2012) en la entidad bancaria. Así también de la herramienta se adaptó la Tabla H-3 en el documento del resultado alcanzado para medir el impacto de los riesgos en lo que se refiere a los efectos que puedan ocasionar si el evento se materializa (NIST, 2012) en la entidad bancaria. En base a estos factores de probabilidad general de ocurrencia y el impacto generado se califica el nivel de riesgo para cada uno de los riesgos identificados por medio de la Tabla I-3 y Tabla I-4 (NIST, 2012) adaptado en el documento del resultado alcanzado.

La medición de los riesgos identificados permite el planteamiento de valores cualitativos dentro de la clasificación de muy bajo, bajo, moderado, alto y muy alto; así como de valores semicuantitativos en rangos numéricos (NIST, 2012) como métodos de clasificación relativa al riesgo asociado a los resultados que pueda tener una entidad bancaria. En base al criterio del profesional cualificado se identifica y califica cualitativamente cada uno de los riesgos para obtener los factores de probabilidad general de ocurrencia y el impacto generado, que en conjunto permiten determinar el nivel de riesgo estimado para un activo de información, lo mencionado se detalla en la Tabla 26.

Tabla 26

*Extracto de clasificación del riesgo asociado al activo de información*

| Tipo de columna | Descripción de la columna |
|---|---|
| N° | 1 |
| Tipo | Banco de datos |
| Activo de información | Banco de datos de la actividad financiera de los clientes naturales y jurídicos de la entidad bancaria |

| Tipo de columna | Descripción de la columna | | | | |
|---|---|---|---|---|---|
| Riesgo | Falta de esquema de reemplazo periódicos ocasiona o genera indisponibilidad. | Almacenamiento no protegido ocasiona o genera robo de activos contenedores de información. | Falta de procedimientos de registro y cancelación del registro ocasiona o genera acceso no autorizado a la información. | Falta de conciencia de seguridad ocasiona o genera modificación no autorizada de la información. | Falta de cuidado al descartarlo ocasiona o genera uso extralaboral de la información. |
| Probabilidad de temporalidad | Bajo | Bajo | Moderado | Moderado | Moderado |
| Probabilidad de impacto adverso | Muy alto | Alto | Alto | Muy alto | Alto |
| Probabilidad general de ocurrencia | Moderado | Bajo | Moderado | Alto | Moderado |
| Impacto de los eventos de la amenaza | Muy alto | Muy alto | Alto | Alto | Bajo |
| Nivel del riesgo | Alto | Moderado | Moderado | Alto | Bajo |

*Nota*. Elaboración propia.

Por último, el documento para verificar el presente resultado esperado al identificar los riesgos de ciberseguridad y privacidad de datos para las entidades bancarias en el Perú se encuentra en el Anexo F sección 2. También, con la matriz de riesgos validada y aprobada al 100% por un especialista en seguridad de la información y privacidad de datos se alcanzan los indicadores objetivamente en el acta de validación ubicada en el Anexo F sección 3.

### 6.3. Discusión

La identificación de los riesgos permite a la entidad bancaria anticipar y evaluar los riesgos antes la posible afectación en su funcionamiento interno. Sin embargo, la identificación de riesgos generalmente no es un proceso estándar y con un único resultado, sino que depende en gran medida del criterio profesional sobre la evaluación que el riesgo pueda ocasionar en los activos de información. De acuerdo con la evaluación de riesgos en NIST SP 800-37 en

TASK P-14, las evaluaciones de riesgos de privacidad se ven influenciadas por factores contextuales, como la sensibilidad de la información personal, los tipos de organizaciones involucradas y las percepciones y comprensión de los individuos sobre la privacidad y el procesamiento de datos (RMFISO, 2018). Por consiguiente, con el fin de identificar y listar los riesgos de un activo de información se hace uso de un término específico que combina la vulnerabilidad y amenaza en una sola frase. Esta característica en particular facilita el análisis posterior de los riesgos al permitir la rápida identificación de cada uno, evitando posibles errores humanos generados en la conjugación de los riesgos que posteriormente serán usados en el diseño de los controles para mitigar los riesgos ya identificados.

Adicionalmente, es importante destacar la importancia de las escalas de evaluación utilizadas en los riesgos que permiten determinar la importancia y relevancia de cada uno de los riesgos identificados, de esta forma permitiendo poder priorizar los esfuerzos futuros en su mitigación. De esta forma el NIST CSF 2.0 en la subcategoría ID.AM-5 describe que los activos se priorizan según su criticidad e impacto que pueda tener en la misión (CSF 2.0, 2024) de la entidad bancaria. De esta forma la evaluación realizada no se basa sólo en la probabilidad de ocurrencia, sino también en la magnitud de su posible impacto en cada uno de los activos al realizar su operativa diaria. En otras palabras, la medición de los niveles de riesgo a calificar para cada activo de información permite relacionar la probabilidad de que el riesgo ocurra y genere impactos adversos dentro de la entidad bancaria.

Por último, el planteamiento de los valores cualitativos y semicuantitativos para la clasificación de los riesgos permite ajustar la evaluación de riesgos a las necesidades específicas de una entidad bancaria para ser aplicado a sus realidades al realizar la medición adecuada. Por lo tanto, la evaluación no debe ser considerado un proceso estático y requiere el mantenimiento adecuado en el tiempo de uso para asegurar que los posibles cambios se ajusten a la operativa interna y el entorno de seguridad de la información interno estén reflejados en

los valores asignados durante la medición de los riesgos. Por último, en concordancia con los mencionado es necesario que la entidad bancaria deba realizar la revisión periódica de los riesgos ya identificados, de tal modo que le permita ajustar los valores según sea necesario para garantizar que la evaluación de riesgos siga siendo efectiva.

# Capítulo 7. Diseñar los controles en ciberseguridad y privacidad de datos como parte del proceso de cumplimiento de las entidades bancarias

## 7.1. Introducción

En este capítulo se presenta los resultados obtenidos desde el cuarto objetivo planteado para el proyecto de fin de carrera que consiste en diseñar los controles de seguridad para los riesgos de ciberseguridad y privacidad de datos en las entidades bancarias en Perú. En primer lugar, por medio del análisis de las situaciones de riesgos identificadas en el capítulo 6 del presente documento. De tal forma que para cada uno de los riesgos y sus activos de información relacionados se formulen controles de seguridad adecuados para poder mitigar las diversas situaciones de riesgo.

## 7.2. Resultados alcanzados

### 7.2.1. R1 para O4. Diseño de controles para los riesgos de ciberseguridad y privacidad de datos identificados.

Inicialmente se presenta un diagrama de flujo, representado en la Figura 6, que permite visualizar de forma clara y ordenada los pasos seguidos para desarrollar los resultados alcanzados al diseñar los controles en ciberseguridad y privacidad de datos como parte del proceso de cumplimiento de las entidades bancarias en el Perú. A través de este diagrama se observa la forma secuencial y lógica utilizada para lograr los objetivos planteados, proporcionando una guía visual para facilitar la comprensión de la explicación del proceso abordado. La explicación detallada de cada una de las partes del diagrama de flujo presentado en la Figura 6 para alcanzar los resultados obtenidos en el presente capítulo se encuentra en el Tabla 38 Anexo G.

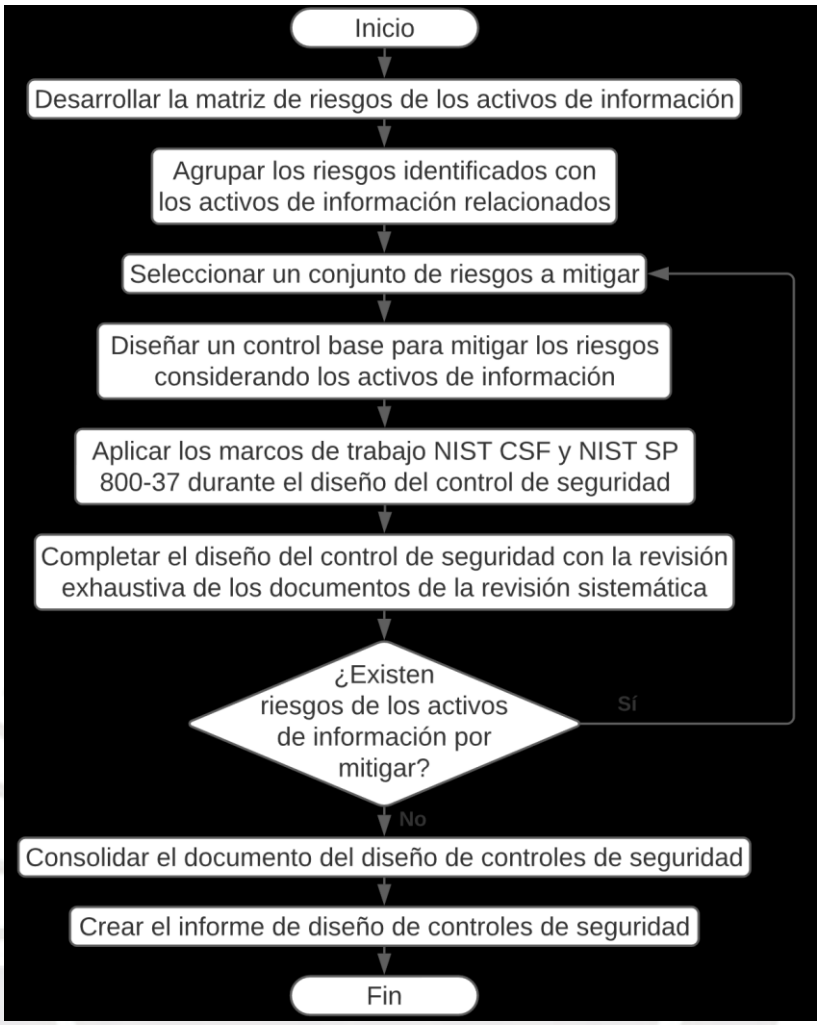



*Figura 6.* Diagrama de flujo al diseñar los controles de seguridad

*Nota. Elaboración propia.*

En base al conjunto de riesgos identificados en el capítulo 6 del presente documento se realiza la revisión de cada uno de estos. De este modo se evalúan los riesgos en base a su cantidad de ocurrencias y la relación de cada riesgo con cada uno con los activos de información considerados en el análisis. De esta forma al realizar la revisión general es necesario que todos los riesgos identificados estén presentes entre todos los activos de información identificados previamente, dado a que existe la posibilidad que posteriormente a la culminación de revisión de los riesgos del capítulo 6 existan riesgos repetidos para un mismo activo de información. Por lo tanto, para la revisión se considera que por cada activo de

información se deben tener 5 riesgos significativos relacionados. De esta manera, se verifica para el presente trabajo que del conjunto de riesgos contabilizados es de 325 entre todos los activos de información, como confirmación de que no existen riesgos repetidos para un mismo activo.

Considerando la revisión planteada de los riesgos identificados entre los activos correspondientes, se procede a realizar el planteamiento de un control base con el objetivo de mitigar uno o más de los riesgos detectados. De esta forma el NIST SP 800-37 representa en el TASK P-5 que se deben identificar y documentar controles comunes a nivel organizacional que puedan ser compartidos por los sistemas internos (RMFISO, 2018) para la entidad bancaria. Inicialmente el diseño de dicho control base debe caracterizarse por ser simple y sencillo con el fin de abordar directamente las situaciones de riesgo identificadas para cada uno de los activos de información. Es importante tener en cuenta que los riesgos asociados al control base deben considerar estar relacionados. Asimismo, se deben considerar los documentos identificados en la revisión sistemática como referencia adicional para la realización del planteamiento inicial del diseño de los controles de seguridad. Esta actividad se realiza tomando en consideración el criterio profesional que vincule los temas de seguridad cibernética con la efectividad del control para poder resolver las situaciones de riesgo presentes en una entidad bancaria. Además, para el diseño de los controles el planteamiento del control debe tener un enfoque aplicable al activo y que permita que la ejecución del control permita la posibilidad de la actualización posterior, esto último considerando la revisión de las recomendaciones planteadas en el marco de trabajo NIST CSF y NIST SP 800-37 al abordar los riesgos y diseñar dicho control de seguridad.

Posteriormente en el proceso de diseño del control se emplean los puntos relevantes de los marcos de trabajo NIST CSF y NIST SP 800-37 referentes a las funciones, categorías y subcategorías recomendadas a usar para el diseño de controles. Se agrupan los puntos clave de

ambos marcos de trabajo relacionados con el control, con el propósito de mejorar el control y realizar las correcciones necesarias para completar el diseño del control de seguridad. Durante el proceso se consideran los riesgos a mitigar y los activos de información para que el control se ajuste a las necesidades específicas a suplir en la entidad bancaria con los activos de información relacionados a los riesgos mitigados. El control presenta la afectación mediante su nombre y la descripción de su ejecución, de este modo durante su planteamiento el control puede ir cambiando para ser ajustado de acuerdo con las necesidades del encargado de diseñar el control de seguridad. Además, se agregaron los responsables involucrados de ejecutar y revisar el control de seguridad estableciendo las recomendaciones de seguridad establecidas en la NIST SP 800-37. También, se agrega la periodicidad en la que se recomienda que el control sea ejecutado, el valor asignado en un inicio debe ser evaluado en el tiempo al considerar si está siendo efectivo para mitigar los riesgos. Sobre lo mencionado para el contexto de una entidad bancaria para cubrir los riesgos de seguridad y poder cumplir con sus obligaciones de cumplimiento se realiza el diseño consolidado de los controles destinados a mitigar los riesgos y evitar una afectación en las operaciones. A continuación, se muestra en la Tabla 27 el extracto del diseño realizado para un control de seguridad.

Tabla 27

*Extracto del diseño de un control de seguridad*

| **Nombre de la columna** | **Contenido de la columna extraída** |
|---|---|
| ID | C36 |
| NIST CSF | Identificar:<br>ID.SC-3<br>ID.SC-4<br><br>Proteger:<br>PR.AT-1<br>PR.AT-5 |
| NIST SP 800-37 | Preparar:<br>TASK P-9 |

| **Nombre de la columna** | **Contenido de la columna extraída** |
|---|---|
| | TASK P-10<br>TASK P-11<br><br>Seleccionar:<br>TASK S-1<br>TASK S-2<br>TASK S-3<br>TASK S-4<br>TASK S-5<br>TASK S-6<br><br>Implementar:<br>TASK I-1<br>TASK I-2 |
| Nombre del control | Control para la generación inicial de acuerdos de confidencialidad con la entidad bancaria |
| Descripción del control de seguridad | Se deben establecer acuerdos de confidencialidad, NDA por sus siglas en inglés, con los proveedores para proteger la información confidencial y sensible tratada en los sistemas de información. |
| Detalles del diseño para la implementación del control de seguridad | El control establece la realización de la revisión de los acuerdos de confidencialidad generados por la entidad bancaria con los proveedores al establecer ciertos compromisos necesarios para la realización de sus actividades. Esto implicaría la realización de las actividades necesarias de protección de los datos sensibles usados por los proveedores del servicio.<br><br>Para lograr esto se deben incluir cláusulas los aspectos de ciberseguridad y privacidad de datos en los acuerdos de confidencialidad. Esto último se debe realizar mediante la inclusión de cláusulas específicas que aborden los aspectos de seguridad en las mejores prácticas de seguridad de la información. La importancia de esta actividad recae en que es necesario que se actualicen las cláusulas establecidas para mantener seguros los sistemas. Además, es fundamental que esta actividad deba ser acompañada del equipo legal en forma complementaria para abordar los puntos relacionados al cumplimiento de las obligaciones legales en ciberseguridad y privacidad de datos. |
| Responsables involucrados | Representante Designado del Oficial de Autorización, Proveedor de Controles Comunes, Arquitecto de Seguridad o Privacidad, Funcionario Senior Responsable de la Gestión de Riesgos, Oficial Senior de Seguridad de la Información de la Agencia, Oficial Senior de Privacidad de la Agencia, Administrador de Sistema, Propietario de Sistema, Oficial de Seguridad o Privacidad del Sistema, Usuario del Sistema, Ingeniero de Seguridad o Privacidad de Sistemas. |
| Periodicidad | Revisión semestral. |
| Controles relacionados | C1, C37, C41, C43, C44, C48. |

| Nombre de la columna | Contenido de la columna extraída |
|---|---|
| Riesgos mitigados | R41: Contratos inadecuados/inexistencia de contratos ocasiona o genera fuga de información.<br>R42: Contratos inadecuados/inexistencia de contratos ocasiona o genera incumplimiento del plan de mantenimiento.<br>R43: Contratos inadecuados/inexistencia de contratos ocasiona o genera modificación no autorizada de la información. |
| Respuesta a los riesgos | Mitigar |
| Documentos relacionados de la Revisión Sistemática | - E9: Analysis of General Data Protection Regulation Compliance Requirements and Mobile Banking Application Security Challenges<br>- E10: Security Risk Management in Online System<br>- E11: Data Privacy and System Security for Banking and Financial Services Industry based on Cloud Computing Infrastructure |

*Nota*. Elaboración propia.

El documento para verificar el presente resultado esperado alcanzado al diseñar los controles de seguridad en ciberseguridad y privacidad de datos para las entidades bancarias se encuentra en el Anexo G sección 2. Además, al tener el informe del diseño de controles validado y aprobado al 100% por un especialista en seguridad de la información o privacidad de datos se alcanzan los indicadores objetivamente en el acta de validación ubicada en Anexo G sección 3.

### 7.3. Discusión

Durante todo el proceso del diseño de controles es importante tener en consideración los riesgos a ser mitigados, así como los activos de información involucrados; pero esta situación puede variar dependiendo de la situación actual de la entidad bancaria. De este modo el planteamiento del control base al realizar el diseño de los controles debe ser realizado sobre los conocimientos previos del profesional que realiza esta labor. De tal forma que el control base, como su nombre lo indica, pueda definir el objetivo final a lograrse con el diseño del control de seguridad. Los controles deben ser diseñados dependiendo del riesgo, sistema, o pueden hibridar entre ambos de acuerdo con la arquitectura de seguridad o privacidad (RMFISO, 2018) de la entidad bancaria. Por lo tanto, durante su planteamiento el diseño del

control puede cambiar y adaptarse a los riesgos de seguridad a mitigar con el uso de las metodologías de trabajo planteadas en los marcos de trabajo actualizados. Por esta razón se debe realizar la revisión periódica del control diseñado para comprender si se abordan las necesidades específicas de la entidad bancaria para salvaguardar la seguridad de los activos de información y la información que contengan. La revisión periódica planteada debe ir acompañada de un plan de mantenimiento adecuado sobre la documentación y su posible formalización posterior de los controles propuestos al ser implementados.

Por consiguiente, en el proceso se ha procedido con la actualización del marco de trabajo de NIST CSF 1.1 a la versión 2.0. Este proceso incluyo el mapeo detallado entre ambas versiones, considerando todos los tipos de movimientos, cambios y actualizaciones que pudieron ocurrir entre las diversas funciones del marco de trabajo. Los ajusten se encuentran documentados en la versión de NIST CSF 1.1 en donde se explica los movimientos, la principal modificación del marco de trabajo fue la inclusión de una nueva función llamada Gobernar que trae información de varias otras funciones. En general se ha logrado mantener los controles con algunos pequeños ajustes aplicados dependiendo del cambio revisado sobre cada una de las funciones.

Adicionalmente al momento de diseñar los controles de seguridad se asignaron responsables involucrados encargados del diseño y posterior revisión subsiguiente de las recomendaciones establecidas en la herramienta del marco de trabajo NIST SP 800-37. De este modo se pueden agregar, eliminar o actualizar la asignación de responsables al revisar las recomendaciones planteadas por los marcos de trabajo para el uso de la herramienta. Para garantizar la eficacia y evitar conflictos en las actividades NIST 800-37 en el TASK P-1 menciona que se deben asegurar que no haya conflictos de interés al asignar a la misma persona a múltiples roles de gestión de riesgos (RMFISO, 2018). Así también se deben realizar revisiones periódicas del diseño planteado que evalúen la eficacia y eficacia de los roles por

parte de los responsables involucrados para los controles de seguridad asignados. De este modo se puede comprobar que los controles sigan siendo efectivos durante su tiempo de uso.

Además, en cuanto a la periodicidad para el control de seguridad diseñado, se debe comprender que su implementación requiere la evaluación continua de los resultados alcanzados. Esta evaluación debe realizarse en intervalos adecuados y ajustar la periodicidad asignada al control según sea necesario. El conjunto de medidas permite garantizar que los controles abordan de manera efectiva las diversas situaciones de riesgo. Por lo tanto, desde el planteamiento inicial del diseño del control se debe considerar las posibilidades de cambio para ajustarse de acuerdo con la necesidad y realidad de la entidad bancaria.

En conclusión, el diseño de los controles de ciberseguridad y privacidad de datos en el contexto del cumplimiento de entidades bancarias se aborda utilizando los marcos de trabajo del NIST CSF 2.0 y NIST SP 800-37. Estos marcos de trabajo proporcionan las mejores pautas para abordar los riesgos identificados en los temas de ciberseguridad y privacidad de datos en el diseño de controles planteado. Los controles diseñados se ajustan a las necesidades y características específicas de una entidad bancaria, teniendo en consideración los diversos tipos de activos de información. También, se asignan responsables involucrados de la revisión y verificación del diseño para su posterior implementación al considerar la eficacia del diseño planteado. De esta manera, los controles de seguridad aseguran la protección en ciberseguridad y privacidad de datos de los activos de información de la entidad bancaria ante la posible materialización de las amenazas de su entorno, en relación con el cumplimiento de sus obligaciones en la normativa vigente.

# Capítulo 8. Desarrollar una guía que integre los análisis y controles diseñados, asegurando su efectividad y aplicabilidad en las entidades bancarias en el Perú

## 8.1. Introducción

En este capítulo se presenta los resultados obtenidos hasta el quinto objetivo planteado para el proyecto de fin de carrera que consiste en desarrollar una guía sobre los controles de seguridad para los riesgos de ciberseguridad y privacidad de datos en las entidades bancarias en Perú. De este modo se presenta el consolidado sobre el análisis realizado y de todos los controles formulados en el capítulo 7 para mitigar las situaciones de riesgo. Esto permite completar la guía para el análisis de riesgos de ciberseguridad y privacidad de datos para el aseguramiento del cumplimiento de entidades bancarias en el Perú.

## 8.2. Resultados alcanzados

### 8.2.1. R1 para O5. Guía para el análisis de riesgos de ciberseguridad y privacidad de datos para el aseguramiento del cumplimiento de entidades bancarias en el Perú.

Inicialmente se llevó a cabo la transcripción de toda la información generada en el diseño de los controles de seguridad del capítulo 7 (O4) en un informe consolidado con la información de todos los controles como el nombre asignado, descripción detallada, la explicación para su posible implementación, los responsables involucrados, periodicidad esperada, controles relacionados, riesgos mitigados y la respuesta a los riesgos. Para lograr trascribir toda la información se usó como complemento un *script* para consolidar en un documento Google Docs que recorre todo el documento de Google Sheet generado en el diseño de controles (O4). De tal manera que permite recopilar y organizar adecuadamente todos los datos en un documento formal al agregar el índice a todas las hojas, asignar el nombre de los controles de seguridad, toda la información relacionada al control diseñado y produciendo la

estructura estéticamente agradable para la guía. Adicionalmente durante el proceso de consolidación del documento de la guía el script realiza un proceso de búsqueda de los activos de información que están relacionados con cada uno de los riesgos a ser mitigados por los controles de seguridad. Posteriormente cuando se genera el documento consolidado se agrega manualmente la estructura inicial del análisis llevado a cabo con información para la guía respecto a la portada y un espacio para el texto introductorio.

El código fuente del script usado para la generación del informe de diseño de controles de seguridad se encuentra en el Anexo H sección 1; también, el documento base para realizar el informe y el informe generado de la guía para el quinto objetivo del proyecto del presente resultado esperado al generar la guía del diseño de controles para abordar los riesgos identificados de ciberseguridad y privacidad de datos se encuentra en el Anexo H sección 1. Además, al tener el informe del diseño de controles validado y aprobado al 100% por un especialista en seguridad de la información o privacidad de datos se alcanzan los indicadores objetivamente en el acta de validación ubicada en Anexo H sección 3.

### 8.3. Discusión

La consolidación de la información generada en el diseño de los controles de seguridad en una guía detallada ha permitido desarrollar una guía integral que aborda los riesgos de ciberseguridad y privacidad de datos en las entidades bancarias del Perú. Al organizar adecuadamente todos los datos relevantes en un solo lugar se ha logrado estructurar los controles de seguridad en un solo documento. En relación con esto, la NIST SP 800-37 en TASK S-4 destaca la importancia de que los planes de privacidad y seguridad colaboren para garantizar la presentación de los controles adecuados y la definición clara de roles y responsabilidades (RMFISO, 2018). Este proceso permite presentar de forma eficaz todos los conocimientos desarrollados en el proceso de análisis realizado, lo que se facilita su uso y comprensión.

En el proceso de creación de la guía el uso del script para la transcripción y organización de la estructura final de la guía resultante ha sido clave. Esto ha permitido automatizar la recopilación de información relevante, asegurando que todos los aspectos críticos estén contenidos en la guía, y que ante la posibilidad de cualquier cambio estos se generen de forma precisa en el documento final y así minimizar la posibilidad de errores humanos en la trascripción. De modo que la estructura final generada permite la inclusión de información adicional sobre el proceso como la porta, un texto introductorio, y el índice con respecto al conjunto de controles de seguridad planteados. Esta organización no solo mejora la experiencia del usuario final al usar el documento guía, sino que también asegura que los controles sean fácilmente identificables y diferenciables entre sí.

# Capítulo 9. Conclusiones y Trabajos Futuros

## 9.1. Conclusiones

El avance realizado en relación con los objetivos planteados ha sido significativo en la guía para el análisis de riesgos en ciberseguridad y privacidad de datos para el aseguramiento del cumplimiento normativo de las entidades bancarias en el Perú. En este sentido, se ha logrado identificar el conjunto de obligaciones de cumplimiento en ciberseguridad y privacidad de datos para las entidades bancarias (O1). De este modo la identificación de las obligaciones de cumplimiento proporciona una base sólida para que las entidades bancarias puedan gestionar adecuadamente las obligaciones identificadas a lo largo de su vigencia legal. Así como permite realizar el seguimiento adecuado de los cambios en los requisitos legales y normativos en los términos de ciberseguridad y privacidad de datos que deben requerir cumplir las entidades bancarias.

Así también se ha logrado identificar las vulnerabilidades y amenazas de ciberseguridad y privacidad de datos para las entidades bancarias (O2). Esto último permite tener una comprensión detallada de las vulnerabilidades y amenazas que afectan a las entidades bancarias entre sus diversos activos de información. De tal forma que la entidad bancaria pueda tener plena consiente sobre la situación actual, facultándola de emprender acciones específicas para generar el mantenimiento sobre las nuevas vulnerabilidades y amenazas que surjan en el tiempo ante cualquier cambio que pueda generarse en sus obligaciones de cumplimiento. En conjunto es esencial identificar de manera conjunta las vulnerabilidades y amenazas, ya que ello posibilita la formulación de estrategias eficaces para mitigar situaciones de riesgo y salvaguardar la integridad de los activos de información.

Asimismo, se ha realizado la identificación y evaluación de los riesgos de ciberseguridad y privacidad de datos para las entidades bancarias (O3). Esta evaluación de

riesgos permite que las entidades bancarias puedan tomar decisiones informadas en base a las situaciones de riesgos identificadas. Además, posibilita la diversificación de los esfuerzos, facilitando así el abordaje oportuno de las diversas situaciones de riesgo al ser evaluadas. Este enfoque contribuye a tomar medidas con mayor prontitud y eficacia, permitiendo proteger la infraestructura interna e información confidencial de los clientes.

Además, se han diseñado los controles de seguridad ante las situaciones de riesgos en ciberseguridad y privacidad de datos como parte del proceso de cumplimiento de las entidades bancarias (O4). El diseño de estos controles de seguridad proporciona un marco sólido de seguridad que permite garantizar la integridad y confidencialidad de los activos de información disponibles en la entidad bancaria. De forma que se abordan de manera específica las necesidades inherentes propias de la actividad realizada en las entidades bancarias con el diseño de los controles de seguridad.

Por último, considerando el objetivo general del proyecto de fin de carrera al elaborar una guía para el análisis de riesgos de ciberseguridad y privacidad de datos para el aseguramiento del cumplimiento de las entidades bancarias en el Perú, usando los marcos de trabajo NIST CSF y NIST SP 800-37. Se ha logrado generar una guía al analizar los riesgos de ciberseguridad y privacidad de datos en una entidad bancaria con el uso de los marcos de trabajo NIST CSF y NIST SP 800-37 que proporcionan las mejores pautas para abordar los riesgos identificados en base al diseño de los controles de seguridad (O5). De tal modo que al diseñar los controles de seguridad se ajusten a las necesidades específicas de una entidad bancaria para asegurar el cumplimiento normativo sobre los activos de información analizados.

## 9.2. Trabajos Futuros

En el presente trabajo de fin de carrera se ha abordado la guía para el análisis de riesgos de ciberseguridad y privacidad de datos para el aseguramiento del cumplimiento de entidades bancarias en el Perú siguiendo los lineamientos presentes de las herramientas NIST CSF y

NIST SP 800-37. De modo que el trabajo realizado puede ser adaptada en trabajos futuros bajo la misma estructura, pero con el uso de diferentes marcos de trabajo que puedan surgir en el tiempo y que estén relacionados a la temática de ciberseguridad y privacidad de datos del trabajo actual. Esta adaptabilidad presentada en los resultados alcanzados es crucial, ya que permite realizar los cambios necesarios y generar el mantenimiento para atender posibles necesidades futuras siguiendo las mejores prácticas en seguridad de la información. Por esta razón, será fundamental estar informado acerca de las nuevas estrategias de respuesta ante los riesgos de ciberseguridad y privacidad de datos, así como sobre los nuevos desafíos de seguridad relevantes para el entorno de las entidades bancarias.

Asimismo, el presente trabajo puede ser adaptado a trabajos futuros con la documentación relevante de las obligaciones de cumplimiento de las entidades bancarias. Por lo tanto, esta situación dependerá de la generación de nueva regulación y normativa que pueda surgir en el tiempo en los ámbitos de ciberseguridad y privacidad de datos. Esto posibilitaría mantener actualizado los documentos de obligaciones de cumplimiento identificados en el presente proyecto de fin de carrera, y adaptar la guía de análisis de riesgos ante las nuevas exigencias legales y regulatorias en el Perú. Esta práctica facilitaría la actualización de las vulnerabilidades, amenazas y riesgos identificados, posibilitando la formulación del diseño de controles de seguridad adecuados a los cambiantes riesgos de ciberseguridad y privacidad de datos en el entorno bancario, así como garantizar el cumplimiento de las obligaciones normativas identificadas para las entidades bancarias.

Adicionalmente se plantea como trabajo futuro la implementación y evaluación de la guía de análisis de riesgos de ciberseguridad y privacidad de datos en entidades bancarias en el Perú. Este enfoque como trabajo futuro permitiría llevar a cabo la implementación del diseño de controles de seguridad presentados en la presente guía para abordar las vulnerabilidades, amenazas y riesgos identificados para las entidades bancaria. Además, brindaría la oportunidad

de evaluar la aplicabilidad y medir la efectividad de los controles de seguridad planteados en un entorno operativo realista. Así como de comprobar en un entorno directo a la entidad bancaria la evaluación de riesgos efectuada en la matriz de riesgos para cada uno de los activos de información identificados.

En conclusión, en la medida que el entorno cibernético de los activos de información de la entidad bancaria requiera ser adaptado ante la aparición de nuevas vulnerabilidades, amenazas y riesgos es importante que las entidades bancarias puedan responder adecuadamente ante los nuevos desafíos en ciberseguridad y privacidad de datos para asegurar el cumplimiento regulatorio de las entidades bancarias. Esta situación brinda una visión más amplia y realista en el campo de ciberseguridad y privacidad de datos al adaptarse al contexto actual de las entidades bancarias. De este modo, a través de su adaptación presente y futura se puede generar nuevo conocimiento con el uso de las mejores prácticas que al ser incorporadas al presente trabajo proporcionarán una guía sólida y adaptada para su eventual implementación.

## Referencias


Addae, J. A., Simpson, G., & Ampong, G. O. A. (2019). Factors influencing information security policy compliance behavior. *Proceedings - 2019 International Conference on Cyber Security and Internet of Things, ICSIoT 2019*, 43-47. https://doi.org/10.1109/ICSIoT47925.2019.00015

Agencia EFE. (2020). *Ciberseguridad: en el 2020 van 15 denuncias contra empresas en el Perú*. Gestion. https://gestion.pe/peru/ciberseguridad-en-el-2020-van-15-denuncias-contra-empresas-en-el-peru-noticia/

Al Batayneh, A. A., Qasaimeh, M., & Al-Qassas, R. S. (2021). A Scoring System for Information Security Governance Framework Using Deep Learning Algorithms: A Case Study on the Banking Sector. *Journal of Data and Information Quality*, *13*(2), 9. https://doi.org/10.1145/3418172

Al-Alawi, A. I., & Al-Bassam, S. A. (2019). Assessing the factors of cybersecurity awareness in the banking sector. *Arab Gulf Journal of Scientific Research*, *37*(4), 17-32.

Alsalamah, A. (2017). Security risk management in online system. En A. Alsalamah (Ed.), *Proceedings - 2017 5th International Conference on Applied Computing and Information Technology, 2017 4th International Conference on Computational Science/Intelligence and Applied Informatics and 2017 1st International Conference on Big Data, Cloud Compu* (pp. 119-124). IEEE. https://doi.org/10.1109/ACIT-CSII-BCD.2017.59

Ashiku, L., & Dagli, C. (2019). Cybersecurity as a centralized directed system of systems using SoS explorer as a tool. *2019 14th Annual Conference System of Systems Engineering, SoSE 2019*, 140-145. https://doi.org/10.1109/SYSOSE.2019.8753872

Autoridad Nacional de Protección de Datos Personales. (2013). *Decreto supremo Nº 003-2013-JUS. Reglamento de la Ley Nº 29733, Ley de Protección de Datos Personales*. https://cdn.www.gob.pe/uploads/document/file/1913756/DS-3-2013-JUS.REGLAMENTO.LPDP_.pdf.pdf

Autoridad Nacional de Protección de Datos Personales. (2019a). *El MINJUSDH inicia proceso administrativo sancionador al BCP*. https://www.gob.pe/institucion/anpd/noticias/108680-el-minjusdh-inicia-proceso-administrativo-sancionador-al-bcp

Autoridad Nacional de Protección de Datos Personales. (2019b, noviembre). *Guía práctica para la observancia del «Deber de Informar»*. https://cdn.www.gob.pe/uploads/document/file/472765/Gu%C3%ADa_Deber_de_Informar.pdf

Autoridad Nacional de Protección de Datos Personales. (2020). *ANPD sanciona a entidad bancaria con S/ 166 mil (40 UITs) por no resguardar la confidencialidad de los datos personales de sus clientes*. https://www.gob.pe/institucion/anpd/noticias/305427-anpd-sanciona-a-entidad-bancaria-con-s-166-mil-40-uits-por-no-resguardar-la-confidencialidad-de-los-datos-personales-de-sus-clientes

Becker, M., & Buchkremer, R. (2019). A practical process mining approach for compliance management. *Journal of Financial Regulation and Compliance*, *27*(4), 464-478. https://doi.org/10.1108/JFRC-12-2018-0163

Conrad, S. S. (2019). Protecting Personal Information and Data Privacy: What Students Need to Know. *J. Comput. Sci. Coll.*, *35*(3), 77–86. https://doi.org/10.5555/3381569.3381580

*Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*. (2018). https://doi.org/10.6028/NIST.CSWP.04162018

International Business Machines. (2020). *Cost of a Data Breach Report*. https://www.ibm.com/downloads/cas/RZAX14GX

International Business Machines. (2022). *X-Force Threat Intelligence Index 2022*. https://www.ibm.com/downloads/cas/ADLMYLAZ

International Organization for Standardization. (2018). *Information technology — Security techniques — Information security risk management*. https://www.iso.org/standard/75281.html

International Organization for Standardization. (2021). *Compliance management systems — Requirements with guidance for use*. https://www.iso.org/standard/75080.html

Kitchenham, B., & Charters, S. (2007). Guidelines for performing systematic literature reviews in software engineering. En *Technical report, Ver. 2.3 EBSE Technical Report. EBSE*.

Kulik, T., Dongol, B., Larsen, P. G., Macedo, H. D., Schneider, S., Tran-Jørgensen, P. W. V., & Woodcock, J. (2022). A Survey of Practical Formal Methods for Security. *Formal Aspects of Computing*, *34*(1), 39. https://doi.org/10.1145/3522582

Lakshmi, K. K., Gupta, H., & Ranjan, J. (2020). Analysis of General Data Protection Regulation Compliance Requirements and Mobile Banking Application Security Challenges. *ICRITO 2020 - IEEE 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)*, 1028-1032. https://doi.org/10.1109/ICRITO48877.2020.9197954

*Ley N° 29733. Ley de Protección de Datos Personales*. (2011). https://diariooficial.elperuano.pe/pdf/0036/ley-proteccion-datos-personales.pdf

Mahalle, A., Yong, J., Tao, X., & Shen, J. (2018). Data Privacy and System Security for Banking and Financial Services Industry based on Cloud Computing Infrastructure. *Proceedings of the 2018 IEEE 22nd International Conference on Computer Supported Cooperative Work in Design, CSCWD 2018*, 75-80. https://doi.org/10.1109/CSCWD.2018.8465318

Malinka, K., Hujnak, O., Hanacek, P., & Hellebrandt, L. (2022). E-Banking Security Study-10 Years Later. *IEEE Access*, *10*, 16681-16699. https://doi.org/10.1109/ACCESS.2022.3149475

Ministerio de Justicia y Derechos Humanos. (2013). *Resolución directoral Nº 019-2013-JUS/DGPDP. Directiva de Seguridad*. https://www.minjus.gob.pe/wp-content/uploads/2013/10/RD-Directiva-de-Seguridad.pdf

Ministerio de Justicia y Derechos Humanos. (2020). *Resolución directoral Nº 02-2020-JUS/DGPDP. Directiva para el Tratamiento de Datos Personales mediante Sistemas de Videovigilancia*. https://cdn.www.gob.pe/uploads/document/file/523241/RD-N_-02-2020.pdf

Ministerio de Justicia y Derechos Humanos. (2021). *Autoridades impulsan gobernanza de datos e interoperabilidad del sistema de justicia*. https://www.gob.pe/institucion/minjus/noticias/483667-autoridades-impulsan-gobernanza-de-datos-e-interoperabilidad-del-sistema-de-justicia

National Institute of Standards and Technology. (2012). *Guide for Conducting Risk Assessments*. https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final

Petticrew, M., & Roberts, H. (Eds.). (2006). *Systematic Reviews in the Social Sciences*. Blackwell Publishing Ltd. https://doi.org/10.1002/9780470754887

Pocher, N., & Veneris, A. (2022). Privacy and Transparency in CBDCs: A Regulation-by-Design AML/CFT Scheme. *IEEE Transactions on Network and Service Management*, *19*(2), 1776-1788. https://doi.org/10.1109/TNSM.2021.3136984

*Risk management framework for information systems and organizations*. (2018). https://doi.org/10.6028/NIST.SP.800-37r2

Scott, B. F. (2021). Red teaming financial crime risks in the banking sector. *Journal of Financial Crime*, *28*(1), 98-111. https://doi.org/10.1108/JFC-06-2020-0118

Superintendencia de Banca y Seguros del Perú. (2009). *Programa Finanzas en el Cole*. https://www.sbs.gob.pe/Portals/3/jer/enlaces/Manual-del-docente2.pdf

Superintendencia de Banca y Seguros del Perú. (2013). *Resolución S.B.S. Nº 6523-2013. Reglamento de Tarjetas de Crédito y Débito*. https://intranet2.sbs.gob.pe/dv_int_cn/718/v3.0/Adjuntos/6523-2013.pdf

Superintendencia de Banca y Seguros del Perú. (2019a). *Ciberseguridad: Una hoja de ruta para su desarrollo en los sistemas supervisados*. https://www.sbs.gob.pe/boletin/detalleboletin/idbulletin/1213#

Superintendencia de Banca y Seguros del Perú. (2019b). *Resolución S.B.S. Nº 5570-2019. Modificatoria de la Resolución S.B.S. Nº 6523-2013 del Reglamento de Tarjetas de Crédito y Débito*. https://intranet2.sbs.gob.pe/dv_int_cn/1877/v1.0/Adjuntos/5570-2019.R.pdf

Superintendencia de Banca y Seguros del Perú. (2020). *Resolución S.B.S. Nº 877-2020. Reglamento para la Gestión de la Continuidad del Negocio*. https://intranet2.sbs.gob.pe/dv_int_cn/1894/v1.0/Adjuntos/877-2020.R.pdf

Superintendencia de Banca y Seguros del Perú. (2021). *Resolución S.B.S. Nº 504-2021. Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad*. https://intranet2.sbs.gob.pe/dv_int_cn/2046/v2.0/Adjuntos/504-2021.R.pdf

Superintendencia de Banca y Seguros del Perú. (2022). *Ciberseguridad: construyendo resiliencia en el sistema financiero*.

Teodoro, N., Gonçalves, L., & Serrão, C. (2015). NIST cybersecurity framework compliance: A generic model for dynamic assessment and predictive requirements. *Proceedings - 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2015*, *1*, 418-425. https://doi.org/10.1109/Trustcom.2015.402

*The NIST Cybersecurity Framework (CSF) 2.0*. (2024). https://doi.org/10.6028/NIST.CSWP.29

Wodo, W., Stygar, D., & Błaśkiewicz, P. (2021). Security issues of electronic and mobile banking. *Proceedings of the 18th International Conference on Security and Cryptography, SECRYPT 2021*, 631-638. https://doi.org/10.5220/0010466606310638

Zetzsche, D. A., Anker-Sørensen, L., Passador, M. L., & Wehrli, A. (2022). DLT-based enhancement of cross-border payment efficiency – a legal and regulatory perspective. *Law and Financial Markets Review*, *15*(1-2), 1-46. https://doi.org/10.1080/17521440.2022.2065809

# Anexos

## Anexo A: Plan de Proyecto

### Justificación

Conforme un reporte desarrollado por International Business Machines (IBM) sobre el panorama global de empresas por sector en cuando a la cantidad de ataques cibernéticos recibidos o a los que están expuestas padecer, se puede observar en la Figura 7 que entre los principales afectados está el sector financiero (IBM, 2022). En otras palabras, las entidades financieras entre las que se encuentran las entidades bancarias son las más perjudicadas en la medida de los servicios ofrecidos por la naturaleza de sus operaciones. De esta forma el sector bancario en el Perú enfrenta riesgos significativos, por ejemplo, se ha reportado que tras un ataque cibernético de un *hacker* se filtraron los datos de identificación personal, números de tarjetas y cuentas bancarias de los clientes (Agencia EFE, 2020). En consecuencia, las operaciones inherentes internas de las entidades bancarias exhiben ciertos riesgos de sufrir ataques cibernéticos debido a las actividades relacionadas con el manejo del dinero y el tratamiento de datos sensibles provistos por los clientes en sus actividades particulares.

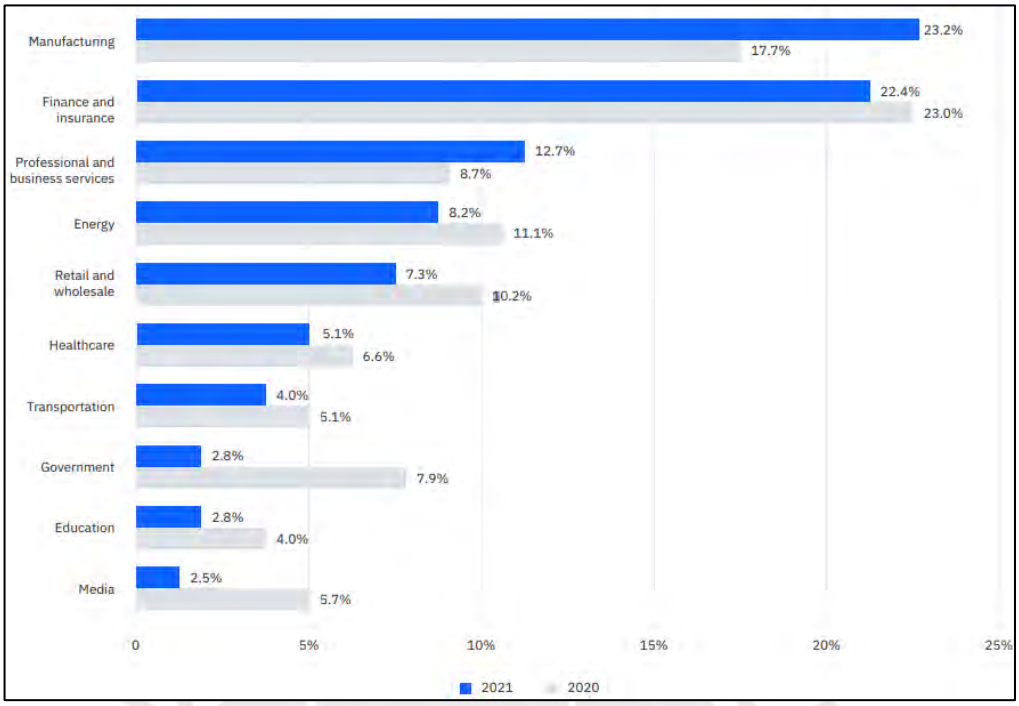



*Figura 7.* Desglose de los 10 principales ataques por industrias 2020 y 2021

*Nota. Figura tomada* (IBM 2022). La figura representa por medio del gráfico de barras comparativo entre los años 2020 y 2021 los sectores en la industria que tienen la mayor proporción de ataques cibernéticos. Se destaca del gráfico el sector financiero como uno de los principales afectados.

Por lo que ante los ataques cibernéticos se deben desarrollar diversas formas de respuesta por parte de las entidades bancarias en el Perú para asegurar el cumplimiento regulatorio debido a que son fiscalizados por las entidades regulatorias. Entre las medidas de cumplimiento que deben seguir está, por ejemplo, en el desarrollo de medidas de protección a los bancos de datos de que tengan información de clientes (Agencia EFE, 2020). Este aspecto forma parte de las obligaciones de cumplimiento que deben cumplir las entidades bancarias al desarrollar mecanismos y procesos que permitan lograr los estándares regulatorios de cumplimiento local. No obstante, en ocasiones no se logran cumplir con todas las medidas de cumplimiento necesarios para mantener seguros los sistemas de información. Esto último representa la necesidad de identificar correctamente los riesgos de las vulnerabilidades y

amenazas generadas por posibles brechas de seguridad no identificadas previamente dentro de los sistemas de información como se muestra en la Figura 8.

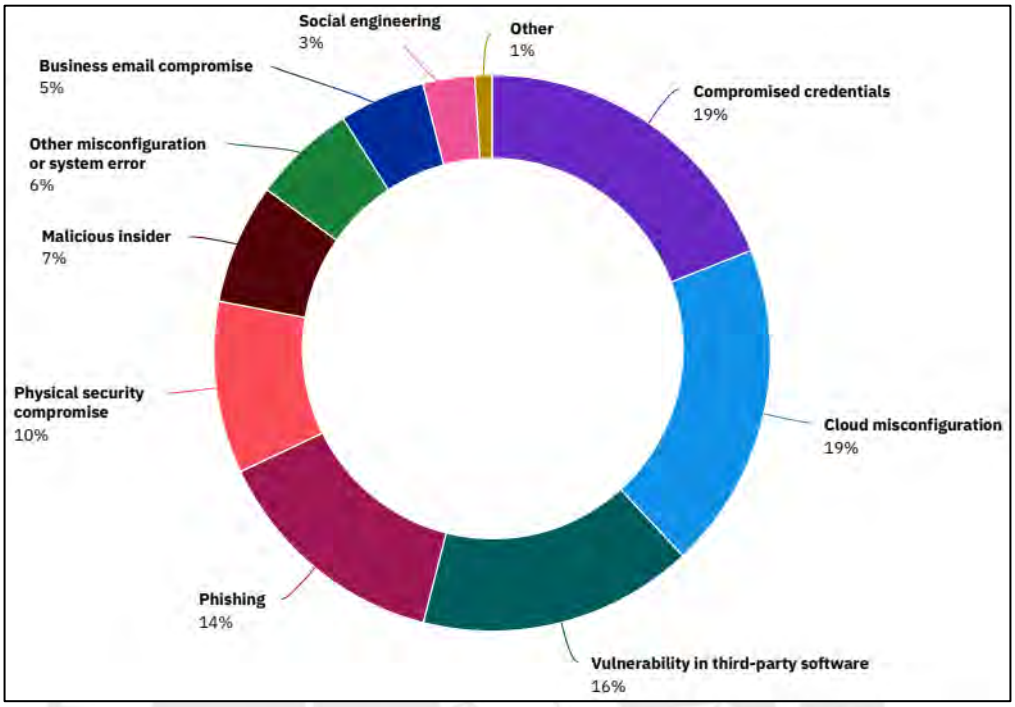



*Figura 8.* Tipos de amenazas que ocasionaron la filtración de datos

*Nota. Figura tomada* (IBM, 2020). La figura representa por medio del gráfico circular para el año 2020 los porcentajes de amenazas que ocasionan los ataques cibernéticos.

Por tal motivo, los resultados presentados anteriormente resaltan la necesidad de llevar a cabo un análisis riguroso de los riesgos de ciberseguridad y privacidad de datos para las entidades bancarias en base a las obligaciones de cumplimiento locales. El cumplimiento de dichas obligaciones de cumplimiento se basará en la reglamentación y normativas locales que deben ser debidamente desarrolladas por las diversas entidades bancarias del Perú y servirá como guía en las cuales no han sido analizadas de manera adecuada hasta el momento.

En este sentido, se espera que el proyecto de fin de carrera pueda ser utilizado por cualquier entidad bancaria en el Perú que desee realizar el análisis de riesgo adecuado sobre sus activos de información partiendo de las obligaciones de cumplimiento de ciberseguridad y privacidad de datos, según la normativa peruana. Además, permitirá desarrollar las medidas de

control necesarias con el diseño de controles a ser implementados ante las diversas vulnerabilidades y amenazas que aún no han sido identificadas adecuadamente, con el fin de garantizar el cumplimiento a seguir por parte la entidad bancaria.

**Viabilidad**

El proyecto de fin de carrera es viable debido a la disponibilidad de herramientas y recursos necesarios proporcionados por la biblioteca universitaria en la PUCP. También, la información respecto a las normativas de cumplimiento en ciberseguridad y privacidad de datos para las entidades bancarias es de acceso público en el Perú. En este sentido, la reglamentación y leyes necesarias que presentan la normativa de cumplimiento a seguir por las entidades bancarias están disponibles para acceso gratuito; por lo que no es necesario la compra de recursos físicos adicionales, herramientas de software o normativas complementarias que produzcan algún costo adicional en el proyecto de fin de carrera.

Adicionalmente, la formación requerida en ciberseguridad y privacidad de datos en las entidades bancarias se complementa con los conocimientos adquiridos en la carrera universitaria de ingeniería informática y las prácticas preprofesionales en el área de seguridad bancaria. Por último, el tiempo previsto para la realización del proyecto de carrera se enmarca en el plazo de 2 ciclos académicos.

**Alcance**

El presente proyecto de fin de carrera está relacionado al área de Tecnología de la información (TI) y tiene como objetivo el presentar el análisis de los riesgos de ciberseguridad y privacidad de datos para el aseguramiento del cumplimiento de las entidades bancarias en el Perú. La metodología de trabajo a desarrollar está dentro del ámbito tecnológico y será aplicada bajo el contexto del cumplimiento regulatorio que tienen las entidades bancarias peruanas en los temas de ciberseguridad y privacidad de datos. Así mismo el modelo de trabajo a desarrollar en el proyecto de fin de carrera para el análisis de los riesgos ciberseguridad y privacidad de

datos tiene como fin poder ser adaptado a cualquier entidad bancaria en el Perú debido a que las normas regulatorias para el cumplimiento en las entidades bancarias aplican a nivel nacional.

En ese sentido, el proceso de identificación del conjunto obligaciones de cumplimiento locales en ciberseguridad y privacidad de datos será guiado por la ISO 37301 cláusula 4.5 para identificar de forma adecuada los compromisos de cumplimiento y realizar a lo largo del tiempo que abarca el proyecto de fin de carrera el mantenimiento de las obligaciones de cumplimiento identificadas de las entidades bancarias. Posteriormente, se desarrollará la catalogación del conjunto de vulnerabilidades, amenazas y riesgos a partir de las obligaciones de cumplimiento identificadas en base al análisis de riesgo para la entidad bancaria. Por último, se presentará el diseño de los controles de los riesgos en ciberseguridad y privacidad de datos de forma que se puedan abordar los riesgos identificados previamente. En la catalogación y el diseño de los controles se usará como guía los marcos de trabajo NIST CSF y NIST SP 800-37 porque permitirá establecer bajo buenas prácticas el proceso de identificación, protección y respuesta ante situaciones de riesgo de una entidad bancaria en la seguridad de los sistemas de información.

**Limitaciones**

El proyecto de fin de carrera requiere del análisis de riesgos de ciberseguridad y privacidad de datos a partir de las obligaciones de cumplimiento, por lo que para este proceso se selecciona el conjunto de normativas de cumplimiento relacionadas a los temas de ciberseguridad y privacidad de datos que estén definidas dentro del marco legal vigente en el Perú para las entidades bancarias. Adicionalmente, se utilizan las normativas y estándares de trabajo en ciberseguridad y privacidad de datos en su última versión hasta la fecha de diciembre de 2022 debido a que la actualización de la normativa vigente podría significar un impacto mayor en el alcance del proyecto en términos de temporalidad.

**Identificación de los riesgos del proyecto**

En la presente sección para la identificación de los riesgos que podrían afectar el desarrollo del proyecto de fin de carrera. Para esto se usará el umbral de riesgo de la Tabla 28 Anexo A para medir la probabilidad, el impacto y la severidad de los riesgos en la calificación de severidad para la matriz de riesgo de la Tabla 29 Anexo A.

Tabla 28 Anexo A

*Umbral de Riesgo*

| Impacto / Probabilidad | Bajo (1) | Moderado (2) | Alto (3) |
|---|---|---|---|
| **Si ocurre (5)** | 5 | 10 | 15 |
| **Probable (4)** | 4 | 8 | 12 |
| **Posible (3)** | 3 | 6 | 9 |
| **Improbable (2)** | 2 | 4 | 6 |
| **No ocurre (1)** | 1 | 2 | 3 |

Tabla 29 Anexo A Matriz de riesgos

*Matriz de riesgos*

| Descripción del riesgo | Síntomas | P | I | S | Mitigación | Contingencia |
|---|---|---|---|---|---|---|
| No se tiene acceso a internet para realizar las actividades programadas de los entregables de tesis. | No se puede realizar las actividades programas de los entregables de tesis. | 2 | 2 | 4 | Contratar un plan de internet por celular para realizar las actividades programadas. | Activar el plan de internet por celular contratado previamente. |
| Pérdida parcial o total de la información contenida en el documento del proyecto de tesis. | El archivo de tesis estaba en el interior de una computadora que se extravió o descompuso. | 4 | 3 | 12 | Mantener los archivos del documento de tesis en el almacenamiento de la nube. | Acceder al almacenamiento en la nube y descargar el archivo de tesis. |
| Problemas de conexión a internet al realizar las | La conexión a internet es inestable por lo que el trabajo se | 4 | 2 | 8 | Contratar una operadora de internet diferente. También, | Activar el plan de internet contratado previamente. |

| Descripción del riesgo | Síntomas | P | I | S | Mitigación | Contingencia |
|---|---|---|---|---|---|---|
| actividades programadas. | ve interrumpido ocasionalmente. | | | | contratar un plan de internet por celular | |
| No encontrar especialistas en ciberseguridad y privacidad de datos en el sector bancario. | Después de haber contactado con especialistas en ciberseguridad y privacidad de datos en el sector bancario ninguno acepta la propuesta de revisión del entregable. | 3 | 3 | 9 | Contactar con mi asesor de tesis para encontrar algún especialista en ciberseguridad y privacidad de datos en el sector bancario. | Enviar solicitudes de revisión a los profesores de la PUCP que tengan experiencia en los temas de ciberseguridad y privacidad de datos en el sector bancario. |
| Los especialistas en ciberseguridad y privacidad de datos en el sector bancario no realizan la validación del entregable. | No se recibe respuesta alguna del especialista después de la fecha programada de revisión establecida. | 3 | 3 | 9 | Reservar un horario con anticipación para la realización de las reuniones y poder presentar oportunamente los resultados de la revisión del entregable. | Enviar un email para coordinar una nueva reunión. También, coordinar con otro especialista que realice la validación del entregable. |
| No se tiene energía eléctrica en el lugar de trabajo en donde se redacta el documento de tesis. | Ningún equipo electrónico conectado a la corriente eléctrica funciona. | 2 | 3 | 6 | Usar un equipo con la batería completamente cargada y mantener un plan de datos activo. | Conseguir una laptop que tenga una batería completamente cargada y mantener el modo de batería. |
| Tener una enfermedad que imposibilite al tesista de avanzar con la presentación de los entregables de tesis por un tiempo prolongado. | La imposibilidad de realizar los avances de los entregables de tesis por una enfermedad. | 2 | 3 | 6 | Realizar los entregables con días o semanas de anticipación a la fecha programada de entrega para evitar cualquier contratiempo en la presentación. | Descansar por un tiempo prolongado posponiendo los siguientes entregables hasta recuperarme de la enfermedad. |

*Nota.* Esta tabla muestra la matriz de riesgos en donde la columna "P" hace referencia a la probabilidad de que el riesgo ocurra, la columna "I" representa el impacto que ocasiona en el proyecto, y la columna "S" la severidad del riesgo que se calcula como la multiplicación de la probabilidad y el impacto.

**Estructura de descomposición del trabajo.**

Esta sección muestra en la Figura 9 el diagrama de la estructura de descomposición del trabajo (EDT) desarrollado para la planificación del proyecto de fin de carrera mediante la gestión del proyecto y producto. En la gestión del proyecto se realizan las actividades propias para la realización del documento del proyecto de fin de carrera, la presentación de los entregables en tesis 1, las reuniones con el asesor de tesis y los especialistas en seguridad de la información o privacidad de datos para la revisión y validación de los entregables. También, en la gestión del producto a realizarse se descomponen las actividades a partir de los objetivos específicos presentados para el presente proyecto de fin de carrera.

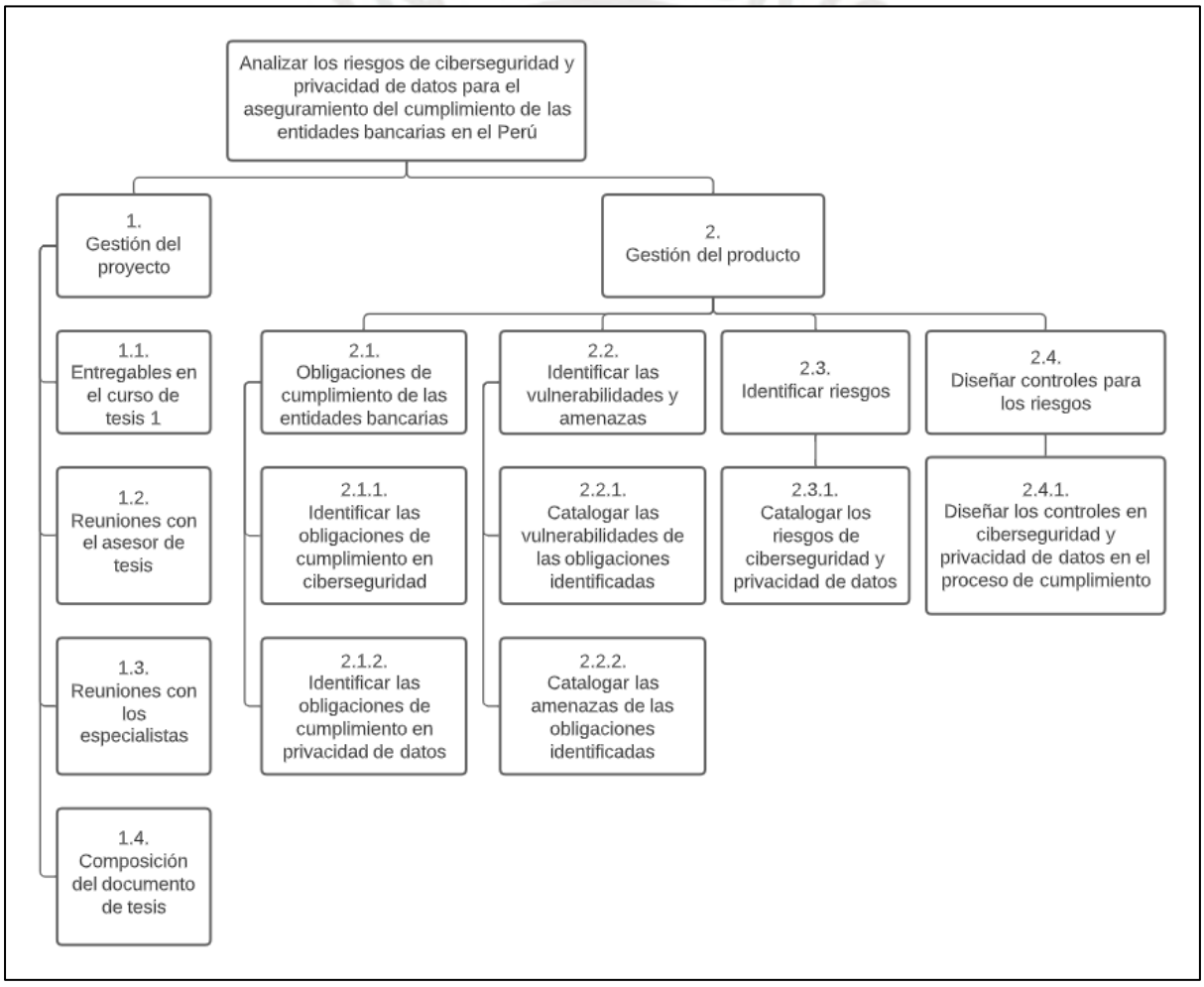



*Figura 9.* Estructura de descomposición del proyecto

*Nota*. El EDT se representa mediante un diagrama que divide las actividades entre la gestión del proyecto y el producto resultante.

**Lista de tareas.**

En esta sección en la Tabla 30 se presenta la lista de tareas a realizarse en el proyecto de fin de carrera mediante la descomposición de cada sección en el EDT con la duración en día que tomará la realización de la tarea, las horas que tomará en ser terminada la tarea, el costo estimado de la realización de la tarea y el método de verificación y validación para comprobar que la tarea fue realizada con éxito.

Tabla 30 Anexo A

*Lista de tareas*

| EDT | Nombre de la tarea | Duración (días) | Esfuerzo (horas-persona) | Costo estimado (S/.) | Método de verificación y validación |
|---|---|---|---|---|---|
| 1. | Gestión del proyecto | 347 | 182 | 1820 | - |
| 1.1. | Entregables en el curso de tesis 1 | 104 | 104 | 1040 | Revisión de los profesores del curso |
| - | Entregable 1.1 | 19 | 16 | 160 | Revisión de los profesores del curso |
| - | Entregable 1.2 | 7 | 14 | 140 | Revisión de los profesores del curso |
| - | Entregable 1.3 | 6 | 14 | 140 | Revisión de los profesores del curso |
| - | Entregable 1.4 | 5 | 12 | 120 | Revisión de los profesores del curso |
| - | Entregable 1.5 | 7 | 8 | 80 | Revisión de los profesores del curso |
| - | Entregable 1 | 3 | 4 | 40 | Revisión de los profesores del curso |
| - | Entregable 2.1 | 9 | 12 | 120 | Revisión de los profesores del curso |
| - | Entregable 2 | 4 | 8 | 80 | Revisión de los profesores del curso |
| - | Entregable 3 | 16 | 8 | 80 | Revisión de los profesores del curso |
| - | Entregable 4 | 13 | 8 | 80 | Revisión de los profesores del curso |
| 1.2. | Reuniones con el asesor de tesis (semanalmente) | 31 | 22 | 220 | Correos de confirmación |

| EDT | Nombre de la tarea | Duración (días) | Esfuerzo (horas-persona) | Costo estimado (S/.) | Método de verificación y validación |
|---|---|---|---|---|---|
| 1.3. | Reuniones con los especialistas | 16 | 6 | 60 | Correos de confirmación |
| 1.4. | Composición del documento de tesis | 347 | 50 | 500 | Correos de confirmación |
| 2. | Gestión del producto | 172 | 113 | 1130 | - |
| 2.1. | Obligaciones de cumplimiento de las entidades bancarias | 69 | 40 | 400 | Documento validado por un especialista en seguridad de la información o privacidad de datos en entidades bancarias |
| 2.1.1. | Identificar las obligaciones de cumplimiento en ciberseguridad | 21 | 20 | 200 | Documento validado por un especialista en seguridad de la información en entidades bancarias |
| 2.1.2. | Identificar las obligaciones de cumplimiento en privacidad de datos | 20 | 20 | 200 | Documento validado por un especialista en privacidad de datos en entidades bancarias |
| 2.2. | Identificar las vulnerabilidades y amenazas | 58 | 28 | 280 | Documento validado por un especialista en seguridad de la información o privacidad de datos |
| 2.2.1. | Catalogar las vulnerabilidades de las obligaciones identificadas | 44 | 14 | 140 | Documento validado por un especialista en seguridad de la información o privacidad de datos |
| 2.2.2. | Catalogar las amenazas de las obligaciones identificadas | 14 | 14 | 140 | Documento validado por un especialista en seguridad de la información o privacidad de datos |
| 2.3. | Identificar riesgos | 20 | 20 | 200 | Documento validado por un especialista en seguridad de la información o privacidad de datos |
| 2.3.1. | Catalogar los riesgos de | 20 | 20 | 200 | Documento validado por un especialista en |

| EDT | Nombre de la tarea | Duración (días) | Esfuerzo (horas-persona) | Costo estimado (S/.) | Método de verificación y validación |
|---|---|---|---|---|---|
| | ciberseguridad y privacidad de datos | | | | seguridad de la información o privacidad de datos |
| 2.4. | Diseñar controles para los riesgos | 25 | 25 | 250 | Documento validado por un especialista en seguridad de la información o privacidad de datos |
| 2.4.1. | Diseñar los controles en ciberseguridad y privacidad de datos en el proceso de cumplimiento | 25 | 25 | 250 | Documento validado por un especialista en seguridad de la información o privacidad de datos |

*Nota.* El EDT sigue el formato de la Figura 9.

**Cronograma del proyecto**

En esta sección se presenta el cronograma del proyecto mediante la descomposición de las actividades a realizarse en el EDT conformando en la Tabla 31 la división por medio de la fecha de inicio y fin entre cada una de las tareas.

Tabla 31 Anexo A Cronograma del Proyecto

*Cronograma del Proyecto*

| EDT | Nombre de la tarea | Fecha de inicio | Fecha de fin | Tiempo en días |
|---|---|---|---|---|
| 1. | Gestión del proyecto | 02/08/2022 | 15/07/2023 | 347 |
| 1.1. | Entregables en el curso de tesis 1 | 02/08/2022 | 14/11/2022 | 104 |
| - | Entregable 1.1 | 02/08/2022 | 21/08/2022 | 19 |
| - | Entregable 1.2 | 22/08/2022 | 29/08/2022 | 7 |
| - | Entregable 1.3 | 30/08/2022 | 05/09/2022 | 6 |
| - | Entregable 1.4 | 06/09/2022 | 11/09/2022 | 5 |
| - | Entregable 1.5 | 12/09/2022 | 19/09/2022 | 7 |
| - | Entregable 1 | 20/09/2022 | 23/09/2022 | 3 |
| - | Entregable 2.1 | 24/09/2022 | 03/10/2022 | 9 |
| - | Entregable 2 | 17/10/2022 | 21/10/2022 | 4 |
| - | Entregable 3 | 22/10/2022 | 07/11/2022 | 16 |
| - | Entregable 4 | 08/11/2022 | 21/11/2022 | 13 |

| EDT | Nombre de la tarea | Fecha de inicio | Fecha de fin | Tiempo en días |
|---|---|---|---|---|
| 1.2. | Reuniones con el asesor de tesis (semanalmente) | 02/08/2022 – 14/11/2022<br>20/03/2023 – 15/07/2023 | | 31 |
| 1.3. | Reuniones con los especialistas | 20/03/2023 | 15/07/2023 | 16 |
| 1.4. | Composición del documento de tesis | 02/08/2022 | 15/07/2023 | 347 |
| 2. | Gestión del producto | 20/01/2023 | 15/07/2023 | 172 |
| 2.1. | Obligaciones de cumplimiento de las entidades bancarias | 20/01/2023 | 30/03/2023 | 69 |
| 2.1.1. | Identificar las obligaciones de cumplimiento en ciberseguridad | 20/01/2023 | 10/02/2023 | 21 |
| 2.1.2. | Identificar las obligaciones de cumplimiento en privacidad de datos | 11/03/2023 | 31/03/2023 | 20 |
| 2.2. | Identificar las vulnerabilidades y amenazas | 01/04/2023 | 29/05/2023 | 58 |
| 2.2.1. | Catalogar las vulnerabilidades de las obligaciones identificadas | 01/04/2023 | 15/05/2023 | 44 |
| 2.2.2. | Catalogar las amenazas de las obligaciones identificadas | 16/05/2023 | 29/05/2023 | 14 |
| 2.3. | Identificar riesgos | 30/05/2023 | 19/06/2023 | 20 |
| 2.3.1. | Catalogar los riesgos de ciberseguridad y privacidad de datos | 30/05/2023 | 19/06/2023 | 20 |
| 2.4. | Diseñar controles para los riesgos | 20/06/2023 | 15/07/2023 | 25 |
| 2.4.1. | Diseñar los controles en ciberseguridad y privacidad de datos en el proceso de cumplimiento | 20/06/2023 | 15/07/2023 | 25 |

*Nota.* El EDT sigue el formato de la Figura 9.

Adicionalmente, en la universidad se desarrolló un cronograma para la presentación de avances de los entregables por semana de actividades, la lista de tareas se puede visualizar en el Anexo C.

**Lista de recursos.**

***Personas involucradas y necesidades de capacitación.***

- Tesista: Edinson Ramiro Tavara Davila
- Asesor: Fernando M. Huamán Monzón
- Especialista: Experto en seguridad de la información o privacidad de datos.

- Necesidad de capacitación: Las actividades a realizar en el proyecto de fin de carrera están dentro del ámbito de la carrera de ingeniería informática y las prácticas preprofesionales.

***Materiales requeridos para el proyecto.***

- Electricidad
- Servicio de internet
- Plan de datos

***Estándares utilizados en el proyecto.***

- ISO 37301 cláusula 4.5
- NIST CSF
- NIST SP 800-37 Rev. 2

***Equipamiento requerido.***

- Una computadora personal

***Herramientas requeridas.***

- Microsoft Office Suite

**Costeo del proyecto.**

En esta sección se presenta el coste parcial y total del proyecto mediante la descomposición de los recursos a ser utilizados para el horizonte del proyecto.

Tabla 32 Anexo A

*Costeo del Proyecto*

| Ítem | Descripción | Unidad | Cantidad | Valor unidad (S/.) | Monto Parcial (S/.) | Monto Total (S/.) |
|---|---|---|---|---|---|---|
| 0. | Costo total del proyecto | - | - | - | - | 12600 |

| Ítem | Descripción | Unidad | Cantidad | Valor unidad (S/.) | Monto Parcial (S/.) | Monto Total (S/.) |
|---|---|---|---|---|---|---|
| 1. | Estudiantes o tesistas | - | - | - | - | 5240 |
| 1.1. | Edinson Ramiro Távara Dávila | Hora | 262 | 20 | | - |
| 2. | Otros participantes | - | - | - | - | 2800 |
| 2.1. | Mg. Fernando M. Huamán Monzón | Hora | 22 | 100 | 2200 | - |
| 2.2. | Especialistas en seguridad de la información o privacidad de datos | Hora | 6 | 100 | 600 | - |
| 3. | Materiales e insumos | - | - | - | - | 1260 |
| 3.1. | Electricidad | Mes | 9 | 25 | 225 | - |
| 3.2. | Servicio de internet | Mes | 9 | 100 | 900 | - |
| 3.3. | Plan de datos | Mes | 9 | 15 | 135 | - |
| 4. | Equipamiento requerido | - | - | - | - | 3300 |
| 4.1. | Computadora personal | Unidad | 1 | 3000 | 3000 | - |
| 4.2. | Microsoft Office Suite | Anual | 1 | 300 | 300 | - |

## Anexo B: Información Relacionada a la Revisión Sistemática

1. Cadenas de búsqueda usadas en la revisión sistemática

En esta sección en la Tabla 33 Anexo B se presenta para cada una de las cadenas de búsqueda usadas en las bases de datos la cantidad de resultados encontrados y de estudios seleccionados.

Tabla 33 Anexo B

*Resultado de las cadenas de búsqueda*

| **Base de datos** | **Cadenas de búsqueda usadas** | **Cantidad de resultados** | **Cantidad seleccionado** |
|---|---|---|---|
| Scopus | (("cyber security" OR cybersecurity) OR ("data privacy" OR "data protection")) AND (risks OR vulnerabilities OR threats) AND (compliance OR compliant) AND (banking OR "financial" OR bank) | 65 | 6 |
| IEEE Explorer | (("cyber security" OR cybersecurity) OR ("data privacy" OR "data protection")) AND (risks OR vulnerabilities OR threats) AND (compliance OR compliant) AND (banking OR "financial" OR bank) | 20 | 9 |
| ACM | (("cyber security" OR cybersecurity) OR "data privacy") AND (risks OR vulnerabilities OR threats) AND compliance AND (banking OR "financial sector" OR bank) | 75 | 6 |

*Nota.* Esta tabla muestra los resultados cuantitativos del uso de cada cadena de búsqueda en la base de datos correspondiente.

2. Cadenas de búsquedas con los criterios de inclusión usados en las bases de datos

Para la base de datos Scopus se usó la siguiente cadena de búsqueda: “TITLE-ABS-KEY ( ( ( "cyber security" OR cybersecurity ) OR ( "data privacy" OR "data protection" ) ) AND ( risks OR vulnerabilities OR threats ) AND ( compliance OR compliant ) AND ( banking OR "financial" OR bank ) ) AND ( LIMIT-TO ( DOCTYPE , "ar" ) OR LIMIT-TO ( DOCTYPE , "cp" ) ) AND ( LIMIT-TO ( PUBYEAR , 2022 ) OR LIMIT-TO ( PUBYEAR , 2021 ) OR LIMIT-TO ( PUBYEAR , 2020 ) OR LIMIT-TO ( PUBYEAR ,

2019 ) OR LIMIT-TO ( PUBYEAR , 2018 ) OR LIMIT-TO ( PUBYEAR , 2017 ) OR LIMIT-TO ( PUBYEAR , 2016 ) OR LIMIT-TO ( PUBYEAR , 2015 ) OR LIMIT-TO ( PUBYEAR , 2014 ) OR LIMIT-TO ( PUBYEAR , 2013 ) ) AND ( LIMIT-TO ( LANGUAGE , "English" ) )".

Para la base de datos ACM Digital Library se usó la siguiente cadena de búsqueda: "[[All: "cyber security"] OR [All: cybersecurity] OR [All: "data privacy"]] AND [[All: risks] OR [All: vulnerabilities] OR [All: threats]] AND [All: compliance] AND [[All: banking] OR [All: "financial sector"] OR [All: bank]] AND [Publication Date: (01/01/2012 TO 12/31/2022)]".

Para la base de datos IEEE Explorer se usó la siguiente cadena de búsqueda: "(("cyber security" OR cybersecurity) OR ("data privacy" OR "data protection")) AND (risks OR vulnerabilities OR threats) AND (compliance OR compliant) AND (banking OR "financial" OR bank)". Con los filtros de años desde el 2013 hasta el 2022.

3. Artículos seleccionados en la revisión sistemática

En esta sección en la Tabla 34 Anexo B se detallan los artículos seleccionados en la revisión sistemática catalogados por un ID en cada uno de los estudios.

Tabla 34 Anexo B

*Artículos seleccionados en la revisión sistemática*

| ID del estudio | Referencia APA del estudio |
|---|---|
| E1 | Scott, B. F. (2021). Red teaming financial crime risks in the banking sector. Journal of Financial Crime, 28(1), 98-111. https://doi.org/10.1108/JFC-06-2020-0118 |
| E2 | Tan, V., Cheh, C., & Chen, B. (2021). From Application Security Verification Standard (ASVS) to Regulation Compliance: A Case Study in Financial Services Sector. Proceedings - 2021 IEEE International Symposium on Software Reliability Engineering Workshops, ISSREW 2021, 69-76. https://doi.org/10.1109/ISSREW53611.2021.00046 |
| E3 | Wodo, W., Stygar, D., & Błaśkiewicz, P. (2021). Security issues of electronic and mobile banking. Proceedings of the 18th International Conference on Security and |

| ID del estudio | Referencia APA del estudio |
|---|---|
| | Cryptography, SECRYPT 2021, 631-638. https://doi.org/10.5220/0010466606310638 |
| E4 | Zetzsche, D. A., Anker-Sørensen, L., Passador, M. L., & Wehrli, A. (2022). DLT-based enhancement of cross-border payment efficiency – a legal and regulatory perspective. Law and Financial Markets Review, 15(1-2), 1-46. https://doi.org/10.1080/17521440.2022.2065809 |
| E5 | Al-Alawi, A. I., & Al-Bassam, S. A. (2019). Assessing the factors of cybersecurity awareness in the banking sector. Arab Gulf Journal of Scientific Research, 37(4), 17-32. |
| E6 | Becker, M., & Buchkremer, R. (2019). A practical process mining approach for compliance management. Journal of Financial Regulation and Compliance, 27(4), 464-478. https://doi.org/10.1108/JFRC-12-2018-0163 |
| E7 | Pocher, N., & Veneris, A. (2022). Privacy and Transparency in CBDCs: A Regulation-by-Design AML/CFT Scheme. IEEE Transactions on Network and Service Management, 19(2), 1776-1788. https://doi.org/10.1109/TNSM.2021.3136984 |
| E8 | Kruglova, I. A., & Dolbezhkin, V. A. (2019). Objective Barriers to the Implementation of Blockchain Technology in the Financial Sector. Proceedings - 2018 International Conference on Artificial Intelligence: Applications and Innovations, IC-AIAI 2018, 47-50. https://doi.org/10.1109/IC-AIAI.2018.8674451 |
| E9 | Lakshmi, K. K., Gupta, H., & Ranjan, J. (2020). Analysis of General Data Protection Regulation Compliance Requirements and Mobile Banking Application Security Challenges. ICRITO 2020 - IEEE 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions), 1028-1032. https://doi.org/10.1109/ICRITO48877.2020.9197954 |
| E10 | Alsalamah, A. (2017). Security risk management in online system. En A. Alsalamah (Ed.), Proceedings - 2017 5th International Conference on Applied Computing and Information Technology, 2017 4th International Conference on Computational Science/Intelligence and Applied Informatics and 2017 1st International Conference on Big Data, Cloud Compu (pp. 119-124). IEEE. https://doi.org/10.1109/ACIT-CSII-BCD.2017.59 |
| E11 | Mahalle, A., Yong, J., Tao, X., & Shen, J. (2018). Data Privacy and System Security for Banking and Financial Services Industry based on Cloud Computing Infrastructure. Proceedings of the 2018 IEEE 22nd International Conference on Computer Supported Cooperative Work in Design, CSCWD 2018, 75-80. https://doi.org/10.1109/CSCWD.2018.8465318 |
| E12 | Malinka, K., Hujnak, O., Hanacek, P., & Hellebrandt, L. (2022). E-Banking Security Study-10 Years Later. IEEE Access, 10, 16681-16699. https://doi.org/10.1109/ACCESS.2022.3149475 |
| E13 | Addae, J. A., Simpson, G., & Ampong, G. O. A. (2019). Factors influencing information security policy compliance behavior. Proceedings - 2019 International Conference on Cyber Security and Internet of Things, ICSIoT 2019, 43-47. https://doi.org/10.1109/ICSIoT47925.2019.00015 |

| ID del estudio | Referencia APA del estudio |
|---|---|
| E14 | Ashiku, L., & Dagli, C. (2019). Cybersecurity as a centralized directed system of systems using SoS explorer as a tool. 2019 14th Annual Conference System of Systems Engineering, SoSE 2019, 140-145. https://doi.org/10.1109/SYSOSE.2019.8753872 |
| E15 | Teodoro, N., Gonçalves, L., & Serrão, C. (2015). NIST cybersecurity framework compliance: A generic model for dynamic assessment and predictive requirements. Proceedings - 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2015, 1, 418-425. https://doi.org/10.1109/Trustcom.2015.402 |
| E16 | Conrad, S. S. (2019). Protecting Personal Information and Data Privacy: What Students Need to Know. J. Comput. Sci. Coll., 35(3), 77–86. https://doi.org/10.5555/3381569.3381580 |
| E17 | Kulik, T., Dongol, B., Larsen, P. G., Macedo, H. D., Schneider, S., Tran-Jørgensen, P. W. V., & Woodcock, J. (2022). A Survey of Practical Formal Methods for Security. Formal Aspects of Computing, 34(1), 39. https://doi.org/10.1145/3522582 |
| E18 | Harley, K., & Cooper, R. (2021). Information Integrity: AreWe There Yet. En ACM Computing Surveys (Vol. 54, Número 2). ACM PUB27 New York, NY, USA. https://doi.org/10.1145/3436817 |
| E19 | Al Batayneh, A. A., Qasaimeh, M., & Al-Qassas, R. S. (2021). A Scoring System for Information Security Governance Framework Using Deep Learning Algorithms: A Case Study on the Banking Sector. Journal of Data and Information Quality, 13(2), 9. https://doi.org/10.1145/3418172 |
| E20 | Akanfe, O., Valecha, R., & Rao, H. R. (2021). Design of an Inclusive Financial Privacy Index (INF-PIE): A Financial Privacy and Digital Financial Inclusion Perspective. ACM Transactions on Management Information Systems, 12(1). https://doi.org/10.1145/3403949 |
| E21 | Jhaveri, M. H., Cetin, O., Gañán, C., Moore, T., & Van Eeten, M. (2017). Abuse reporting and the fight against cybercrime. ACM Computing Surveys, 49(4). https://doi.org/10.1145/3003147 |

*Nota.* Esta tabla muestra los artículos seleccionados en la revisión sistemática de la literatura mediante un identificador. Así como, el formato APA con la descripción del artículo.

4. Archivo de formulario de extracción

Véase el archivo "20161438_EdinsonTávara_FernandoHuamán_EP AnexoB3_Formulario_extracción.xlsx" mediante el siguiente enlace: https://docs.google.com/spreadsheets/d/1HcXzR0FSfPd4hKVZ1hJZHvi6KGjnWpox/edit?usp=sharing&ouid=111417509798076541550&rtpof=true&sd=true

**Anexo C: Cronograma de actividades en la universidad**

Véase el siguiente enlace: https://docs.google.com/spreadsheets/d/1KDK4w58o6dfRLaAtWytpUZpFUG0ipmEl/edit?usp=drive_link&ouid=111417509798076541550&rtpof=true&sd=true

**Anexo D: Obligaciones de cumplimiento en ciberseguridad y privacidad de datos para las entidades bancarias en el Perú**

1. Secciones del diagrama de flujo

En esta sección, se proporciona una exposición detallada de cada uno de los elementos que componen el diagrama de flujo.

Tabla 35 Anexo D. Detalle del diagrama de identificación de las obligaciones

*Detalle del diagrama de identificación de las obligaciones de cumplimiento*

| **Símbolo** | **Nombre asignado** | **Explicación de su contenido** |
|---|---|---|
| Proceso | Inicio | Este es el punto de partida del proceso. Aquí comienza el flujo de trabajo para identificar y gestionar las obligaciones de cumplimiento de las entidades bancarias entre todos los documentos. |
| Proceso | Identificar los documentos que contengan obligaciones de cumplimiento | En este punto se busca y localiza todos los documentos que contengan información sobre obligaciones de cumplimiento. Esto podría incluir regulaciones, leyes o guías complementarias que refleje los requisitos legales de las entidades bancarias. |
| Proceso | Revisar cada documento de obligaciones de cumplimiento | Una vez identificados los documentos, se procede a revisar detalladamente cada uno de ellos para identificar todo el contenido entre las diversas obligaciones de cumplimiento que contienen. |
| Decisión | ¿El documento contiene obligaciones de cumplimiento relacionadas a entidades bancarias? | En esta fase, se clasifica el nivel de relevancia de los documentos y su contenido con las obligaciones de cumplimiento en relación con las entidades bancarias por cada documento. Puede ser “Totalmente” si existen obligaciones de cumplimiento que se consideran relevantes para las entidades bancarias y serán catalogadas. Se considera “Parcialmente” si solo contiene algunas obligaciones relacionadas o nuevas pero que se consideran útiles para las entidades bancarias para lograr el cumplimiento en sus requisitos legales. Por último, se considera "Ninguna" si no hay |

| Símbolo | Nombre asignado | Explicación de su contenido |
|---|---|---|
| | | obligaciones específicas para entidades bancarias que finalmente no serán catalogadas. |
| Proceso | No consolidar el documento de obligaciones de cumplimiento | Si un documento identificado no requiere ser combinado con otros, significa que las obligaciones encontradas en él no necesitan ser agrupadas con las de otros documentos similares. |
| Proceso | Consolidar el documento de obligaciones de cumplimiento con comentarios adicionales del análisis | En caso de que el documento contenga obligaciones relevantes más no necesariamente adicionales para las entidades bancarias. Estos documentos se consolidan con los otros que también tengan obligaciones por analizar en profundidad, y se agregan comentarios adicionales con las razones del análisis realizado. |
| Proceso | Catalogar detalladamente el documento que contiene las obligaciones de cumplimiento | Se lleva a cabo una clasificación exhaustiva y detallada del contenido a clasificar del documento que contiene las obligaciones de cumplimiento. Esto puede incluir algunas etiquetas sobe si contenido está enfocado en privacidad de datos o ciberseguridad, e información relevante para su posterior identificación, búsqueda y gestión. |
| Decisión | ¿Existen documentos de obligaciones por analizar? | Aquí se verifica si hay más documentos que deben ser analizados para identificar nuevas obligaciones de cumplimiento. |
| Proceso | Analizar el contenido de los documentos que presentan obligaciones de cumplimiento | Si se identificaron documentos que contienen obligaciones de cumplimiento por analizar se seleccionan para su revisión. Sobre cada uno se analiza para identificar las obligaciones de cumplimiento presentes. Generalmente al identificar las obligaciones de cumplimiento estas suelen variar en cantidad y extensión, pero toda obligación de cumplimiento debe ser catalogada de alguna forma antes de poder ser analizada. |
| Decisión | ¿La obligación de cumplimiento es usada por una entidad bancaria? | Se analiza en profundidad la implicancia de la obligación de cumplimiento para conocer si aplica para una entidad bancaria. Para el presente trabajo de fin de carrera la obligación de cumplimento usada por las entidades bancarias se categoriza como obligación primaria, y las no usadas por las entidades bancarias se representan bajo ciertos criterios secundarios. |
| Proceso | Catalogar la obligación de cumplimiento con un código | Si la obligación de cumplimiento es relevante para las entidades bancarias, se asigna como obligación primaria bajo un código o etiqueta específica para poder identificarla posteriormente de forma ordenada. |
| Proceso | No se cataloga la obligación de cumplimiento y se presentan comentarios adicionales | Si la obligación de cumplimiento no es relevante para las entidades bancarias, se realizan comentarios adicionales para explicar su situación. |

| Símbolo | Nombre asignado | Explicación de su contenido |
|---|---|---|
| Decisión | ¿Existen obligaciones de cumplimiento por analizar? | En esta etapa, se verifica si aún quedan obligaciones de cumplimiento por analizar en los documentos restantes. |
| Proceso | Unificar las obligaciones de cumplimiento catalogadas a ser usadas | Una vez catalogadas las obligaciones de cumplimiento se procede a unificar todas las obligaciones de cumplimiento. Este proceso adiciona la información relevante de la obligación de cumplimiento para su posterior identificación, búsqueda y gestión. |
| Proceso | Fin | Finaliza el proceso de identificación y gestión de obligaciones de cumplimiento. |

*Nota*. Elaboración propia.

2. Resultados alcanzados

En esta sección se presenta el documento de los resultados alcanzados del primer objetivo del proyecto de fin de carrera con las obligaciones de cumplimiento en ciberseguridad y privacidad de datos para las entidades bancarias en el Perú. Véase el siguiente enlace: docs.google.com/spreadsheets/d/1TSq3jqHJ681qBZSFOnY5TvYUNxJl5rsh9sWds7-pV2g

3. Acta de validación

En esta sección, se presenta el acta de validación del resultado, la cual ha sido evaluada y validada por un especialista en seguridad de la información o privacidad de datos. Véase el siguiente enlace: https://drive.google.com/file/d/1cwflxcLFOGjsbLhDzADOpRu5B15xzdtY

**Anexo E: Vulnerabilidades inherentes y amenazas de ciberseguridad y privacidad de datos para las entidades bancarias**

1. Secciones del diagrama de flujo

En esta sección, se proporciona una exposición detallada de cada uno de los elementos que componen el diagrama de flujo.

Tabla 36 Anexo E

*Detalle del diagrama de identificación de vulnerabilidades y amenazas*

| Símbolo | Nombre asignado | Explicación de su contenido |
|---|---|---|
| Proceso | Inicio | Este es el punto de partida del proceso. Aquí comienza el flujo de trabajo para identificar y gestionar las |

| | | |
|---|---|---|
| | | obligaciones de cumplimiento para identificar las vulnerabilidades y amenazas de ciberseguridad y privacidad de datos para las entidades bancarias. |
| Proceso | Identificar las obligaciones de cumplimiento | Se buscan y localizan todas las obligaciones de cumplimiento presentes en los documentos o fuentes relevantes.<br>Este proceso representa la actividad realizada en el Anexo D sección 1. |
| Proceso | Analizar una de las obligaciones de cumplimiento | Se selecciona una de las obligaciones de cumplimiento identificadas para llevar a cabo un análisis más detallado sobre la misma. |
| Proceso | Se analiza la información contenida en la obligación de cumplimiento | Se lleva a cabo un análisis exhaustivo de la información contenida en la obligación de cumplimiento seleccionada. El objetivo es poder identificar y describir situaciones presentes y que estén relacionadas sobre activos de información, vulnerabilidades, y amenazas propias de la entidad bancaria. |
| Proceso | Identificar, describir y catalogar por tipo los activos de información de lo analizado de la obligación de cumplimiento | Se identifican y describen los activos de información que están involucrados en el cumplimiento de la obligación seleccionada. Estos activos también pueden ser clasificados por tipo durante su categorización. |
| Proceso | Identificar, describir y catalogar por tipo las vulnerabilidades de lo analizado de la obligación de cumplimiento | En este punto se examina la obligación de cumplimiento seleccionada para identificar y describir las vulnerabilidades que podrían afectar su cumplimiento. Estas vulnerabilidades se clasifican por tipo. |
| Proceso | Identificar, describir y catalogar por tipo las amenazas de lo analizado de la obligación de cumplimiento | Se identifican y describen las amenazas potenciales que pueden afectar la adecuada implementación de la obligación de cumplimiento. Estas amenazas también se clasifican por tipo para su manejo adecuado. |
| Proceso | Consolidar el documento con los activos, vulnerabilidades y amenazas identificadas | Se unifica la información obtenida sobre activos de información, vulnerabilidades y amenazas en un solo documento para facilitar su gestión y seguimiento en el tiempo de uso. |
| Decisión | ¿Existen obligaciones de cumplimiento por analizar? | Se verifica si aún hay más obligaciones de cumplimiento por analizar. |
| Proceso | Revisión exhaustiva de documentos de la revisión sistemática para identificar | Una vez terminada de analizar las obligaciones de cumplimiento, se procede a analizar los activos de información para identificar vulnerabilidades y amenazas relacionadas. Esto último con el uso de los |

| | | |
|---|---|---|
| | vulnerabilidades y amenazas relacionadas a los activos de información | resultados obtenidos con los documentos de la revisión sistemática sobre los principales riesgos en ciberseguridad y privacidad de datos en las entidades bancarias que puedan surgir por las vulnerabilidades y amenazas relacionadas a los activos de información. Este proceso también permite actualizar la información sobre los activos de información, vulnerabilidades y amenazas identificadas previamente en la entidad bancaria. |
| Proceso | Fin | Finaliza el proceso de identificación de las vulnerabilidades y amenazas de ciberseguridad y privacidad de datos para las entidades bancarias. |

*Nota. Elaboración propia.*

2. Resultados alcanzados

En esta sección se presenta el documento de los resultados alcanzados del segundo objetivo del proyecto de fin de carrera con las vulnerabilidades inherentes y amenazas de ciberseguridad y privacidad de datos para las entidades bancarias. Véase el siguiente enlace: docs.google.com/spreadsheets/d/1SMfuz85KhFdsc2oOzW6I9kDmOvjloBHbK8Ty5GAcxnQ

3. Acta de validación

En esta sección se presenta el acta de validación del resultado validado por un especialista en seguridad de la información o privacidad de datos. Véase el siguiente enlace: https://drive.google.com/file/d/1cvJjtorICY1usSKnDtS44aFDacr3Jp8K

**Anexo F: Riesgos de ciberseguridad y privacidad de datos para las entidades bancarias**

1. Secciones del diagrama de flujo

En esta sección, se proporciona una exposición detallada de cada uno de los elementos que componen el diagrama de flujo.

Tabla 37 Anexo F

*Detalle del diagrama de identificación de riesgos*

| **Símbolo** | **Nombre asignado** | **Explicación de su contenido** |
|---|---|---|
| Proceso | Inicio | Este es el punto de partida del proceso. Aquí comienza el flujo de trabajo para identificar los riesgos de |

| Símbolo | Nombre asignado | Explicación de su contenido |
|---|---|---|
| | | ciberseguridad y privacidad de datos para las entidades bancarias. |
| Proceso | Identificar los activos de información, vulnerabilidad y amenazas relacionados a las obligaciones de cumplimiento | En esta etapa, se busca y localiza todos los activos de información que están relacionados con las obligaciones de cumplimiento. También se identifican las vulnerabilidades y amenazas que pueden afectar estos activos y, por ende, el cumplimiento de las obligaciones de cumplimiento.<br>Este proceso representa la actividad realizada en el Anexo E sección 1. |
| Proceso | Analizar uno de los activos de información | Se selecciona uno de los activos de información identificados para llevar a cabo un análisis más detallado sobre este activo. |
| Proceso | Seleccionar las vulnerabilidades y amenazas consideradas más relevantes del activo de información | Se identifican y seleccionan las vulnerabilidades y amenazas más relevantes y significativas que afectan al activo de información seleccionado. Para el presente trabajo se seleccionan las 5 principales vulnerabilidades y amenazas del activo de información consideradas y evaluadas por un especialista en seguridad bancaria. |
| Proceso | Identificar los riesgos con el uso de la vulnerabilidades y amenazas para el activo de información | Se analiza en conjunto las vulnerabilidades y amenazas seleccionadas que pueden dar lugar a riesgos para el activo de información y para el cumplimiento de las obligaciones asociadas. |
| Proceso | Evaluar el riesgo identificado del activo de información | Se evalúa la magnitud y el impacto de los riesgos identificados en el activo de información. Esto último implica realizar la valoración de la probabilidad de ocurrencia de los riesgos y el grado de impacto si se materializan. |
| Decisión | ¿Existen activos de información por analizar sus riesgos? | Se verifica si aún hay más activos de información que requieren del análisis de riesgos. |
| Proceso | Consolidar el documento de la matriz de riesgos | Si no hay más activos de información por analizar, se procede a consolidar la información obtenida en una matriz de riesgos que contenga los activos, las vulnerabilidades, las amenazas y los riesgos asociados a cada uno. |
| Proceso | Fin | Finaliza el proceso de análisis y gestión de riesgos de los activos de información relacionados con las obligaciones de cumplimiento. |

*Nota*. Elaboración propia.

2. Resultados alcanzados

En esta sección se presenta el documento de los resultados alcanzados del tercer objetivo del proyecto de fin de carrera con los riesgos de ciberseguridad y privacidad de datos para las entidades bancarias. Véase el siguiente enlace: https://docs.google.com/spreadsheets/d/1lDGhXuANZj6ASw8SB_s8kwUbPnw-OdjeaywX6eVDWyQ

3. Acta de validación

En esta sección se presenta el acta de validación del resultado validado por un especialista en seguridad de la información o privacidad de datos. Véase el siguiente enlace: https://drive.google.com/file/d/1cuinBsjwVRJFKyGkmTZu2XGIQasduhwy

**Anexo G: Controles en ciberseguridad y privacidad de datos como parte del proceso de cumplimiento de las entidades bancarias**

1. Secciones del diagrama de flujo

En esta sección se explica detalladamente cada una de las partes del diagrama de flujo.

Tabla 38 Anexo G Detalle de diagrama del diseño de controles de ciberseguridad y privacidad de datos

*Detalle de diagrama del diseño de controles de ciberseguridad y privacidad de datos*

| **Símbolo** | **Nombre asignado** | **Explicación de su contenido** |
|---|---|---|
| Proceso | Inicio | Este es el punto de partida del proceso. Aquí comienza el flujo de trabajo para identificar, agrupar y poder mitigar los riesgos asociados con los activos de información. |
| Proceso | Identificar los riesgos de los activos de información | Se identifican y evalúan los riesgos que afectan a los activos de información. Esto incluye los riesgos de ciberseguridad, riesgos de privacidad de datos, riesgos operativos, entre otros.<br>Este proceso representa la actividad realizada en el Anexo F sección 1. |
| Proceso | Agrupar los riesgos identificados con los activos de información relacionados | Los riesgos identificados se agrupan y relacionan con los activos de información correspondientes. Esto permite una mejor comprensión de los riesgos asociados con cada activo. Esto permitirá generar una idea general sobre el diseño del control a ser planteado para los riesgos asociados. |

| Símbolo | Nombre asignado | Explicación de su contenido |
|---|---|---|
| Proceso | Seleccionar un conjunto de riesgos a mitigar | Se selecciona un conjunto específico de riesgos que se abordarán y mitigarán durante el proceso. |
| Proceso | Diseñar un control base para mitigar los riesgos considerando los activos de información | Aquí se diseña un control o conjunto de controles de seguridad que ayudarán a mitigar los riesgos seleccionados. Estos controles se diseñan teniendo en cuenta los activos de información involucrados. |
| Proceso | Aplicar los marcos de trabajo NIST CSF y NIST SP 800-37 durante el diseño del control de seguridad | Se aplican como guía las recomendaciones planteadas en los marcos de trabajo NIST Cybersecurity Framework (CSF) y NIST Special Publication (SP) 800-37 para garantizar que los controles de seguridad sean adecuados y efectivos. |
| Proceso | Completar el diseño del control de seguridad con la revisión exhaustiva de los documentos de la revisión sistemática | Se completa el diseño del control de seguridad mediante una revisión exhaustiva de los documentos relacionados con la revisión sistemática. Esto garantiza que los controles estén en línea con los requisitos y las mejores prácticas en seguridad bancaria. |
| Decisión | ¿Existen riesgos de los activos de información por mitigar? | Se verifica si aún hay más riesgos de los activos de información que requieren ser mitigados. |
| Proceso | Consolidar el documento del diseño de controles de seguridad | Si no hay más riesgos por mitigar, se procede a consolidar la información obtenida en un documento que contenga el diseño de los controles de seguridad para cada riesgo. |
| Proceso | Crear el informe de diseño de controles de seguridad | Se realiza la creación de la guía con el informe detallado del diseño de los controles de seguridad y cómo se abordarán los riesgos de los activos de información. Para el presente trabajo se hace uso de un script que hace uso del documento del diseño de controles de seguridad para generar un informe del diseño. Este paso representa la información incluida en el capítulo 8. |
| Proceso | Fin | Finaliza el proceso de diseño y mitigación de controles de seguridad para los riesgos de los activos de información. Así como la guía para el análisis de riesgos planteada. |

*Nota*. Elaboración propia.

2. Resultados alcanzados

En esta sección se presenta el documento de los resultados alcanzados del cuarto objetivo del proyecto de fin de carrera con el diseño de los controles en ciberseguridad y

privacidad de datos como parte del proceso de cumplimiento de las entidades bancarias. Véase el siguiente enlace:

https://docs.google.com/spreadsheets/d/1Up_ImmL6hhOP-cWddFAjwvPi5I_vXZEq6eaPNwqWbHM

3. Acta de validación

En esta sección se presenta el acta de validación del resultado validado por dos especialistas en seguridad de la información o privacidad de datos. Véase el siguiente enlace: https://drive.google.com/drive/folders/12qJdYjINf3cCkiNk8qFxo_jq-HqKcfNA

**Anexo H: Guía para el análisis de riesgos sobre los controles diseñados**

1. Resultados alcanzados

En esta sección se presenta el documento de los resultados alcanzados para el quinto objetivo del proyecto de fin de carrera con el procedimiento realizado para generar el informe consolidado con los controles de seguridad de la guía para el análisis de riesgos, con la carpeta con el código fuente para generar la guía, la plantilla introductoria y la guía final. Véase el siguiente enlace:

drive.google.com/drive/folders/1-NDV7vLSdJsXhqGzJFWvzvuhIkpX6BK5

2. Acta de validación

En esta sección se presenta el acta de validación del resultado validado por dos especialistas en seguridad de la información o privacidad de datos. Véase el siguiente enlace:

https://drive.google.com/drive/folders/1zqGtLIagI7jl6e1kVGKvzTcv4ALbkh1M