PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

FACULTAD DE CIENCIAS E INGENIERÍA

DISEÑO DE UN MODELO PARA IDENTIFICAR AMENAZAS NO INTENCIONALES DE CIBERSEGURIDAD EN INSTITUCIONES PÚBLICAS GENERADAS POR PERSONAL INTERNO A PARTIR DE SU COMPORTAMIENTO SOBRE LA INFRAESTRUCTURA DE TI

Tesis para obtener el título profesional de Ingeniero Informático

AUTOR:

Anderson Jesús Castillo Lopez

ASESORES:

Dra. Mariuxi Alexandra Bruzza Moncayo
Dr. Manuel Francisco Tupia Anticona

Lima, julio del 2022

Resumen

En la actualidad, el uso de las tecnologías de la información y comunicación (TIC) en los sistemas públicos han tomado un rol cada vez más importante e imprescindible. Las necesidades por parte de los gobiernos para mejorar, transparentar y agilizar sus actividades y procesos nos han llevado a su uso sostenible y evolutivo en el tiempo.

Esta evolución ha permitido desarrollar sistemas más complejos con el fin de brindar un mejor servicio a los ciudadanos y organizaciones públicas. Sin embargo, debido a la sensibilidad de la información que se maneja en dichos sistemas, se han vuelto blanco de diversos tipos de ataques con el fin de afectar la confidencialidad, integridad y disponibilidad para propósitos desconocidos o de beneficios económicos.

Si bien la mayoría de los ataques de ciberseguridad provienen de agentes externos, existe agentes internos como los trabajadores que sin ninguna intención pueden abrir una puerta que permite que las organizaciones se vean vulnerables. Por esta razón el presente proyecto de tesis tiene como finalidad elaborar un modelo de identificación de amenazas no intencionales de ciberseguridad basado en el estándar de la familia de normas ISO 27000, marcos de referencia como COBIT 2019 y NIST v1.1.

Este modelo está conformado por una lista de componentes de los cuales se tiene los objetivos y métricas del modelo, una herramienta de análisis situacional, una lista de patrones de comportamiento, una matriz de gestión de riesgos y una guía aplicativa del modelo, los cuales forman parte de los objetivos del presente proyecto siendo el principal objetivo tener un modelo funcional.

Finalmente, se presentan las conclusiones como la implementación de los componentes junto con la verificación a través del juicio experto, así como también haber participado en la 4th International Conference on Information Technology & Systems 2021 en Ecuador (Castillo, Tupia, & Bruzza, 2021).

Tabla de Contenido

Capítulo 1. Generalidades

1.1 Problemática

Para poder definir la problemática, se ha identificado un vacío relacionado a la inexistencia de un modelo para identificar amenazas no intencionales de ciberseguridad por parte del personal interno en organización públicas en el estado peruano. Para resolver este vacío, para el presente proyecto de tesis se ha desarrollado un árbol de problemas y una breve descripción para validar el propósito del tema propuesto y de su problemática.

1.1.1 Árbol de Problemas

Para facilitar la realización de otros componentes importantes en el desarrollo del tema, como son los objetivos, es necesario primero identificar el problema central relacionando sus causas y efectos, lo que ayudará a sustentar el tema en mención, y efectuar un análisis completo y adecuado de la situación actual. En la Tabla 1 se muestra el árbol de problemas asociado a la problemática (Hernández-Hernández & Garnica-González, 2015).

Tabla 1: Árbol de problemas para el presente proyecto de fin de carrera

<table>
<tr><th colspan="2"></th><th>1</th><th>2</th><th>3</th></tr>
<tr><td rowspan="3">ÁRBOL DE PROBLEMAS</td><td>PROBLEMAS EFECTOS</td><td>Medición poco confiable del expertise del personal interno de las organizaciones públicas peruanas</td><td>Problemas en la continuidad del negocio ante las frecuentes amenazas no intencionales de ciberseguridad en las distintas áreas de las organizaciones públicas</td><td>Gestión poco fiable, parcial o nula de amenazas por parte de las instituciones públicas peruanas</td></tr>
<tr><td>PROBLEMA CENTRAL</td><td colspan="3">Inexistencia de un modelo para identificar amenazas no intencionales de ciberseguridad por parte del personal interno en organizaciones públicas peruanas basado en buenas prácticas internacionales</td></tr>
<tr><td>PROBLEMAS CAUSAS</td><td>No se han identificado patrones de comportamiento en el personal interno de las organizaciones públicas peruanas</td><td>No se ha propuesto un proceso de gestión de riesgos para las amenazas internas no intencionales en las organizaciones públicas peruanas.</td><td>No se ha propuesto el uso de buenas prácticas para gestionar las amenazas no intencionales de ciberseguridad ocasionadas por el personal interno según su comportamiento en infraestructura tecnológica en organizaciones públicas peruanas</td></tr>
</table>

1.1.2 Descripción

Gobierno electrónico es el uso de las tecnologías de la información y comunicación para ofrecer servicios a los ciudadanos, empresas y funcionarios mediante Internet (CEPAL, 2009). Estos servicios utilizan el Internet como medio para poder atender los requerimientos de la sociedad mediante la aprobación de políticas públicas. El Internet al ser un sistema de comunicación para la transferencia de paquetes de datos en distintas redes informáticas a través de protocolos (Metcalfe & Boggs, 1976), implica que se establezca políticas de seguridad para proteger la información que se está enviando y los servicios que se brinda si hablamos de un gobierno electrónico (Grönlund & Horan, 2005). Por lo tanto, para proteger la información que se envía a través de internet, es necesario hacer uso de la seguridad de la información (IS, por sus siglas en inglés) como concepto clave, ya que es la que se ocupa de la información independientemente del formato en la que se encuentre. Otro concepto importante, relacionado a la Seguridad de la información, es la Ciberseguridad, la cual involucra manejo de información digital sensible dentro de organizaciones públicas. Es necesario hacer énfasis en este concepto, el cual podría entenderse como un componente de la Seguridad de la Información (IS) (ISACA, 2015), ya que la información que se maneja es información digital que se transmite a través de sistemas interconectados en organizaciones.

La protección de la información ha sido una prioridad de las personas que tienen la necesidad de mantener información segura y privada (ISACA, 2015); sin embargo, con el avance de la tecnología, el objetivo de la protección de la información se ha visto en la necesidad de incluir dentro de sus objetivos la confidencialidad, disponibilidad e integridad de la información (CIA, por sus siglas en inglés) (ISACA, 2015). En un mundo digitalizado donde el Internet forma parte de las actividades diarias, servicios, organizaciones y gobiernos, la seguridad se vuelve una cualidad fundamental (Fundación Telefónica, 2016) que debe cuidarse y gestionarse constantemente. Cualidad que vela por información de carácter público, privado, laboral, publicitario, intelectual, informativo o de negocio de cada persona u organización. Esto debido a una relación entre el nivel de voluntad que tiene un usuario al momento de compartir información, dependiendo de su contenido, y otro usuario que tiene la intención de obtenerla a pesar de no tener permisos o accesos a dicha información con la finalidad de beneficiarse, siendo un usuario interno, externo o ex colaboradores de la organización (Fundación Telefónica, 2016). Estos tipos de usuario o entidades pueden afectar el funcionamiento normal de una organización. Estas intenciones pueden convertirse en posibles amenazas que perjudican a los usuario o entidades, las cuales

se dividen en amenazas internas y externas (Hunker & Probst, 2011). Estos ataques internos o externos pueden afectar la red privada (ordenadores de los trabajadores) y su infraestructura (servidores, redes, repositorios, etc.) (Fundación Telefónica, 2016). Dentro de las amenazas identificadas que pueden afectar a las organizaciones, se encuentra el robo de información, espionaje, el uso inadecuado de redes sociales por parte de colaboradores de la organización, ransomware (tipo de programa que prohíbe el acceso a la información propia a cambio de brindar un pago para liberar dicha información), amenazas persistentes avanzadas (APT) y factores humanos (Fundación Telefónica, 2016). Siendo este último, uno de los factores que mayor amenaza genera.

De acuerdo a un informe hecho por investigadores de seguridad de IBM en el 2018 (OSI, 2018), el 95 % de los ciberataques son debido a fallos humanos. Estos ataques en su mayoría pueden ser de un agente externo; sin embargo, la vulnerabilidad producto de un error humano empieza desde adentro de la institución (OSI, 2018), Este error se debe a un comportamiento inadecuado que genera una respuesta negativa por parte del personal. Este hecho se origina ante una falta de medidas impuesta por la institución o gobierno que gestiona la seguridad de la información en instituciones públicas. En un informe realizado por la compañía conocida como NortonLifeLock (anteriormente conocida como Symantec) en el 2018 (Symantec, 2018), reveló que el 54.6 % de correos que reciben los usuarios son spam, los cuales son correos que generan confianza en el usuario y tienen la finalidad de obtener información financiera o de otra índole. Este tipo de amenaza se conoce como phishing (OSI, 2018).

Uno de los sectores con mayor volumen de ataques e incidentes es el sector de Gobierno, de acuerdo a un reporte realizado por IBM en 2020 (IBM et al., 2020), el gobierno se encuentra en el sexto lugar como uno de los sectores más atacados por amenazas de ciberseguridad como se presenta en la Figura 1 entre los años 2018 y 2019 (IBM et al., 2020). El informe muestra que los gobiernos son un objetivo de alto valor para los agentes cibernéticos debido al dinero que manejan y principalmente información confidencial, no solo del gobierno sino de los ciudadanos (IBM et al., 2020).

Sector	2019 rank	2018 rank	Change
Financial Services	1	1	–
Retail	2	4	2
Transportation	3	2	-1
Media	4	6	2
Professional services	5	3	-2
Government	6	7	1
Education	7	9	2
Manufacturing	8	5	-3
Energy	9	10	1
Healthcare	10	8	-2

Figura 1: Top 10-targeted industries ranked by attack volume, 2019 vs. 2018 (Source: IBM X-Force)

Esta situación es preocupante debido a las consecuencias que genera tanto en pérdidas económicas como de información y credibilidad, si hablamos de gobierno. Un claro ejemplo fue el caso de un soldado de la marina americana, quien publicó un conjunto de documentos clasificados al medio público, ya que trabajó como analista de inteligencia (Chinyemba & Phiri, 2018). También se registran incidentes bancarios, como el caso de una administradora, quien robó más de $225,000.00 de una cuenta bancaria debido a problemas familiares de salud (Chinyemba & Phiri, 2018). Estos hechos prueban que, ante una inexistente aplicación de la ciberseguridad en las organizaciones, estas podrían salir perjudicadas de distintas maneras.

Para que una organización pública se vea lo menos afectada posible por estos acontecimientos y cumpla de manera eficaz su función en la sociedad, es necesario tomar medidas que puedan aplicarse, ya sea políticas de seguridad, estándares o modelos. Según estudios realizados por la INE, Instituto Nacional de Estadística de España, en un informe presentado por la Fundación Telefónica a nivel mundial en el 2015 (Fundación Telefónica, 2016), el 94.7 % de las empresas se preocupan por tener políticas de seguridad para evitar la destrucción de los datos que se utilizan en sus operaciones. El 85.5 % de las empresas con más de 250 empleados, utiliza políticas de seguridad para salvaguardar los datos confidenciales y las empresas de mayor tamaño realizan periódicamente revisiones de sus planes de seguridad ante nuevos hechos o peligros de seguridad (Fundación Telefónica, 2016).

Estas medidas por parte de las organizaciones van de la mano con los estudios e investigaciones que se han podido encontrar y que van avanzando en paralelo, de los

cuales se nombra algunas a continuación para entender el propósito del tema propuesto. Principalmente, algunas medidas o políticas de ciberseguridad se basan en normas como la ISO 27001 (Halim & Yusof, 2019), las cuales ya definen estándares que son validados a nivel internacional sobre seguridad. Algunos modelos, conocidos como el Marco para el Control de Acceso a Datos Digitales de Amenaza interna (PDDAITC, por sus siglas en inglés) (Halim & Yusof, 2019). Otras técnicas también utilizadas mediante algoritmos de predicción y detección de amenazas internas conocido como IDPA (por sus siglas en inglés) (Gheyas & Abdallah, 2016), también se emplean marcos de trabajo desarrollados por el NIST (Instituto Nacional de Estándares y Tecnología) basado en estándares internacionales (Lechner, 2017). BCW framework es otro marco de trabajo enfocado en la intervención del cambio de comportamiento, necesaria para poder identificar amenazas en base al comportamiento del personal interno (Alshaikh et al., 2019), OSN-LMC , un marco de trabajo que permite mitigar amenazas en base a funciones OSN, las cuales son actividades en las redes sociales en línea, por sus siglas en inglés, (Abdul Molok et al., 2018) y también se pueden utilizar métodos y procedimientos como entrevistas, encuestas, estadísticas que puedan de manera objetiva identificar amenazas difíciles de detectar. Estos estudios forman parte de investigaciones, algunos propuestos y otros se han diseñado para hacer frente a las amenazas en general que suelen presentarse en la información digital manejada en los diferentes servicios del gobierno electrónico.

Por consiguiente, a partir de toda la revisión sistemática del estado del arte, se ha podido demostrar la importancia de los modelos, medidas o técnicas para detectar amenazas de ciberseguridad en la administración pública. Sin embargo, pese a los modelos existentes y estudios sobre identificación de amenazas, el enfoque es más general y no está dirigido directamente al tema del proyecto, también se encontró que las medidas de mitigación pueden estar separadas o enfocadas de forma más general, razón por la que se identifica un vacío consistente en la inexistencia de modelos que identifiquen amenazas de ciberseguridad no intencionales por parte del personal interno en organizaciones públicas en el estado peruano debido a una escasa normativa legal (Gestión, 2019) y falta de iniciativas por parte del gobierno para promover el uso de controles y medidas a favor de la ciberseguridad en el Perú (GARCÍA, 2019), la cual involucra diversas amenazas y en especial la que se busca presentar en el tema propuesto (Gestión, 2019). Este vacío se debe a que existen problemas causa identificados en el árbol de problemas.

Los problemas causa involucrados contribuyen al problema central por la falta de medidas para resolverlos. El primer problema causa está dirigido a una falta de

identificación de patrones comportamiento, los mismo que reflejan un incremento de intentos de ciberataques en el Perú en los últimos meses con gran impacto en los empleados que ejercen teletrabajo (Gestión, 2020). El segundo y tercero problema causa, se han definido más que todo ante una ausencia en la preocupación por la Ciberseguridad en el Perú que, a pesar de tener algunas leyes, no es un tema principal, razón por la cual no existe un entendimiento claro de lo que comprende la Ciberseguridad (GARCÍA, 2019).

1.1.3 Problema seleccionado

Para resolver este vacío, es necesario identificar el problema central de lo propuesto anteriormente, para lo cual, debemos reconocer que las investigaciones y modelos revisados, propuestos en otros países, son un claro ejemplo de lo beneficioso que puede ser para el gobierno electrónico y las organizaciones en el Perú el desarrollo de un modelo que permita resolver los problemas causa involucrados, y así también que pueda ser validado y desarrollado en base al contexto peruano. Por lo tanto, según lo expuesto en la problemática, se ha considerado como problema central, la inexistencia de un modelo para identificar amenazas de ciberseguridad no intencionales por parte del personal interno en las organizaciones públicas peruanas.

1.2 Objetivos

Se establecen los objetivos con sustento base en el problema central y problemas causa.

1.2.1 Objetivo general

Diseñar un modelo para identificar amenazas no intencionales de ciberseguridad en instituciones públicas peruanas generadas por personal interno a partir de su comportamiento sobre la infraestructura de TI.

1.2.2 Objetivos específicos

- **O 1.** Asociar la lista de patrones comportamiento en el personal interno de las organizaciones públicas para las amenazas no intencionales de ciberseguridad.
- **O 2.** Definir los componentes del modelo a alto nivel que incluya los patrones de comportamiento y la matriz de gestión de riesgos para la Ciberseguridad.
- **O 3.** Diseñar los componentes del modelo basado en estándares para la seguridad de la información en el Perú en amenazas no intencionales de ciberseguridad.

O 4. Validar los componentes del modelo propuesto con un especialista de una institución pública relacionada a la gestión de amenazas no intencionales de Ciberseguridad.

1.2.3 Resultados esperados

O 1. Asociar la lista de patrones comportamiento en el personal interno de las organizaciones públicas para las amenazas no intencionales de ciberseguridad.

R 1. Lista de patrones de comportamiento en base a las actividades sobre la infraestructura de TI, que el personal interno realiza, y que se van a considerar para evaluar las amenazas.

O 2. Definir los componentes del modelo a alto nivel que incluya los patrones de comportamiento y la matriz de gestión de riesgos para la Ciberseguridad.
Modelo definido a nivel de componentes:

R 2. Análisis Situacional

R 3. Objetivos, métricas e indicadores

R 4. Patrones de comportamiento

R 5. Matriz de gestión de riesgos de Ciberseguridad

R 6. Guía de aplicación del modelo

O 3. Diseñar los componentes del modelo basado en estándares para la seguridad de la información en el Perú en amenazas no intencionales de Ciberseguridad.

R 7. Documentación detallada sobre los componentes del modelo

O 4. Validar los componentes del modelo propuesto con un especialista de una institución pública relacionada a la gestión de amenazas no intencionales de Ciberseguridad.

R 8. Protocolo para efectuar la validación.

R 9. Informe de los resultados de la validación del modelo.

1.2.4 Mapeo de objetivos, resultados y verificación

Objetivo 1: Asociar la lista de patrones comportamiento en el personal interno de las organizaciones públicas para las amenazas no intencionales de Ciberseguridad sobre la infraestructura de TI.			
Resultado	**Medio de verificación**	**Indicador objetivamente verificable**	**Herramientas**
R1. Lista de patrones de comportamiento en base a las actividades sobre la infraestructura de TI, que el personal interno realiza, y que se van a considerar para evaluar las amenazas	Matriz de trazabilidad en base a la revisión sistemática.	Consideración de 100% de los artículos científicos obtenidos en la revisión sistemática que incluyan aproximaciones a patrones de comportamiento, a manera de huella digital trazable, de empleados públicos sobre las infraestructuras de TI y que podrían resultar en amenazas a la ciberseguridad	Revisión Sistemática **1.** Factores contribuyentes de la UIT (CERT, 2013) **2.** Patrones de incidentes (CERT, 2013) **3.** Teoría de la red de actores (ANT) y Teoría del comportamiento planeado (TPB) (Mat Roni, 2015)
Objetivo 2: Definir los componentes del modelo a alto nivel que incluya los patrones de comportamiento y la matriz de gestión de riesgos para la Ciberseguridad.			
Resultado	**Medio de verificación**	**Indicador objetivamente verificable**	**Herramientas**
R2. Análisis Situacional **R3.** Objetivos, métricas e indicadores **R4.** Patrones de comportamiento **R5.** Matriz de gestión de riesgos de Ciberseguridad **R6.** Guía de aplicación del modelo	Informe con la hoja de ruta de creación de los componentes del modelo a alto nivel	Conformidad al 100% de dos especialistas	**1.** CERT insider threat components **2.** Comprehensive UIT Feature Model **3.** Norma ISO 27001, 27002, 27103 y 27032 **4.** COBIT® 2019 for Information Security **5.** NIST Cybersecurity Framework 1.1
Objetivo 3: Diseñar los componentes del modelo basado en estándares para la seguridad de la información en el Perú en amenazas no intencionales de Ciberseguridad.			
Resultado	**Medio de verificación**	**Indicador objetivamente verificable**	**Herramientas**
R7. Documentación detallada sobre los componentes del modelo	Informe con la documentación completa del modelo y la guía de aplicación	Conformidad al 100% de dos especialistas	Ver herramientas empleadas para alcanzar el objetivo 2
Objetivo 4: Validar los componentes del modelo propuesto con un especialista de una institución pública relacionada a la gestión de amenazas no intencionales de Ciberseguridad.			
Resultado	**Medio de verificación**	**Indicador objetivamente verificable**	**Herramientas**

R8. Protocolo para efectuar la validación.	**1.** Informe que contiene la verificación de los resultados de la aplicación del modelo realizado por el experto **2.** Acta de conformidad del experto sobre el modelo desarrollado	Conformidad al 100% de dos especialistas	Entrevistas con especialistas de entidades del estado
R9. Informe de los resultados de la validación del modelo.		Conformidad al 100% de dos especialistas	Entrevistas con especialistas de entidades del estado

1.3 Métodos y Procedimientos

Herramientas para utilizar por cada resultado esperado

R1: Lista de patrones de comportamiento en base a las actividades sobre la infraestructura de TI, que el personal interno realiza, y que se van a considerar para evaluar las amenazas	
Herramientas	**Descripción**
Factores contribuyentes de la UIT	Estos factores permiten identificar actividades o comportamientos por parte del personal y se encuentran divididos en los siguientes: **1. Factores Humanos/ Cognitivos** -Fatiga, Somnolencia, Carga de trabajo mental, Falta de situación de conciencia, etc. **2. Factores Psicosociales/Socioculturales** **-**Genero, Sentimientos, Cultura y subcultura, Influencia de drogas y hormonas, etc. **3. Factores Organizacionales** - Requerimientos de procesos de negocio
Patrones de Incidentes	Son patrones de incidencia principales ya que son los más recurrentes y están divididos de la siguiente manera: **1.UIT-HACK** - Son patrones que permiten la liberación de datos producto de la acción de malos actores. **2.DISC** - Son patrones que especifican una acción por parte de un colaborador interno que concluye en la pérdida de datos **3. PHYS y PORT** - Patrones relacionados al mal uso de dispositivos por parte de los colaboradores fuera o dentro de las instituciones que manejan información sensible
Teoría de la red de actores (ANT) y Teoría de comportamiento Planeado (TPB)	**1.ANT** -Esta teoría se guía por un principio que identifica como actor no solo los humanos sino a sus componentes técnicos que coexisten de forma paralela para así entender el origen del comportamiento interno **2.TPB** - Teoría con capacidad predictiva del comportamiento humano a un nivel individual

R2. Análisis Situacional, **R3.** Objetivos, métricas e indicadores **R4.** Patrones de comportamiento **R5.** Matriz de gestión de riesgos de Ciberseguridad **R6.** Guía de aplicación del modelo **R7.** Documentación detallada sobre los componentes del modelo	
Herramientas	**Descripción**
CERT insider threat components	Componentes del programa de amenazas del Equipo de respuesta ante emergencias informáticas (CERT, por sus siglas en inglés). Como parte de la construcción del modelo, se tomará en consideración algunos componentes para la fortaleza la mitigación de amenazas de acuerdo al contexto donde se aplicará el modelo.
Comprehensive UIT Feature Model	Modelo de características de amenazas internas no intencionales (UIT). El modelo captura incidentes de UIT de forma que pueda estructurar la incidencia de UIT en base a las causas, roles y otra información importante. El modelo clasifica 4 características obligatorias para cada incidente de UIT que son las siguientes: **1.** Roles **2.** Causas **3.** Modo de presentación de datos **4.** Industria
Normas ISO 27001, 27002 y 27032	**ISO 27001** Como parte del modelo, se hará uso de la norma ISO 27001 para la gestión de riesgo que contempla un modelo de identificación de amenazas. De acuerdo al estándar se tomará en cuenta las siguientes fases: **-**Análisis y evaluación de riesgos **-**Implementación de controles **-**Definir un plan de tratamiento de riesgos **-**Fijar el alcance del modelo **-**Proceso documental **ISO 27002** Proporciona buenas prácticas y controles para la seguridad de la información en base a 11 dominios de control de seguridad de la información. Como parte del modelo se toma en consideración algunos de los dominios que se muestran a continuación: -Políticas de seguridad -Organización de la seguridad de la información -Gestión de activos -Control de acceso -Seguridad de las operaciones -Gestión de incidentes que afectan la seguridad de la información **ISO 27032** Define una guía para la seguridad del ciberespacio, la cual cubre algunos aspectos adicionales que no se consideran en otras normas iso de seguridad y define un marco de ciberseguridad. Dentro de los dominios característicos de la ISO 27032, se considera los siguientes: -Seguridad de la Información -Seguridad de Redes -Seguridad de Internet

COBIT® 2019 for Information Security	Marco de trabajo que busca describir la seguridad en un contexto corporativos. El marco busca aumentar la necesidad de controlar los riesgos en niveles aceptables, cumplir los requisitos regulatorios y mantener siempre la disponibilidad de los sistemas y servicios
NIST Cybersecurity Framework 1.1	Marco que permite comprender, administrar y expresar riesgos de ciberseguridad para partes interesadas internas y externas. Se puede utilizar para la gestión de riesgos de ciberseguridad. El Framework posee 5 funciones principales que se presentan a continuación: **1.** Identificar **2.** Proteger **3.** Detectar **4.** Responder **5.** Recuperar Cada función mencionada comprende 3 elementos: Categorías, Subcategorías y Referencias informativas.

R8: Protocolo para efectuar la validación. **R9:** Informe de los resultados de la validación del modelo.	
Herramientas	**Descripción**
Entrevistas y envío del modelo a especialistas en Seguridad de la Información y Ciberseguridad de una institución pública	Se hará contacto con un especialista en Seguridad de la Información y Ciberseguridad de una institución pública para poder validar el modelo. El modelo no será aplicado en la institución, sino que el oficial de Seguridad de la Información verificará la confiabilidad del modelo para su futura utilidad.

Capítulo 2. Marco Legal/Regulatorio/Conceptual/otros

El presente capítulo tiene como objetivo sustentar teóricamente los conceptos relevantes que ayudan a contextualizar el diseño de un modelo para identificar amenazas no intencionales de ciberseguridad por parte del personal interno en organizaciones públicas, y poder así relacionarlos con la problemática expuesta. La misma problemática que hace referencia a la inexistencia de modelos que permitan identificar este tipo de amenazas en organizaciones públicas del estado peruano. Los conceptos que se presentan a continuación serán explicados detalladamente con ejemplos, en caso sea pertinente, para su mayor entendimiento relacionados con la realidad del país.

Marco Conceptual

2.1 Gobierno Electrónico

El término de gobierno electrónico o e-Government (e-Gov) por sus siglas en inglés, surge a fines de los 90; sin embargo, la historia de la computación en las organizaciones gubernamentales inicia en la década de los 70 (Kraemer, 1978). Los conceptos de gobierno electrónico se remontan al uso de las tecnologías de información dentro de los gobiernos, lo cual ha cambiado a lo largo de los años, donde su uso se enfoca más en los servicios al ciudadano (Grönlund & Horan, 2005). A pesar de que en un principio se buscaban soluciones computacionales, el término de gobierno electrónico ha ido evolucionando, ampliando fronteras y teniendo un enfoque mayor, relacionado con la toma de decisiones, valor y servicios (Grönlund & Horan, 2005). Ambas partes de lo que significa gobierno electrónico, ya sea con servicios y uso de tecnología dentro de los gobiernos como servicios hacia el ciudadano, van de la mano y evolucionan constantemente ante los nuevos retos y cambios de la tecnología (Grönlund & Horan, 2005). Dentro de las definiciones sobre gobierno electrónico, la E-government Act norteamericana de 2002 define el término como:

“El uso por del Gobierno de aplicaciones basadas en Internet y otras tecnologías de la información, combinado con el proceso que implementa estas tecnologías para desarrollar el acceso y envío de información gubernamental y servicios; o llevar a cabo mejoras en las operaciones gubernamentales." (U.S, 2002).

En síntesis, el gobierno electrónico se define como el uso de las tecnologías de información y comunicación junto con sus procesos involucrados para mejorar los servicios hacia los ciudadanos en la administración pública del estado. La evolución del

Gobierno Electrónico podría representarse a nivel cronológico como se muestra en la Figura 1 (CEPAL, 2009).

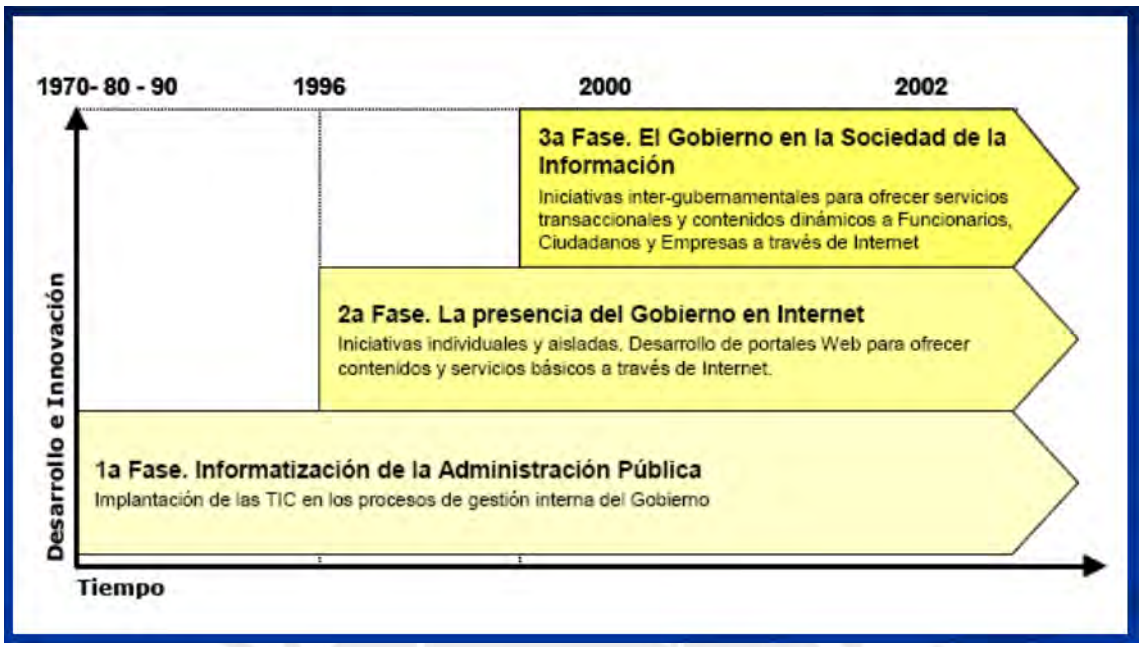


Figura 1: Gobierno Electrónico y Gestión Pública. Comisión Económica para América Latina y el Caribe (CEPAL) (2009)

Un claro ejemplo de Gobierno Electrónico es el que se está aplicando en la actualidad en el gobierno peruano, el cual sigue en proceso de evolución y mantiene un canal de comunicación con los ciudadanos y una entidad rectora de los sistemas nacionales de transformación digital y el uso correcto (https://www.gob.pe/). La aplicación de Gobierno Electrónico en el Perú empezó a inicios del 2000, donde implicó un proceso de reforma continuo, ya que en el Perú el desarrollo del Gobierno Electrónico a mediados del 2007 se aplicaba en contextos concretos y no de manera uniforme. El proceso de reforma se ve dividido en cuatro etapas, siendo la última etapa, definido como una etapa de Consolidación entre el 2005 al 2011, el inicio de políticas inclusivas y leyes que permiten buscar el acercamiento con la sociedad y sus servicios para beneficio de todos. Actualmente la Secretaría de Gobierno Digital (SEGDI), antes conocida como la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI), se encarga de promover, difundir y reconocer las buenas prácticas y la aplicación de Gobierno Electrónico en el Perú para beneficio de la sociedad (PCM. ONGEI., 2013). Este claro ejemplo se relaciona con el tema propuesto ya que los servicios de gobierno electrónico brindados por las instituciones del estado requieren de la aplicación de normas y estándares en la seguridad de la información.

2.1.1 Tipos de Gobierno Electrónico

Acorde con los estudios primarios, se ha podido identificar 8 tipos de interacciones que se han implementado en gobierno electrónico, los cuales brindan beneficios al gobierno, ciudadano, empresa, empleados, organizaciones sin fines de lucro, organizaciones sociales y políticas propuesto en (Fang, 2002); sin embargo, en la actualidad se manejan 4 tipos principales. Los ejemplos presentados por cada tipo han sido propuestos en (PCM. ONGEI., 2013)

- **De Gobierno a Gobierno (G2G)**
  Provee departamentos del gobierno para la cooperación y comunicación, las cuales permiten la conexión intergubernamental facilitando el intercambio de información a través de bases en línea para lograr mayor eficiencia y efectividad. Por ejemplo, el sistema Integrado de Administración Financiera (SIAF).
- **De Gobierno a Empresa (G2B)**
  Iniciativas por parte del gobierno de generar transacciones electrónicas y un mercado electrónico que faciliten los servicios y licitaciones con empresas. Por ejemplo, el portal del Sistema Electrónico de Adquisiciones y Compras del Estado (SEACE).
- **De Gobierno a Ciudadano (G2C)**
  Se puede definir como la facilidad de brindar servicios al ciudadano de manera online enfocados en la información pública del estado y comunicación. Por ejemplo, el Portal al Ciudadano y Empresa (PSCE).
- **De Gobierno a Empleado (B2E)**
  Se define como la prestación de servicios públicos al empleado que permitan capacitarlo en el uso de las tecnologías y comunicaciones. Por ejemplo, los cursos virtuales impartidos por la Escuela Nacional del Servicio Civil (SERVIR).

2.1.2 Tecnología de Información y Comunicaciones (TIC)

Acorde con la búsqueda de estudios primarios sobre las TIC, se puede definir según lo propuesto en (Servicios TIC, 2006):

"*Las Tecnologías de la Información y la Comunicación, también conocidas como TIC, son el conjunto de tecnologías desarrolladas para gestionar información y enviarla de un lugar a otro. Abarcan un abanico de soluciones muy amplio. Incluyen las tecnologías para almacenar información y recuperarla después, enviar y recibir información de un sitio a otro, o procesar información para poder calcular resultados y elaborar informes*"

Otros estudios sobre las TIC la definen de la siguiente manera:

"Las TIC son cambiantes, siguiendo el ritmo de los continuos avances científicos y en un marco de globalización económica y cultural, contribuyen a que los conocimientos sea efímeros y a la continua emergencia de nuevos valores, provocando cambios en nuestras estructuras económicas, sociales y culturales, e incidiendo en casi todos los aspectos de nuestra vida: el acceso al mercado de trabajo, la sanidad, la gestión burocrática, la gestión económica, el diseño industrial y artístico, el ocio, la comunicación, la información, nuestra forma de percibir la realidad y de pensar, la organización de las empresas e instituciones, sus métodos y actividades, la forma de comunicación interpersonal, la calidad de vida, la educación... Su gran impacto en todos los ámbitos de nuestra vida hace cada vez más difícil que podamos actuar eficientemente prescindiendo de ellas" (Salinas Ibáñez, 2004).

A manera de sintetizar la información presentada por los estudios primarios, se puede definir a las TIC como un conjunto de herramientas o tecnologías que van evolucionando en el transcurso del tiempo y forman canales de comunicación junto a las nuevas tecnologías para el desarrollo y avance de la sociedad. Considerando a nivel más tecnológicos, las TIC facilitan el procesamiento de grandes cantidades de datos, canales de comunicación, accesibilidad y desarrollo de capacidades humanas para adaptarse a los cambios. Los ejemplos de TIC pueden ser medios de almacenamiento y procesamiento como servidores, correos electrónicos, Smartphone, discos duros, videojuegos, servicios en la nube, etc. El uso de las TIC puede ser aplicado en distintas áreas como educación, comercio, medicina, gobierno electrónico, redes sociales, etc. Las TIC son la base del tema propuesto debido a que los incidentes o amenazas no intencionales dentro de las organizaciones ocurren dentro de ellas.

Si bien antes se realizó una breve definición del gobierno electrónico, es necesario mencionar que el gobierno electrónico necesita hacer uso de las TIC como medio para cumplir con los servicios y recursos brindados por parte del gobierno a los ciudadanos. Un ejemplo claro de esta relación se ve en el plan de acción realizado por la UE, en el año 2000 denominado “eEurope 2002”, en la cual se presentaron 3 objetivos principales que se muestran a continuación:

- Una Internet más rápida, barata y segura
- Invertir en las personas y en la formación
- Estimular el uso de Internet

Este caso es un claro ejemplo del uso de las TIC en el gobierno electrónico, ya que cada objetivo implica la creación de redes, sistemas y medidas que ayuden a cumplirlos a través del plan de acción (eEurope 2002, 2000).

2.2 Seguridad de la Información (SI)

Seguridad

Es un concepto proveniente del latín securitas. La seguridad se puede entender comúnmente como la reducción de riesgos o la confianza en una entidad, agente o recurso. Sin embargo, esta definición dependerá del campo o área asociada (Delgado, n.d.).

Información

Se define como los datos significativos, ya sea de una organización, persona o sistema (Delgado, n.d.).

Activos

Se define como cualquier recurso, servicio o producto que tiene un valor para la organización. Unos de los activos principales en las organizaciones son los activos de información. Estos activos de información pueden ser aplicaciones, sistemas, redes de comunicación, servicios de información, datos, etc.

Finalmente se puede definir a la Seguridad de la Información (SI) como un conjunto de medidas para prevenir o solucionar eventos que afecten la información de las organizaciones. Este conjunto de medidas busca proteger y resguardar la información en base a sus dimensiones de confidencialidad, integridad y disponibilidad conocido como CIA, por sus siglas en inglés (Delgado, n.d.).

1. **Confidencialidad**
   Es el acceso y el resguardo de la información
2. **Integridad**
   Se define como el mantenimiento y consistencia de la información
3. **Disponibilidad**
   Se define como su nombre lo indica, a la disponibilidad del uso de la información por parte personas que tienen accesos autorizados y están en la capacidad de usarlos

Como claro ejemplo se puede aplicar políticas de seguridad de información relacionada a los dispositivos móviles y el teletrabajo, ya que su uso inadecuado puede generar fuga de información por parte de los trabajadores sin conocimiento de ellos mismos. Esta fuga de información se puede dar a través de redes sociales, instalación de programas sin ser verificados o uso de correos personales. Si se tiene políticas de seguridad de la información de la mano con procedimientos y herramientas se puede prevenir los incidentes mencionados.

2.3 Ciberseguridad

Según ISACA, define la ciberseguridad como:

"Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados" (ISACA, 2015).

Es así como la ciberseguridad se puede entender como la protección de computadoras, ordenadores y todo lo relacionado al ciberespacio. Sin embargo, este concepto involucra más que la protección en sí. En la actualidad el mundo del internet está abarcando gran parte de las actividades humanas, no dejando brecha alguna con lo relacionado a actividades apartadas del Internet (Fundación Telefónica, 2016). Esto implica que la seguridad sea algo fundamental y que se busque tanto como la salud de la persona (Fundación Telefónica, 2016). Al involucrarse la seguridad dentro de las actividades que se realizan en Internet, implica siempre el cuidado de la información, actividad o tecnología que pueda ser usada por parte de las personas. Por lo tanto, la ciberseguridad, más que un concepto, toma protagonismo como un proceso que implica la prevención, detección y reacción como funciones principales dentro de un aprendizaje continuo del propio proceso (Fundación Telefónica, 2016). Acorde con lo propuesto se muestra en la Figura 2 (Fundación Telefónica, 2016) las etapas de la gestión de la ciberseguridad planteadas.

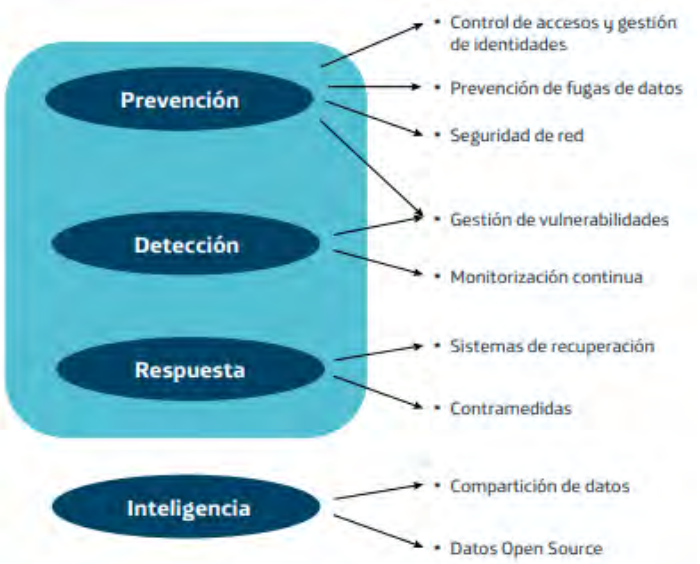


Figura 2: Etapas de Gestión de Ciberseguridad. Ciberseguridad, La protección de la información en un mundo digital. Fundación Telefónica (2016)

Cada etapa involucra ciertas actividades relacionadas a la seguridad de la información. Nuestro campo de investigación está relacionado a la etapa de detección como objetivo del tema propuesto.

2.3.1 Etapa de Detección

En el campo de la ciberseguridad, la etapa de detección es un proceso que puede identificar una incidencia en el momento que se produce o después de un tiempo de haber ocurrido el hecho. Existen herramientas que pueden detectar las incidencias en el momento que ocurren, ya sea antivirus, protocolos de seguridad, etc. Sin embargo, cuando estos no son detectados, los problemas pueden ser mayores e incluso nunca llegan a identificarse. En la actualidad existen, gracias a la ciberseguridad, patrones para identificar ataques o amenazas, el problema ocurre cuando estos patrones son desconocidos (Fundación Telefónica, 2016).

- **Vulnerabilidad**

  Las vulnerabilidades son consideradas puntos débiles dentro de un sistema de información, que involucra factores como el software, hardware e incluso los seres humanos. Estas vulnerabilidades pueden permitir que un agente interno o externo afecte la confidencialidad, integridad y disponibilidad de un sistema dentro de una organización (Microsoft, 2011). Ejemplo de vulnerabilidad pueden ser variados, depende del enfoque que se de en determinadas áreas si hablamos de organizaciones, a nivel de TI, se pueden encontrar fallos de diseño, errores

de configuración en la seguridad de información, falta de políticas de seguridad, errores en la programación, etc.

- **Gestión de Vulnerabilidades**

  Uno de los principales problemas en las organizaciones es que no se hace un análisis de vulnerabilidades cada cierto tiempo, sino que se realiza de manera anual o trimestral, esto puede generar que muchos incidentes no sean detectados y se pierda información sin poder ser identificados los actores. Es por eso que una gestión de vulnerabilidades es necesaria para un monitoreo continuo de riesgos y vulnerabilidades y se debe tener las responsabilidades claras para ser asignadas al personal adecuado. Es así como se muestra en la Figura 3, los tres pasos básicos propuestos en (Fundación Telefónica, 2016).

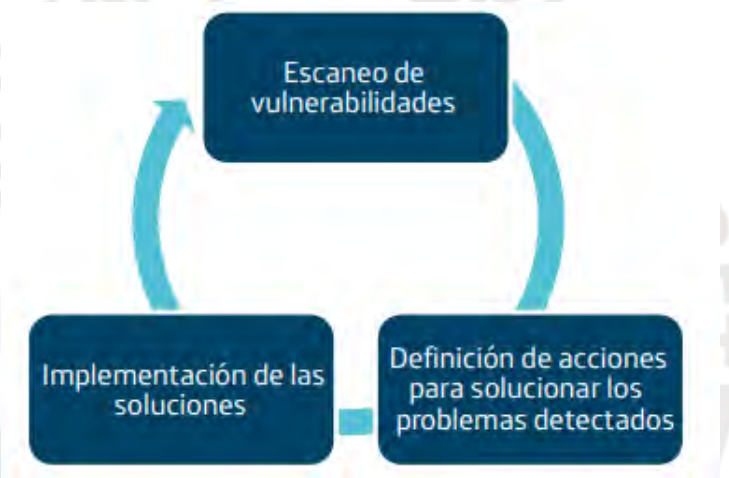


Figura 3: Pasos para afrontar la gestión de vulnerabilidades. Ciberseguridad, La protección de la información en un mundo digital. Fundación Telefónica (2016)

La gestión de vulnerabilidades en la etapa de Detección, es un concepto relacionado a la problemática debido a que una amenaza se origina al encontrarse vulnerabilidades dentro de una organización, por lo cual un ejemplo claro de la aplicación de esta etapa son las vulnerabilidades que se pueden encontrar en una organización en base a la problemática que se tiene, las cuales deben ser consideradas dentro de una gestión que forme parte de la solución del problema. Entre las vulnerabilidades más comunes, se puede encontrar falta de conocimiento de los procesos o actividades por parte del personal, fallas de seguridad, uso de cifrados y contraseñas débiles, mal uso de las tecnologías por parte del personal, falta de políticas de seguridad, etc.

2.3.2 Agentes Internos/Personal Interno

Los agentes internos son personas con acceso privilegiado que forman parte de la organización o fueron colaboradores de la organización con derechos de acceso a recursos sensibles de la organización y que pueden comprometer la información mediante actos con o sin intención. (Hunker & Probst, 2011)

2.3.3 Amenazas de Ciberseguridad

En la ciberseguridad, las amenazas son consideradas actos maliciosos que intentan acceder a la información, infraestructura o red de una organización con o sin la autorización del propietario. Este acceso puede provenir de otra organización, usuarios remotos con intenciones maliciosas o usuarios dentro de la misma organización. Las amenazas de ciberseguridad se dividen en dos, las amenazas internas y externas. Dentro de las amenazas internas se ubican las amenazas intencionales y no intencionales (Hunker & Probst, 2011). Un ejemplo aplicado a la definición de amenazas en general de ciberseguridad podría ser las acciones hechas por los denominados "Hackers", que buscan acceder a información de la organización para distintos propósitos que en su mayoría benefician al atacante. Los orígenes de las amenazas pueden ser muchos, como son la ingeniería social, botnets, códigos maliciosos, o amenazas persistentes avanzadas (APT).

2.3.3.1 Amenazas Internas Maliciosas

Las amenazas internas maliciosas, parten de un agente interno que tiene la intención y los privilegios para acceder a los recursos de la organización y afectar la confidencialidad, integridad y disponibilidad de la misma. Un agente interno se convierte en malicioso cuando abusa de sus privilegios y comete un crimen. Las amenazas internas maliciosas principales pueden ser divididas en sabotaje de TI, fraude y robo de propiedad intelectual (Wunderlich, 2011) (Silowash et al., 2012).

- **Sabotaje de TI**
  Es un tipo de amenaza, en donde una persona usa las TIC para dirigir un daño dentro de la organización, los medios que puede utilizar pueden ser mediante correos, redes sociales, blogs, chats, etc. De acuerdo con la teoría de comportamientos (TPB), este comportamiento puede ser motivado por una venganza por un mal reconocimiento por parte de la organización (Mat Roni, 2015) (Pitropakis, 2015). Un ejemplo de sabotaje puede darse en el ámbito de desarrollo ante un extrabajador, responsable de un software desarrollado que elimina el software a manera de venganza.
- **Fraude**
  Son incidentes en la cual el usuario usa las TIC para realizar modificación sin autorización para un beneficio propio, estos actos se generan cuando el personal

ve la oportunidad de realizarlo pensando que no será afectado ya que posee privilegios y conoce su campo de acción (Chak, 2015). Un ejemplo de fraude normalmente involucra pérdidas financieras, por lo cual puede existir el caso de un cajero de una entidad financiera que tiene acceso a las cuentas bancarias. El personal puede hacer transferencias bancarias ilegales a través de los privilegios que tiene.

- **Robo de propiedad intelectual (IP)**
  Un robo de propiedad intelectual se produce ante la intención de personal interno de la organización usa las TIC para robar la propiedad intelectual de un sistema, proyecto o recurso motivado por una ventaja de negocio (Chak, 2015). Un ejemplo de robo de propiedad intelectual normalmente ocurre con personal que es partícipe de nuevos proyectos o ideas tecnológicas que benefician a la organización, ante un hecho aislado, si el trabajador es despedido de la organización y tiene conocimiento y acceso de la información puede compartir la idea en otras organizaciones a manera de competitividad y generar pérdidas en la anterior organización, posiblemente por patentes o derechos de autor.

2.3.3.2 Amenazas Internas No Maliciosas (UIT)

Estas amenazas no intencionales, involucran al personal interno de la organización que involuntariamente, y posiblemente influenciados por actos maliciosos, puede cometer incidencias que generan daños en los recursos que incluso pueden ser más críticos que las amenazas maliciosas debido a que no se pueden identificar fácilmente (Hunker & Probst, 2011). Entre las posibles causas se encuentra la falta de entrenamiento, negligencia, o falta de conciencia (CERT, 2013). Un ejemplo común son los ataques “phishing” a través de correos electrónicos que, si bien son intencionales, la respuesta por parte del personal interno, por falta de conocimiento, puede permitir el acceso a este tipo de amenazas.

2.4 Riesgos

Una de las principales definiciones es la del Instituto de Gestión de Riesgo, que define al riesgo como:

“La combinación de la probabilidad de un evento y su consecuencia. Esa consecuencia puede variar de positivo a negativo” (Peddada, 2013).

En síntesis, se puede definir al riesgo como la probabilidad de ocurrencia de un posible peligro, y estos peligros están asociados al nivel de vulnerabilidad (Peddada, 2013). Un ejemplo de riesgo puede estar asociado a las vulnerabilidades de la organización en una respectiva área. Sea el caso de una mala configuración de seguridad, existe un riesgo dependiendo del nivel de vulnerabilidad presentado. Este nivel puede estar

implicado diversos factores, como el desconocimiento de la persona, la falta de tecnología para resolverlo, falta de controles de seguridad, etc.

Los riesgos pueden ser divididos en las siguientes categorías:

1. Riesgos de Negocio
2. Riesgos de Control/Incertidumbre
3. Riesgo de Oportunidad
4. Riesgos Personales

En la siguiente figura se muestra las categorías y subcategorías propuestas en (Peddada, 2013) para los riesgos.

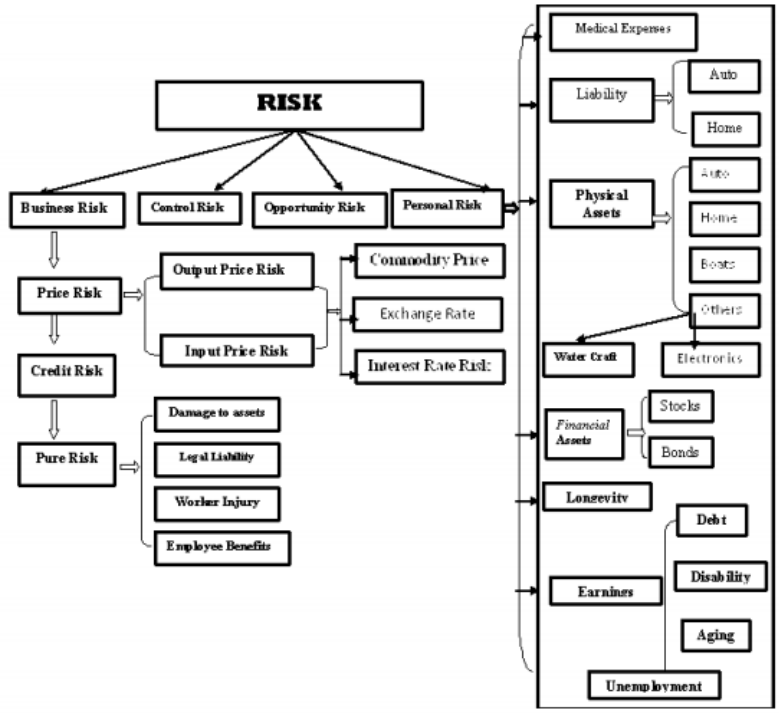


Figura 4: Categoría de Riesgos. Risk Assessment and Control (2013)

2.4.1 Control de Riesgos

El objetivo del control de riesgos es lo que busca obtener como resultado de medidas correctivas o preventivas ante riesgo que pueda impactar en las organizaciones. El control de riesgo es un método para gestionar los riesgos mediante políticas estructuras, procedimientos, etc. y se divide en los siguientes tipos propuestos en (Delgado, n.d.):

- **Control preventivo**

  Control que evita los riesgos antes de que ocurran. Un ejemplo relacionado al tema propuesto, son evaluaciones continuas del personal sin razón, para

obtener estadísticas de comportamiento y con eso tomar medidas preventivas (Delgado, n.d.).

- **Control de investigación**
  Control que busca identificar riesgos posibles en distintas áreas de una organización. Un ejemplo puede ser la implementación de un sistema de seguridad que monitorea a los trabajadores internos de una organización, control e investigación de los flujos de datos en la organización por el uso de la persona (Delgado, n.d.).

- **Control correctivo**
  Control que busca que eventos que ya ocurrieron, no vuelvan a pasar. Este tipo de control ya tiene prevenido los riesgos en base a experiencia propia, y busca que no vuelvan a repetirse. Un ejemplo podría ser la recepción de spam y links inseguros que pudieron causar pérdida de información, un control debería ser el uso de firewalls ante correos engañosos que tienen ciertos patrones en su estructura (Delgado, n.d.).

Un ejemplo de uso del control de riesgos relacionado a la problemática se da en un escenario real dentro de una organización que busca tener un control de las posibles vulnerabilidades que pueden permitir que una amenaza se lleve a cabo, el control de riesgo parte en identificar esas vulnerabilidades y el grado que ocurrencia de la amenaza relacionada a dicha vulnerabilidad. Una vez identificados los riesgos es necesario medirlos y saber cuál de estos puede ser mitigado y de qué manera se procederá a controlarlos. Por esa razón, es que el control de riesgos está relacionado a la problemática ya que representa una forma de medir el impacto que se tiene y permite que el tema propuesto tenga validez en su desarrollo.

2.4.2 Análisis de Impacto de Negocios (BIA)

Es una forma de calcular o estimar el estado de una organización debido a un desastre, incidente o peligro que ya ocurrió y en el cual se ve afectado. Este análisis permite estimar el impacto de operaciones o financiero (Miguel Ángel Mendoza, 2014).

El análisis permite hacer uso eficiente de los recursos antes la identificación de las áreas con mayor impacto ante un peligro o desastre.

Para esta eficiente redistribución de recurso, la BIA maneja los siguientes elementos:

- **Tiempo Objetivo de Recuperación (RTO, por sus siglas en inglés)**
  Es el periodo permitido para la recuperación de un proyecto o recurso de la organización ante un incidente o desastre.

- **Punto Objetivo de Recuperación (RPO, por sus siglas en inglés)**
  Es la limitante de la información que puede servir de respaldo ante algún desastre, que deja inhabilitado algunas operaciones y procesos.

Características del BIA

Según lo propuesto en (Miguel Ángel Mendoza, 2014), se tiene dos objetivos principales por parte del BIA. El primero es obtener una base para los procesos críticos de la organización. El segundo, una vez obtenida la base, es priorizar cada proceso de acuerdo con el impacto en la organización (Miguel Ángel Mendoza, 2014).

Ventajas del BIA

Permite tener un análisis que pueda identificar áreas críticas que necesitan tiempos críticos de operación y a su vez permite también la redistribución de recursos en la organización de acuerdo al impacto de negocio (Miguel Ángel Mendoza, 2014).

Este análisis puede ir de la mano con una evaluación de riesgos, ya que los riesgos están involucrados dentro de los procesos, los cuales pueden afectar el proceso en sí y por ende a la organización (Miguel Ángel Mendoza, 2014).

Un ejemplo de análisis de impacto de negocio está asociado a la aplicación del modelo en una organización, una vez que se haga uso de los patrones y se logre identificar las amenazas en la organización, se puede hacer un análisis de impacto de negocio, comenzando con la evaluación de riesgo y luego revisar si existió algún incidente en la organización. Esta información sería crucial para determinar el impacto que tuvo y la relación con las amenazas identificadas.

2.4.3 Gestión, Evaluación y Control de Riesgos

La evaluación de riesgos es la identificación de los riesgos y calificación de riesgos para saber el nivel de impacto en la organización. Ambos puntos forman parte de la evaluación de riesgos que pertenece a un proceso de gestión de riesgos. El proceso de gestión de riesgo involucra la identificación, análisis, evaluación y mitigación de los riesgos. Este proceso sigue lo sientes pasos para la evaluación de riesgos, ya que el proceso de gestión incluye las mitigaciones y medidas para controlar, resolver o mantener el riesgo (Peddada, 2013):

1. Identificación y medición de exposición a la pérdida
2. Control de pérdidas y financiación de riesgos
3. Evaluación de riesgos
4. Selección de técnicas para la gestión de riesgos

La siguiente Figura muestra una de posibles técnicas para la gestión de riesgos conocido como Matriz de Riesgo y Gestión de las 4T's de Hazard propuesto en (Peddada, 2013).

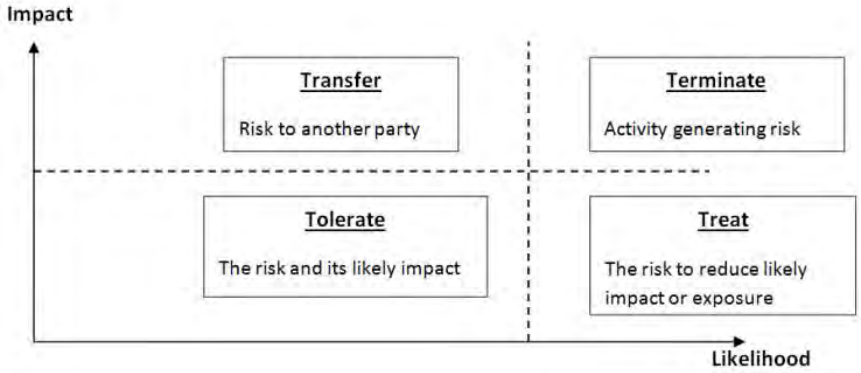


Figura 5: Matriz de Riesgos y las 4T's de Hazard. Risk Assessment and Control (2013)

La matriz propone las medidas que se tomarán con un riesgo dependiendo de la probabilidad y el impacto del riesgo que fue evaluado previamente. Un ejemplo relacionado al tema de investigación aplicando la gestión de riesgos, será la aplicación del proceso de gestión, una vez identificada las amenazas propuestas en el modelo, que evaluará el nivel de riesgo de las amenazas propuestas por el modelo para ver la efectividad de identificación.

2.5 Estándares y Marcos de trabajo

Según ISO, normalización se define como:

"El proceso de formular y aplicar reglas con el propósito de realizar en orden una actividad específica para el beneficio y con la obtención de una economía de conjunto óptimo teniendo en cuenta las características funcionales y los requisitos de seguridad. Se basa en los resultados consolidados de la ciencia, la técnica y la experiencia. Determina no solamente la base para el presente sino también para el desarrollo futuro y debe mantener su paso acorde con el progreso".

Según ISO, los estándares se definen como:

"Los estándares son la sabiduría destilada de personas con experiencia en su tema y que conocen las necesidades de las organizaciones que representan: personas como fabricantes, vendedores, compradores, clientes, asociaciones comerciales, usuarios o reguladores." (International Organization for Standardization, 2011)

De manera de sintetizar la información obtenida, las normas y estándares forman parte de las organizaciones y nacen de investigación y un conjunto de conocimiento reunido por expertos. Estos estándares son creados para el uso interno o de forma compartida para cierto sector o área específica; sin embargo, al tener varias normativas y estándares propuestos por organizaciones, se tiene que llevar a un consenso que permita utilizarlas de manera homogénea para un mejor entendimiento entre las organizaciones. Estos estándares se denominan estándares internacionales cuando se trabaja en conjunto.

2.5.1 ISO

Las normas ISO, también conocido como Organización Internacional de Estandarización, Se remonta a 1946, cuando un grupo de personas provenientes de 25 países se juntaron para discutir el futuro de la estandarización internacional. Siendo en 1947 la fundación oficial con 67 comités técnicos (International Organization for Standardization, 2011). Es así como a través de los años las normas ISO, han ido evolucionando y estableciendo distintos estándares internacionales sujetos a consideración de las organizaciones para su reconocimiento y beneficio propio.

¿Qué es una norma ISO?

Según ISO, las normas ISO son acuerdos hechos por expertos, que definen la mejor manera de hacer algo. Este denominado “algo”, se entiende como la creación de un producto, un servicio o recursos brindados, que las normas ISO pueden avalar y cubrir en tanto cumplan las medidas propuestas y de consenso internacional (International Organization for Standardization, 2011).

ISO/IEC 27001:2013

Esta norma ISO involucra los siguientes puntos dentro de su normativa que es aplicable a cualquier organización:

- Tecnología de Información
- Técnicas de Seguridad
- Sistemas de Gestión de Seguridad de Información (ISMS)
- Requerimientos

Según ISO, la norma ISO/IEC 27001 se especifica como *“los requerimientos para establecer, implementar, mantener y continuar mejorando los sistemas de gestión de seguridad de información dentro del contexto de una organización*”. Adicionalmente la norma incluye requerimientos para la evaluación y tratamiento de los riesgos de

seguridad a la medida de las necesidades de la organización. Un ejemplo marcado en la historia en el Perú es la certificación obtenida por la compañía de teléfonos Telefónica del Perú siendo acreedor de la ISO 27001 en el año 2009.

2.5.2 COBIT

COBIT fue creado en 1996 por la Asociación para la Auditoría y Control de Sistemas de Información (ISACA) y presenta 5 versiones actualmente. Es conocido como un marco de gobierno que permite brindar una serie de componentes que relacionan a la gerencia de las organizaciones con los requerimientos, problemas y riesgos dentro de la organización para proponer las mejores prácticas para un buen sistema de gobierno (ISACA, 2019)

COBIT define los componentes para sostener un sistema de gobierno, lo cual implica una serie de procesos, estructuras organizacionales, políticas, procedimientos, flujo de información, cultura y comportamiento organizacional. COBIT también define los factores de diseño para la construcción de un sistema de gobierno en las organizaciones. (ISACA, 2019)

COBIT® 2019

Es la última versión del marco, la cual se basa en tres principios fundamentales del marco de gobierno. Estos principios propuestos en (ISACA, 2019) son los siguientes:

1. Un marco de gobierno basado en un modelo que posee componentes claves relacionados entre sí, para maximizar el modelo y permitir la automatización.
2. Un marco de gobierno abierto y flexible que facilite la adición de nuevos contenidos y buscar posibles soluciones de manera flexible ante distintos escenarios.
3. Un marco de gobierno que debe alinearse lo mayor posible a estándares, marcos y regulaciones.

El siguiente gráfico, propuesto en (ISACA, 2019), muestra la estructura de los principios fundamentales del marco COBIT® 2019.

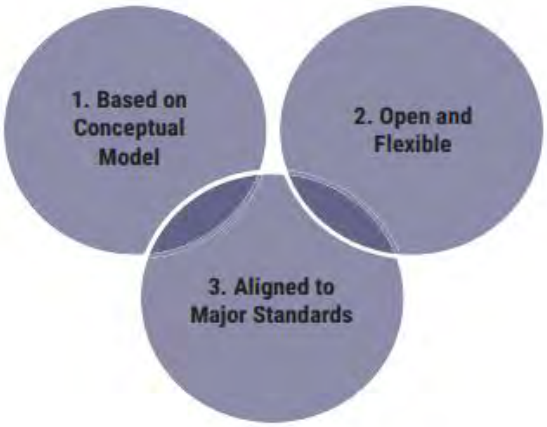


Figura 6: Principios del Marco de Gobierno. COBIT® 2019 FRAMEWORK: INTRODUCTION & METHODOLOGY. ISACA. 2018

Los estándares, marcos y normativas son fundamentales en todo modelo que busca ser implementado en las organizaciones. La función de todos los elementos mencionados anteriormente, permiten que los modelos tengan mayor validez al momento de ser utilizados en las organizaciones. Esta validez se debe a que dichos elementos han sido probados y desarrollados por expertos en base a experiencia, investigación y estudios recopilados a través del tiempo; sin embargo, sabemos que la globalización y el avance tecnológico no se detiene, es por eso que se debe tener las bases ya mencionadas, pero también estar abiertos a nuevos paradigmas que permiten ir a la par con la evolución y desarrollo humano.

2.6 Normativas Legales

En los últimos años, en el Perú se ha presentado diversos ciberataques debido al avance de las tecnologías usadas dentro de las organizaciones públicas y privadas. Como prueba de estos acontecimientos, de acuerdo con un estudio por parte de la empresa de seguridad de informática conocida como ESET, en septiembre de 2018 y septiembre del 2019, se calcula que el 14 % de casos de spyware detectados en Latinoamérica fueron registrados en el Perú (Gestión, 2019). Un spyware es un programa que transmite información recopilada de un ordenador, sin autorización del usuario, a otro ordenador y así como estos programas, existen diversos tipos de ataques que limitan el uso del ordenador y expone información sensible (Gestión, 2019).

En el Perú, en vista de todos los acontecimientos de ciberataque a nivel nacional y mundial, también considerando el avance tecnológico que se tiene en estos tiempos, el Perú ha buscado formas de proteger a las organizaciones mediante normativas y proyectos de ley relacionados a la ciberseguridad que presentan a continuación. Sin

embargo, cabe mencionar que los esfuerzos aún son mínimos y no se ve avance considerable todavía.

LEY N° 30999 "Ley de Ciberdefensa"

Esta ley fue promulgada por parte del estado, la cual tiene como objetivo establecer un marco normativo relacionado a la ciberdefensa del Estado peruano de manera de regulación de operaciones militares dentro del ciberespacio a cargo del Ministerio de Defensa (Ley N° 30999, 2019). La finalidad de esta ley es la protección de recursos y activos críticos que puedan ser atacados en el ciberespacio.

PROYECTO DE LEY N° 4352/2018-CR y 4237/2018-CR

Ambos proyectos de ley nacen por la iniciativa del congreso. El proyecto de ley N° 4352/2018-CR o "Ley de Ciberseguridad", busca establecer un marco normativo en base a la seguridad digital del Estado Peruano. El alcance está enfocado en todas las entidades del sector público, entidades del sector privado, academia y sociedad civil. El proyecto de ley N° 4237/2018-CR, tiene como finalidad promover la seguridad e informática en el Perú mediante la conformación de un Consejo Nacional de Ciberseguridad (Proyecto de Ley N° 4237/2018-CR, 2019) (Proyecto de Ley N° 4352/2018-CR, 2019).

Resolución Directoral para la Gestión de Riesgos de Seguridad de la Información

Existe una resolución directoral, aprobada por el Ministerios de Economía y Finanzas y de acuerdo con el Decreto Supremo N° 117-2014-EF, el cual propone y establece normas de seguridad informática, e implementación de soluciones para la protección de las redes, equipos y sistemas de información del Ministerio. Es así como el 06 de abril de 2016, se aprueba la "Metodología de Gestión de Riesgos de Seguridad". Esta metodología está enfocada a ser aplicada contra factores o influencias adversas que dificultan los objetivos institucionales. El documento aprueba el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014" y su metodología de gestión de riesgos tiene como función principal brindar soporte al sistema de gestión de seguridad de la información del Ministerio de Economía y Finanzas. El documento identifica tipos de amenazas, define conceptos y presenta prácticas y procedimientos para mitigar riesgos (Resolución Directoral por parte del MEF, 2016).

Estas leyes y políticas desarrolladas en el Perú nos permiten abordar el tema propuesto en base al contexto actual que maneja el Perú en relación a la ciberseguridad y plantea establecer límites y propuestas que faciliten y adapten la investigación, que tiene objetivo el diseño de un modelo, según las normativas y consideraciones por parte del Estado peruano.

Capítulo 3. Estado del Arte

3.1 Introducción

Para determinar el estado del arte del problema, se hará uso de la guía para la revisión de literatura sistemática (SLR) (Keele, 2007).

3.2 Objetivos de revisión

El objetivo de la SLR es identificar todos los patrones de actividad de usuarios de infraestructuras tecnológicas al interior de organizaciones públicas, que pudieran constituir amenazas a la ciberseguridad, para lo cual se espera que estos patrones se presenten en la forma de marcos o modelos de acuerdo al tema propuesto en la investigación. El tipo de revisión que se realizará será la revisión empírica, puesto que se necesita determinar los marcos, modelos o medidas que se han utilizado para el problema en particular. La utilidad de este tipo de revisión permite identificar palabras claves, planteamientos, modelos, diseños y análisis para poder comparar los nuestros resultados con estudios previos con el fin de responder al planteamiento del problema (Hernández et al., 2014).

3.3 Preguntas de revisión

De acuerdo con el objetivo de revisión, es necesario proponer un conjunto de preguntas que permitan identificar fuentes de estudio primario que puedan dar mayor soporte al tema propuesto. Para estructurar los elementos de las preguntas de investigación, se emplearán los principios PICOC, tal como se puede apreciar en (Petticrew & Roberts, 2008), según se muestra en la tabla 2.

Tabla 2: Criterios PICOC

Atributos	Descripción
Población	Ciberseguridad
Intervención	Modelos o marcos para la identificación de amenazas no intencionales de ciberseguridad generadas por personal interno
Comparación	Casos de estudio en donde se han empleado o desarrollado modelos, marcos o medidas para identificar las amenazas generadas por personal interno en organizaciones públicas
Resultados	Modelos o marcos para identificar las amenazas no intencionales de ciberseguridad generadas por personal interno, patrones de comportamiento, medidas tomadas
Contexto	Casos de estudio sobre modelos de identificación de amenazas de ciberseguridad generadas por personal interno en instituciones públicas desde el 2010 al 2020

Las preguntas de investigación serían las siguientes:

1. ¿De qué manera los modelos, marcos o medidas están identificando amenazas no intencionales para la ciberseguridad generadas por el propio personal interno de instituciones públicas?
2. ¿De qué manera las actividades del personal interno de una organización sobre la infraestructura de TI pueden considerarse una amenaza no intencional a la ciberseguridad?
3. ¿Cuáles han sido los factores de éxito para definir modelos, marcos o medidas para identificar amenazas no intencionales por personal interno en instituciones públicas y en qué buenas prácticas se han basado?

3.4 Estrategia de búsqueda

Para la estrategia de búsqueda, se definió los siguientes términos particulares propuestos en (Izard, 2009):

- Adición de sinónimos y definiciones alternativas que sean necesarias.
- Se hará la revisión de títulos, documentos y palabras clave
- Uso de operadores lógicos AND y OR

3.4.1 Motores de búsqueda a usar

- PROQUEST
- SCOPUS
- SPRINGER

3.4.2 Cadenas de búsqueda a usar

Para la cadena de búsqueda, los elementos incluidos en la cadena se tomarán como referencia a partir de términos discrimínales de la tabla 2 que utiliza los criterios de PICOC en base al tema propuesto. Estos elementos de búsqueda se pueden apreciar en la tabla 3 que se muestra a continuación.

Tabla 3. Términos Discrimínales de PICOC

Atributos	Elementos de búsqueda
Población	Ciberseguridad
Intervención	Amenazas no intencionales, personal interno
Comparación	(Elementos ya mencionados o no encontrados)
Resultados	(Elementos ya mencionados o no encontrados)
Contexto	Instituciones públicas

La cadena de búsqueda es:

"Amenazas internas no intencionales de ciberseguridad en el sector público"

Se ha definido una única cadena de búsqueda para responder las tres preguntas de guías de la SRL por cuanto:

- Al identificar en los estudios, escenarios de amenazas internas no intencionales específicas se pueden identificar tanto los marcos o modelos usados para definirlas o hacerles frente, como las buenas prácticas involucradas.
- Al identificar en los estudios, escenarios de amenazas internas no intencionales pueden identificarse también los patrones de actividad precisamente del personal interno.
- Los marcos o modelos detectados en los estudios indicarán las buenas prácticas seguidas en, por ejemplo, los casos de éxito.

Tabla 4: Número de artículos encontrados en cada motor de búsqueda

Base de datos indexada	Cadena de búsqueda	Filtros	Total de artículos	Artículos seleccionados
PROQUEST	(Insider Threats Cyber Security) AND ft(unintentional OR "human error" OR unintended) AND ft(public sector OR public organization OR public administration)	● Revisado por pares ● Inglés, español ● De 2010 - 2020	221	11
SCOPUS	(ALL("Insider threats") AND ALL("public administration" OR "public sector" OR "public organization") AND ALL(cyber security) AND ALL("unintentional" OR "human error" OR "unintended")) AND PUBYEAR > 2009 AND PUBYEAR < 2021	● Inglés, español ● De 2010 - 2020	32	22
SPRINGER	((Insider Threats Cyber Security) AND ft(human error OR unintentional OR unintended) AND ft(public sector OR public organization OR public administration))	● Inglés, español ● De 2010 - 2020	16	1
Total			265	34

3.4.3 Criterios de inclusión/exclusión

Planteamiento de los criterios de inclusión

Los criterios de inclusión que ayudan a delimitar los artículos encontrados y priorizar su información.

- El estudio presenta casos en donde se aprecia la identificación de amenazas internas a la ciberseguridad.

- El estudio presenta marcos o modelos para la identificación de amenazas internas a la ciberseguridad.
- El estudio versa sobre amenazas internas a la ciberseguridad no intencionales.
- El estudio se centra en instituciones públicas.

Planteamiento de los criterios de exclusión

Los criterios de exclusión se han definido de manera restrictiva en base al tema propuesto para ayudar a filtrar artículos que no sean imprescindibles en la investigación.

- El estudio es redundante y posee menos detalle que otro estudio de la misma autoría.
- El estudio no presenta ningún tema relacionado a la ciberseguridad
- El estudio no describe ninguna actividad referente al personal interno de infraestructura de TI

3.5 Formulario de extracción de datos

Modelo adaptado del formulario de extracción de datos propuesto en (RIAZ, M., MENDES, E., & TEMPERO, 2008).

Tabla 5: Formulario de extracción de datos

Campos	Descripción	Observaciones
ID	Un único identificador en el formato	Generales
Título	Título del documento encontrado	
Autor	Autor(es) del documento encontrado	
Año de publicación	Año de publicación del documento encontrado	
Tipo de referencia	Revista, conferencia, libro, paper, etc.	
Tipo de estudio	Encuesta, experimento, caso de estudio, etc.	
País	País de publicación del documento encontrado	
Método de investigación para identificación de amenazas internas no intencionales	Qué método utilizan para identificar las amenazas no intencionales por parte del personal interno en organizaciones públicas	P1
El modelo identifica DISC	Sí/No	P1
El modelo identifica UIT-HACK	Sí/No	P1
El modelo identifica PHYS	Sí/No	P1
El modelo identifica PORT	Sí/No	P1
El modelo identifica otros tipo de UIT	Qué otras amenazas internas no intencionales se identifican en el modelo	P1
Modelo o marco para identificar amenazas no	Qué modelo, marco o medidas de ciberseguridad ante amenazas internas	P1

intencionales para la ciberseguridad	no intencionales existentes o nuevas se identifican	
Se identifica IS-CHEC como técnica para detectar causas de UIT en las actividades del personal	Sí/No	P2
Se identifica otras técnicas para detectar causas de UIT en las actividades del personal	Qué otras técnicas existen para detectar causas de UIT	P2
Se identifican UIT en el área de negocios	Sí/No	P2
Se identifican UIT en el área de soporte	Sí/No	P2
Se identifican UIT en el área de investigación y desarrollo	Sí/No	P2
Se identifican UIT en otras áreas de la organización	Qué otras áreas de la organización identifican UIT	P2
Roles del personal interno de infraestructura de TI	Qué roles se asumen por parte del personal interno en infraestructura de TI	P2
Tipo de actividades del personal interno	Qué tipo de actividades por parte del personal interno se identifican	P2
Programa de amenazas internas CERT	Se identifican un programa de amenazas internas CERT como buenas prácticas	P3
ISO 27001 (ISMS)	Se identifica el estándar ISO 27001 como buenas prácticas	P3
Identificación de otras buenas prácticas en el modelo	Qué otras buenas prácticas se han identificado	P3
Se identifican factores de riesgo organizacionales	Sí/No	P3
Se identifican factores de riesgo humano	Sí/No	P3
Se identifican factores de riesgo psicosocial y demográfico	Sí/No	P3
Se identifican otro tipo de factores de riesgo	Qué otros tipos de factores de riesgo se identifican en las actividades del personal	P3

3.6 Resultados de la revisión

Los estudios primarios recopilados para responder las siguientes preguntas se muestran a continuación con información del título, autor y año de publicación:

Tabla 6: Artículos recopilado por título, autor y años de publicación

ID	Título	Autor	Año de publicación	Referencia
A-01	Protecting Information with Cybersecurity	John M. BorkyThomas H. Bradley	2019	(Borky & Bradley, 2019)

A-03	Real-Time Information Security Incident Management: A Case Study Using the IS-CHEC Technique	MARK EVANS , YING HE , CUNJIN LUO , IRYNA YEVSEYEVA , HELGE JANICKE , EFPRAXIA ZAMANI, AND LEANDROS A. MAGLARAS	2019	(Evans, He, Luo, et al., 2019)
A-04	Evaluating information security core human error causes (IS-CHEC) technique in public sector and comparison with the private sector	Evans M., He Y., Maglaras L., Yevseyeva I., Janicke H.	2019	(Evans, He, Maglaras, et al., 2019)
A-05	Framework for digital data access control from internal threat in the public sector	Halim H., Yusof M.M.	2019	(HALIM & YUSOF, 2019)
A-07	An investigation into information security threats from insiders and how to mitigate them: A case study of Zambian public sector	Chinyemba M.K., Phiri J.	2018	(CHINYEMBA & PHIRI, 2018)
A-08	The enemy has passed through the gate: Insider threats, the dark triad, and the challenges around security	Fischbacher-Smith D.	2015	(Fischbacher-Smith, 2015)
A-09	“An Investigation into Cyber Security Threats by Insiders: A case of Public Organisations” Thesis 2019	Melissa K. Chinyemba	2019	(Chinyemba et al., 2018)
A-11	“An Investigation of Information Security Threats from Organisational Insiders and how to mitigate them using a User Awareness and Access Control Model”	MK Chinyemba, J Phiri	2018	(Chinyemba & Phiri, 2018b)
A-12	“Identifying Botnets Intrusion & Prevention–A Review”	LK Musambo, MK Chinyemba, J Phiri	2017	(Musambo et al., 2017)
A-13	Towards a Taxonomy of Information Security Management Practices in Organisations'	Alshaikh, M., Ahmad, A., Maynard, S. and Chang, S.	2014	(Alshaikh et al., 2014)
A-16	'Information Security Policy: A Management Practice Perspective'	Alshaikh, M., MAYNARD, S., Ahmad, A. and Chang, S.	2015	(Alshaikh et al., 2015)
A-17	An Exploratory Study of Current Information Security Training and Awareness Practices in Organizations'	alshaikh, M., Maynard, S., Ahmad, A. and Chang, S.	2018	(Alshaikh et al., 2018)
A-18	'Strategies to Mitigate Knowledge Leakage Risk caused by the use of mobile devices: A Preliminary Study'	Agudelo Serna, C., Bosua, Ahmad and Maynard, S.	2017	(Agudelo-Serna et al., 2018)
A-19	'Exploring Knowledge Leakage Risk in Knowledge-Intensive Organisations: behavioural aspects and key controls' ,	Altukruni, H., Maynard, S., Alshaikh, M. and Ahmad, A.	2019	(Altukruni et al., 2019)

A-20	'Dynamic Information Security Management Capability: Strategising for Organisational Performance'	Onibere, M., Ahmad, A. and Maynard, S.	2019	(Onibere et al., 2019)
A-22	'Toward Sustainable Behaviour Change: An Approach for Cyber Security Education Training and Awareness'	Alshaikh, M., Naseer, H., Ahmad, A. and Maynard, S.	2019	(ALSHAIKH ET AL., 2019)
A-23	A framework for assessing the insider threat in Parastatals in Kenya. MSc Thesis	Abuli, M.J.	2016	(Michael Juma Abuli, 2016)
A-24	An analysis of insider dysfunctional behavours in an accounting information system environment	Mat Roni, M.S.	2015	(MAT RONI, 2015)
A-28	'A case analysis of securing organisations against information leakage through online social networking'	Molok, N., Ahmad, A. and Chang, S.	2018	(ABDUL MOLOK ET AL., 2018)
A-30	Unintentional Internal Threats: A Foundational Study	CERT	2013	(CERT, 2013)
A-31	- Thesis -The Internal Threat	Jacinda L. Wunderlich	2011	(Wunderlich, 2011)
A-32	Managing Internal Threat	Ernest and Young	2016	(Ernst and Young, 2016)
A-33	Review and insight on the behavioral aspects of cybersecurity	Maalem Lahcen Rachid Ait;Caulkins, Bruce;Mohapatra, Ram;Kumar, Manish	2020	(Maalem Lahcen, Rachid Ait Caulkins, Bruce Mohapatra, Ram, Kumar, 2020)
A-38	Aspects of human weaknesses in cyber security	Moinescu, Radu;Răcuciu, Ciprian;Glăvan, Dragoş;Antonie, Narcis-Florentin;Eftimie, Sergiu	2019	(Moinescu, Radu;Răcuciu, Ciprian;Glăvan, Dragoş;Antonie, Narcis-Florentin;Eftimie, 2019)
A-39	Mitigating cyber-attacks through the measurement of non-IT professionals' cybersecurity skills	Carlton, Melissa; Levy, Yair;Ramim, Michelle	2019	(Carlton et al., 2019)
A-41	Human-centered strategies for cyber-physical systems security	Ceesay, E N;Myers, K;Watters, P A	2018	(Ceesay et al., 2018)
A-42	The inhospitable vulnerability	Chen, Hsiangting Shatina;Fiscus, Joseph	2018	(Chen & Fiscus, 2018)
A-44	Employees Attitude towards Cyber Security and Risky Online Behaviours: An Empirical Assessment in the United Kingdom	Hadlington, Lee	2018	(Hadlington, 2018)

A-47	An Overview of Cybersecurity Regulations and Standards for Medical Device Software	Lechner, Nadica Hrgarek	2017	(LECHNER, 2017)
A-50	Introduction to the special issue on insider threat modeling and simulation	Moore, Andrew P;Kennedy, Kirk A;Dover, Thomas J	2016	(Moore et al., 2016)
A-52	Cybersecurity:risks, vulnerabilities and countermeasures to prevent social engineering attacks	Conteh, Nabie Y;Schmick, Paul J	2016	(Conteh & Schmick, 2016)
A-53	Detection and prediction of insider threats to cyber security: a systematic literature review and meta-analysis	Gheyas, Iffat A;Abdallah, Ali E	2016	(GHEYAS & ABDALLAH, 2016)
A-56	DATA LOSS PREVENTION AND CONTROL: INSIDE ACTIVITY INCIDENT MONITORING, IDENTIFICATION, AND TRACKING IN HEALTHCARE ENTERPRISE ENVIRONMENTS	Tu, Manghui;Spoa-Harty, Kimberly;Xiao, Liangliang	2015	(Tu et al., 2015)
A-57	Unintentional Insider Threat: Contributing Factors, Observables, and Mitigation Strategies	Greitzer, Frank L. Strozer, Jeremy Cohen, Sholom Bergey, John Cowley, Jennifer Moore, Andrew Mundie, David	2014	(Greitzer et al., 2014)

Como parte de la investigación, se ha seleccionado cada artículo relacionado con la pregunta de investigación. Esta relación se basa en la respuesta de la pregunta a los campos del formulario de extracción de datos.

Los resultados de la revisión según cada motor de búsqueda fueron los siguientes:

Tabla 7: Artículos encontrados por pregunta y motor de búsqueda

Base de Datos	Preguntas de Investigación		
	P1. ¿De qué manera los modelos, marcos o medidas están identificando amenazas no intencionales para la ciberseguridad generadas por el propio personal interno de instituciones públicas?	**P2. ¿De qué manera las actividades del personal interno de una organización sobre la infraestructura de TI pueden considerarse una amenaza no intencional a la ciberseguridad?**	**P3. ¿Cuáles han sido los factores de éxito para definir modelos, marcos o medidas para identificar amenazas no intencionales por personal interno en instituciones públicas y en qué buenas prácticas se han basado?**
PROQUEST	8	1	6
SCOPUS	18	9	14
SPRINGER	1	0	1
Total (*)	**27**	**10**	**21**

(*) Algunos artículos fueron utilizados para responder más de una pregunta.

3.6.1 Respuesta a la pregunta *"¿De qué manera los modelos, marcos o medidas están identificando amenazas no intencionales para la ciberseguridad generadas por el propio personal interno de instituciones públicas?".*

Para responder la pregunta de investigación, se hará uso del formulario de extracción que puede ser visto en el **Anexo B**, el cual permite identificar aquellos estudios que presentan algún modelo, medida o marco para la identificación de amenazas no intencionales por parte del personal interno. Adicionalmente se muestra la Tabla 8, la cual contiene el campo más relevante del formulario de extracción de datos para resolver la pregunta 1. A continuación, se presentan los resultados obtenidos que permiten responder la pregunta de investigación.

Tabla 8: Artículos que reportan algún método, marco o medida para la detección UIT

Modelo para detectar UIT por parte del personal interno	Número de veces que se usó un modelo	Artículos
Microsoft Threat Modeling Process, STRIDE, DREAD	1	(Borky & Bradley, 2019)
PDDAITC	1	(Halim & Yusof, 2019)
Insider Threat mitigation model	1	(Chinyemba & Phiri, 2018)
Enfoque de sistemas para amenazas internas	1	(Fischbacher-Smith, 2015)
Information Security Policy Management Practice Model	1	(ALSHAIKH ET AL., 2015)
ISTA Program	1	(Alshaikh et al., 2018)
Research Conceptual Model	1	(Agudelo-Serna et al., 2018)
Modelo KLBR	1	(Altukruni et al., 2019)
Modelo ISM	1	(Onibere et al., 2019)
BCW Framework	1	(Alshaikh et al., 2019)
Framework to Internal Threat	1	(Michael Juma Abuli, 2016)
OSN-LMC	1	(Abdul Molok et al., 2018)
Comprehensive UIT Feature Model	1	(CERT, 2013)
Framework para mitigar e identificar amenazas internas	1	(Wunderlich, 2011)
Insider threat program maturity model	1	(Ernest and Yung, 2016
Framework Interdisciplinary	1	(Maalem Lahcen, Rachid Ait Caulkins, Bruce Mohapatra, Ram, Kumar, 2020)
Medidas para identificación y prevención	7	(Evans, He, Luo, et al., 2019), (Evans, He, Maglaras, et al., 2019), (Chinyemba & Phiri, 2018b), (Musambo et al., 2017), (Chen & Fiscus, 2018), (Conteh & Schmick, 2016), (Hadlington, 2018)

Framework NIST	1	(Lechner, 2017)
ABM, GT, SD, BBN, NA	1	(Moore et al., 2016)
IDPA	1	(Gheyas & Abdallah, 2016)
WDOA y UODP	1	(Tu et al., 2015)

Las amenazas internas de ciberseguridad son un tipo de amenaza que ha ido teniendo mayor impacto en las organizaciones. En los últimos años, este tipo amenaza se ha ido identificando como parte de las políticas y medidas dentro de las organizaciones por el fuerte impacto que pueden causar tanto en la información como a nivel monetario. Una amenaza interna de ciberseguridad es cuando una agente, que puede ser un trabajador en cierta área, tiene acceso autorizado a los datos, servicios o sistemas de información de la organización y puede generar alguna acción accidental o intencional que ponga en riesgo la confidencialidad, integridad o disponibilidad de la infraestructura de TI (Ernst and Young, 2016). Existen dos tipos de amenazas internas, las amenazas intencionales y las amenazas no intencionales. Las amenazas intencionales son aquellas donde existe, como el mismo nombre lo indica, una intención por parte del colaborador de perjudicar a la organización para un beneficio o como muestra de venganza ante un mal trato o falta de reconocimiento. El otro tipo de amenaza, la cual es más difícil de detectar, es la amenaza no intencional. Este tipo de amenaza involucra una acción por parte del personal interno sin la intención de perjudicar a la organización. El objetivo de la pregunta es poder entender de qué manera los modelos, marcos o medidas pueden identificar amenazas no intencionales por parte del personal interno; sin embargo, es necesario aclarar que, dentro de los estudios revisados, se han encontrado modelos integrados que involucran los dos tipos de amenazas internas, además se ha podido evidenciar modelos que no solo identifican, sino que presentan medidas, componentes y formas de mitigar estos peligros.

Los modelos investigados, permiten tener de manera estructurada una forma de trabajo que sirva a las organizaciones para tomar medidas preventivas o correctivas ante cualquier escenario posible de acción por parte del personal interno. Para conocer las amenazas que existen dentro de las organizaciones y cómo se generan, es necesario hacer una investigación previa con información real de acontecimientos, sensaciones o experiencias por parte de los trabajadores que ayuden a identificar patrones de comportamiento o factores que involucran una amenaza. Dentro de los estudios revisados, una metodología de investigación frecuente es la realización de encuestas, entrevistas y cuestionarios a las distintas organizaciones donde los participantes tienen distintos roles o funciones dentro de su organización. Estas fuentes de información

permiten tener un conocimiento real de la problemática a la cual se le aplicará medidas o políticas de seguridad. Una vez que se ha recolectado la información necesaria, se puede identificar distintas problemáticas que atraviesa la institución. Luego que se identificó información relevante, es importante empezar con la construcción de un modelo adecuado para el contexto y la problemática actual.

Dentro de los estudios revisados se han encontrado modelos que pueden identificar distintos tipos de amenazas no intencionales. Uno de los modelos propuestos en (CERT, 2013) ha recolectado un conjunto de amenazas no intencionales tipificadas de la siguiente manera:

1. **DISC (Divulgación Accidental)**

Información sensible publicada en sitios web o enviada accidentalmente a personas equivocas por correo, fax, mensajes, etc.

2. **UIT-HACK (Código malicioso)**

Entradas externas a través de la ingeniería social (las cuales pueden ser phishing emails, USB no autorizados, etc.). Estos tipos de amenazas si bien son externas involucran al personal interno por la falta de conocimiento o descuido en sus actividades.

3. **PHYS (Eliminación inadecuada o accidental de registros)**

Información que ha sido eliminada de forma inadecuada, estas pueden ser documentos físicos.

4. **PORT (Equipo portátil)**

Equipos portátiles con información sensible que han sido distribuidos al personal. Estos pueden ser computadoras, teléfonos, PDA, discos duros, etc.

Estos tipos de amenazas sirven de fuente para construir un modelo que permita identificarlas y tomar acciones preventivas. Adicionalmente, es necesario enfocarnos también en el personal interno de la organización, el cual, mediante su comportamiento puede ocasionar un problema. Para poder analizar el comportamiento de la persona, existe una técnica propuesta en (Evans et al., 2019) (Evans, He, Maglaras, et al., 2019) para relacionar los incidentes de UIT con los errores humanos en las tareas del colaborador. Esta técnica es conocida como IS-CHEC, la cual permite identificar las causas de los errores humanos relacionadas a amenazas internas. Una vez que se tiene conocimiento de estos componentes, se puede empezar a proponer un modelo. Dentro de los modelos estudiados, existen modelos que ya están implementados y pueden ser

muy útiles para detectar amenazas priorizadas como es el caso del Proceso de modelado de amenazas de Microsoft (Borky & Bradley, 2019). Este modelo se encarga de descomponer una aplicación con el fin de identificar flujos de datos, elementos de entrada y salida y dependencias, para luego identificar vulnerabilidades que son comparados con amenazas conocidas. Existen frameworks como el PDDAITC propuesto en (Halim & Yusof, 2019) que, además de identificar las amenazas internas, maneja un control por elementos tanto para las amenazas internas, aplicación, base de datos y políticas de seguridad. Esto permite no solo identificar las UIT sino también ir mitigándolas. Otros modelos también pueden ser aplicados de acuerdo al contexto, esto implica que la identificación de amenazas y su mitigación dependan mucho de la región o país en específico que, a pesar de basarse en estándares internacionales, el modelo depende de las necesidad y dificultades de las organizaciones en una región específica como es el modelo propuesto en (Chinyemba & Phiri, 2018). Sin embargo, no solo existen modelos para la identificación de UIT, también hay algoritmos para predecir y detectar amenazas internas como es el IDPA (Gheyas & Abdallah, 2016) y métodos combinados que provienen de técnicas como ABM, GT, SD, BBN propuestos en (Moore et al., 2016).

Existe una práctica conocida como ingeniería social que consiste en la obtención de información confidencial por medio de información engañosa que puede confundir al personal interno de una organización, para estos casos que ya existen amenazas identificadas se deben tomar medidas (Conteh & Schmick, 2016) ya que, a pesar de ser ataques externos, al involucrar al personal interno y su falta de conocimiento se vuelve una UIT por defecto. Adicionalmente, como parte de la investigación, se ha encontrado estudios que buscan medir el nivel de madurez y conciencia sobre la seguridad cibernética (Hadlington, 2018) (Ernst and Young, 2016), esto es un factor clave en las organizaciones donde se puede lograr identificar si los trabajadores son conscientes de los peligros que ellos mismos pueden ocasionar.

Por otro lado, se ha podido encontrar frameworks asociados a estándares como el NIST (Lechner, 2017), los cuales ya contemplan distintas amenazas que permiten que el modelo sea más estable y aceptado. Otros tipos de framework son el BCW, ITSRA y OSN-LMC, los cuales se enfocan en el comportamiento objetivo, en controles por capas y errores humanos con exposición de información en redes sociales respectivamente.

Finalmente, todos estos modelos mencionados tienen distintas maneras de identificar las amenazas internas no intencionales (UIT), ya sea por el comportamiento del personal, tipificando amenazas ya conocidas, siguiendo estándares internacionales o utilizando métodos algorítmicos y técnicas de predicción, cada uno tiene una forma

distinta de identificarlos siguiendo algún lineamiento base de referencia. Sin embargo, a pesar de identificar distintas formas, todos tienen el mismo fin, el cual es poder ayudar a las organizaciones a mitigar y prevenir este tipo de amenazas que cada vez está creciendo y generando grandes pérdidas tanto de información como económicas, ya que cuando hablamos de organizaciones públicas, se expone no solo a la empresa sino la economía de un país y los servicios que brinda a la sociedad.

3.6.2 Respuesta a la pregunta "*¿De qué manera las actividades del personal interno de una organización sobre la infraestructura de TI, pueden considerarse una amenaza no intencional a la ciberseguridad?*".

Para responder la pregunta de investigación, se hará uso del formulario de extracción que puede ser visto en el **Anexo B**, la cual permite identificar aquellos estudios que utilicen alguna técnica o método para detectar las causas en las que una actividad, por parte del personal de una organización, podría transformarse en una amenaza interna no intencional. Adicionalmente se muestra la Tabla 9, la cual contiene el campo más relevante del formulario de extracción de datos para resolver la pregunta 2. A continuación, se presentan los resultados obtenidos que permiten responder la pregunta de investigación

Tabla 9: Artículos que reportan algún método o técnica para la detección de causas relacionadas a actividades propensas a UIT

Técnicas para detectar causas de UIT en las actividades del personal	Número de veces que se usó una técnica o método de identificación de causas	Artículos
Comprehensive UIT Feature Model	1	(CERT, 2013)
Entrevistas y Cuestionarios	4	(Chinyemba & Phiri, 2018), (Chinyemba et al., 2018), (Chinyemba & Phiri, 2018b , (Abdul Molok et al., 2018)
IS-CHEC	2	(Evans, He, Luo, et al., 2019), (Evans, He, Maglaras, et al., 2019)
Framework	1	(Michael Juma Abuli, 2016)
Social Cognition Theory	1	(Maalem Lahcen, Rachid Ait Caulkins, Bruce Mohapatra, Ram, Kumar, 2020)
TPB (Teoría del comportamiento planeado)	1	(Mat Roni, 2015)

Las actividades del personal interno en una organización forman parte de distintos procesos que permiten el correcto funcionamiento de la organización. Estas actividades

pueden volverse una amenaza que afecte los servicios y la información que manejan las instituciones públicas. Motivo por el cual se considera necesario identificar cuando una actividad por parte del personal puede convertirse en una amenaza interna no intencional (UIT). Para poder identificarlas es necesario conocer las causas que lo generan y cómo llega a convertirse en un problema crítico.

De los estudios seleccionados como respuesta a la pregunta 2, se ha podido observar que cualquier actividad en la organización puede ser una amenaza no intencional; sin embargo, existen actividades más críticas que otras, dependiendo del área donde se realiza. Las áreas con mayor índice de amenazas son las áreas de negocio, soporte, desarrollo, recursos humanos y TI. Estas áreas son fundamentales en la organización que en su mayoría están fuertemente relacionadas con la infraestructura de TI. Adicionalmente, es importante también hacer énfasis en los roles de la organización, ya que dichos roles dan al personal mayor libertad y facilidad en el manejo de la información.

Una actividad puede convertirse en una amenaza no intencional dependiendo de las causas que lo ocasionan. Dentro de los estudios primarios se ha podido identificar métodos o técnicas que permiten encontrar las causas o propiamente la actividad que genera una posible amenaza. Una de la técnica encontrada es nombrada las causas de errores humanos fundamentales de seguridad de la información (IS-CHEC) (Evans, He, Maglaras, et al., 2019). Esta técnica se divide en dos partes o elementos. El primer elemento es el elemento de mapeo, la cual tiene como función tomar todos los registros incidentes de la organización para disponer de ellos y luego pasar por el segundo elemento, que es el elemento de análisis. El elemento de análisis tiene como función, por medio de componentes, identificar las causas probables del incidente y mitigarlas en un proceso. Es ahí donde se puede identificar las causas probables de una amenaza que forma parte de una actividad dentro de un proceso. Dos de estos componentes son el GISAT y el CHEC, de los cuales uno representa una tarea que afecta la seguridad de la información y el otro identifica si es una causa de error humano respectivamente. Ambos permiten tipificar las actividades y relacionarlas a un posible incidente no intencional (Evans et al., 2019).

Otro método para identificar si una actividad es una posible amenaza no intencional se ha hecho por medio de cuestionarios y encuestas, las cuales permiten saber de manera objetiva las posibles causas de una amenaza no intencional probable. Las encuestas y cuestionarios hechos a una población determinada dan como resultado que las organizaciones no tienen un alto nivel de madurez de buenas prácticas (Chinyemba & Phiri, 2018). Estos resultados nos permiten inferir que muchas de las actividades dentro

de cada proceso de la organización no manejan estándares de seguridad o control en el uso y forma de trabajo del personal interno. La falta de un control más el error humano hacen posible que una actividad sea propensa a convertirse en una amenaza no intencional.

Los estudios primarios también proponen diversas teorías que pueden ser aplicadas y buscan explicar el comportamiento del personal que puede generar un impacto negativo en sus actividades sea intencional o no intencionalmente. Una de las teorías que se hace mención es la teoría de comportamiento planificado (TPB). Esta teoría plantea que la intención es determinante en el comportamiento real de la persona y que, por medio de determinantes conceptuales, la percepción de la persona ante recursos y oportunidades y factores externos que no puede controlar se puede predecir el comportamiento deliberado (Mat Roni, 2015). Si bien esta teoría lo que busca es predecir un comportamiento con intención, no podemos dejar de lado que, dentro de las actividades de la persona, podemos encontrar una intención sin un fin en específico que también podría ser causal de una amenaza interna sin intención.
Por otro lado, existen dentro de los estudios primarios la propuesta de un modelo conocido como modelo completo de funciones de una UIT, que permiten identificar por medio de componentes la estructura de una amenaza interna no intencional (UIT) y los roles que participan en su ejecución (CERT, 2013). Este modelo nos puede dar una mirada amplia de la estructura de una UIT y así poder identificar si ciertas actividades, por parte del personal interno, pueden ser consideradas como una amenaza. Adicionalmente, existen también actividades relacionadas a las redes sociales. Estas actividades pueden ser identificadas como OSN Functions. Este tipo de actividades está relacionada básicamente a la interacción del personal interno de una organización con sus redes sociales. Las OSN Functions pueden ser una posible amenaza sin intención por parte del personal, ya que, al exponer parte de su información, puede poner en riesgo o exponer información de la organización. Este tipo de funciones pueden ser la publicación de información, actualización de estatus, solicitudes de amistad, carga de fotos y videos, aplicaciones externas y links a sitios externos (Abdul Molok et al., 2018).

Finalmente, se puede concluir, en base a los estudios primarios, que las actividades del personal interno pueden ser amenazas internas no intencionales a partir de distintas causas como áreas involucradas, comportamiento intencional, roles específicos, manejo de redes sociales, controles de seguridad no aplicados y no menos importante el error humano.

3.6.3 Respuesta a la pregunta *"¿Cuáles han sido los factores de éxito para definir modelos, marcos o medidas para identificar amenazas no intencionales por personal interno en instituciones públicas y en qué buenas prácticas se han basado?"*

Para responder la pregunta de investigación, se hará uso del formulario de extracción que puede ser visto en el **Anexo B**, el cual permite identificar aquellos estudios que utilicen buenas práctica, estándares o normativas dentro de sus modelos e identifiquen factores de éxito que permitan identificar UIT. Adicionalmente se muestra la Tabla 10, la cual contiene el campo más relevante del formulario de extracción de datos para resolver la pregunta 3. A continuación, se presentan los resultados obtenidos que permiten responder la pregunta de investigación.

Tabla 10: Artículos que reportan buenas prácticas, estándares o normativas en el diseño de sus modelos

Buenas prácticas utilizadas en el modelo	Número de veces que se identificó buenas prácticas	Artículos
CERT	1	(Ernst and Young, 2016)
ISO 27001 (ISMS)	4	(Halim & Yusof, 2019), (Chinyemba & Phiri, 2018), (Chinyemba & Phiri, 2018b), (CERT, 2013)
Prácticas de gestión de seguridad de la información	1	(Alshaikh et al., 2014)
ISO 27005	1	(Agudelo-Serna et al., 2018)
Políticas de Seguridad de Información	2	(Wunderlich, 2011), (Moinescu, Radu;Răcuciu, Ciprian;Glăvan, Dragoş;Antonie, Narcis-Florentin;Eftimie, 2019)
NIST	3	(Maalem Lahcen, Rachid Ait Caulkins, Bruce Mohapatra, Ram, Kumar, 2020), (Chen & Fiscus, 2018), (Lechner, 2017)
Herramientas de CSI	1	(Carlton et al., 2019)
Implementing a Holistic Cyber Loss Mitigation Strategy	1	(Ceesay et al., 2018)
Solo presentan factores de éxito, no se identificó buenas prácticas	7	(Borky & Bradley, 2019), (Evans, He, Maglaras, et al., 2019), (Fischbacher-Smith, 2015), (Altukruni et al., 2019), (Abdul Molok et al., 2018), (Gheyas & Abdallah, 2016), (Greitzer et al., 2014)

Todas las preguntas propuestas en la investigación guardan una relación complementaria, esto quiere decir que las tres preguntas permiten conocer más a fondo las causas, factores, modelos y buenas prácticas desarrollados para la identificación de

las UIT. Según los modelos identificados en la primera pregunta, muchos de ellos han podido ser diseñados en base dos elementos muy importantes. Uno de ellos son los factores de éxitos, los cuales son determinantes para que un modelo sea diseñado y permita cumplir su función en una organización. Estos factores guardan una relación directa con el comportamiento de los trabajadores y el medio que los rodea, en otras palabras, los factores engloban distintas conductas y características ya antes mencionadas solo que están categorizadas en factores humanos, organizacionales, psicosociales y demográficos. Dentro de los estudios revisados, dichos factores fueron considerados o mencionados dentro los modelos o medidas propuestas en (Borky & Bradley, 2019) (Evans, He, Maglaras, et al., 2019) (Abdul Molok et al., 2018) (Altukruni et al., 2019) (Gheyas & Abdallah, 2016). A continuación, se muestran los factores por categoría (Greitzer et al., 2014).

Factores Humanos

- Error Humano
- Fatiga
- Carga de trabajo mental
- Conciencia de la situación

Factores Organizacionales

- Procedimientos o instrucciones inadecuados
- Mala comunicación
- Falta de conocimiento, habilidades
- Recursos insuficientes
- Prácticas de seguridad inadecuadas

Factores Psicosociales y Demográficos

- Factores culturales
- Género
- Estado de ánimo
- Edad
- Influencia de drogas y hormonas

Otros de los elementos importantes para el diseño de modelos son las buenas prácticas y normativas base sobre la cual fueron implementados algunos modelos. En la mayoría

de los artículos se ha gestionado políticas de seguridad de la información como también uso de herramientas CSI (Alshaikh et al., 2014) (Carlton et al., 2019) (Wunderlich, 2011) (Moinescu, Radu; Răcuciu, Ciprian; Glăvan, Dragoş; Antonie, Narcis-Florentin; Eftimie, 2019). Estas políticas son un conjunto de medidas adoptadas por la organización ante distintos escenarios para prevenir acontecimientos como amenazas internas de ciberseguridad. Adicionalmente, entre las principales buenas prácticas también se ha tomado como base la ISO 27001 conocida como un estándar internacional del sistema de gestión de la seguridad de la información. La cual también propone un framework implementado conocido como ISMS (CERT, 2013). Esta normativa evalúa los sistemas de gestión de la seguridad de información para ver si cumple los estándares propuestos que permitan acreditar las normas ISO. Si un modelo está basado en una buena práctica como las normas ISO, al aplicarlo en una organización. La organización podría ser evaluada para ver si cumple las evaluaciones correspondientes para su certificación. Otras de las buenas prácticas es la conocida como CERT, que es un equipo de respuesta ante emergencia de seguridad computacionales. Este equipo propone medidas para gestión de seguridad de la información (Ernst and Young, 2016).

Finalmente, se ha podido identificar que muchos de los modelos utilizan normativas y buenas prácticas internacionales como un factor crítico de éxito para el diseño de sus modelos o medidas que deben ser aplicadas dentro de la organización de forma preventiva o correctiva.

3.7 Conclusiones

En los estudios preliminares, a pesar de no haber identificado el uso de softwares para el diagnóstico y gestión de amenazas internas, sí se ha podido identificar modelos estudiados que, en su mayoría, utilizan estándares o buenas prácticas dentro de sus propuestas para tener un mayor alcance que permita mitigar las amenazas internas de ciberseguridad, tanto intencionales como no intencionales, no solo en organizaciones públicas sino también en privadas. Estos modelos nacen con el objetivo de identificar, controlar y mitigar amenazas internas relacionadas al personal de la organización. Estas amenazas necesitan ser identificadas antes de la construcción del modelo, para eso se utiliza distintas metodologías, algoritmos, factores de riesgo, teorías de comportamiento y encuestas que puedan generar una base de datos que luego sirva como fuente necesaria para el desarrollo de una investigación, modelo, marco de trabajo sólido, políticas de seguridad o alguna medida que pueda contribuir en la solución parcial o completa de un problema como son las amenazas de ciberseguridad por parte del personal interno.

Con la revisión de literatura se ha podido evidenciar que no existen modelos actuales para la identificación de amenazas UIT dentro de las organizaciones públicas en el Perú. Otro punto importante, que forma parte de los modelos que se busca identificar, es la falta de estudios sobre amenazas no intencionales por parte del personal interno en dichas organizaciones públicas y por ende no se efectúa un análisis de riesgo ante estos tipos de amenazas.

Finalmente, si bien existen estudios a nivel mundial sobre modelos tanto para identificar e incluso mitigar todo tipo de amenazas de ciberseguridad en base a estándares u otras técnicas aplicadas. Dentro del Perú, pese a que existen ciertos programas de auditoría relacionado a la seguridad de la información y ciberseguridad, no se ha identificado estudios o modelos específicos para las amenazas no intencionales de ciberseguridad en función al comportamiento del personal interno en las organizaciones públicas, lo que implica la evaluación y consideración del tema propuesto ante la problemática actual dentro del país.

Capítulo 4. Definición de los componentes del modelo a alto nivel

4.1 Introducción

El capítulo presentado desarrolla el Objetivo Específico 2 (OE2). El objetivo del capítulo es definir los componentes necesarios para la creación del modelo de identificación de amenazas no intencionales internas de Ciberseguridad para instituciones públicas, el mismo que ha sido denominado como MANIC, para el presente y siguientes capítulos. Los componentes han sido definidos como parte de los resultados obtenidos de la investigación que involucra los patrones de comportamiento, la gestión de riesgos y buenas prácticas. La definición y diseño del modelo forma parte de una de las fases de la ciencia del diseño. Las cuales permiten la creación de un artefacto que en este caso es el modelo junto con sus componentes con la finalidad de ser utilizado en la organización para identificar las amenazas involucradas y su respectiva propuesta de tratamiento a través de una guía aplicativa.

4.2 Resultados Alcanzados (RE2, RE3, RE4, RE5, RE6)

El resultado alcanzado es el conjunto de componentes a alto nivel que se han definido de manera estructurada para la construcción de MANIC.

Los componentes que se han definido han sido desarrollados en conjunto con los especialistas basados en los estándares internacionales como el ISO 27001, ISO 27002 y un marco de trabajo desarrollado por las normas NIST. Dentro de estos estándares y marcos de trabajo se siguieron las funciones principales del NIST como un enfoque para iniciar la construcción del modelo empezando por la identificación y terminando en la recuperación. Otra de las premisas seguidas fue la gestión de riesgos que se ha incluido dentro de los componentes en base a las normas ISO 27001 y 27002. Estas herramientas junto con la experiencia pragmática y teórica de los especialistas han sido de utilidad para definir los componentes a alto nivel de MANIC. Las demás herramientas serán utilizadas para la implementación de los componentes que se llevará a cabo en el siguiente capítulo.

Los componentes se han descrito en un Informe de Hoja de Ruta en el **Anexo C** que presenta cada uno en detalle y descripción. A continuación, se muestra la estructura del modelo.

Tabla 11: Estructura de los componentes del modelo (MANIC)

Modelo de Detección de Amenazas No Intencionales Internas de Ciberseguridad (MANIC) para instituciones públicas			
	Nombre	**Descripción**	**Estándares principales**
COMPONENTES	**1. Análisis situacional**	Herramienta de análisis GAP que va a permitir determinar el estado actual (AS-IS) de la organización en lo referente a Ciberseguridad	ISO 27002, ISO 27032, ISO 27103, Normas NIST
	2. Objetivos de Ciberseguridad	Corresponde a los objetivos (TO-BE) de Ciberseguridad que van a ser cubiertos por la aplicación del marco MANIC en cualquier entidad del estado	Estado del arte
	3. Métricas e indicadores	Indicadores que miden si el objetivo ha sido alcanzado o no	Propia autoría
	4. Lista de patrones de comportamiento	Patrones de comportamiento que se pretenden detectar en la institución estatal.	Estado del arte
	5. Matriz de gestión de riesgos de Ciberseguridad	Implica desde la identificación de riesgos, análisis, evaluación de riesgos, tratamiento de riesgos y proposición de controles: • Procesos de negocio • Activos de información digital involucrados • Vulnerabilidades • Amenazas <- Internas no intencionales • Riesgos • Impacto para la organización • Probabilidad de ocurrencia del riesgo • Tratamiento del riesgo o Propuesta de controles	ISO 31000, ISO 27005
	6. Guía de aplicación del modelo	Guía de pasos mediante la cual se va a aplicar el modelo en cualquier institución del estado	Propia autoría

Componentes del modelo (MANIC)

Los componentes del modelo que se presentan a continuación están definidos en orden de aplicación.

a) Análisis Situacional (RE2)

Herramienta de análisis GAP que va a permitir determinar el estado actual (AS-IS) de la organización en lo referente a Ciberseguridad.

Herramienta:

Matriz de Análisis Situacional, desarrollada en formato Excel, con un conjunto de criterios relacionados a la Ciberseguridad clasificados en una escala del 1 al 5 para ser aplicado en la institución que permita dar una calificación final. Los criterios serán relacionados a las normas ISO 27002, 27103 y NIST (Instituto Nacional de Estándares y Tecnología).

b) Objetivos de Ciberseguridad (RE3)

Corresponde a los objetivos (TO-BE) de Ciberseguridad que van a ser cubiertos por la aplicación del marco MANIC en cualquier entidad del estado. Estos objetivos van a incluir las amenazas no intencionales de Ciberseguridad, de manera que puedan permitir su detección o controlar sus efectos de dichas amenazas. Los objetivos serán listados y definidos de forma infinitiva.

c) Métricas e indicadores (RE3)

Indicadores que miden si el objetivo ha sido alcanzado o no. Los indicadores se harán por cada objetivo planteado.

d) Lista de patrones de comportamiento (RE4)

Patrones de comportamiento que se pretenden detectar en la institución estatal. Estos patrones están definidos en base al comportamiento social del usuario y a sus actividades trazables en la red de la organización las cuales están relacionadas con las amenazas internas.

Las causas probables en relación con las amenazas internas basado en el estado del arte son las siguientes:

- Los empleados tienen una vida social fuera de la organización, la cual marca el comportamiento de cada uno.
- Los empleados tienen accesos y privilegios a los recursos de la organización para el desarrollo normal de sus actividades
- Los empleados tienen una interacción continua con las actividades de la organización debido a sus tareas diarias.
- El uso indebido intencional o no intencional de sus privilegios compromete la seguridad de los datos dentro y fuera de la organización.

e) Matriz de gestión de riesgos de Ciberseguridad (RE5)

Implica desde la identificación de riesgos, análisis, evaluación de riesgos, propuesta de tratamiento de riesgos y proposición de controles. El diseño de la matriz estará basado en las normativas ISO 31000, 27005.

La matriz de gestión de riesgos define los siguientes puntos dentro de su gestión:

• Procesos de negocio
• Activos de información digital involucrados
• Vulnerabilidades
• Amenazas no intencionales **(*)**
• Riesgos
• Impacto para la organización
• Probabilidad de ocurrencia del riesgo
• Tratamiento del riesgo
  o Propuesta de controles

(*) Las principales amenazas consideradas son las no intencionales; sin embargo, también es relevante considerar algunas amenazas intencionales debido a la estrecha relación de ambos tipos.

f) Guía de aplicación del modelo (RE6)

Conjunto de pasos mediante el cual se va a aplicar el modelo en cualquier institución del estado.

La estructura tiene 2 validaciones. La primera validación fue realizada por la profesora Melissa K. Chinyemba, la cual forma parte de la Universidad de Zambia, África. La segunda validación fue realizada por la oficial de Seguridad de Información, Jennifer Ayllón, quien es especialista en CyberSecurity & Tecnologías del Ministerio de Trabajo y Promoción del Empleo (MTPE).

4.3 Discusión

Los resultados obtenidos en la Tabla 11, son un conjunto de componentes descritos a un nivel de detalle que permite conocer en qué consiste cada uno y qué medios o herramientas son necesarias para su elaboración. Estos componentes son parte de un todo que viene a ser el modelo que se busca diseñar. Todos estos componentes serán aplicados en el orden que se señala como parte del modelo para poder identificar las amenazas y su respectivo tratamiento.

Los resultados mantienen una coherencia con estudios y modelos previamente encontrados, si bien no está enfocado en el mismo tema, cumple la misma función de detectar, evaluar y mitigar de acuerdo a las necesidades y el contexto específico. Estos pueden ser generalizados, en el sentido que pueden utilizarse no solo para la identificación de amenazas no intencionales internas sino también para amenazas intencionales dentro de las organizaciones públicas. Esto permite flexibilidad en el uso del modelo cumpliendo las mismas funciones.

Capítulo 5. Diseño de los componentes del modelo

5.1 Introducción

El capítulo presentado desarrolla el Objetivo Específico 3 (OE3). El objetivo del capítulo es presentar el diseño de los componentes del modelo denominado MANIC. El diseño de los componentes tiene como fin principal su aplicación dentro de una institución pública. El modelo será diseñado en base a estándares principales y la revisión del estado del arte. Cada componente del modelo será explicado al detalle con su resultado esperado respectivo.

5.2 Resultados Alcanzados (RE7)

Los resultados alcanzados forman parte del Resultado Esperado 7 (RE7), el cual presenta la documentación detallada de cada uno de los componentes del modelo.

5.2.1 Análisis Situacional

Este componente permite presentar el estado actual (AS-IS) de la organización pública mediante el uso de una matriz de análisis situacional. Esta matriz está diseñada en formato Excel y busca evaluar, mediante requerimientos basados en la normativa NIST y una escala de evaluación por estados (No Aplica, Incompleto, En Proceso, Ejecutado, Optimizado), qué tan aplicable es la Ciberseguridad en la organización.

La matriz de análisis situacional ubicada en el **Anexo D** tiene como objetivo poder medir cada requerimiento y cuantificar los resultados, para tener identificado posibles vulnerabilidades dentro de la organización y poder relacionarlo con la lista de patrones de comportamiento definidos con el fin de seleccionar qué patrones están en ejecución dentro de la organización.

a) Elementos de la Matriz Situacional

- Encabezados

  Está identificado de fondo azul, y será divido en los siguientes títulos:

  - **Sección**
    Enumeración de la categoría o grupo de requerimientos
  - **Requerimiento**

    Descripción del grupo o detalle con las normativas a ser evaluadas
  - **Código NIST**

    Referencia del requerimiento asociado a marco de trabajo o ISO
  - **Estado**

    No Aplica, Incompleto, En Proceso, Ejecutado y Optimizado.

- **Documento o Evidencia**

  Documento o prueba del cumplimiento o no del requerimiento en la organización

- **Comentarios u Observaciones**

  Alguna observación o detalle en consideración respecto al estado del requerimiento

- Categoría

  Agrupa un conjunto de subcategorías en base a conceptos que tienen el mismo objetivo de evaluación en cuanto a Ciberseguridad.

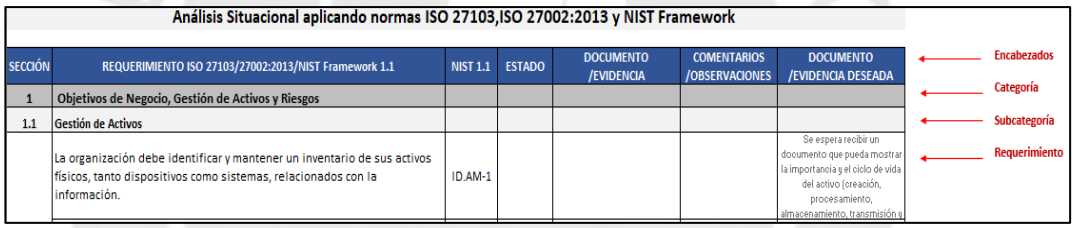
- Subcategoría

  Agrupa un conjunto de requerimientos en base a la función que busca evaluar en la organización relacionado a Ciberseguridad.

- Requerimiento

  Requisito a ser evaluado en la organización basado en la normativa de NIST, ISO 27103 y ISO 27002

  Estructura de la Matriz:



Análisis Situacional aplicando normas ISO 27103,ISO 27002:2013 y NIST Framework

SECCIÓN	REQUERIMIENTO ISO 27103/27002:2013/NIST Framework 1.1	NIST 1.1	ESTADO	DOCUMENTO /EVIDENCIA	COMENTARIOS /OBSERVACIONES	DOCUMENTO /EVIDENCIA DESEADA
1	Objetivos de Negocio, Gestión de Activos y Riesgos					
1.1	Gestión de Activos					
	La organización debe identificar y mantener un inventario de sus activos físicos, tanto dispositivos como sistemas, relacionados con la información.	ID.AM-1				Se espera recibir un documento que pueda mostrar la importancia y el ciclo de vida del activo (creación, procesamiento, almacenamiento, transmisión u

Figura 7: Matriz de Análisis Situacional (Autoría Propia)

b) Aplicación de la Matriz Situacional

- Selección del estado del requerimiento

  Para la aplicación de la Matriz Situacional, el primer paso es la selección del estado del requerimiento de acuerdo con los documentos o evidencias que validen el cumplimiento nulo (no aplica), parcial (incompleto o en proceso) y completo (ejecutado u optimizado) en la organización.

SECCIÓN	REQUERIMIENTO ISO 27103/27002:2013/NIST Framework 1.1	NIST 1.1	ESTADO
1	Objetivos de Negocio, Gestión de Activos y Riesgos		
1.1	Gestión de Activos		
	La organización debe identificar y mantener un inventario de sus activos físicos, tanto dispositivos como sistemas, relacionados con la información.	ID.AM-1	Incompleto
	La organización debe identificar y mantener un inventario de sus plataformas y aplicaciones de software	ID.AM-2	En proceso

Figura 8: Asignación de estados por requerimiento (Autoría Propia)

- Cálculo de cumplimiento por estado

  El cálculo final se determina una vez que se evalúe todos los requerimientos, el cual muestra los resultados por estado en categoría y subcategoría donde fue evaluada la organización.

Resultados de la Matriz de Análisis Situacional

Clasificación Matriz	Estado	Significado	Total	Porcentaje de requerimientos por estado (%)
Nivel 0	No Aplica	El requisito no es aplicable en la organización	0	0%
Nivel 1	Incompleto	El requisito no muestra evidencia de su ejecución o los documentos presentados no sustentan la conformidad del requisito evaluado	1	50%
Nivel 2	En proceso	El requisito se ejecuta parcialmente o la documentación presentada evidencia su ejecución pero a un mínimo nivel de conformidad	1	50%
Nivel 3	Ejecutado	El requisito se ejecuta conforme a la entidad, se presentan los documentos que sustentan su aplicación	0	0%
Nivel 4	Optimizado	El requisito se ejecuta conforme a la entidad, presenta los documentos necesarios para su validación y existe mejora continua en su aplicación	0	0%
Total			2	100%

SECCIÓN	REQUERIMIENTO ISO 27103/27002:2013/NIST Framework 1.1	Total	No Aplica	Incompleto	En proceso	Ejecutado	Optimizado
1	Objetivos de Negocio, Gestión de Activos y Riesgos	23	0	1	1	0	0
1.1	Gestión de Activos	5	0	1	1	0	0
1.2	Ambiente de Negocio	5	0	0	0	0	0
1.3	Gobernanza	4	0	0	0	0	0
1.4	Gestión de Riesgos	9	0	0	0	0	0

Figura 9: Resultados de la aplicación de la matriz (Autoría Propia)

La matriz situacional tiene 2 validaciones. La primera validación fue realizada por la profesora Melissa K. Chinyemba, la cual forma parte de la Universidad de Zambia, África. La segunda validación fue realizada por la oficial de Seguridad de Información, Jennifer Ayllón, quien es especialista en CyberSecurity & Tecnologías del Ministerio de Trabajo y Promoción del Empleo (MTPE).

Objetivos y Métricas de Ciberseguridad

La definición de los objetivos y las métricas asociadas para medir el cumplimiento de cada objetivo se ha definido en base a la revisión sistemática previamente desarrollada. Dentro de esta revisión y como parte fundamental del modelo, se busca que los objetivos que se pretende alcanzar están muy relacionados con la identificación de amenazas no intencionales de Ciberseguridad por parte del personal interno con el fin de reducir el impacto de ocurrencia en la organización.

a) Objetivos

Los objetivos propuestos tienen la finalidad de reducir las amenazas no intencionales de Ciberseguridad (UIT, por sus siglas en inglés). Estos objetivos principalmente tienes dos enfoques. El primer enfoque está relacionado con la búsqueda de conciencia y entrenamiento del personal y el segundo está enfocado en la seguridad y control de los procesos y activos de la organización. La Organización debe:

O 1. Crear conciencia de las amenazas intencionales y no intencionales de Ciberseguridad dentro y fuera de la organización.

El objetivo planteado va alineado al tema principal del modelo, el cual busca la identificación de amenazas no intencionales. Como parte de la aplicación del modelo, lo que se busca con este objetivo es lograr que los colaboradores sepan con qué amenazas tendrán que lidiar diariamente, lo cual tiene un impacto positivo en la identificación más rápida de dichas amenazas.

O 2. Generar expertise en los empleados en reconocimiento de phishing, diferentes tipos de malware y otros vectores de amenazas en las redes sociales.

Este objetivo se plantea en base a las actividades que realizan los colaboradores, debido a que están en constante cercanía con este tipo de amenazas que, si bien son externas, depende mucho del colaborador volverse internas si permite su fácil aplicación en la organización. Como parte del cumplimiento de este objetivo, se busca reducir este tipo de amenazas mediante un accionar rápido del colaborador, lo cual beneficia a la organización.

O 3. Entrenar y desarrollar conciencia en los empleados sobre los sesgos cognitivos que puedan perjudicar sus actividades diarias.

Este objetivo plantea una autoevaluación del colaborador que permita identificar en sí mismo cuando existen factores personales, sociales o económicos que puedan alterar el ritmo de trabajo habitual dentro y fuera de la organización. Estas evaluaciones deben tener la aprobación del colaborador y el adecuado tratamiento de sus datos cumpliendo con la ley de protección de datos personales (LPDP). El objetivo fue planteado en base a la revisión sistemática sobre factores causales de amenazas no intencionales internas (UIT, por sus siglas en inglés). La institución se verá

beneficiada con este objetivo debido a que se podrá prevenir la mayoría de los casos mediante medidas de contingencia a colaboradores que pasen por este tipo de eventos.

O 4. Proteger los activos digitales de la organización mediante una gestión de activos de Ciberseguridad.

Este objetivo busca la protección de activos digitales, los cuales son necesarios dentro de las actividades del personal interno, por lo tanto, su protección busca reducir la ocurrencia de amenazas no intencionales, en caso el empleado no pueda identificarlos de acuerdo con las medidas que propone el modelo.

O 5. Controlar los accesos y permisos de cada empleado de la organización.

El objetivo planteado busca no otorgar permisos a cualquier persona, ya que cada empleado de la organización maneja distintos accesos y permisos para el uso de los activos digitales, por lo tanto, el modelo propone medidas que permitan un adecuado control de accesos y permisos. Este objetivo permite que cualquier usuario con desconocimiento no pueda manipular o hacer uso de activos o información que no le corresponde evitando posibles problemas internos de seguridad.

O 6. Mejorar la usabilidad del Sistema de Información para reducir la probabilidad de errores humanos.

El objetivo propuesto se debe a la interacción humano computador, en la cual una usabilidad inadecuada puede generar errores por parte del colaborador que a su vez pueden ocasionar posibles amenazas no intencionales de ciberseguridad. Si se mejora la usabilidad de los sistemas de software donde interactúan los usuarios eso beneficiara a la reducción de amenazas.

b) **Métricas por Objetivo**

Métricas por Objetivo		Unidad de medida	Propósito de métrica	Mecanismo para medir la métrica	Frecuencia de medición	Responsable de la medición
Objetivos	**Objetivo 1 - Objetivo 2**					
	M1. Test de Ingeniería Social a los colaboradores	Resultados esperados por cada área a nivel cuantitativo	Identificar los colaboradores con resultados desaprobatorios y	Evaluación realizada por medio del área de TI	Mensual	Área de TI/ RRHH

		las causas de dichos resultados			
M2. Cursos a manera de evaluación y capacitación sobre Ciberseguridad	Nota cuantitativa esperada por cada área	Evaluar si el colaborador ha aprobado los cursos y capacitaciones de manera satisfactoria	Evaluación digital realizado por una consultoría o TI	Mensual	Área de TI o consultoría
Objetivo 3					
M3. Evaluaciones psicológicas de los empleados	Resultados cualitativos de la evaluación	Conocer el comportamiento de los colaboradores y posibles factores que puedan afectar su trabajo habitual	Evaluación digital realizado por un especialista de gestión humana o psicólogo	Mensual	Área de RRHH
M4. Evaluaciones del nivel de satisfacción dentro de la organización	Resultados cualitativos en la escala de Likert	Conocer el nivel de satisfacción del empleado al trabajar en la organización	Encuestas realizadas por el área de RRHH	Mensual	Área de RRHH
Objetivo 4					
M5. Número de incidentes de seguridad relacionado con la pérdida, eliminación, corrupción de activos digitales	Número de incidentes de seguridad agrupado por áreas	Identificar las áreas con mayor número de incidentes de seguridad y averiguar las causas	Registros por medio de mesa de ayuda	Diario	Mesa de ayuda
M6. Reporte de incumplimiento de las políticas de seguridad de la información relacionado a la gestión de activos digitales	Número de incidentes por incumplimiento agrupado por áreas	Identificar las áreas con mayor número de incumplimientos de políticas y averiguar las causas	Registros por medio de mesa de ayuda	Diario	Mesa de ayuda
Objetivo 5					
M7. Número de casos por detección de accesos no autorizados	Número de casos reportados por área	Identificar las áreas con mayor número casos donde se detecte accesos no autorizados debido a una falta de control sobre los permisos de los empleados	Registros por medio de mesa de ayuda	Diario	Mesa de ayuda

	M8. Número de estaciones de trabajo que implemente la detección y registro automático de los accesos respecto al total de estaciones de trabajo	Número de estaciones de trabajo con la implementación automática	Identificar si las estaciones cumplen con la detección y registro automático de cada usuario	Sistema de detección y registro de usuarios	Diario	Áreas de TI
	Objetivo 6					
	M9. Nivel de usabilidad de los softwares de la organización	Nivel de satisfacción del usuario medido en la "Escala de Sistemas de Usabilidad" con un nivel mínimo de aceptación del 78%	Identificar qué softwares tienen un nivel bajo de satisfacción en cuanto a usabilidad	Sistema de escalas de usabilidad	Quincena	Área de TI
	M10. Número de Incidentes en el uso de Sistemas de Información de la Organización	Número de incidentes producidos	Identificar los Sistemas de Información con mayor número de incidentes por usabilidad que requieran una modificación o corrección	Registros por medio de mesa de ayuda	Diario	Mesa de ayuda

Los objetivos tienen tiene 2 validaciones. La primera validación fue realizada por la profesora Melissa K. Chinyemba, la cual forma parte de la Universidad de Zambia, África. La segunda validación fue realizada por la oficial de Seguridad de Información, Jennifer Ayllón, quien es especialista en CyberSecurity & Tecnologías del Ministerio de Trabajo y Promoción del Empleo (MTPE).

5.2.2 Patrones de comportamiento

El diseño de los patrones de comportamiento se ha definido mediante la revisión sistemática previamente desarrollada, los cuales están construidos en base a un conjunto de factores que, agrupados de diferentes maneras, pueden permitir que ciertas amenazas, relacionadas a dichas causas, se hagan efectivas (CERT, 2013) (Greitzer et al., 2014).

La elaboración del diseño está conformada por tres etapas. La primera es la selección e identificación de factores involucrados con el personal interno tanto en sus actividades como en su comportamiento, la segunda es la selección de incidentes o amenazas internas no intencionales (UIT) y la última etapa es la asociación de los factores con las

amenazas UIT. Esta asociación define cada uno de los patrones de comportamiento que serán detallados en el siguiente capítulo, el cual forma parte del Objetivo Específico 1 (OE1).

a) Identificación de factores

De acuerdo con la revisión sistemática, existen investigaciones que demuestran una relación muy estrecha entre ciertos factores que contribuyen a la identificación de UIT. Estos factores principalmente están enfocados en el error humano; sin embargo, la vista actual del error humano involucra no solo factores causales próximos sino también factores causales distales, aquellos que van más profundo y sobre el error humano. A continuación, se presenta el conjunto de factores agrupados en base a ciertas relaciones que contribuyen a la identificación de las UIT dentro de las organizaciones (CERT, 2013).

1. Factores Organizacionales Generales

1.1. Requerimientos de procesos de negocio (BPR)

Los requerimientos de procesos de negocio son las actividades habituales que forman parte de los procesos de una organización para cumplir con los objetivos de negocio. Estos procesos son fundamentales y más cuando los procesos dependen de un sistema. Los sistemas que se encargan de ejecutar los procesos deben cumplir con ciertas medidas de seguridad y debe ser de fácil entendimiento para los usuarios, de lo contrario se vuelven factores causales de una posible UIT.

Posibles causas de una UIT:

- Las medidas de seguridad son confusas y poco útil
- Los sistemas son difíciles de entender

1.2. Flujo de datos

La información que maneja una organización está constituida por un conjunto de datos de distintas características. El flujo de datos dentro de la organización es fundamental como parte de los procedimientos dentro de la organización, por lo tanto, el tener inadecuados procedimientos y falta de comunicación para el flujo de datos son posibles causales de una UIT (CERT, 2013).

Posibles causas de una UIT:

- Inadecuados procedimientos

- Escasa comunicación

1.3. Escenario de trabajo

Los escenarios de trabajo son como el ambiente que involucra distintos elementos que forman parte del trabajo habitual del empleado. Estos elementos pertenecen a un ambiente determinado y pueden presentar problemas de gestión, uso adecuado o malas prácticas asociadas al usuario como consecuencia del escenario (CERT, 2013).

Posibles causas de una UIT:

- Distracciones
- Recursos insuficientes
- Sistemas de gestión deficientes
- Inadecuadas prácticas de seguridad
- Contraseñas débiles

1.4. Planificación/Control del trabajo

Como parte de los procesos de negocio, los procedimientos y actividades entre las distintas áreas deben seguir un plan de trabajo y control al mismo tiempo para mantener las actividades alineadas con los objetivos de cada área y de la empresa. Si no se sigue un plan de trabajo y menos un control en las actividades diarias esto puede ser fuentes de incidentes o amenazas de UIT (CERT, 2013).

Posibles causas de una UIT:

- Estrés laboral
- Presión en los tiempos
- Dificultad en las tareas
- Falta de conocimiento o habilidad
- Cambios en la rutina relacionados a trabajo remoto sin considerar controles de seguridad.
- Prácticas de planeamiento y control del trabajo deficientes
- Falta de educación antiphishing.
- Herramientas antiphishing poco útiles ante sitios web maliciosos

2. Factores Humanos

2.1. Fatiga o somnolencia

La fatiga o somnolencia afecta directamente el desempeño humano según estudios. Existe una relación inversa entre el rendimiento y la somnolencia (Gander, 2002). Las causas de la fatiga o somnolencia en los trabajadores muchas veces se deben a cambios de turno, trabajo de noche o exceso de horas laborales, las cuales genera una mayor tasa de ocurrencia de errores humanos (CERT, 2013).

2.2. Carga de trabajo mental

La carga de trabajo mental es la sensación de estar cognitivamente cansado por la experiencia de trabajo. Esta carga tiene una estrecha relación, según estudios (Yerkes, 1908), con el error humano que depende del rendimiento, que muchas veces llega a su límite y luego desciende, por eso es importante mantener un balance entre el estrés y la carga laboral (CERT, 2013).

2.3. Falta de conciencia de la situación (SA)

De acuerdo con Endsley, la situación de conciencia es "la percepción de los elementos en el entorno dentro de un volumen de tiempo y espacio, la comprensión de su significado y la proyección de su situación en un futuro próximo" (Endsley 1995), esto nos dice que ante una falta de percepción se pierde reconocimiento del entorno y sus elementos, los cuales pueden generar error humano. Se espera que esta conciencia se vaya desarrollando dentro de una organización a través de la experiencia y la enseñanza.

2.4. Mente distraída

Una mente distraída o errante se define como la pérdida de la atención mientras se realiza una actividad (Smallwood, 2006). Esto se puede deber a un conjunto de pensamientos por lo que pasa el empleado al momento de hacer una actividad. Estos pensamientos no necesariamente están involucrando con la tarea realizada (James, 1892). Como consecuencia de eso, es posible la ocurrencia de una UIT y más si son procesos que están en constante actividad donde se necesita la mayor concentración (ej. Búsqueda de

información en un sistema, actualización de datos, registro de información en un sistema, etc.)

2.5. Sesgos cognitivos

Son factores que involucran ciertas diferencias o falta de características necesarias para realizar las actividades con normalidad. Entre estos sesgos cognitivos podemos encontrar una percepción errónea de las cosas, falta de memoria, juicio crítico, etc. Estos sesgos reducen el rendimiento y aumentan la tasa de error humano (CERT, 2013).

3. Factores Socioculturales y Psicológicos

3.1. Cultura

La cultura organizacional es importante para que los colaboradores pueden estar alineados con las políticas y formas de trabajo. La convivencia laboral es importante que pueda ser entendida por todos, esta cultura organizacional si está bien definida, permite buscar en cada colaborador una tolerancia al riesgo, comprender los valores de la organización, participación continua dentro de la organización y comportamientos adecuados; sin embargo, si no existe una cultura dentro de la organización, esto da libertad al empleado a tomar decisiones que no estén alineadas con la organización y pueda ser causal de riesgo y amenazas UIT (Boholm, 2003; Douglas, 1992).

3.2. Estado de ánimo

De acuerdo con estudios, el estado de ánimo de una persona frente a sus actividades tiene una estrecha relación con la decisión de tomar riesgos. A pesar de que existen distintos estudios sobre un estado de ánimo negativo, positivo o neutral, se debe considerar que cada estado de ánimo en un empleado puede ser una decisión distinta frente a un riesgo, por lo cual es necesario monitorear este tipo de estados. El tomar riesgos puede ser positivo o negativo dependerá si existe un objetivo positivo o simplemente una acción descontrolada y sin pensar que puede generar una UIT (CERT, 2013).

3.3. Edad

La edad es un factor importante dentro de la ocurrencia de una UIT, debido a distintos estudios, se sabe que los jóvenes tienen una percepción menor de los riesgos que una persona mayor (Ivers, 2009). Sin embargo, este factor también se ve afectado por el entorno en el que la persona vive o interactúa, ya que la percepción del riesgo puede variar. Una posible causa para generar una UIT es que los jóvenes al estar más expuesto e interactuar más con las tecnologías es más susceptible al phishing que una persona mayor que no utiliza tanto la tecnología.

3.4. **Influencia de Drogas/Hormonas/Enfermedades**

La influencia de drogas u hormonas es un factor principal en la ocurrencia de UIT, debido a que puede afectar negativamente las habilidades cognitivas, así como también reducir la productividad y tener menos cuidado al tomar riesgos que posiblemente no esté consciente de haberlo tomado (CERT, 2013).

b) Selección de amenazas no intencionales internas (UIT)

De acuerdo con la revisión sistemática realizada, se identificaron cuatro tipos de vectores de amenazas no intencionales (UIT threat vectors) en base a un conjunto de incidentes recolectados (CERT, 2013; Greitzer et al., 2014).

- **DISC**

  Este tipo de amenaza también se conoce como divulgación accidental, debido a que sube o publica información sensible de forma accidental a un sitio web, también se presenta en envío de información por correo electrónico, fax o vía internet (CERT, 2013).

  Incidentes asociados a DISC (J. Carlton Collins, 2019)**:**

  - Enviar información sensible por correo o fax accidentalmente
  - Divulgación de datos a través de internet, social media, cloud o móviles

- **UIT-HACK**

  Este tipo de amenazas también se conoce como código malicioso, el cual es considerado como un medio electrónico de entrada externo producto de ingeniería social (ej. ataque de phishing vía correo, drive USB no autorizado), el cual es ejecutado vía software, como un malware o spyware. A diferencia de los otros tipos de amenaza, este tipo en

particular necesita de agentes externos para que ocurra el incidente. La interacción entre un agente externo que puede motivar la acción o simplemente el descuido de un agente interno para ejecutarse dentro de la organización (CERT, 2013).

Dentro de este tipo de amenaza, se definen tres patrones principales de incidentes:

Incidentes asociados a UIT-HACK (ENISA, 2008; J. Carlton Collins, 2019)**:**

- Acceso no autorizado
- Robo de ID/Phishing
- Aplicaciones maliciosas/Malware (Ataques de spyware, rasomware, troyano, gusano, etc.)
- Ingeniería social

- **PHYS**

  Este tipo de amenaza está relacionado con la pérdida accidental o incorrecta de registros físicos, ya sea por pérdida, robo o eliminación como por ejemplo documentos en papel. A pesar de que son medios físicos, si involucran información para acceder a los medios digitales se puede considerar como una amenaza de UIT (CERT, 2013).

  Incidentes asociados a DISC (ENISA, 2008; J. Carlton Collins, 2019):

  - Información sensible física en escritorios o lugares inseguros
  - Eliminación de información sensible de forma incorrecta
  - Pérdida de información sensible

- **PORT**

  Este tipo de amenaza está relacionado con la pérdida de un equipo portable que se tiene en posesión. Esta pérdida, robo o descarte de dispositivos que almacenan datos ya sea una laptop, PDA, teléfonos inteligentes, dispositivos de memoria portátil, CD, disco duro, etc. (CERT, 2013).

  Incidentes asociados a PORT (ENISA, 2008; J. Carlton Collins, 2019):

  - Uso no autorizado de los recursos
  - Robo de equipos portables
  - Pérdida de equipos portables

- Robo de unidades de respaldo

c) Asociación de factores con UIT

La asociación de los factores y amenazas no intencionales internas de Ciberseguridad están relacionadas mediante una causa efecto que permite la ocurrencia de dichas amenazas. En esta sección se pretende mostrar cómo estará estructurado esta asociación con todos los factores y amenazas identificadas con la finalidad de establecer los patrones de comportamiento. En el siguiente capítulo se procederá a describir cada uno de ellos de acuerdo a las asociaciones encontradas.

	Tipo de Amenazas	UIT-HACK				DISC		PHYS		PORT		
		Robo de ID/Acceso no autorizado	Phishing	Aplicaciones maliciosas/ Malware	Ingeniería Social	Enviar información sensible por correo o fax accidentalmente	Divulgación de datos a través de internet, social media, cloud o móviles	Información sensible física en escritorios o lugares inseguros	Eliminación de información sensible de forma incorrecta	Robo de equipos portables	Perdida de equipos portables	Robo de unidades de respaldo
Factores Causales	**Factores Organizacionales generales**											
	Requerimientos de proceso de negocio (BPR)											
	Flujo de datos											
	Escenario de trabajo											
	Planificación/Control del trabajo											
	Factores Humanos											
	Fatiga o somnolencia											
	Carga de trabajo mental											
	Falta de conciencia de la situación (SA)											
	Mente distraída											
	Sesgos cognitivos											
	Factores Psicosociales, Socioculturales y otros											
	Cultura											
	Estado de animo											
	Edad											
	Influencia de Drogas/Hormonas/Enfermedades											

Figura 10: Matriz de Trazabilidad (Autoría Propia)

Los patrones de comportamiento mencionados tienen 2 validaciones. La primera validación fue realizada por la profesora Melissa K. Chinyemba, la cual forma parte de la Universidad de Zambia, África. La segunda validación fue realizada por la oficial de Seguridad de Información, Jennifer Ayllón, quien es especialista en CyberSecurity & Tecnologías del Ministerio de Trabajo y Promoción del Empleo (MTPE).

5.2.3 Matriz de gestión de riesgos

La matriz de gestión de riesgos forma parte de los componentes del modelo y es una herramienta que está basada en la gestión de riesgos de acuerdo con la norma ISO/IEC 31000:2018. La función de esta matriz es poder identificar y medir el impacto de los riesgos en base a la probabilidad de ocurrencia de ciertas amenazas no intencionales de Ciberseguridad (UIT), amenazas que se han identificado previamente en base a los patrones de comportamiento definidos en el capítulo siguiente. Otra de las funciones

principales de la matriz es poder proponer medidas que puedan reducir el impacto de estos riesgos para lograr los objetivos propuestos por el modelo.

La construcción de la matriz inicia con la definición de los procesos, activos involucrados, vulnerabilidades relacionadas a los activos y las amenazas en consecuencia de estas vulnerabilidades. Todos estos pasos permiten identificar los riesgos, su impacto, probabilidad de ocurrencia y finalmente proponer medidas de tratamiento como se ve en la Figura 11.

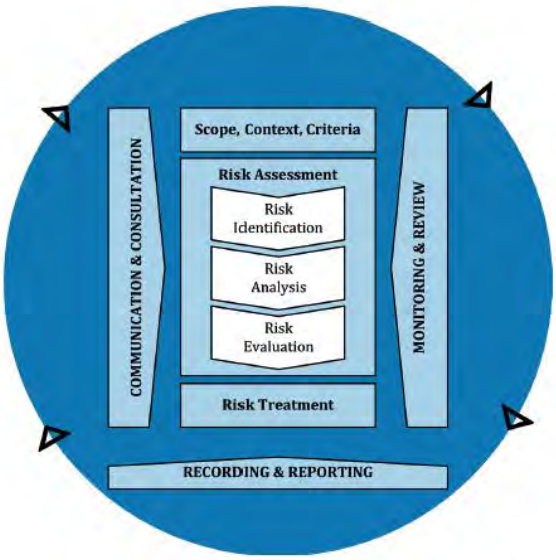


Figura 11: Proceso de la gestión de riesgos (ISO/IEC 31000:2018)

5.2.3.1 Definición de los procesos relacionados a TI

Los procesos relacionados a TI son bienes importantes de la organización que permiten la continuidad del negocio y sus actividades. Estos procesos al ser un valor importante de la organización deben ser protegidos y definidos adecuadamente. El soporte de estos procesos está a cargo de los recursos tecnológicos y humanos. Acorde con la norma ISO/IEC 27005:2018 un proceso de negocio o TI también se considera un activo o bien primario que deberá ser respaldado por otros activos o también considerados activos de apoyo. Estos procesos o actividades son los más apropiados para definir una política de seguridad de la información o plan de continuidad del negocio.

Entre los principales tipos de procesos que existen acorde con norma ISO/IEC 27005:2018 se tiene los siguientes:

- Procesos cuya pérdida o degradación imposibilite el cumplimiento de la misión de la organización

- Procesos que contienen procesos privados o procesos que involucran tecnología patentada por la misma organización
- Procesos cuya modificación, pueden afectar en gran medida el cumplimiento de la misión de la organización
- Procesos que son necesarios para que la organización cumpla con los contratos aplicables, requisitos legales o reglamentarios identificados como parte de la organización.

Acorde con las buenas prácticas de ITIL v4 relacionado a las Tecnologías de Información (TI) se definen distintos procesos en la **Tabla 12**. Los procesos, si bien forman parte de las buenas prácticas de ITIL, deben ser validados por un especialista con el fin de alinearse con escenarios reales e incluso considerar otros procesos que estén alineados con el marco.

Tabla 12: Procesos de TI (según ITIL v4)

Procesos de TI	Descripción
Gestión estratégica de los servicios TI	Asegura que la estrategia de TI este definida, actualizada y logre su propósito.
Gestión de la demanda	El proceso busca adaptar el suministro a la demanda con la finalidad de predecir la demanda y regularla.
Gestión de la cartera de servicio	Proceso que describe los servicios de un proveedor en términos de valor para la organización. Este proceso es utilizado para gobernar inversiones en gestión del servicio a través de la empresa en terminas de valor financiero.
Gestión financiera de los servicios TI	Proceso que busca asegurar los fondos para la entrega y consumo de servicios. Este proceso es responsable por gestionar el presupuesto, la contabilidad y la asignación de costos, también cuantifica el valor que los servicios de TI generan en la organización.
Gestión del catálogo del servicio	Gestiona la información contenida en el catálogo de servicios y asegura que sea completa y brinde los detalles, estados, interfaces y dependencias de todos los servicios. Este proceso debe estar en constante actualización.
Gestión del nivel de servicio	Proceso encargado de definir, documentar, acordar, monitorear, medir y reportar los niveles de servicio de TI. El proceso se encarga de mejorar y establecer una comunicación con el negocio y los clientes con la finalidad de evitar ambigüedades del nivel de servicio que se brinda.
Gestión de la disponibilidad	Enfocado en la calidad del servicio para el cliente. Este proceso debe estar definido también por parte del proveedor para fidelización de los clientes.
Gestión de la continuidad del servicio TI	Está relacionado al proceso de gestión de continuidad de la organización, asegurando que la infraestructura y servicio de TI pueden ser restablecidos en los plazos solicitados
Gestión de la seguridad de información	Proceso encargado de la disponibilidad, confidencialidad, integridad e autenticidad de la información. Parte del proceso consiste en disponer de información útil en el momento que se requiera y resistir a ataques. Además, debe gestionar quienes pueden acceder a la información con los derechos respectivos y finalmente la información debe estar completa, exacta y protegida.
Gestión de cambios	Proceso que busca responder a los requerimientos del cliente y mantener al mismo tiempo una reducción de incidentes y doble trabajo.

Gestión de activos y configuración del servicio	Proceso encargado de optimizar el desempeño de los activos y la configuración del servicio con la finalidad de optimizar costos y riesgos causados por activos mal gestionados o innecesarios
Gestión de entrega y despliegue	Proceso enfocado en tener planes de liberación, despliegues claros. Las versiones desarrolladas deben ser construidas, instaladas, probadas y desplegadas de forma eficiente, y ante nuevo servicio o cambio se debe cumplir con los requerimientos acordados.
Validación y prueba del servicio	Las pruebas de los servicios permiten que se cumpla con el propósito del servicio y debe permitir asegurar su uso. Esto implica tanto para servicios antiguos como para los nuevos.
Evaluación del cambio	Proceso encargado de evaluar el desempeño ante un cambio en el servicio ante algún impacto en el negocio, servicios existentes y la infraestructura de TI
Gestión del conocimiento	Proceso encargado de recolectar, analizar, almacenar y compartir conocimiento e información dentro de la organización.
Proceso de operación	Dentro de los procesos de operación se tiene los siguientes: o Atención de solicitudes o Gestión de incidentes o Gestión de problemas o Gestión de accesos

5.2.3.2 Definición de los activos de información involucrados

Los activos de información son todo aquellos datos o información en formato físico o digital que brinda valor para la organización (ISO/IEC 27005:2018). Acorde con la norma ISO 27005, los activos pueden clasificarse en activos primarios y activos de soporte. Sin embargo; si hablamos de activos de información específicamente, se puede dividir en los siguientes:

- **Información**

  Considerado como uno de los activos primarios que comprende principalmente

  - Información vital para el negocio y el cumplimiento de la misión de la organización
  - Información personal cumpliendo con las leyes de protección de datos
  - Información estratégica para alcanzar los objetivos
  - Información de mucho valor que requiere un procesamiento, almacenamiento y transmisión adecuada

- **Hardware**

  Elementos físicos que dan soporte y ejecución de los procesos de negocio

Dentro de este tipo de activo se tiene principalmente los siguientes:

- Equipos de procesamiento de datos
- Equipos informáticos portátiles como laptops, asistente personal digital (PDA), teléfonos portátiles de la organización, etc.
- Equipos informáticos fijos como servidores, ordenadores fijos utilizados como estación de trabajo
- Periféricos de procesamiento como impresoras, discos extraíbles
- Medios electrónicos que pueden conectarse a la computadora para almacenamiento de datos a pesar de su tamaño como disquetes, CD ROM, USB, disco duro, llave de memoria, etc.
- Otros medios como papeles, fax, documentación.

- **Software**

  Tipo de activo que involucra todos los programas necesarios para el funcionamiento de un conjunto de procedimientos que junto con el hardware cumplen la función de apoyar los procesos de negocio y TI.

  Entre los principales tipos de software se tiene los siguientes:

  - Sistema Operativo

    Incluye todos los programas de una computadora que forman la base desde donde se ejecutan los demás programas como servicios y aplicaciones. Los principales elementos del sistema operativo son todos los servicios de administración de equipos (CPU, memoria, disco y red), así como servicios de gestión de tareas y de derecho de usuarios
  - Software de servicio, mantenimiento o administración

    Son aquellos softwares que complementan los servicios del sistema operativos y forman parte de los sistemas de información; sin embargo, no son utilizados directamente por el usuario.
  - Paquetes de software

    Productos comercializados diseñados para tareas específicas, las cuales brindan servicios para los usuarios y aplicaciones como por ejemplo los softwares de gestión de base de datos, software de mensajería electrónica, software de servidor web, etc.
  - Aplicaciones de negocio

Dentro de las aplicaciones de negocio existen dos tipos principales, las aplicaciones empresariales estándar y las aplicaciones empresariales específicas. Con una gran cantidad de aplicaciones al servicio del usuario existen softwares de cuentas, control de máquinas, atención al cliente, gestión de facturas de clientes para un negocio específico, etc.

- **Network**

  Este activo agrupa todos los dispositivos de telecomunicación utilizados para interconectar varias computadoras físicas que se encuentran separadas o elementos de un sistema de información.

  - Medios y soporte

    Equipos y medios de comunicación y telecomunicación que están enfocadas en las características físicas y técnicas de los equipos que permiten la comunicación a un nivel de red o enlace que utiliza ciertos protocolos para la comunicación. Estos pueden ser redes telefónicas, ethernet, bluetooth, especificaciones de protocolo inalámbrico como la red wifi, etc.

  - Interruptores controlados activos o pasivos

    Dispositivos de comunicación intermedio no lógicos con funciones de enrutamiento y filtros al momento de enviar información por los canales de comunicación mencionados anteriormente. Estos activos pueden ser routers, switches, hubs, etc.

  - Interfaz de comunicación

    Interfaces de comunicación de las unidades de procesamiento como por ejemplo servicio general de radio por paquetes (GPRS), adaptador Ethernet.

5.2.3.3 Identificación de vulnerabilidades

Una vulnerabilidad es una brecha que puede ser explotada por una o varias amenazas con el fin de dañar activos o la organización. Acorde con la normativa ISO/IEC 27005:2018, las vulnerabilidades se pueden identificar en distintas áreas como las que se presentan a continuación:

- Organización
- Procesos y procedimientos
- Personal

- Entorno físico
- Configuración de sistemas de información
- Hardware, software y equipos de comunicación
- Dependencia de terceros

Como parte del desarrollo de la matriz de gestión de riesgos, es necesario identificar qué vulnerabilidades pueden afectar los activos de información de la organización. Los cuales brindan soporte y funcionamiento a los procesos de negocio y de TI. De acuerdo con la norma ISO/IEC 27005:2018 y en relación con los activos definidos en el acápite anterior se presentan las siguientes vulnerabilidades:

Tabla 13: Ejemplo de vulnerabilidades (ISO/IEC 27005:2018)

Tipo	Vulnerabilidad
Hardware	Mantenimiento insuficiente / instalación defectuosa de medios de almacenamiento
	Susceptibilidad a la humedad, polvo, suciedad.
	Sensibilidad a la radiación electromagnética.
	Falta de control de cambios de configuración eficiente
	Susceptibilidad a variaciones de voltaje
	Susceptibilidad a las variaciones de temperatura.
	Almacenamiento sin protección
	Falta de control en las copias de documentos o información
Software	Pruebas de software insuficientes o nulas
	Defectos conocidos en el software
	No "cerrar sesión" al salir de la estación de trabajo
	Eliminación o reutilización de medios de almacenamiento de forma inadecuada
	Falta de tareas de auditoría
	Asignación incorrecta del derecho de acceso
	Software ampliamente distribuido
	Interfaz de usuario complicada o poco usable
	Falta de documentación
	Configuración incorrecta de parámetros
	Fechas incorrectas
	Falta de mecanismos de identificación y autenticación como la autenticación de usuarios.
	Tablas de contraseñas desprotegidas
	Mala gestión de contraseñas
	Servicios innecesarios habilitados
	Software nuevo o recién en pruebas de desarrollo
	Especificaciones poco claras o incompletas para desarrolladores

	Ausencia de un control de cambios efectivo
	Descarga y usos incontrolados de software
	Falta de copias de seguridad
	Falta de protección física del edificio, puertas y ventanas
	No producir informes de gestión
Network	Falta de prueba al enviar o recibir un mensaje
	Líneas de comunicación desprotegidas
	Tráfico sensible no protegido
	Cableado de unión deficiente
	Punto único de falla
	Falta de identificación y autenticación del remitente y receptor en el envío de correos
	Arquitectura de red insegura
	Transferencia de contraseñas en claro
	Gestión de red inadecuada (resistencia de enrutamiento)

5.2.3.4 Identificación de amenazas no intencionales (UIT)

Acorde con la norma ISO/IEC 27005:2018, una amenaza tiene el potencial de dañar los activos de la organización como son los procesos, información y sistemas. Las amenazas pueden ser clasificadas por su origen, ya sea natural o humano, y también por su intención, accidentales o intencionales. Estas amenazas pueden originarse tanto dentro como fuera de la organización y es posible poder identificarlas y agruparlas para los respectivos controles medidas.

La recopilación de amenazas y la medición del impacto dentro de la organización depende del juicio experto por parte de los especialistas e incidentes previos que sirven para la recopilación de información. En el caso de las amenazas no intencionales de Ciberseguridad (UIT), tienen un origen humano y accidental debido a que existen un agente que sin conocimiento o sin intención permite que esta amenaza se haga efectiva dentro de la organización.

Las amenazas pueden estar dirigidas a uno o más activos dentro de la organización. De acuerdo a la norma ISO/IEC 27005:2018 podemos clasificarlas en tres tipos:

- D (Deliberada)
- A (Accidental)
- E (Ambiental)

Para esta sección, se clasificará y listará las amenazas asociadas a los patrones de comportamiento de acuerdo al formato presentado en la norma ISO/IEC 27005:2018.

Tabla 14: Definición de las UIT asociadas a los patrones de comportamiento (ISO/IEC 27005:2018)

Tipo	Amenaza	Origen
Compromiso de funciones	Robo de ID/Acceso no autorizado	Accidental Deliberada
Acciones no autorizadas	Phishing	Deliberada
	Aplicaciones maliciosas/Malware (Spyware, Rasomware, Gusanos, Troyanos, etc.)	
	Ingeniería Social	
	Uso de software falsificado o copiado	
Compromiso de información	Enviar información sensible por correo o fax accidentalmente	Accidental
	Divulgación de datos a través de internet, social media, cloud o móviles	Accidental Deliberada
	Información sensible física en escritorios o lugares inseguros	Accidental
	Eliminación de información sensible de forma incorrecta	Accidental Deliberada
	Robo de equipos portables	Deliberada
	Perdida de equipos portables	Accidental
	Robo de unidades de respaldo	Deliberada
	Manipulación de software	Accidental
Fallas Técnicas	Mal funcionamiento del software	Accidental
	Incumplimiento de la mantenibilidad del sistema de información	Accidental Deliberado

5.2.3.5 Identificación de riesgos, medición del impacto y probabilidad de ocurrencia

Siguiendo el enfoque de la norma ISO 31000:2018 relacionado a la gestión de riesgos, se hará uso de una matriz de gestión de riesgos que permita identificar los riesgos de una organización en base a las amenazas no intencionales de Ciberseguridad que involucran no solo los factores causales o de comportamiento por parte del empleado sino también las vulnerabilidades de los activos de la organización. Estos activos se ven involucrados en varios procesos de TI que fueron definidos previamente, por lo cual, el procedimiento de análisis de riesgos será presentado a través de una matriz que parte desde el proceso de TI hasta la amenaza involucrada con el fin de medir su impacto en la organización y la probabilidad de ocurrencia.

Para la forma de evaluación se considera un nivel de riesgo que indicará si el riesgo es Bajo, Medio, Alto o Muy Alto. Estos niveles serán el resultado del análisis y serán representados por un color especifico como se muestra a continuación:

Tabla 15: Nivel de Riesgo (Autoría Propia)

Min	Max	Nivel de Riesgo
1	2	**Bajo**
3	6	**Medio**
8	10	**Alto**
12	16	**Muy Alto**

Al igual que el nivel de riesgo, debemos definir la escala de evaluación para el impacto y la probabilidad de ocurrencia con la finalidad de calcular el riesgo presentado.

a) Medición del impacto del riesgo

El impacto del riesgo se hará en una escala del 1 al 4 como se muestra a continuación:

Tabla 16: Escala de calificación para medir el impacto del riesgo (Autoría Propia)

Calificación	Nivel de Impacto	Descripción
1	**Bajo**	Ocasiona retrasos de menos de 24 horas en los servicios de TI y sus activos
2	**Medio**	Ocasiona retrasos de menos de 2 días en los servicios de TI y sus activos
3	**Alto**	Genera un impacto en los servicios de TI y activos críticos de la organización
4	**Muy Alto**	Genera un impacto alto al detener el funcionamiento del negocio y los servicios de TI

b) Probabilidad de ocurrencia

La probabilidad de ocurrencia del riesgo se hará en una escala del 1 al 4 como se muestra a continuación:

Tabla 17: Escala de calificación para medir la probabilidad de ocurrencia del riesgo (Autoría Propia)

Calificación	Nivel de Probabilidad	Descripción
1	**Bajo**	Sucede una vez al año
2	**Medio**	Sucede múltiples veces al año
3	**Alto**	Puede suceder una vez cada mes
4	**Muy Alto**	Puede suceder al menos una vez a la semana

c) Impacto en función de la confidencialidad, integridad y disponibilidad de la información (CIA)

El impacto en función de las características de la información que pueda verse afectado será mencionado de forma cualitativa para reforzar los controles y propuesta de tratamiento de riesgos. Al igual que el impacto del riesgo se

utilizará definiciones como Bajo, Medio, Alto y Muy Alto dependiendo de cada caso.

d) **Identificación y análisis de riesgo – MANIC**

Una vez que se define la forma de evaluación de cada riesgo, se procede con la elaboración de la matriz de gestión de riesgos que se muestra en la **Tabla 18**.

5.2.3.6 Tratamiento de los riesgos (Controles)

Siguiendo el enfoque de la norma ISO 31000:2018 relacionado a la gestión de riesgos, es necesario decidir cómo tratar cada uno de los riesgos específicamente, para eso primero se debe identificar y evaluar los riesgos. En segundo lugar, debemos decidir qué tipo de tratamiento se debe tomar por cada riesgo identificado.

Dentro de los tipos u opciones de tratamiento de riesgo se tienen los siguientes:

- Eliminar la actividad, proceso o activo digital que involucra el riesgo.
- Transferir el riesgo a un tercero u otra área de la organización que pueda encargarse del riesgo.
- Mitigar el riesgo a través de controles propios.
- Tolerar o aceptar el riesgo identificado.

Como parte de una gestión de riesgos, para este proyecto, se buscará proponer controles de mitigación de los riesgos y amenazas identificadas en la matriz de gestión de riesgos. Los controles que propone tienen como objetivo principal reducir los riesgos que parten de un estado inherente, propio de las operaciones y procesos de la organización, a un estado residual, producto de aplicar todas las medidas posibles para reducir o eliminar el riesgo identificado.

Dentro de la tipología básica de controles se tienen los siguientes tipos:

- **Controles preventivos**

  Controles que buscan reducir las vulnerabilidades

- **Controles detectivos**

  Controles que buscan descubrir las amenazas o los escenarios con anticipación para poder activar otros controles
- **Controles correctivos**

  Controles que se activan para reducir o contrarrestar el impacto de la ocurrencia de una amenaza
- **Controles disuasivos**

Controles que buscan reducir la probabilidad de ocurrencia de una amenaza

- **Controles compensatorios**

  Controles que buscan contribuir en la reducción del riesgo hasta niveles aceptables

Los controles propuestos en la **Tabla 18** buscan reducir el riesgo y serán justificados y apoyados con medidas asociadas a los escenarios y a los factores causales generados por el personal que fueron identificados en los patrones de comportamiento.

Tabla 18: Matriz de Gestión de Riesgos (Autoría propia)

ID	Procesos de TI	Recurso Afectado (Activos)	Vulnerabilidad	Descripción de la Amenaza	RIESGO INHERENTE					Controles existentes		Descripción del control y justificación	RIESGO RESIDUAL			
					I	P	Total	Nivel	Impacto en la Información (CIA)	I	P		I	P	Total	Nivel
1	Proceso de operación	Software de servicio, mantenimiento o administración	Asignación incorrecta del derecho de acceso	Robo de ID/Acceso no autorizado	4	2	8	Alto	**ALTO.** Debido a la administración de acceso que permiten acceder a la información de la organización	4	2	**Imponer el registro detallado para acceso o cambios en datos sensibles:** Control correctivo y preventivo que ayuda a reducir el impacto de una robo de identidad o acceso no autorizado debido al registro de cambios del usuario que sufrió el incidente **Proteger la información mediante lista de control de acceso:** Control correctivo y preventivo que verifica los accesos en cada proceso o actividad del usuario una vez que ingreso al sistema **Mejorar la conciencia de las amenazas internas y las amenazas internas involuntarias:** Control preventivo para reducir el error humano creando conciencia en las acciones realizadas como parte de los procesos que realiza y la cultura organizacional alerta ante amenazas de Ciberseguridad **Mejorar la usabilidad del software para reducir la probabilidad de errores humanos inducidos por el sistema:** Control detectivo y preventivo ya que puede evitar que la amenaza se haga efectiva bloqueando el sistema en caso existe un descuido del colaborador o mandando alertas ante fallas de seguridad del sistema **Usar contraseñas cifradas o de complejidad alta:** Control preventivo que reduce la probabilidad de la amenaza protegiendo y aumentando el nivel de seguridad de las contraseñas	1	1	1	Bajo
			Tablas de contraseñas desprotegidas		4	1	4	Medio	**ALTO.** Debido a la administración de acceso que permiten acceder a la información de la organización	4	2		1	1	1	Bajo
		Equipos informáticos fijos como servidores, ordenadores fijos utilizados como estación de trabajo	No "cerrar sesión" al salir de la estación de trabajo		4	3	12	Muy Alto	**ALTO.** Debido a la administración de acceso que permiten acceder a la información de la organización	4	3		1	1	1	Bajo
		Equipos informáticos portátiles como laptops, asistente personal digital (PDA), teléfonos portátiles de la organización	Falta de control de seguridad en las copias de documentos o información almacenada en el equipo	Pérdida de equipos portables	4	2	8	Alto	**MUY ALTO.** Debido a que la información puede terminar en manos de personas con intenciones maliciosas o competidores	3	2	**Mantener la preparación de los empleados (prácticas que reducen el estrés y la ansiedad, la fatiga y el aburrimiento, etc.):** Control preventivo que permite reducir factores causales relacionados al estrés, distracción mental, sesgos cognitivos, etc. que puedan ocasionar un descuido por parte del empleado **Inculcar disciplina en el proceso para fomentar el seguimiento de políticas y pautas:** Control preventivo para reducir la pérdida de activos siguiendo buenas prácticas en el uso de los activos de la organización dentro y fuera del lugar de trabajo	2	1	2	Bajo
			Falta de control de seguridad en las copias de documentos o información almacenada en el equipo	Robo de equipos portables	4	3	12	Muy Alto	**MUY ALTO.** Debido a que la información puede terminar en manos de personas con intenciones maliciosas o competidores	3	1	**Llevar a cabo capacitación y concientización sobre la percepción del riesgo y los sesgos cognitivos que afectan la decisión:** Control preventivo encargado de evitar poner en riesgo los activos de la organización por parte del empleado mediante capacitación en su uso adecuado, respaldo de la información almacenado en el activo ante algún incidente o robo y el estado de alerta en cualquier momento	2	3	6	Medio
		Información de mucho valor que requiere un procesamiento, almacenamiento y transmisión adecuada	Líneas de comunicación desprotegidas	Phishing	4	3	12	Muy Alto	**ALTO.** Debido a que por medio de esta amenaza se puede acceder a cualquier información tanto personal como de la organización	4	3	**Mantener la preparación de los empleados (prácticas que reducen el estrés y la ansiedad, la fatiga, enfermedades etc.):** Control preventivo que permite reducir factores causales relacionados al estrés, distracción mental, sesgos cognitivos, etc. que puedan ocasionar un descuido por parte del empleado **Implementar una planificación y un control del trabajo efectivos para reducir la presión del trabajo, administrar los factores de tiempo, reducir la dificultad de la tarea, etc. :** Control preventivo y correctivo que ayuda en la reducción de carga laboral para evitar errores humanos mediante una correcta planificación y control del trabajo por parte de los empleados	1	1	1	Bajo

												Mejorar la conciencia de las amenazas internas y las amenazas internas involuntarias: Control preventivo y detectivo que ayuda en la identificación de amenazas para reforzar los conocimientos y estar alerta antes amenazas de Ciberseguridad **Reconocer el phishing y otros vectores de amenazas de las redes sociales mediante cursos aplicativos y test de ingeniería social:** Control preventivo que permite reconocer y evitar los ataques de phishing que puedan presentarse en los siguientes escenarios: **Aplicar políticas y buenas prácticas de seguridad para evitar el phishing:** Control preventivo que busca activar ciertos protocolos de seguridad cuando se ha identificado o no el phishing, como por ejemplo: - Ver mensajes inesperados con sospecha - Utilizar software anti-malware. - Conectarse a proveedores de servicios con firewalls. - Establecer opciones para evitar la instalación de software ejecutable en dispositivos móviles. - Tener cuidado con las conexiones inesperadas y las confirmaciones de actualización.				
			Arquitectura de red insegura	Divulgación de datos a través de internet, social media, cloud o móviles	2	4	8	Alto	**MEDIO.** Debido a que la mayor cantidad de información divulgada es del mismo colaborador; sin embargo, existe la posibilidad de compartir información crítica	2	2	**Llevar a cabo capacitación y concientización sobre la percepción del riesgo y los sesgos cognitivos que afectan la decisión:** Control preventivo encargado de evitar poner en riesgo los activos de la organización, en este caso la información, por parte del empleado mediante capacitación en su uso adecuado y comunicación por canales oficiales de la organización **Mejorar el flujo de datos mejorando la comunicación y manteniendo procedimientos precisos:** Control preventivo que permite tener canales de comunicación oficiales de acuerdo a los procedimientos para evitar la divulgación de información por medio de otros canales no oficiales **Mantener los valores y las actitudes del personal que se alinean con la misión y la ética de la organización a través de cursos de ética y trabajos de integración:** Control preventivo que busca generar un ambiente y cultura organizacional adecuada con la finalidad que marca los mismos interés de la organización en cada uno de los trabajadores **Deshabilitar el acceso inalámbrico en dispositivos si no se requiere** Deshabilite el acceso inalámbrico en dispositivos que no tienen un propósito de negocio para el acceso inalámbrico.	1	3	3	Medio
		Medios electrónicos que pueden conectarse a la computadora para almacenamiento de datos a pesar de su tamaño como disquetes, CD ROM, USB, disco duro, llave de memoria, etc.	Medios electrónicos externos poco seguros y de uso personal	Aplicaciones maliciosas/Malware	4	3	12	Muy Alto	**MUY ALTO.** Debido a intereses de terceros que buscan perjudicar a la organización para fines competitivos, personales, financieros, etc.	4	3	**Mantener la preparación de los empleados (prácticas que reducen el estrés y la ansiedad, la fatiga, enfermedades etc.):** Control preventivo que permite reducir factores causales relacionados al estrés, distracción mental, sesgos cognitivos, etc. que puedan ocasionar un descuido por parte del empleado **Configurar equipos para no auto ejecutar contenido:** Configure los equipos para no ejecutar automáticamente el contenido de medios extraíbles.	1	1	1	Bajo
2	Validación y prueba del servicio	Software de servicio, mantenimiento o administración	Pruebas de software insuficientes o nulas	Ingeniería Social	4	1	4	Medio	**MUY ALTO.** Debido a intereses de terceros que buscan perjudicar a la organización para fines competitivos,	3	3	**Implementar una planificación y un control del trabajo efectivos para reducir la presión del trabajo, administrar los factores de tiempo, reducir la dificultad de la tarea, etc. :** Control preventivo y correctivo que ayuda en la reducción de carga laboral para evitar errores humanos mediante una correcta planificación y control del trabajo por parte de los empleados	2	1	2	Bajo

									personales, financieros, etc.			**Mejorar la conciencia de las amenazas internas y las amenazas internas involuntarias:** Control preventivo y detectivo que ayuda en la identificación de amenazas para reforzar los conocimientos y estar alerta antes amenazas de Ciberseguridad **Reconocer el phishing y otros vectores de amenazas de las redes sociales mediante cursos aplicativos y test de ingeniería social:** Control preventivo que permite reconocer y evitar los ataques de phishing que puedan presentarse en los siguientes escenarios: **Aplicar políticas y buenas prácticas de seguridad para evitar el malware:** Control preventivo que busca activar ciertos protocolos de seguridad cuando se ha identificado o no el malware como por ejemplo: - Ver mensajes inesperados con sospecha - Utilizar software anti-malware. - Conectarse a proveedores de servicios con firewalls. - Establecer opciones para evitar la instalación de software ejecutable en dispositivos móviles. - Tener cuidado con las conexiones inesperadas y las confirmaciones de actualización. - Borrado de memoria remota para equipos perdidos - Tener actualizado el software antivirus **Llevar a cabo capacitación y concientización sobre la percepción del riesgo y los sesgos cognitivos que afectan la decisión.** **haciendo:** Control preventivo y detectivo para reducir la ocurrencia de este tipo de amenazas a falta de conocimiento y sentido de alerta ante casos sospechosos o ataques dirigidos sin saber cómo accionar **Mejorar la usabilidad de las herramientas de seguridad:** Control preventivo, correctivo y disuasivo para proteger y reportar los casos ocurridos por ataques relacionado a este tipo de amenazas como ransomware, spyware, phishing e ingeniería social **Configurar escaneo antimalware de dispositivos removibles:** Configure los dispositivos para que automáticamente realicen un análisis antimalware de los medios extraíbles cuando se inserten o se conecten. Centralizar los registros antimalware y de ingeniería social: Control preventivo que busca enviar todos los eventos de detección de malware y eventos por ingeniería social a los servidores de la organización para análisis y alerta				
		Paquetes de software	Defectos conocidos en el software	Aplicaciones maliciosas/Malware	3	2	6	Medio	**MUY ALTO.** Debido a intereses de terceros que buscan perjudicar a la organización para fines competitivos, personales, financieros, etc.	3	2		1	1	1	Bajo
		Aplicaciones de negocio	Software ampliamente distribuido		4	2	8	Alto	**MUY ALTO.** Debido a intereses de terceros que buscan perjudicar a la organización para fines competitivos, personales, financieros, etc.	4	4		1	1	1	Bajo
3	Gestión de entrega y despliegue	Software de servicio, mantenimiento o administración	Interfaz de usuario complicada o poco usable	Eliminación de información sensible de forma incorrecta o por error	2	3	6	Medio	**MEDIO.** El impacto de esta amenaza dependerá de los controles o políticas de seguridad tomadas por la organización (ej. Backups, almacenamiento en la nube, etc.)	4	4	**Mejorar el flujo de datos mejorando la comunicación y manteniendo procedimientos precisos:** Control preventivo que permite tener canales de comunicación oficiales de acuerdo a los procedimientos para evitar la divulgación de información por medio de otros canales no oficiales **Implementar una planificación y un control del trabajo efectivos para reducir la presión del trabajo, administrar los factores de tiempo, reducir la dificultad de la tarea, etc. :** Control preventivo y correctivo que ayuda en la reducción de carga laboral para evitar errores humanos mediante una correcta planificación y control del trabajo por parte de los empleados **Mantener la preparación de los empleados (prácticas que reducen el estrés y la ansiedad, la fatiga, enfermedades etc.):** Control preventivo que permite reducir factores causales relacionados al estrés, distracción mental, sesgos cognitivos, etc. que puedan ocasionar un descuido por parte del empleado **Asegurar los respaldos regulares automatizados:**	1	1	1	Bajo
		Aplicaciones de negocio	Configuración incorrecta de parámetros	Modificación de información sensible de forma incorrecta o por error	3	3	9	Alto	**MEDIO.** El impacto de esta amenaza dependerá de los controles o políticas de seguridad tomadas por la organización (ej. Backups,	4	4		1	1	1	Bajo

									almacenamiento en la nube, etc.)			Asegúrese de que se realizan regularmente copias de respaldo de todos los datos de sistemas de manera automatizadas **Asegurar la protección de las copias de respaldo:** Asegúrese de que las copias de seguridad estén protegidas adecuadamente a través de la seguridad física o el cifrado cuando se almacenan, así como también cuando se mueven a través de la red ya sea remota o a través de la nube				
4	Gestión de la disponibilidad	Equipos de procesamiento de datos	Almacenamiento sin protección	Ingeniería Social	4	2	8	Alto	**MUY ALTO.** Debido a intereses de terceros que buscan perjudicar a la organización para fines competitivos, personales, financieros, etc.	4	3	**Aplicar políticas y buenas prácticas de seguridad para evitar el malware:** **Control preventivo que busca activar ciertos protocolos de seguridad cuando se ha identificado o no el malware como por ejemplo:** - Ver mensajes inesperados con sospecha - Utilizar software anti-malware. - Conectarse a proveedores de servicios con firewalls. - Establecer opciones para evitar la instalación de software ejecutable en dispositivos móviles. - Tener cuidado con las conexiones inesperadas y las confirmaciones de actualización. - Borrado de memoria remota para equipos perdidos - Tener actualizado el software antivirus **Llevar a cabo capacitación y concientización sobre la percepción del riesgo y los sesgos cognitivos que afectan la decisión.** **haciendo:** Control preventivo y detectivo para reducir la ocurrencia de este tipo de amenazas a falta de conocimiento y sentido de alerta ante casos sospechosos o ataques dirigidos sin saber cómo accionar **Mejorar la usabilidad de las herramientas de seguridad:** Control preventivo, correctivo y disuasivo para proteger y reportar los casos ocurridos por ataques relacionado a este tipo de amenazas como ransomware, spyware, phishing e ingeniería social **Configurar escaneo antimalware de dispositivos removibles:** Configure los dispositivos para que automáticamente realicen un análisis antimalware de los medios extraíbles cuando se inserten o se conecten. **Centralizar los registros antimalware y de ingeniería social:** Control preventivo que busca enviar todos los eventos de detección de malware y eventos por ingeniería social a los servidores de la organización para análisis y alerta	1	1	1	Bajo
		Equipos informáticos fijos como servidores, ordenadores fijos utilizados como estación de trabajo	Almacenamiento sin protección	Aplicaciones maliciosas/Malware	4	2	8	Alto	**MUY ALTO.** Debido a intereses de terceros que buscan perjudicar a la organización para fines competitivos, personales, financieros, etc.	4	3		1	1	1	Bajo
5	Gestión de la seguridad de información	Información vital para el negocio y el cumplimiento de la misión de la organización	Tráfico sensible no protegido	Ingeniería Social	4	1	4	Medio	**MUY ALTO.** Debido a intereses de terceros que buscan perjudicar a la organización para fines competitivos, personales, financieros, etc.	3	2		2	1	2	Bajo
		Información personal cumpliendo con las leyes de protección de datos	Líneas de comunicación desprotegidas	Divulgación de datos a través de internet, social media, cloud o móviles	3	1	3	Medio	**MEDIO.** Debido a que la mayor cantidad de información divulgada es del mismo colaborador; sin embargo, existe la posibilidad de compartir información crítica	3	3	**Aplicar firewalls basados en host o filtrado de puertos:** Aplique firewalls basados en host o herramientas de filtrado de puertos en los sistemas finales, con una regla de denegación predeterminada que descarta todo el tráfico, excepto los servicios y puertos que están explícitamente permitidos **Implementar firewalls de aplicación:** Coloque firewalls de aplicaciones frente a servidores críticos para verificar y validar el tráfico que va al servidor. Cualquier tráfico no autorizado debe ser bloqueado y registrado **Deshabilitar el acceso inalámbrico en dispositivos si no se requiere** Deshabilite el acceso inalámbrico en dispositivos que no tienen un propósito de negocio para el acceso inalámbrico. **Mantener los valores y las actitudes del personal que se alinean con la misión y la ética de la organización a través de cursos de ética y trabajos de integración:** Control preventivo que busca generar un ambiente y cultura organizacional adecuada con la finalidad que marca los mismos interés de la organización en cada uno de los trabajadores	1	1	1	Bajo

6	Gestión de activos y configuración del servicio	Todos los activos	Falta de protección física del edificio, puertas y ventanas	Información sensible física en escritorios o lugares inseguros	1	2	2	Bajo	**BAJO.** El impacto no es tan grande debido a que no es información digital; sin embargo, si se tiene accesos, contraseñas, datos personales el impacto podría ser mayor	3	2	**Llevar a cabo capacitación y concientización sobre la percepción del riesgo y los sesgos cognitivos que afectan la decisión:** Control preventivo encargado de evitar poner en riesgo los activos de la organización por parte del empleado mediante capacitación en su uso adecuado, respaldo de la información almacenado en el activo ante algún incidente **Impartir curso de capacitación y concientización de políticas de salud y seguridad en el trabajo:** Control preventivo para reducir los riesgos de dejar activos o elementos de la estación de trabajo del colaborador en lugares inseguros que puedan causar incidentes graves como pérdida de información sensible y accidentes físicos o perjudiciales	1	1	1	Bajo
			Falta de políticas de seguridad para la protección de activos	Aplicaciones maliciosas/Malware	3	3	9	Alto	**MUY ALTO.** Debido a intereses de terceros que buscan perjudicar a la organización para fines competitivos, personales, financieros, etc.	4	4	**Aplicar políticas y buenas prácticas de seguridad para evitar el malware:** **Control preventivo que busca activar ciertos protocolos de seguridad cuando se ha identificado o no el malware como por ejemplo:** - Ver mensajes inesperados con sospecha - Utilizar software anti-malware. - Conectarse a proveedores de servicios con firewalls. - Establecer opciones para evitar la instalación de software ejecutable en dispositivos móviles. - Tener cuidado con las conexiones inesperadas y las confirmaciones de actualización. - Borrado de memoria remota para equipos perdidos - Tener actualizado el software antivirus	1	1	1	Bajo

5.2.3.7 Diseño de la guía de implementación

La guía de implementación provee un conjunto de pasos para poder implementar el modelo dentro de una organización con la finalidad de identificar las amenazas no intencionales de ciberseguridad y proponer controles que puedan lograr reducir su impacto y lograr los objetivos planteados por el modelo. La guía se presenta a continuación:

GUIA PARA LA IMPLEMENTACIÓN DEL MODELO DE IDENTIFICACIÓN DE AMENAZAS NO INTENCIONALES DE CIBERSEGURIDAD

(MANIC)

JULIO 2022

1. Guía de implementación

El objetivo de esta guía es proveer un conjunto de pasos para implementar el modelo MANIC basado en un conjunto de componentes que buscan gestionar las amenazas no intencionales de ciberseguridad en la organización, el cual es adaptable a las necesidades y/o requerimientos de la entidad pública.

El entorno general de la entidad pública debe ser analizado para determinar aspectos gestión de activos, gobernanza, ambiente de negocio, políticas de ciberseguridad, gestión de riesgos, etc. Estos incidirán en los procesos de TI y en las métricas que dicha entidad considere pertinentes y útiles.

De la misma forma, la definición de procesos, objetivos y el establecimiento de las métricas es referencial, pues la entidad pública puede organizar sus recursos y capacidades partiendo de las ideas generales propuestas en la presente guía. Así, deberá considerar su situación específica y las políticas regulatorias asociadas a ciberseguridad para que los procesos de TI, activos identificados, amenazas y escenarios de riesgo sean de utilidad para los planteamientos que la organización realice.

1.1. Requisitos del personal para la ejecución de la guía

La guía de implementación debe ser ejecutada por personal capacitado. Este personal deberá tener los conocimientos necesarios relacionados a Ciberseguridad, esto involucra las amenazas de ciberseguridad, buenas prácticas, marcos de trabajo, conocimientos de TI, etc. Adicionalmente, también es necesario tener conocimientos relacionados a la gestión de riesgos. El personal, que puede ser considerado un equipo de trabajo, debe ser consciente de la responsabilidad de su rol dentro de la organización, así como también tener los conocimientos para poder aplicar los controles propuestos por el modelo MANIC. Dentro de las funciones que maneja, deberá tener habilidades de comunicación e interrelación con otras áreas debido a que el impacto de los riesgos involucra no solo el área de TI sino también áreas de negocio y áreas operativas

1.2. Fases de la implementación

La guía de implementación de MANIC consta de las siguientes fases:

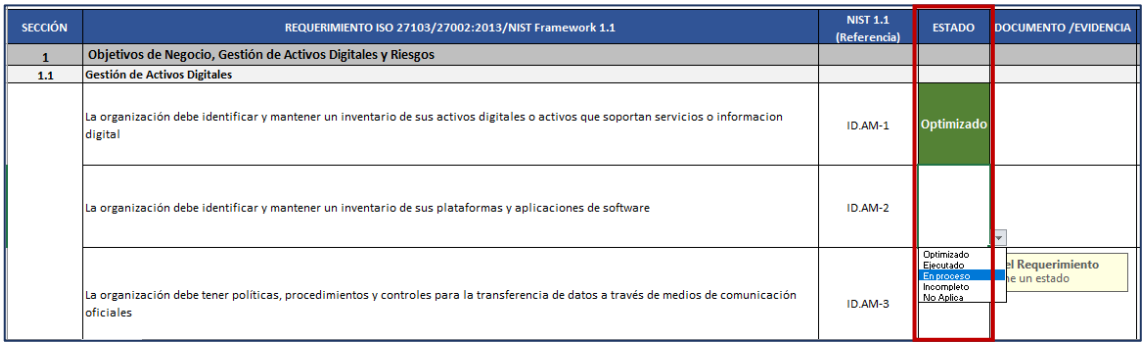
Figura 1. Fases del modelo MANIC

1.2.1. Análisis Situacional

Previo al desarrollo del modelo, se debe establecer el estado actual de organización en relación a ciberseguridad, es así como el modelo brinda una herramienta para identificar las áreas más afectadas y con menos controles y políticas de ciberseguridad en relación a sus procesos, activos, datos, personas y gestión de riesgos. La herramienta tiene por nombre **"Matriz de Análisis Situacional.xlsx"** y permite evaluar de forma cuantitativa el cumplimiento o no de ciertas normas y controles de ciberseguridad.

1.2.1.1. Paso 1: Selección del estado de cada norma de ciberseguridad

La matriz cuenta con dos pestañas, la primera pestaña identifica un conjunto de normas agrupadas por categorías donde el usuario debe seleccionar el estado de cumplimiento de cada norma y presentar los documentos que validen el nivel de cumplimiento asignado como se muestra en la siguiente imagen:

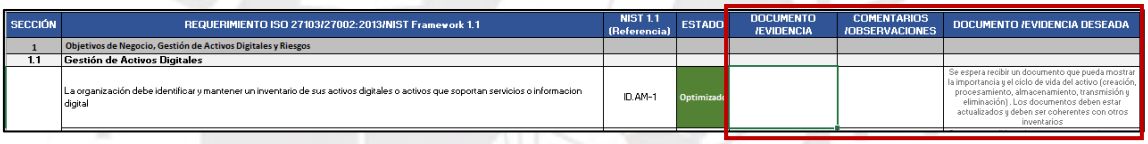


SECCIÓN	REQUERIMIENTO ISO 27103/27002:2013/NIST Framework 1.1	NIST 1.1 (Referencia)	ESTADO	DOCUMENTO /EVIDENCIA
1	Objetivos de Negocio, Gestión de Activos Digitales y Riesgos			
1.1	Gestión de Activos Digitales			
	La organización debe identificar y mantener un inventario de sus activos digitales o activos que soportan servicios o informacion digital	ID.AM-1	Optimizado	
	La organización debe identificar y mantener un inventario de sus plataformas y aplicaciones de software	ID.AM-2		
	La organización debe tener políticas, procedimientos y controles para la transferencia de datos a través de medios de comunicación oficiales	ID.AM-3	Optimizado Ejecutado En proceso Incompleto No Aplica	el Requerimiento ne un estado

Figura 2. Matriz de análisis situacional

1.2.1.2. Paso 2: Redactar la documentación o evidencia del estado

Luego de asignar el estado de acuerdo con el nivel de cumplimiento por parte de la organización se deben presentar los documentos o evidencias que respalden la calificación asignada.

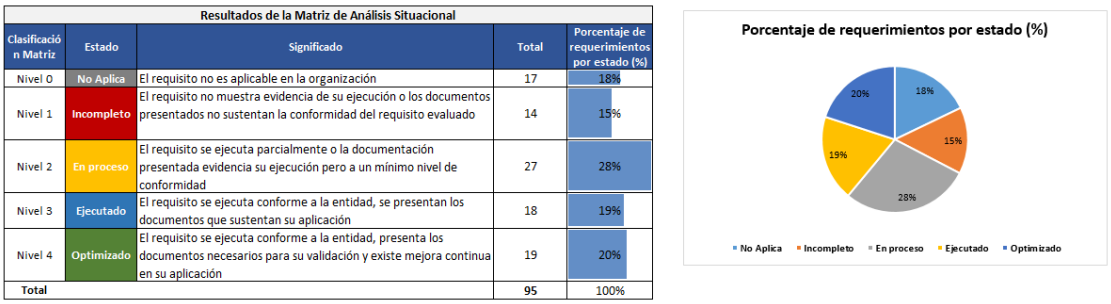


SECCIÓN	REQUERIMIENTO ISO 27103/27002:2013/NIST Framework 1.1	NIST 1.1 (Referencia)	ESTADO	DOCUMENTO /EVIDENCIA	COMENTARIOS /OBSERVACIONES	DOCUMENTO /EVIDENCIA DESEADA
1	Objetivos de Negocio, Gestión de Activos Digitales y Riesgos					
1.1	Gestión de Activos Digitales					
	La organización debe identificar y mantener un inventario de sus activos digitales o activos que soportan servicios o informacion digital	ID.AM-1	Optimizado			Se espera recibir un documento que pueda mostrar la importancia y el ciclo de vida del activo (creación, procesamiento, almacenamiento, transmisión y eliminación). Los documentos deben estar actualizados y deben ser coherentes con otros inventarios

Figura 3. Registro de evidencia o documentación

1.2.1.3. Paso 3: Revisión de los resultados

Una vez que se evaluaron todas las normas relevantes para la organización, se procede con la revisión de los resultados en la segunda pestaña.



Resultados de la Matriz de Análisis Situacional				
Clasificación Matriz	Estado	Significado	Total	Porcentaje de requerimientos por estado (%)
Nivel 0	No Aplica	El requisito no es aplicable en la organización	17	18%
Nivel 1	Incompleto	El requisito no muestra evidencia de su ejecución o los documentos presentados no sustentan la conformidad del requisito evaluado	14	15%
Nivel 2	En proceso	El requisito se ejecuta parcialmente o la documentación presentada evidencia su ejecución pero a un mínimo nivel de conformidad	27	28%
Nivel 3	Ejecutado	El requisito se ejecuta conforme a la entidad, se presentan los documentos que sustentan su aplicación	18	19%
Nivel 4	Optimizado	El requisito se ejecuta conforme a la entidad, presenta los documentos necesarios para su validación y existe mejora continua en su aplicación	19	20%
Total			95	100%

Figura 4. Análisis de resultados de la matriz situacional

Estos resultados permiten identificar los niveles con mayor frecuencia para luego pasar al nivel detallado del análisis.

SECCIÓN	REQUERIMIENTO ISO 27103/27002:2013/NIST Framework 1.1	Total	No Aplica	Incompleto	En proceso	Ejecutado	Optimizado
1	Objetivos de Negocio, Gestión de Activos Digitales y Riesgos	24	5	5	6	4	4
1.1	Gestión de Activos Digitales	5	1	1	2	0	1
1.2	Ambiente de Negocio	5	1	1	2	0	1
1.3	Gobernanza	4	1	2	0	0	1
1.4	Gestión de Riesgos	10	2	1	2	4	1
2	Control de Accesos, Políticas de seguridad, Mantenimiento y Protección de In	31	6	5	7	6	7
2.1	Control de Accesos y Gestión de Identidad	5	1	1	1	1	1
2.2	Conciencia y Capacitación	3	2	0	0	0	1
2.3	Seguridad de Datos	7	1	2	1	2	1
2.4	Procesos y Procedimientos de protección de la Información	11	2	2	3	1	3
2.5	Mantenimiento	2	0	0	2	0	0
2.6	Tecnología de Protección	3	0	0	0	2	1
3	Detección de Anomalías, Eventos y Monitoreo	13	3	1	3	3	3
3.1	Anomalías y Eventos	4	2	1	0	0	1
3.2	Monitoreo continuo de Seguridad	5	0	0	1	3	1
3.3	Procesos de Detección	4	1	0	2	0	1
4	Plan de Respuestas	13	1	2	3	4	3

Figura 5. Análisis detallado de resultados de la matriz situacional

En los resultados detallados podemos identificar las categorías más afectadas con la finalidad enfocar esfuerzos en esas áreas para reducir los riesgos.

1.2.2. Establecimiento de los objetivos

Cada entidad pública tendrá la creación de valor como parte de sus objetivos reflejados en la visión del negocio por lo que, en este paso, las entidades públicas realizarán un mapeo comparando sus objetivos con los objetivos propuestos por MANIC y se adaptará aquello que se considere pertinente.

1.2.2.1. Paso 1: Selección de objetivos propuestos por MANIC

Una vez realizado el análisis situacional, se procede a seleccionar aquellos objetivos propuestos por MANIC, que cubren los objetivos de la entidad pública y, como resultado, se tendrán las métricas correspondientes a dichos objetivos.

1.2.2.2. Paso 2: Justificación de los objetivos propuestos por MANIC

La entidad pública que implementará el modelo deberá justificar la relación de sus objetivos con los objetivos propuestos en el modelo y su relación con los objetivos de TI.

1.2.3. Establecimiento de las métricas

Cada objetivo, propuesto por el modelo MANIC, contiene métricas propuestas que permiten medir el cumplimiento de los objetivos. Las métricas pueden ser adaptadas a la estructura de la organización donde se vaya a implementar. Así, si en caso ya existe un proceso en la organización, se deben adecuar sus propias métricas con la propuesta de MANIC y considerar, más adelante, el detalle de implementación. Si el proceso no existe en la

organización, se deberá tomar las métricas propuestas por MANIC y evaluar su implementación.

1.2.4. Establecimientos de los patrones de comportamiento

La organización deberá identificar los patrones de comportamiento propuestos por el modelo MANIC dentro de sus procesos de TI con la finalidad tener el conjunto de amenazas y factores, asociados a los colaboradores, para realizar un análisis de riesgo de dichos patrones y proponer controles de mitigación.

1.2.5. Análisis de riesgos de Ciberseguridad

A partir de la identificación de amenazas y los patrones de comportamiento, se debe también identificar los procesos, activos y vulnerabilidades asociadas a ellas. Por lo tanto, como parte de la ejecución del modelo MANIC, el último paso brinda una herramienta para poder mapear los escenarios de riesgo que pudieran afectar a la organización. Los escenarios deberán ser seleccionados de acuerdo al contexto y negocio de la organización para poder hacer uso de la propuesta de controles que brinda el modelo en su matriz de gestión de riesgos.

1.2.5.1. Paso 1: Establecimiento de los procesos de TI

Se procede a seleccionar aquellos procesos de TI propuestos por MANIC, que se alineen a los procesos de la entidad pública y, como resultado se podrá mapear los procesos dentro de la matriz de riesgos que propone MANIC.

1.2.5.2. Paso 2: Establecimiento de los activos digitales

Una vez identificado los procesos de TI que están alineados con los de la organización, se procede a seleccionar aquellos activos digitales de TI propuestos por MANIC, que se alinean o coincidan con los activos de la entidad pública y, como resultado de podrá mapear los activos dentro de la matriz de riesgos que propone MANIC.

1.2.5.3. Paso 3: Establecimiento de las vulnerabilidades

Una vez identificadas los activos de TI que estén alineados con los de la organización, se procede a seleccionar aquellas vulnerabilidades asociadas a los activos que se obtuvieron en el paso 2 propuestos por MANIC. Las vulnerabilidades propuestas por el modelo MANIC,

buscan ser generales para adaptarse a cualquier situación o característica del activo de la organización. Como resultado se podrá mapear las vulnerabilidades dentro de la matriz de riesgos que propone MANIC. En caso la vulnerabilidad no se encuentre listada en la matriz, podrá agregar nuevas vulnerabilidades y asociarse con las amenazas identificadas por el modelo para tener en consideración los controles asociados a las amenazas y así implementar los controles de considerarlo pertinente.

1.2.5.4. Paso 4: Establecimiento de las amenazas no intencionales

Una vez identificado las vulnerabilidades que están alineados con los de la organización, se procede a seleccionar aquellas amenazas no intencionales de ciberseguridad propuestos por MANIC, que cubren las vulnerabilidades de la entidad pública en relación a sus activos y, como resultado se podrá mapear las amenazas dentro de la matriz de riesgos que propone MANIC.

1.2.5.5. Paso 5: Validación con la matriz de gestión de riesgos

Una vez que seleccionadas las amenazas, procesos, activos y vulnerabilidades, se procede con el mapeo de los escenarios de riesgo dentro de la matriz de gestión de riesgos, la cual identifica cada escenario y presenta una validación estimada del impacto y probabilidad de ocurrencia con la finalidad de proponer controles para reducir o eliminar la amenaza. Adicionalmente, la matriz propone medir un impacto en la información en caso se vea afectada su confidencialidad, disponibilidad e integridad de forma cualitativa para alertar a la organización sobre este punto. Para la evaluación del riesgo se utiliza la siguiente tabla:

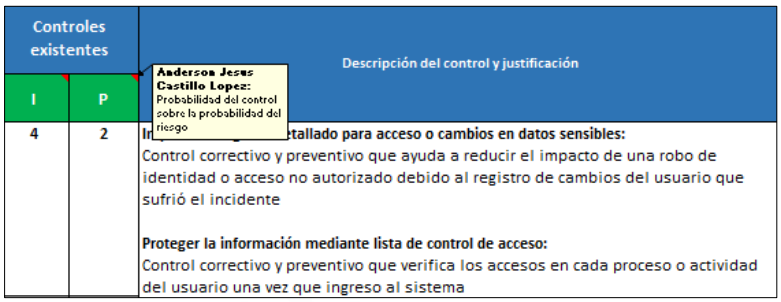
Tabla 1: Nivel de Riesgo (Autoría Propia)

Min	Max	Nivel de Riesgo
1	2	Bajo
3	6	Medio
8	10	Alto
12	16	Muy Alto

Con esta tabla, una vez que se tiene el impacto estimado y la probabilidad estimada a juicio del personal encargado de la evaluación, se procede a calcular el producto I (impacto) x P (probabilidad). Este resultado deberá ser evaluado en los rangos de la Tabla 1 y así poder identificar el nivel de riesgo asociado.

Los controles propuestos pueden ya estar dentro de la lista de controles de la organización, en caso se encuentre mapeado algún control previamente, existen dos columnas encargadas de verificar los controles existentes, las cuales miden el impacto y probabilidad

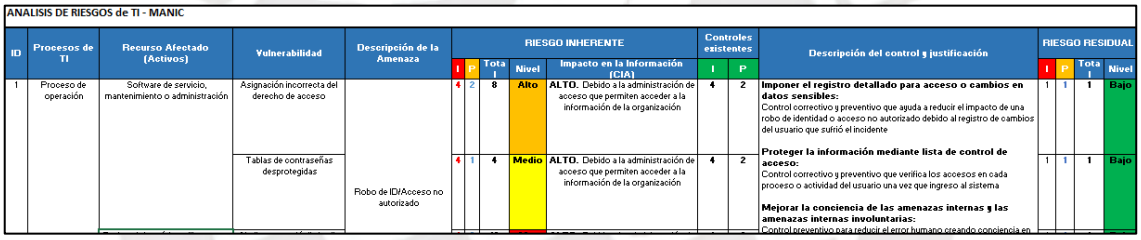
de control para reducir el riesgo. Esta evaluación que se encuentra en la matriz, se muestra en la siguiente figura:



Controles existentes		Descripción del control y justificación
I	P	
4	2	**Anderson Jesus Castillo Lopez:** Probabilidad del control sobre la probabilidad del riesgo **...talladó para acceso o cambios en datos sensibles:** Control correctivo y preventivo que ayuda a reducir el impacto de una robo de identidad o acceso no autorizado debido al registro de cambios del usuario que sufrió el incidente **Proteger la información mediante lista de control de acceso:** Control correctivo y preventivo que verifica los accesos en cada proceso o actividad del usuario una vez que ingreso al sistema

Figura 6. Medición de los controles existentes en la matriz de gestión de riesgos de MANIC

La matriz de gestión de riesgos se representa mediante una herramienta en formato Excel denominada **"Matriz de Gestión de Riesgos.xlsx"** y permite a la organización tener mapeados a nivel general los posibles impactos y controles para lograr cumplir los objetivos que propone MANIC. La matriz se muestra a continuación:



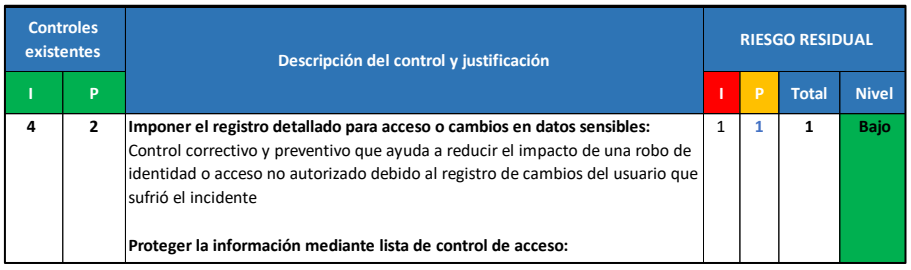
ANALISIS DE RIESGOS de TI - MANIC

ID	Procesos de TI	Recurso Afectado (Activos)	Vulnerabilidad	Descripción de la Amenaza	RIESGO INHERENTE					Controles existentes		Descripción del control y justificación	RIESGO RESIDUAL			
					I	P	Total	Nivel	Impacto en la Información (CIA)	I	P		I	P	Total	Nivel
1	Proceso de operación	Software de servicio, mantenimiento o administración	Asignación incorrecta del derecho de acceso	Robo de ID/Acceso no autorizado	4	2	8	Alto	ALTO. Debido a la administración de acceso que permiten acceder a la información de la organización	4	2	**Imponer el registro detallado para acceso o cambios en datos sensibles:** Control correctivo y preventivo que ayuda a reducir el impacto de una robo de identidad o acceso no autorizado debido al registro de cambios del usuario que sufrió el incidente **Proteger la información mediante lista de control de acceso:** Control correctivo y preventivo que verifica los accesos en cada proceso o actividad del usuario una vez que ingreso al sistema **Mejorar la conciencia de las amenazas internas y las amenazas internas involuntarias:** Control preventivo para reducir el error humano creando conciencia en	1	1	1	Bajo
			Tablas de contraseñas desprotegidas		4	1	4	Medio	ALTO. Debido a la administración de acceso que permiten acceder a la información de la organización	4	2		1	1	1	Bajo

Figura 7. Matriz de gestión de riesgos de MANIC

1.2.5.6. Paso 6: Verificación de controles

Finalmente, en este paso se verifican los controles propuestos por MANIC con la finalidad de que sean implementados por parte de la organización. Si bien un conjunto de controles ayuda a mitigar varios riesgos, la verificación se puede realizar independientemente para asi poder medir el cumplimiento de estos para el logro de los objetivos de la organización como parte principal del modelo que se ha propuesto. Los controles tienen la siguiente estructura:



Controles existentes		Descripción del control y justificación	RIESGO RESIDUAL			
I	P		I	P	Total	Nivel
4	2	**Imponer el registro detallado para acceso o cambios en datos sensibles:** Control correctivo y preventivo que ayuda a reducir el impacto de una robo de identidad o acceso no autorizado debido al registro de cambios del usuario que sufrió el incidente **Proteger la información mediante lista de control de acceso:**	1	1	1	Bajo

Figura 8. Verificación de controles propuestos por MANIC

Para la columna de riesgo residual, existe un impacto y probabilidad asignados producto de relación entre el impacto y probabilidad de los controles frente a los riesgos definidos como se muestra en la siguiente figura:

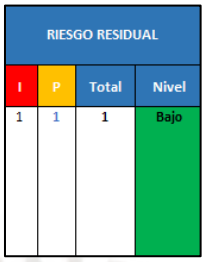


Figura 9. Cálculo del impacto y probabilidad residual propuestos por MANIC

Para el cálculo del impacto y probabilidad se maneja la siguiente formula de Excel que ya se encuentra integrada en la herramienta y se muestra su lógica en la siguiente tabla:

Tabla 2: Cálculo del riesgo residual (Autoría Propia)

Impacto/Probabilidad del Control Existente	Impacto/Probabilidad de la Amenaza	Resultado
0	I(x)	0
1	I(x)	I(x)
2	I(x)>2	I(x) -1
3	I(x)>3	I(x) -2
4	I(x)>4	I(x) -3
>4	I(x)	1

X: Amenaza
I(x): Impacto de la amenaza
P(x): Probabilidad de la amenaza

La estructura inicia con la verificación de la existencia de los controles en la organización y de implementarlo, o ya estando en funcionamiento, muestran la reducción del riesgo hasta un nivel aceptable.

La matriz de gestión de riesgos tiene 2 validaciones. La primera validación fue realizada por la profesora Melissa K. Chinyemba, la cual forma parte de la Universidad de Zambia, África. La segunda validación fue realizada por la oficial de Seguridad de Información, Jennifer Ayllón, quien es especialista en CyberSecurity & Tecnologías del Ministerio de Trabajo y Promoción del Empleo (MTPE).

Discusión

Los resultados obtenidos son parte de los componentes del modelo que permiten en primer lugar dar un análisis inicial de la organización y en segundo lugar definir los objetivos alcanzables por el modelo en base a los resultados previos con respecto a Ciberseguridad. Estos resultados son parte del modelo y la primera evaluación que se aplica en la organización.

Estos resultados son consistentes con proyectos e investigaciones previas debido a que la base fundamental de su diseño son las normativas, estándares principales y la revisión del estado del arte hecho previamente. Por lo tanto, la generalización de estos resultados es posible gracias a que se sigue un estándar ya validado. Sin embargo, existen algunas limitaciones debido al tema específico del proyecto que no permite ser adaptado en otros ámbitos que no sean de Ciberseguridad.

Capítulo 6. Asociación de la lista de patrones de comportamiento

6.1 Introducción

El capítulo presentado desarrolla el Objetivo Específico 1 (OE1). El objetivo del capítulo es presentar la lista de los patrones de comportamiento definidos en base a la asociación de factores y amenazas que se vio en el capítulo anterior. Los patrones de comportamiento tienen como fin principal la identificación de las amenazas que puedan presentar un riesgo dentro de la organización. La construcción de los patrones de comportamiento ya fue definida en el capítulo anterior. En este capítulo se detalla cada uno de los patrones definidos y se puede visualizar la Matriz de Trazabilidad en **Anexo E**, la cual permite visualizar la construcción de estos patrones en base a la asociación de los factores y las amenazas.

6.2 Resultados Alcanzados (RE1)

6.2.1 Lista de Patrones de Comportamiento

Patrones de Comportamiento por UIT-HACK

a) Patrón de Comportamiento relacionado a phishing

La definición de este patrón está asociada con la ocurrencia de un ataque por phishing dentro de la organización en base a factores causales relacionados con los empleados de la organización. Para conocer esta relación, primero es necesario entender que significa phishing y luego se definirá los factores que pueden aumentar la probabilidad de ocurrencia de la amenaza, mas no su inminente accionar. Phishing es un tipo de ataque en donde las víctimas son engañadas mediante correos electrónicos falsos o sitios web fraudulentos que a los ojos del usuario se muestra como un sitio confiable; sin embargo, la finalidad de este ataque consiste en el robo de identidad, información personal o de la organización (Kumaraguru et al., 2007).

Como parte de la revisión sistemática, se encuentran ciertos factores asociados a la ocurrencia de este tipo de amenaza que se describen a continuación (CERT, 2013):

- Carga de trabajo
- Falta de conciencia de la situación (SA)

- Planificación/Control de trabajo relacionado al estrés laboral
- Enfermedades asociadas a drogas u hormonas
- Mente distraída alineado a atención que presenta el colaborador en sus labores
- Sesgos cognitivos alineado al criterio y nivel de conciencia del empleado
- Escenario de trabajo alineada a la falta de atención en el trabajo

Estos factores pueden influenciar en el accionar de un empleado si se encuentran con un alto nivel de carga laboral, estrés o si no es consciente de los elementos asociados al ambiente de trabajo o si en caso sufre de alguna enfermedad que no le permita cumplir con las funciones normales (CERT, 2013).

b) Patrón de Comportamiento relacionado a malware

De la misma forma que el patrón de comportamiento anterior, el malware agrupa diferentes tipos de amenazas y es conocido como un software malicioso que inicia su accionar de forma intencionada por un agente externo o mal actor (Kumaraguru et al., 2007); sin embargo, la ocurrencia de este tipo de amenazas depende de un agente interno y es ahí donde se examina qué factores pueden ser causales de una posible ocurrencia de esta amenaza (CERT, 2013).

Como parte de los posibles factores causales se tiene los siguientes:

- Carga de trabajo
- Falta de conciencia de la situación (SA)
- Planificación/Control de trabajo relacionado deficientes herramientas de anti-malware, estrés laboral
- Enfermedades asociadas a drogas u hormonas
- Escenarios de Trabajo asociados a malas prácticas respecto a la distribución o préstamo de dispositivos USB a externos de la organización que pudiera infectar

De la misma forma que el patrón anterior, estos factores son una posible causal de ocurrencia de esta amenaza; sin embargo, debe aclararse que este patrón para que pueda ser definido y usado debe obligatoriamente involucrar a un agente interno sino no formaría parte de una UIT, además también debemos tener en cuenta que

la relación de los factores y el ataque por malware no es directa y depende de ciertas herramientas que puedan demostrar su relación parcial o total (CERT, 2013).

c) Patrón de Comportamiento relacionado a ingeniería social

Ingeniería social es un concepto que define cualquier acto que influye a una persona realizar una acción que para los fines del proyecto nos centraremos en las formas maliciosas de la ingeniería social que debe ser entendida en base de factores psicológicos, fisiológicos y tecnológicos que influyen a la persona (Kyeremeh et al., 2019). Si bien algunas de las amenazas ya mencionadas están forman parte de la ingeniería social, buscamos separarla por ser una de las más ocurrentes en las organizaciones. La ingeniería social, así como los patrones antes mencionados está relacionado con ciertos factores causales que se presentan a continuación:

- Carga de trabajo
- Falta de conciencia de la situación (SA)
- Planificación/Control de trabajo relacionado al estrés laboral
- Enfermedades asociadas a drogas u hormonas
- Requerimientos de procesos de negocio
- Flujo de datos
- Escenarios de trabajo alineado a la falta de atención del empleado
- Fatiga o somnolencia alineado a la falta de atención del empleado
- Sesgos cognitivos alineado al criterio y nivel de conciencia del empleado
- Estado de ánimo muy alineado a si el empleado lo considera importante en ese momento o no

Este patrón involucra más factores debido que adicional a los factores ya mencionados anteriormente, también debemos tener en cuenta los procesos de negocio, el flujo de datos y escenarios de trabajo, los cuales involucran medidas de seguridad confusas, procedimientos inadecuados y prácticas de seguridad inadecuadas respectivamente (Kyeremeh et al., 2019)

d) Patrón de Comportamiento relacionado a accesos no autorizados y robo de ID

El Robo de Identidad es definido como un ataque intencional y no autorizado al uso de información de identidad personal para propósitos ilegales, el cual es un problema que sigue creciendo y que no solo afecta económicamente sino también psicológica y físicamente. Muchas personas terminan con problemas médicos después de un tipo de ataque como este. Si bien no se ha demostrado todavía una relación cercana entre la víctima y el atacante, y tampoco se conoce si existen características como la demográfica y lo socioeconómico, si existe un factor asociado al estilo de vida de la persona y el uso de la información personal en internet para distintas actividades. Asimismo, el estilo de vida si puede influenciar en la posibilidad de ocurrencia de este ataque, por lo cual la edad, y el nivel sociocultural si tienen una influencia con el estilo de vida y patrones de consumo. Por lo cual se puede considerar los siguientes factores como posibles causas relacionadas indirectamente (Burnes et al., 2020):

- Escenario de trabajo relacionado a el uso de contraseñas débiles que pueden ser corrompidas si se encuentra infectado el dispositivo
- Culturales
- Edad debido a que cada persona tendrá sus propios sesgos tanto en la forma habitual de hacer sus labores en el caso de la gente mayor y en los jóvenes en un déficit de privacidad al exponer su información en las redes
- Requerimiento de procesos de negocio (BPR)

Estos son posibles factores causales que están relacionados indirectamente a la ocurrencia de este tipo de ataques.

Patrones de Comportamiento por DISC

e) Patrón de Comportamiento relacionado al envío de información sensible por correo o fax accidentalmente

El envío de información sensible accidentalmente por algún medio de la organización es un riesgo que expone tanto al usuario como a la organización, si bien este tipo de amenazas ocurren de forma accidental, existen posibles causales que puedan afectar la actividad normal del colaborador, lo cual termine en un error

accidental. A continuación, se propone estos factores como posibles causales de la ocurrencia del incidente (CERT, 2013):

- Flujo de datos relacionado a una mala comunicación o procedimientos para envío de información
- Escenario de trabajo relacionado a distracciones, escasas políticas y protocolos de seguridad
- Distracción mental relacionado a la atención al momento de ejecutar una tarea o actividad
- Requerimiento de procesos de negocio
- Planificación/Control del trabajo
- Falta de conciencia de la situación (SA)
- Sesgos cognitivos alineado al criterio y nivel de conciencia del empleado
- Estado de ánimo muy alineado a si el empleado lo considera importante en ese momento o no

Estas propuestas de causal que conforman el patrón de comportamiento, si bien no están relacionadas directamente con este tipo de accidentes, para eso es necesario desarrollar entrevistas y evaluaciones exhaustivas para encontrar una relación directa, se proponen como posibles causas de este tipo de accidentes que pueden convertirse en un peligro para la organización.

f) Patrón de Comportamiento relacionado a la divulgación de datos a través de internet, social media, cloud o móviles

Existen distintas formas de divulgar información que en muchos casos el agente que realiza la divulgación es el mismo colaborador (CERT, 2013). Entre los distintos medios de divulgación se encuentra las redes sociales, las cuales pueden exponer información sensible de la organización en la medida que los empleados adopten las redes sociales como parte de su vida, las cuales están asociados con distintas funciones que pueden realizarse en las redes sociales como por ejemplo el postear información o actualización de estados personales, la aceptación de solicitud de amigos que puedan ver lo que el empleado publica, carga de fotos o videos y aplicaciones externas a la organización. Este tipo de actividades se conoce como OSN functions y pueden ser potenciales peligros para la organización (Abdul Molok

et al., 2018). Asimismo, estas actividades podrían deberse a un problema mayor relacionado a la adicción del uso de internet, el cual debe de acuerdo con los estudios a distintos factores que se presentan a continuación (Wu et al., 2015):

- Planificación/Control del trabajo relacionado al estrés laboral
- Fatiga o somnolencia
- Carga de trabajo mental
- Distracción mental
- Cultural relacionado a la región, localidad y las formas de tolerar los riesgos como parte de su cultura
- Estado de ánimo relacionado a factores personales
- Edad relacionada al nivel de tolerancia al riesgo
- Influencia de Drogas/Hormonas/Enfermedades relacionadas a problemas de adicción al uso de internet, ansiedad, falta de sueño, depresión, etc.
- Sesgos cognitivos alineado al criterio y nivel de conciencia del empleado
- Falta de conciencia de la situación (SA)
- Requerimientos de proceso de negocio

Estos factores causales engloban muchas características que afectan a las personas y su normal actividad diaria, lo cual de acuerdo los estudios y encuestas realizadas son determinante para identificar algún tipo de adicción al uso de internet, es así como se puede evaluar este tipo de factores que pueden influir en la divulgación de información sin ser consciente del riesgo que expone el colaborador para la organización.

Patrones de Comportamiento por PHYS

g) Patrón de Comportamiento relacionado al almacenamiento y eliminación de información sensible física

El almacenamiento, eliminación o pérdida inadecuada de documentos físicos que puedan contener información importante dentro de la organización es un riesgo que se debe tener en cuenta. Dentro de los factores posibles de este tipo de amenaza se tiene los siguientes:

- Flujo de datos relacionado a los procedimiento y mala comunicación

- Escenarios de trabajo relacionado a las malas prácticas y políticas de seguridad
- La edad del colaborador relacionado al nivel de tolerancia al riesgo como propuesta de factor causal del patrón de comportamiento
- Requerimientos de proceso de negocio
- Planificación/Control del trabajo
- Fatiga y somnolencia
- Carga de trabajo mental
- Sesgos cognitivos alineado al criterio y nivel de conciencia del empleado
- Estado de ánimo muy alineado a si el empleado lo considera importante en ese momento o no

Estos factores son posibles causales de ocurrencia de pérdida de documentos físicos, eliminación inadecuada o almacenamiento en lugares inseguros como cajones sin llave o escritorios expuesto a todo público, malos procedimientos para el almacenamiento y comunicación respecto a la gestión de documentos y finalmente se puede considerar la edad como un factor determinante en el grado de tolerancia que puede presentar una persona al ver estos documentos de forma inadecuada (CERT, 2013).

Patrones de Comportamiento por PORT

h) Patrón de Comportamiento relacionado al robo o pérdida de equipos portables

Los dispositivos portátiles brindan al usuario una facilidad en el acceso de datos comerciales o personales de manera inmediata y cuando sea necesario; sin embargo, a medida que su uso aumenta, también aumenta los riesgos asociados (Walters, 2012). Las posibles causas de los incidentes asociados a este patrón normalmente son sencillos debido que, para este patrón el robo o pérdida no es afectado por algún factor ya antes mencionado, esto se debe a que hay mayor responsabilidad del agente externo o individuo que roba el equipo; sin embargo, tanto para la pérdida como para el robo debe existir una situación de conciencia del espacio o ambiente donde se hace uso de estos equipos. Si no existe esta situación de conciencia, aumentamos el riesgo a que la amenaza se haga efectiva. En el caso

particular de la pérdida si se debe considerar tres factores más que son los siguientes:

- Escenario de trabajo relacionado a malas prácticas de uso
- Sesgos cognitivos relacionados a la falta de memoria y juicio crítico
- Distracción mental producto de un déficit de atención o a pensamientos que no estén relacionados al trabajo en el momento de realizar una actividad con los equipos, puede provocar la pérdida de los dispositivos portables

Estos factores sí son posibles causales de la pérdida de equipos portátiles debido a no tener buenas prácticas del uso adecuado o políticas y tener alguna carencia del juicio crítico o la incapacidad de recordar ciertas situaciones o cosas (CERT, 2013).

La lista de patrones de comportamiento definidos tiene 2 validaciones, de las cuales una de ellas será realizada a cargo de la profesora Melissa K. Chinyemba, la cual forma parte de la Universidad de Zambia, África. El segundo especialista está a cargo de la oficial de Seguridad de Información, Jennifer Ayllón, quien es especialista en CyberSecurity & Tecnologías del Ministerio de Trabajo y Promoción del Empleo (MTPE). La validación de estos patrones de comportamiento considera las mejoras u observaciones hechas por los especialistas, lo cual puede permitir la modificación de algunos de estos patrones ya definidos

6.3 Discusión

Los resultados obtenidos son parte de los componentes del modelo, los cuales permiten identificar tanto la amenaza como los posibles factores que lo causan por parte del personal. Este resultado debe ser aplicado dentro de la organización para identificar si alguno de estos patrones se evidencia dentro de la organización y si en caso existen nuevos se debe agregar a la lista.

Estos resultados son consistentes con proyectos e investigaciones previas debido a que considera estudios sobre factores críticos del personal en amenazas no intencionales y también los tipos de amenazas en base a una recopilación de casos sobre incidentes de Ciberseguridad hecha por distintas organizaciones y universidades. Por lo tanto, la generalización de estos resultados es posible gracias a que se siguen estudios previos. Sin embargo, existen algunas limitaciones debido al tema específico del proyecto que no permite ser adaptado en otros ámbitos que no sean de Ciberseguridad.

Finalmente, esta lista de patrones de comportamiento fue validada por un especialista en Ciberseguridad lo que permite que los patrones se puedan adaptar a distintos escenarios y organizaciones con la finalidad de tener un amplio conjunto de patrones modificable y de utilidad para las organizaciones que lo utilicen.

Capítulo 7. Validación de los componentes del modelo

7.1 Introducción

El capítulo presentado desarrolla el Objetivo Específico 4 (OE4). El objetivo del capítulo es validar todos los componentes del modelo de identificación de amenazas no intencionales internas de Ciberseguridad para instituciones públicas, el mismo que ha sido denominado como MANIC, para el presente y siguientes trabajos futuros. Los componentes han sido validados por especialistas en Ciberseguridad con la finalidad de que el modelo que se ha diseñado sea de utilidad dentro de las organizaciones del estado. Este objetivo marca el inicio de trabajos futuros orientados a la aplicación del modelo y su aporte a la sociedad en temas de Ciberseguridad. En este capítulo se detalla las observaciones hechas por los especialistas y su respectivo análisis de los resultados y consideraciones a raíz de las validaciones realizadas.

7.2 Resultados Alcanzados (RE8, RE9)

7.2.1 Selección del especialista de la institución pública

Como parte de la validación, se ha seleccionado a dos especialistas de Ciberseguridad y seguridad de las TIC con la finalidad de poder tener su juicio experto en los componentes del modelo. Para esta selección se tiene como especialistas a la Ing. Jennifer Ayllón, quien es Certificada en Gestión de Servicios de TI, Seguridad de Información, Continuidad de Negocio, Ciberseguridad, Anti-Soborno, CBCI, Scrum Master, ITIL, TOGAF. Con estudios en Gestión de Procesos, Sistemas de Control Interno, Gestión de Riesgos, entre otros y actualmente pertenece al Ministerio de Trabajo y Promoción del Empleo. La segunda especialista, es la Ing. Melissa K. Chinyemba, que actualmente posee un máster de ingeniería en Seguridad de las tecnologías de información y la comunicación y pertenece a la Universidad de Zambia.

7.2.2 Elaboración del protocolo

El protocolo para la validación de los componentes del modelo consiste en el envío de la documentación de los resultados esperados del modelo MANIC vía correo electrónico junto con un acta de validación para la conformidad de la revisión. Estos resultados son evaluados por el juicio experto de los especialistas con el fin de corregir y mejorar el modelo planteado. Se ha presentado cierta dificultad en los tiempos de respuesta de alguno de los especialistas; sin embargo, se ha podido lograr tener la validación por parte de ambos. En algunos casos se tuvo una reunión por video llamada para aclarar ciertas dudas y poder

tener una retroalimentación más clara. El acta de validación y la información de los especialistas se encuentra en **Anexo F.**

7.2.3 Análisis de resultados

El análisis de resultados implica la revisión de las observaciones hechas por los especialistas que deben ser evaluadas dentro del alcance que se propone para el proyecto de tesis. Como parte del análisis, se muestran las siguientes observaciones y sugerencias más relevantes con su respectiva justificación si se debe aplicar o no

A continuación, se muestra en la Tabla 19 el análisis y la justificación de las observaciones hechas por los especialistas

Tabla 19: Análisis de resultados de la validación de los especialistas (Autoría Propia)

Especialista	Observación	Justificación
Ing. Melissa Chinyemba	Se sugiere incluir ISO 27001 y COBIT en las principales normas	**No se consideró.** Esto se debe a que con el marco de trabajo NIST v1.1 ya se está considerando la ISO 27001 y el marco de trabajo COBIT, debido a que las normas que propone NIST están referenciadas y basadas en las buenas prácticas ya mencionadas
	Sería bueno incluir amenazas de seguridad cibernética tanto intencionales como no intencionales	**Si se consideró.** Esta sugerencia si se ha tomado en algunos casos debido a que el accionar del personal de forma inadecuada se complementa con un ataque externo que no será efectivo al menos que el empleado lo permita, por lo tanto, se han definido también amenazas no intencionales
	Algunas normas de NIST framework no fueron incluidas dentro de la matriz situacional	**Si se consideró.** Esta observación si se tomó en cuenta y se agregaron las normas faltantes; sin embargo, no se tomó todas en su totalidad debido a que no se busca una aplicar el marco de trabajo NIST en su totalidad, sino que tomar de referencia ciertas normas involucradas que puedan ser evaluadas dentro de la organización
	Correcciones del código de las normas NIST propuestas en la matriz situacional	**Si se consideró.** Esta observación se tomó en cuenta debido a un error de identificación en los códigos de la norma NIST que se agregó a la matriz situacional

Ing. Jennifer Ayllón	Se sugiere incluir como guía los objetivos indicados en la ISO 27001 e ISO 27032	**No se consideró.** Esto se debe a que con el marco de trabajo NIST v1.1 ya se está considerando la ISO 27001 y el marco de trabajo COBIT, debido a que las normas que propone NIST están referenciadas y basadas en las buenas prácticas ya mencionadas
	Se sugiere considerar ISO 27004 - Medición de la Seguridad de la Información	**Si se consideró.** Esta observación se tomó como referencia para la definición de los objetivos que propone el modelo MANIC
	En gestión de activos se debe aclarar que se tratan de activos digitales o activos que soportan servicios o información digital. Se habla de eventos y anomalías, pero no queda clara la diferencia o escalamiento de estos en los textos. Se recomienda que los niveles Ejecutado, No Aplica, En Proceso, Optimizado, Incompleto, estén en orden de peso para el marco MANIC	**Si se consideró.** Estas observaciones fueron consideradas y se hizo la modificación respectiva en la matriz de análisis situacional
	El conocimiento no siempre está alineado a la conciencia. Se recomendaría incluir test de ingeniería social. Y que la nota sea referente al resultado esperados por áreas.	**Si se consideró.** Esta observación fue considerada y se modificó las métricas existentes para evaluar el cumplimiento de los objetivos
	Se sugirió algunas métricas adicionales y poder estimar un valor en la métrica como límite o medio de evaluación	**Si se consideró.** Esta observación fue considerada y se agregó nuevas métricas para evaluar el cumplimiento de los objetivos
	En la matriz de trazabilidad para los patrones de comportamiento se agregó nuevas relaciones de asociación de factores causales con amenazas no intencionales	**Si se consideró.** Esta observación si se tomó en cuenta para mejorar la matriz de trazabilidad que propone los patrones de comportamiento en base a los factores causales con su respectiva amenaza no intencional de Ciberseguridad
	Sugiero incluir un acápite que indique que personal debería formar parte del equipo de trabajo que ejecute la guía y las competencias debe tener el personal que realice estos trabajos	**Si se consideró.** Esta observación se tomó en cuenta dentro para la guía de implementación del modelo MANIC
	Considerar la fórmula de validación de los riesgos en la guía o en la matriz de gestión de riesgos	**Si se consideró.** Esta observación se tomó en cuenta dentro de la matriz de gestión de riesgos y la guía de

		implementación para poder entender cómo se calcula la validación de riesgo

7.2.4 Control de cambios en base a los resultados

El control de cambios muestra las diferencias entre el documento original y los cambios realizados en base a las observaciones hechas por los especialistas. En esta sección se presenta solo los componentes originales del modelo resaltando los cambios realizados después de analizar su relevancia en el modelo, debido a que los componentes modificados ya se encuentran definidos y desarrollados en los acápites anteriores. Los componentes originales con los cambios mencionados se encuentran en el **Anexo G.**

7.2.5 Elaboración del informe de resultados

El informe de resultados consiste en la presentación de todas las observaciones hechas por los especialistas, la cual incluye los comentarios de los especialistas, nivel de pertinencia de cada componente y recomendación o sugerencia en cada resultado enviado. Las validaciones de los especialistas fueron hechas en dos momentos con fechas establecidas debido a la disponibilidad del especialista y los tiempos para revisar los resultados. Debido a la cantidad de documentos que fueron enviados, tanto en formato Word como en formato Excel, se tiene una carpeta compartida con todos los documentos revisados que se encuentra en el **Anexo H.**

7.3 Discusión

Los resultados obtenidos forman parte del modelo en la medida que permiten dar una validación al modelo previo a su aplicación en una institución pública.

Estos resultados son consistentes con proyectos, marcos de trabajo e investigaciones que permiten tener la conformidad de un experto para dar mayor relevancia al trabajo o proyecto que necesite la aprobación de un especialista. Por lo tanto, la generalización de estos resultados es posible gracias a que son medidas utilizadas en otras investigaciones. Sin embargo, existen algunas limitaciones debido al tema específico del proyecto, ya que el tipo de validación que se hace es de juicio experto debido a la propuesta del tema. Existen otros tipos de proyecto que no necesariamente depende de un juicio experto sino más bien de un análisis o prueba de usuario si hablamos de un tema de desarrollo, por ejemplo y así existen distintos tipos de validaciones dependiendo del tipo de proyecto.

Capítulo 8. Conclusiones y Trabajos Futuros

Los resultados obtenidos forman parte de los componentes del modelo que tienen la finalidad de diseñar un modelo funcional aplicado a organizaciones del estado peruano en busca de la reducción de amenazas no intencionales por parte del personal. Cada uno de los resultados han sido elaborados en base a un cronograma que permite separar las actividades con el fin de facilitar la elaboración de cada componente. Estos componentes están alineados con investigaciones previas y buenas prácticas.

A continuación, se describirán las conclusiones del presente trabajo y algunos de los posibles trabajos futuros que pueden continuar desarrollándose como resultado de la investigación

8.1 Conclusiones

El modelo propuesto, como ya se explicó, consta de cinco fases o componentes. El proceso inicial empieza con la definición de los componentes, que luego pasa a una etapa de diseño de cada uno con foco principalmente en la lista de patrones de comportamiento y la matriz de gestión de riesgos. Estos componentes hacen la diferencia con otras investigaciones y pueden adaptarse a nuevos escenarios que puedan aparecer como parte de los procesos de TI dentro de una o varias organizaciones. Adicionalmente, es necesario mencionar que cada uno de los componentes está alineado con los objetivos específicos del proyecto y el objetivo general.

Los objetivos están alineados a cada capítulo que contiene los resultados necesarios para lograr cumplir con cada uno de los objetivos planteados. Para alcanzar los objetivos fue necesario hacer un diseño top-down que pueda ir de lo más complejo a lo más simple, es así como se fue elaborando cada resultado para al final poder alcanzar los objetivos.

Los logros obtenidos para el cumplimiento de los objetivos son los siguientes:

- Se logró definir los componentes a alto nivel del modelo, para poder desarrollar cada uno de forma más eficiente y ordenada con la finalidad de que se pueda leer su documentación y puedan ser aplicados eficientemente.
- Se logró diseñar los componentes del modelo, partiendo desde un análisis situacional basado en buenas prácticas y marcos de trabajo hasta llegar al análisis de riesgos para poder establecer relaciones entre cada componente. La finalidad de este logro es poder establecer una línea de trabajo para organizaciones que tengan o no un lineamiento para la seguridad. El modelo busca hacer sinergias entre

distintos marcos y estándares para adaptarse a la organización y asi poder identificar los puntos más vulnerables de ciberseguridad para luego centrarse específicamente en vulnerabilidades asociadas a amenazas no intencionales. Esto con la finalidad de mitigar y proponer ciertas medidas específicas para reducir los riesgos asociados.

- Se logró validar los componentes del modelo con los especialistas en Seguridad de la Información y Ciberseguridad, los cuales aportaron desde su conocimiento y experiencia un enfoque más preciso al momento de construir y definir los componentes del modelo MANIC.
- Se logró diseñar una guía de implementación del modelo con la finalidad de permitir la aplicación del modelo dentro de las organizaciones públicas siguiendo un conjunto de pasos.
- Finalmente, se logró definir los patrones de comportamiento del personal, con la finalidad de encontrar factores causales que puedan ser los motivadores para que una amenaza se haga efectiva dentro de la organización.

Tanto el modelo como la guía de implementación fueron validados por especialistas de una institución pública con conocimientos en ciberseguridad, seguridad de la información y buenas prácticas aplicadas a institución del estado. Estas validaciones cuentan con sus respectivas actas y observaciones relevantes para su mejora y uso del modelo propuesto. A continuación, se describen los posibles trabajos futuros.

8.2 Trabajos futuros

Como continuación de este trabajo de tesis y como en cualquier otro proyecto de investigación, existen diversas líneas de investigación que quedan abiertas y en las que es posible continuar trabajando. Durante el desarrollo de esta tesis han surgido algunos tópicos o ramas a seguir investigando que se han dejado abiertas y se esperan atacar en un futuro; Alguna de estas líneas están directamente relacionadas con este trabajo de tesis y otras más generales puede servir para otras investigaciones complementarias.

A continuación, se presentan algunos trabajos futuros que pueden desarrollarse como resultado de esta investigación o que, por exceder el alcance de esta tesis, no han podido ser tratados con la suficiente profundidad.

- Aplicación del modelo en entidades públicas del estado peruano
- Comparar los resultados obtenidos después de aplicar el modelo en una institución pública con los resultados propuestos antes de ser aplicado el modelo

- Implementar el modelo en una solución web o sistema local para integrar los componentes dentro de una sola plataforma con la finalidad de guardar una historia con sus respectivos archivos del modelo asi como una historia de la organización y mantener los componentes juntos. La finalidad de esta implementación es la integración y la toma de decisiones en el menor tiempo posible.
- Realizar un estudio para identificar nuevos patrones de comportamiento por medio de algoritmos de machine learning y sus implicancias

Referencias

Abdul Molok, N. N., Ahmad, A., & Chang, S. (2018). A case analysis of securing organisations against information leakage through online social networking. International Journal of Information Management. https://doi.org/10.1016/j.ijinfomgt.2018.08.013

Agudelo-Serna, C. A., Ahmad, A., Bosua, R., & Maynard, S. B. (2018). Strategies to Mitigate Knowledge Leakage Risk caused by the use of mobile devices: A Preliminary Study. ICIS 2017: Transforming Society with Digital Innovation.

Alshaikh, M., Ahmad, A., Maynard, S. B., & Chang, S. (2014). Towards a taxonomy of information security management practices in organisations. Proceedings of the 25th Australasian Conference on Information Systems, ACIS 2014.

Alshaikh, M., Maynard, S. B., Ahmad, A., & Chang, S. (2015). Information security policy: A management practice perspective. ACIS 2015 Proceedings - 26th Australasian Conference on Information Systems.

Alshaikh, M., Maynard, S. B., Ahmad, A., & Chang, S. (2018). An Exploratory Study of Current Information Security Training and Awareness Practices in Organizations. Proceedings of the 51st Hawaii International Conference on System Sciences. https://doi.org/10.24251/hicss.2018.635

Alshaikh, M., Naseer, H., Ahmad, A., Maynard, S. B., paper Alshaikh, R., & Sean, M. (2019). Toward Sustainable Behaviour Change: an Approach for Cyber Security Education Training and Awareness. Twenty-Seventh European Conference on Information Systems (ECIS2019).

Altukruni, H., Maynard, S., Ahmad, A., & Alshaikh, M. (2019). Exploring Knowledge Leakage Risk in Knowledge-Intensive Organisations: behavioural aspects and key controls. https://doi.org/10.13140/RG.2.2.21492.71046

Boholm, Asa. "The Cultural Nature of Risk: Can There Be an Anthropology of Uncertainty?" Ethnos: Journal of Anthropology 68, 2 (2003): 159-178.

Borky, J., & Bradley, T. (2019). Protecting Information with Cybersecurity (pp. 345–404). https://doi.org/10.1007/978-3-319-95669-5_10

Burnes, D., DeLiema, M., & Langton, L. (2020). Risk and protective factors of identity theft victimization in the United States. Preventive Medicine Reports. https://doi.org/10.1016/j.pmedr.2020.101058

Carlton, M., Levy, Y., & Ramim, M. (2019). Mitigating cyber-attacks through the measurement of non-IT professionals' cybersecurity skills. Information and Computer Security. https://doi.org/10.1108/ICS-11-2016-0088

Ceesay, E. N., Myers, K., & Watters, P. (2018). Human-centered strategies for cyber-physical systems security. ICST Transactions on Security and Safety, 4, 154773. https://doi.org/10.4108/eai.15-5-2018.154773

CEPAL. (2009). Gobierno Electrónico y Gestión Pública. https://www.cepal.org/ilpes/noticias/paginas/5/39255/gobierno_electronico_anaser.pdf

CERT. (2013). Unintentional Insider Threats: A Foundational Study.

Chak, S. K. (2015). Managing Cybersecurity as a Business Risk for Small and Medium Enterprises. Biomass Chem Eng.

J. Carlton Collins. (2019). Check on data breaches at the Privacy Rights Clearinghouse. https://www.journalofaccountancy.com/issues/2019/sep/data-breaches-privacy-rights-clearinghouse.html

Chen, H., & Fiscus, J. (2018). The inhospitable vulnerability: A need for cybersecurity risk assessment in the hospitality industry. Journal of Hospitality and Tourism Technology. https://doi.org/10.1108/JHTT-07-2017-0044

Chinyemba, M. K., & Phiri, J. (2018a). An investigation into information security threats from insiders and how to mitigate them: A case study of Zambian public sector. Journal of Computer Science. ttps://doi.org/10.3844/jcssp.2018.1389.1400

Chinyemba, M. K., & Phiri, J. (2018b). AN INVESTIGATION OF INFORMATION SECURITY THREATS FROM ORGANISATIONAL INSIDERS AND HOW TO MITIGATE THEM USING A USER AWARENESS & ACCESS CONTROL MODEL.

Chinyemba, M. K., Phiri, J., Research, S., & Supervisor. (2018). AN INVESTIGATION INTO THE CYBER SECURITY THREATS BY INSIDERS: A CASE OF ZAMBIAN PUBLIC ORGANISATIONS. References 1.6 Significance of Study. https://doi.org/10.13140/RG.2.2.24071.65443

Conteh, N. Y., & Schmick, P. J. (2016). Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks. International Journal of Advanced Computer Research. https://doi.org/10.19101/ijacr.2016.623006

Delgado, M. F. (n.d.). Taller de Implementación de la Norma ISO 27001. https://www.pecert.gob.pe/images/publicaciones/4.pdf

Douglas, Mary. Risk and Blame. Routledge, 1992.

Endsley, M. R. "A Taxonomy of Situation Awareness Errors," 287-292. Human Factors in Aviation Operations: Proceedings of the 21st Conference of the European Association for Aviation Psychology. Gower Technical, 1995.

eEurope 2002. (2000). eEurope 2002 (Issue June, pp. 1–30). https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52000DC0330&from=ES

Ernst and Young. (2016). Managing Internal Threat.

Evans, M., He, Y., Luo, C., Yevseyeva, I., Janicke, H., Zamani, E., & Maglaras, L. A. (2019). Real-Time Information Security Incident Management: A Case Study Using the IS-CHEC Technique. IEEE Access. https://doi.org/10.1109/ACCESS.2019.2944615

Evans, M., He, Y., Maglaras, L., Yevseyeva, I., & Janicke, H. (2019). Evaluating information security core human error causes (IS-CHEC) technique in public sector and comparison with the private sector. International Journal of Medical Informatics. https://doi.org/10.1016/j.ijmedinf.2019.04.019

Fang, Z. (2002). e-Government in digital era: concept, practice and development. International Journal of the Computer, the Internet and Management.

Fischbacher-Smith, D. (2015). The enemy has passed through the gate: Insider threats, the dark triad, and the challenges around security. Journal of Organizational Effectiveness. https://doi.org/10.1108/JOEPP-03-2015-0010

Fundación Telefónica. (2016). Ciberseguridad, la protección de la información en un mundo digital.

Gander, P.H.; Nesdale, A.; & Signal, L. A Review of Locomotive Engineers' Extended Hours of Service. 2002

GARCÍA, V. (2019). ¿CÓMO ESTÁ AVANZANDO LA CIBERSEGURIDAD EN EL PERÚ? BREVE APROXIMACIÓN AL MARCO NORMATIVO. The Progress of Cybersecurity Regulation in Peru.

Gestión. (2019). Perú carece de una ley de Ciberseguridad que proteja información pública y privada, alerta Comex. https://gestion.pe/economia/ciberseguridad-comex-peru-carece-de-una-ley-de-ciberseguridad-que-proteja-informacion-publica-y-privada-alerta-comex-noticia/?ref=gesr

Gestión. (2020). Los cinco ciberataques más frecuentes en el Perú https://gestion.pe/tecnologia/los-cinco-ciberataques-mas-frecuentes-en-el-peru-hackers-noticia/?ref=gesr

Gheyas, I. A., & Abdallah, A. E. (2016). Detection and prediction of insider threats to cyber security: a systematic literature review and meta-analysis. Big Data Analytics. https://doi.org/10.1186/s41044-016-0006-0

Greitzer, F. L., Strozer, J., Cohen, S., Bergey, J., Cowley, J., Moore, A., & Mundie, D. (2014). Unintentional insider threat: Contributing factors, observables, and mitigation strategies. Proceedings of the Annual Hawaii International Conference on System Sciences. https://doi.org/10.1109/HICSS.2014.256

Grönlund, Å, & Horan, T. A. (2005). Introducing e-Gov: History, Definitions, and Issues. Communications of the Association for Information Systems. https://doi.org/10.17705/1cais.01539

Hadlington, L. (2018). Employees attitude towards cyber security and risky online behaviours: An empirical assessment in the United Kingdom. International Journal of Cyber Criminology. https://doi.org/10.5281/zenodo.1467909

Halim, H., & Yusof, M. M. (2019). Framework for digital data access control from internal threat in the public sector. International Journal of Advanced Computer Science and Applications. https://doi.org/10.14569/ijacsa.2019.0100809

Hernández, R., Fernández, C., & Baptista, P. (2014). Metodología de la investigación. In Journal of Chemical Information and Modeling. https://doi.org/10.1017/CBO9781107415324.004

Hernández-Hernández, N., & Garnica-González, J. (2015). Árbol de Problemas del Análisis al Diseño y Desarrollo de Productos Problem Tree Analysis to the Design and Development Products. Conciencia Tecnológica.

Hunker, J., & Probst, C. W. (2011). Insiders and insider threats an overview of definitions and mitigation techniques. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications.

IBM, Alvarez, M., Bales, D., Chung, J., Craig, S., Dahl, K., DeBeck, C., Eitan, A., Faby, B., Gates, R., Harz, D., Kessem, L., Lee, C., McMillen, D., Moore, S., Prassinos, G., Singleton, C., Usher, M., Vila, A., ... Zarabedian, J. (2020). X-Force Threat Intelligence Index 2020. In IBM X-Force Incident Response and Intelligence Services.

International Organization for Standardization. (2011). ISO - About ISO. http://www.iso.org/iso/about.htm

ISACA. (2015). Cybersecurity Fundamentals Study Guide. CyberSecurity Nexus, 1.

ISACA. (2019). COBIT® 2019 FRAMEWORK: INTRODUCTION & METHODOLOGY. In COBIT® 2019 FRAMEWORK: INTRODUCTION & METHODOLOGY.

ISO/IEC 27005:2018. (2018). Information technology -- Security techniques -- Information security risk management. ISO/IEC.

Izard, C. E. (2009). Emotion Theory and Research: Highlights, Unanswered Questions, and Emerging Issues. Annual Review of Psychology. https://doi.org/10.1146/annurev.psych.60.110707.163539

James, W. Ch. XI, "The Stream of Consciousness." Psychology. Henry Holt and Co., 1892.

Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007). Protecting people from phishing: The design and evaluation of an embedded training email system. Conference on Human Factors in Computing Systems - Proceedings. https://doi.org/10.1145/1240624.1240760

Keele, S. (2007). Guidelines for performing systematic literature reviews in software engineering. In Technical report, Ver. 2.3 EBSE Technical Report. EBSE.

Kraemer, K. L. (1978). Local Government and Information Technology in the United States.

Kyeremeh, K., Kyeremeh Bright, B., & Afful Forson, M. (2019). A Study into the Social Engineering Risk and Its Effects in the Public Institutions in Ghana. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3404246

Lechner, N. H. (2017). An Overview of Cybersecurity Regulations and Standards for Medical Device Software. Central European Conference on Information and Intelligent Systems.

Ley N° 30999. Diario Oficial de la República del Bicentenario, El Peruano, Lima, Perú, / Martes 27 de agosto de 2019.

Maalem Lahcen, Rachid Ait Caulkins, Bruce Mohapatra, Ram, Kumar, M. (2020). Review and insight on the behavioral aspects of cybersecurity.

Mat Roni, S. (2015). An Analysis of Insider Dysfunctional Behaviours in an Accounting Information System Environment.

Metcalfe, R. M., & Boggs, D. R. (1976). Ethernet: Distributed Packet Switching for Local Computer Networks. Communications of the ACM. https://doi.org/10.1145/360248.360253

Michael Juma Abuli. (2016). A Framework for Assessing the Insider Threat in Parastatals in Kenya.

Microsoft. (2011). Informe de inteligencia de seguridad de Microsoft.

Miguel Ángel Mendoza. (2014). Business Impact Analysis (BIA) y la importancia de priorizar procesos. https://www.welivesecurity.com/la-es/2014/11/06/business-impact-analysis-bia/

Moinescu, Radu; Răcuciu, Ciprian; Glăvan, Dragoş; Antonie, Narcis-Florentin; Eftimie, S. (2019). Aspects of human weaknesses in cyber security.

Moore, A. P., Kennedy, K. A., & Dover, T. J. (2016). Introduction to the special issue on insider threat modeling and simulation. Computational and Mathematical Organization Theory. https://doi.org/10.1007/s10588-016-9210-8

Musambo, L. K., Chinyemba, M. K., & Phiri, J. (2017). Identifying Botnets Intrusion & Prevention – A Review. Zambia ICT Journal. https://doi.org/10.33260/zictjournal.v1i1.28

Onibere, M., Ahmad, A., & Maynard, S. (2019). Dynamic Information Security Management Capability: Strategising for Organisational Performance.

OSI. (2018). ¿Sabías que el 95% de las incidencias en ciberseguridad se deben a errores humanos? https://www.osi.es/es/actualidad/blog/2018/12/05/sabias-que-el-95-de-las-incidencias-en-ciberseguridad-se-deben-errores

PCM. ONGEI. (2013). UNA MIRADA AL GOBIERNO ELECTRÓNICO EN EL PERÚ. http://www2.congreso.gob.pe/sicr/cendocbib/con4_uibd.nsf/0D6D8CA5D781070305257E9200775428/$FILE/3_pdfsam_libro_ongei.pdf

Peddada, K. (2013). Risk assessment and control. Journal of Governance and Regulation. https://doi.org/10.22495/jgr_v2_i2_p4

Petticrew, M., & Roberts, H. (2008). Systematic Reviews in the Social Sciences: A Practical Guide. In Systematic Reviews in the Social Sciences: A Practical Guide. https://doi.org/10.1002/9780470754887

Pitropakis, N. (2015). Detecting Malicious Internal Threat in Cloud Computing Environments Ph.D.

Proyecto de Ley N° 4352/2018-CR. Congreso de la República del Perú, Lima, Perú, / Lunes 22 de julio de 2019.

Proyecto de Ley N° 4237/2018-CR. Congreso de la República del Perú, Lima, Perú, / Lunes 22 de julio de 2019.

PWC. (2018). Encuesta Mundial sobre el Estado de la Seguridad de la Información 2018. https://www.pwc.es/es/digital/encuesta-mundial-ciberseguridad-2018.html

Resolución Ministerial N° 081-2014-EF/44, "Políticas de Seguridad de la Información del Ministerio de Economía y Finanzas", Lima, Perú, /Miércoles 06 de abril del 2016

Salinas Ibáñez, J. (2004). Cambios metodológicos con las TIC: estrategias didácticas y entornos virtuales de enseñanza-aprendizaje. Bordón. Revista de Pedagogía.

Servicios TIC. (2006). Definición de TIC. http://www.serviciostic.com/las-tic/definicion-de-tic.html

Silowash, G., Shimeall, T. J., Cappelli, D., Moore, A., Flynn, L., & Trzeciak, R. (2012). Common Sense Guide to Mitigating Threats. In CERT Program.

Smallwood, J. & Schooler, J. W. “The Restless Mind.” Psychological Bulletin 132, 6 (2006): 946-958.

Symantec. (2018). Internet security threat report. In Network Security. https://doi.org/10.1016/S1353-4858 (05)00194-7

Tu, M., Spoa-Harty, K., & Xiao, L. (2015). Data Loss Prevention Management and Control: Inside Activity Incident Monitoring, Identification, and Tracking in Healthcare Enterprise Environments. Journal of Digital Forensics, Security and Law. https://doi.org/10.15394/jdfsl.2015.1196

U.S. (2002). E-Government Act of 2002. https://www.govinfo.gov/content/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf

Walters, P. (2012). The Risks of Using Portable Devices.

Wu, C. Y., Lee, M. B., Liao, S. C., & Chang, L. R. (2015). Risk factors of internet addiction among internet users: An online questionnaire survey. PLoS ONE. https://doi.org/10.1371/journal.pone.0137506

Wunderlich, J. L. (2011). The Insider Threat.

Yerkes R. M. & Dodson J. D. “The Relation of Strength of Stimulus to Rapidity of Habit-Formation.” Journal of Comparative Neurology and Psychology 18, 5 (Nov. 1908): 459-482.

Anexos

Anexo A: Plan de Proyecto

- **Justificación**

De acuerdo con un informe hecho por investigadores de seguridad de IBM en el 2018 (OSI, 2018), el 95 % de los ciberataques son debido a fallos humanos. Estos ataques en su mayoría pueden ser de un agente externo; sin embargo, la vulnerabilidad producto de un error humano empieza desde adentro de la institución (OSI, 2018), Este error se debe a un comportamiento inadecuado que genera una respuesta negativa por parte del personal ante una falta de medidas impuesta por la institución o gobierno que gestiona la seguridad de la información en instituciones públicas. En un informe realizado por la compañía conocida como NortonLifeLock (anteriormente conocida como Symantec) en el 2018 (Symantec, 2018), reveló que el 54.6 % de correos que reciben los usuarios son spam, los cuales son correos que generan confianza en el usuario y tienen la finalidad de obtener información financiera o de otra índole. Este tipo de amenaza se conoce como phishing (OSI, 2018),

En cifras más actuales, de acuerdo a un reporte realizado por IBM en 2020 (IBM et al., 2020), el gobierno se encuentra en el sexto lugar como uno de los sectores más atacados por amenazas de ciberseguridad como se presenta en la Figura 1 entre los años 2019 y 2018 (IBM et al., 2020). El informe muestra que los gobiernos son un objetivo de alto valor para los agentes cibernéticos debido al dinero que manejan y principalmente información confidencial que no solo del gobierno sino de los ciudadanos (IBM et al., 2020).

Sector	2019 rank	2018 rank	Change
Financial Services	1	1	–
Retail	2	4	2
Transportation	3	2	-1
Media	4	6	2
Professional services	5	3	-2
Government	6	7	1
Education	7	9	2
Manufacturing	8	5	-3
Energy	9	10	1
Healthcare	10	8	-2

Figura 1: Top 10-targeted industries ranked by attack volume, 2019 vs. 2018 (Source: IBM X-Force)

Entre los principales vectores de amenaza a nivel mundial que se obtuvo en el 2019 se tienen que las amenazas de tipo phishing representan el 31 % a nivel mundial como se presenta en la Figura 2 (IBM et al., 2020). Esto demuestra un gran avance de este tipo de amenazas que puede ser perjudicial para las organizaciones.

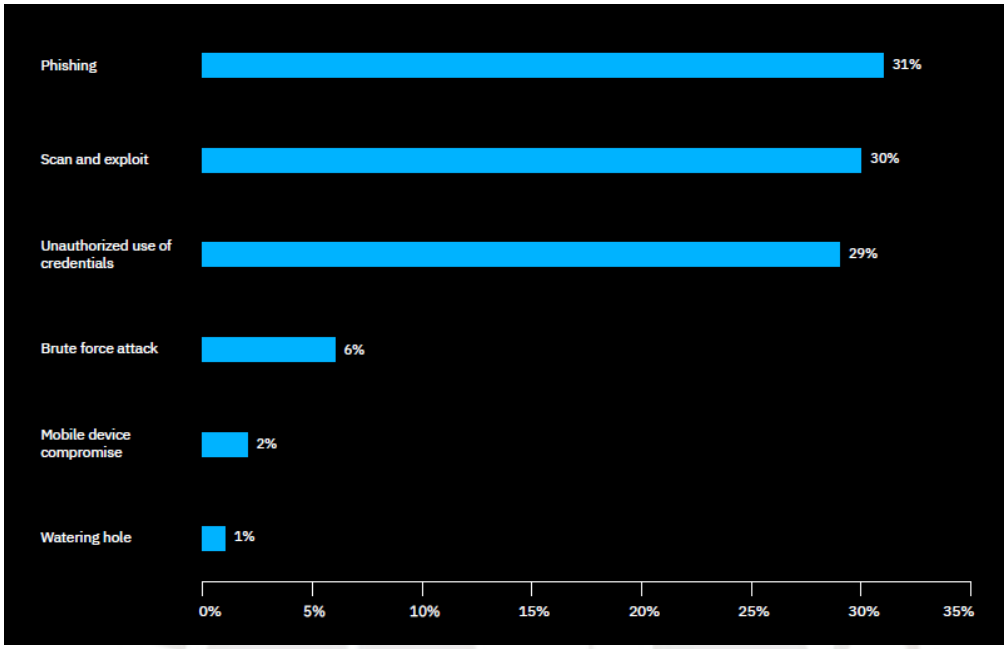


Figura 2: X-Force Threat Intelligence Index (IBM) (2020)

Estos resultados muestran como las amenazas están en constante crecimiento entre distintos sectores. Sin embargo, para poder entender cómo estos resultados impactan en el desarrollo de un gobierno y de sus instituciones, es necesario trasladar estos datos a nivel monetario. En la última encuesta mundial sobre el estado de seguridad de la información 2018, se obtuvo 4.8 millones de dólares en pérdidas a nivel mundial por parte de las empresas (PWC, 2018). El 44 % de los directivos en el mundo reconoce que sus empresas carecen de una estrategia integral de seguridad (PWC, 2018). y el 55% no dispone de procedimientos previamente establecidos para responder a los incidentes de seguridad. Si bien estas cifras y resultados ya tienen cierto año de ser reportados, de acuerdo a la Figura 1, es evidente ver que estos resultados van en aumento, y se espera que en el 2020 tengamos datos similares.

El proyecto planteado contribuirá a generar un modelo para identificar estas amenazas de ciberseguridad en base a los comportamientos de los empleados en relación a la infraestructura de TI (conveniencia). Asimismo, el diseño del modelo ayudará a las organizaciones públicas a poder manejar un control de riesgos en base a las amenazas identificadas, también podrá complementar el entendimiento del comportamiento del colaborador en base a las actividades que realiza identificando los posibles incidentes y

finalmente puede ser de apoyo inicial para políticas de seguridad dentro de las organizaciones públicas (implicación práctica). El objetivo social del proyecto podrá beneficiar a las organizaciones públicas con un mayor control de seguridad con el fin de proteger la información de la institución y sus bienes (relevancia social).

- **Viabilidad**

Dentro de la viabilidad, se tiene como puntos principales para la elaboración del proyecto los siguiente:

  - Acceso a los recursos tecnológicos y documentación existente para establecer el modelo
  - No es necesario la compra de recursos digitales como herramientas o normas para la elaboración del proyecto
  - Acceso a las instituciones públicas que van a validar el modelo.
  - Se tiene los conocimientos necesarios para la elaboración del proyecto

- **Alcance**

El proyecto se relaciona al área de Tecnología de la Información (TI), específicamente a Gobierno electrónico. Se ha elegido esta área en específico, debido al impacto que tiene dentro de las instituciones públicas en el Perú, además que al ser instituciones públicas pueden facilitar la recolección de información. En cuanto a la metodología, el proyecto es de tipo de desarrollo tecnológico, pues pretende diseñar un modelo que será aplicado en instituciones públicas peruanas en el contexto actual del Perú. El modelo está relacionado a la identificación de amenazas no intencionales de ciberseguridad en instituciones públicas por parte del personal interno debido a su comportamiento. El modelo podrá ser adaptado a cualquier institución pública peruana, pero por la validación que se realizará, el modelo será aplicado a municipalidades de la región. El proyecto considera dentro de la problemática todo tipo de personal interno, esto incluye cualquier persona facultada para laborar ya sea hombre o mujer, que tenga relación con la infraestructura de TI en organizaciones públicas peruanas.

- **Restricciones**

El proyecto exige realizar encuestas y entrevistas con expertos para validar el modelo que se pretende desarrollar en el proyecto. Al solicitar acceso y comunicación a los expertos que pertenecen a las instituciones donde se espera validar el modelo, es

posible que no tenga la disponibilidad para concretar la comunicación y la información que puedan brindarnos. Adicionalmente, se puede tener como limitante la validación del componente del modelo debido a su complejidad al momento de la validación. También se debe mencionar la falta de información especializada y actualizada sobre el tema en el Perú; los estudios al respecto son muy escasos y no establecen la realidad actual del sector en todos sus aspectos.

- **Identificación de los riesgos del proyecto**

Umbral de Riesgo

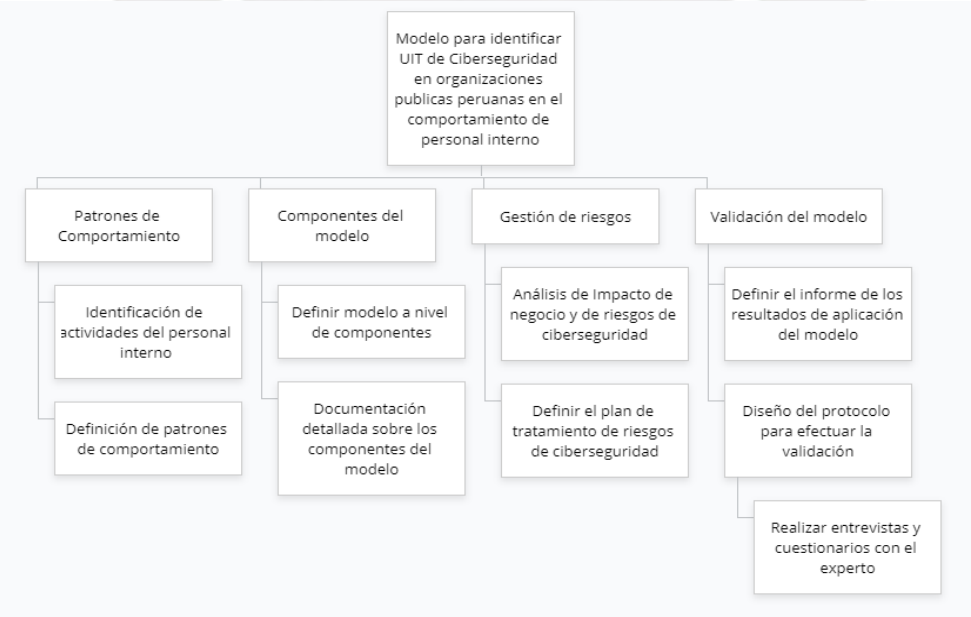
		Impacto		
	Indicadores	Bajo (1)	Moderado (2)	Alto(3)
Probabilidad	Casi Seguro (5)	5	10	15
	Probable (4)	4	8	12
	Posible (3)	3	6	9
	Improbable (2)	2	4	6
	Remota (1)	1	2	3

Matriz de Riesgos

	No se tiene Acceso a experto	**Malograr Equipos que contengan la información del proyecto de tesis**	**Problemas de Conectividad a internet**
Descripción	Problemas con la validación del modelo propuesto por falta de verificación del modelo por parte del experto	Pérdida de la información del proyecto y del modelo que se propone diseñar	No se tiene acceso a la información guardada en los medios de almacenamiento cloud, imposibilidad para presentar el proyecto a los jurados
Síntomas	**1.** Falta de disponibilidad del experto **2.** Desconfianza con brindar información sensible de la institución públicas **3.** Problemas de salud que imposibiliten la comunicación Centralización de la	**1.** No tener un backup de respaldo **2.** No tener la información compartida con los asesores **3.** No manejar versiones anteriores en caso de pérdida de la actual versión	**1.** Mala conectividad **2.** Poco ancho de banda **3.** Caída de la red

	información en una sola persona		
Probabilidad	Probable	Posible	Posible
Impacto	Alto	Alto	Moderado
Severidad	**12**	**9**	**6**
Mitigación	**1.** Elaboración de acta de compromiso **2.** Elaboración de acta de confidencialidad de la información	**1.** Crear un backup en la nube **2.** Crear un backup en la computadora personal **3.** Compartir la información con asesores **4.** Manejar versiones de contingencia	**1.** Programar una hora con menos saturación de la red
Contingencia	**1.** Validar el modelo con los asesores del proyecto cumpliendo la función de especialistas y firmando un acta de validación	**1.** Utilizar las últimos entregables enviados a los profesores del curso o asesores	**1.** Grabar un video expositivo con la presentación del proyecto

- **Estructura de descomposición del trabajo (EDT)**



- **Lista de Tareas**

Diseño de un modelo para identificar amenazas no intencionales de ciberseguridad en instituciones públicas generadas por personal interno a partir de su comportamiento sobre la infraestructura de TI

Total: 10 semanas para la elaboración del proyecto en el semestre 2020-2 + el mes de agosto (2 semanas) = 12 semanas

1. Definición de los patrones de comportamiento en el personal interno de las organizaciones públicas para las amenazas no intencionales de ciberseguridad.
   Duración estimada: 3 semanas
   Esfuerzo asociado: 3 semanas/persona
   a. Identificación de las actividades sobre la infraestructura de TI en base al personal interno de la organización.
   b. Asociación de los patrones preestablecidos en la revisión sistemática con las actividades identificadas.
   c. Reuniones con los asesores

2. Diseño de los componentes del modelo a alto nivel basado en los patrones de comportamiento, que incluya la gestión de riesgos para la ciberseguridad.
   Duración estimada: 1 semana
   Esfuerzo asociado: 1 semana/persona
   a. Definición de los componentes del modelo
      i. Patrones de comportamiento
      ii. Objetivos, métricas e indicadores
      iii. Análisis de impacto de negocio y de riesgos de ciberseguridad
      iv. Plan de tratamiento de riesgos de ciberseguridad
      v. Guía de aplicación
   b. Esquematización de los componentes del modelo
   c. Reuniones con los asesores

3. Implementación de los componentes del modelo basado en estándares para la seguridad de la información en el Perú en amenazas no intencionales de ciberseguridad
   Duración estimada: 4 semanas
   Esfuerzo asociado: 4 semanas/persona
   a. Documentación detallada de los componentes del modelo
      i. Patrones de comportamiento
      ii. Objetivos, métricas e indicadores
      iii. Análisis de impacto de negocio y de riesgos de ciberseguridad
      iv. Plan de tratamiento de riesgos de ciberseguridad
      v. Guía de aplicación
   b. Reuniones con los asesores

4. Validación del modelo propuesto en una institución pública relacionada a la gestión de amenazas no intencionales de ciberseguridad
   Duración estimada: 4 semanas
   Esfuerzo asociado: 4 semanas/persona

   a. Identificación de las instituciones públicas
   b. Selección de las instituciones públicas que van validar el modelo
   c. Elaboración del protocolo de validación
   d. Elaboración de matrices de cada uno de los componentes del modelo a validar
   e. Análisis de los resultados de la validación
   f. Control de cambios en base a los resultados de la validación
   g. Elaboración del informe de los resultados de la aplicación del modelo
   h. Elaboración de conclusiones del proyecto

- **Cronograma del proyecto**
  El cronograma del proyecto presenta las semanas del ciclo regular y los resultados que se espera realizar por cada semana, teniendo en consideración las fechas establecidas.

OBJETIVOS ESPECÍFICOS (OE) Y RESULTADOS ESPERADOS (RE)	TAREAS	RESPONSABLE	FECHA DE INICIO	FECHA FINAL	DIAS	ESTADO	SEMANAS (60 % / 100 %)														
							EXPOSICIÓN 1	EXPOSICIÓN 2	EXPOSICIÓN 3	EXPOSICIÓN 4	AVANCE PARCIAL	AVANCE PARCIAL	EXPOSICIÓN 5	EXÁMENES PARCIALES	EXPOSICIÓN 6	ENTREGABLE FINAL	REVISION DEL JURADO	REVISION DEL JURADO	LEVANTAR OBSERVACION	ULTIMA OBSERVACION	EXPOSICION FINAL	EXPOSICION FINAL
							1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
OE2	**Definición de los componentes del modelo a alto nivel**																						
RE2, RE3, RE4, RE5, RE6	Definir a alto nivel los componentes del modelo	Anderson Castillo	31-Ago	4-Set	4	Terminado																	
OE3	**Diseño de los componentes del modelo (Matriz Situacional, Objetivos e Indicadores)**																						
RE7	Diseño de la Matriz Situacional	Anderson Castillo	31-Ago	8-Set	8	Terminado																	
	Definir Objetivos de Ciberseguridad	Anderson Castillo	5-Set	8-Set	3	Terminado																	
	Definir indicadores para los objetivos de Ciberseguridad	Anderson Castillo	8-Set	11-Set	3	Terminado																	
	Identificación de factores	Anderson Castillo	12-Set	15-Set	3	Terminado																	
	Selección de amenazas no intencionales internas (UIT)	Anderson Castillo	16-Set	18-Set	2	Terminado																	
	Asociación de factores con UIT	Anderson Castillo	18-Set	20-Set	2	Terminado																	
OE1	**Definición de la lista de patrones de comportamiento**																						
RE1	Lista de patrones de comportamiento definidos	Anderson Castillo	21-Set	25-Set	4	Terminado																	
	Verificable (RE1, RE2, RE3, RE4, RE7 parcialmente)	Especialista	29-Set	30-Set	1	Terminado																	
OE3	**Diseño de los componentes del modelo (Matriz de gestión de riesgos, Guía de aplicación)**																						
RE7	Definición de los procesos relacionados a TI	Anderson Castillo	26-Set	29-Set	3	Terminado																	
	Definición de los activos de información involucrados	Anderson Castillo	30-Set	2-Oct	2	Terminado																	
	Identificación de vulnerabilidades	Anderson Castillo	3-Oct	6-Oct	3	Sin empezar																	
	Identificación de amenazas no intencionales	Anderson Castillo	7-Oct	9-Oct	2	Sin empezar																	
	Identificación de riesgos	Anderson Castillo	10-Oct	13-Oct	3	Sin empezar																	
	Medición del impacto en las organizaciones	Anderson Castillo	14-Oct	16-Oct	2	Sin empezar																	
	Medición de probabilidad de ocurrencia de riesgos	Anderson Castillo	15-Oct	19-Oct	4	Sin empezar																	
	Tratamiento de los riesgos (Controles)	Anderson Castillo	19-Oct	23-Oct	4	Sin empezar																	
	Diseño de la guía de implementación	Anderson Castillo	19-Oct	23-Oct	4	Sin empezar																	
OE4	**Validación de los componentes del modelo**																						
RE8	Selección del especialista de la institución pública	Anderson Castillo	19-Oct	23-Oct	4	Sin empezar																	
	Elaboración del protocolo	Anderson Castillo	24-Oct	27-Oct	3	Sin empezar																	
	Indicador Objetivamente Verificable (RE5, RE6, RE7, RE8)	Especialista	27-Oct	28-Oct	1	Sin empezar																	
RE9	Análisis de resultados	Anderson Castillo	28-Oct	30-Oct	2	Sin empezar																	
	Control de cambios en base a resultados	Anderson Castillo	31-Oct	2-Nov	2	Sin empezar																	
	Elaboración del informe de resultados	Anderson Castillo	3-Nov	5-Nov	2	Sin empezar																	
	Elaboración de las conclusiones del proyecto	Anderson Castillo	6-Nov	6-Nov	0	Sin empezar																	
	Reunión semanal con los asesores																						

- **Lista de recursos**
  - **Personas involucradas y necesidades de capacitación**
    i. Mano de obra: horas-hombre (hh)
    ii. Experto en el tema
    iii. Asesores del proyecto de Tesis
  - **Estándares utilizados en el proyecto**
    i. Se hará uso de las normas ISO 27001, 27002 y 27032
  - **Equipamiento requerido**
    i. Laptop Lenovo, Core i7 (7th Gen), 8 GB (RAM), procesador x64

- **Herramientas requeridas**
  - i. Servicio de Internet
  - ii. Software de diseño

- **Costeo del Proyecto**

Ítem	Descripción			Unidad	Cant-	Valor Unidad (S/.)	Monto Parcial (S/.)	Monto Total (S/.)
0	**Costo total del proyecto**			**---**	**---**	**---**	**---**	**2,894.4**
1.	**Estudiantes o tesistas**			**---**	**---**	**---**	**---**	**2,047.5**
1.1	Anderson Castillo Lopez			Horas	195	10.5	2,047.5	
2.	**Otros participantes (en caso aplique)**			**---**	**---**	**---**	**---**	**---**
3.	**Servicios y consultoría (en caso aplique)s**			**---**	**---**	**---**	**---**	**400**
3.1	Melissa K. Chinyemba			Informe	1	400	400	
4.	**Materiales e insumos (en caso aplique)s**			**---**	**---**	**---**	**---**	**---**
5.	**Bienes y equipos**	**Unid1**	**Cant1-**	**Unid2**	**Cant2 -**	**-**	**-**	**446.9**
5.1	Laptop Lenovo	Equipo	1	Meses	3	68.44	205.3	
5.2	Servicio de Internet	Modem	1	Meses	3	37.98	114.1	
5.3	Servicio de Internet de Contingencia	Entel	1	Horas	98	1.30	127.5	
5.4	Software de diseño		1	Horas	50	-	-	
6.	**Pasajes y viáticos**	**Unid1**	**Cant1-**	**Unid2**	**Cant2 -**	**-**	**-**	**-**

Anexo B: Formulario de Extracción de Datos

El formulario de extracción de datos se encuentra en el siguiente link: https://drive.google.com/file/d/1fMXItMUt3KyoGJqhyy_L7px0A9GK9pA2/view?usp=sharing

P1	¿De qué manera los modelos, marcos o medidas están identificando amenazas no intencionales para la ciberseguridad generadas por el propio personal interno de instituciones públicas?
Cadena de busqueda	(Insider Threats Cyber Security) AND (unintentional OR "human error" OR unintended) AND (public sector OR public organization OR public administration)
Total de Articulos	265
Aplico criterios de inclusion/exclusion	34
Articulos para la Pregunta 1	27

ID	Titulo	Autor	Año de publicación	Método de identificación de amenazas internas no intencionales	El modelo identifica DISC	El modelo identifica UIT-HACK	El modelo identifica PHYS	El modelo identifica PORT	El modelo identifica otros tipo de UIT	Modelo o marco para identificar amenazas no intencionales para la ciberseguridad	Referencia
A-01	Protecting Information with Cybersecurity	John M. Borky;Thomas H. Bradley	2019		SI	SI	SI	SI		1) Microsoft Threat Modeli	[62]
A-03	Real-Time Information Security Incident Management:	MARK EVANS , YING HE , CUNJIN LI	2019	IS-CHEC							[11]
A-04	Evaluating information security core human error cause	Evans M., He Y., Maglaras L., Yevseyeva I.	2019	IS-CHEC							[12]
A-05	Framework for digital data access control from internal	Halim H., Yusof M.M.	2019	Interview/Document analysis/Observa	SI	SI	SI	SI		PDDAITC - Framework for I	[32]
A-07	An investigation into information security threats from	Chinyemba M.K., Phiri J.	2018	Survey/Questionnaires	NO	SI	SI	SI		Insider Threat mitigation m	[8]
A-08	The enemy has passed through the gate: Insider threats	Fischbacher-Smith D.	2015							Enfoque de sistemas para a	[28]
A-11	"An Investigation of Information Security Threats from	MK Chinyemba, J Phiri		Questionnaires/Interviews	NO	NO	NO	NO			[9]
A-12	"Identifying Botnets Intrusion & Prevention–A Review"	LK Musambo, MK Chinyemba, J Phiri	2017		NO	SI	NO	NO		1) Anti-malware Software2	[41]
A-16	"Information Security Policy: A Management Practice P	Alshaikh, M., MAYNARD, S., Ahmad,	2015							Information Security Policy	[19]
A-17	An Exploratory Study of Current Information Security Tr	alshaikh, M., Maynard, S., Ahmad, A.	2018	Interviews						ISTA Program	[70]
A-18	"Strategies to Mitigate Knowledge Leakage Risk caused	Agudelo Serna, C., Bosua, Ahmad an	2017	Interviews	SI	SI	NO	SI		Research Conceptual Mode	[17]
A-19	"Exploring Knowledge Leakage Risk in Knowledge-Inten	Altuknuri, H., Maynard, S., Alshaikh,	2019	Focus group questions	NO	NO	NO	NO		Knowledge-leakage behavi	[63]
A-20	"Dynamic Information Security Management Capability	Onibere, M., Ahmad, A. and Maynard	2019	Survey Questionnaire						Dynamic ISM Capability mo	[55]
A-22	"Toward Sustainable Behaviour Change: An Approach fo	Alshaikh, M., Naseer, H., Ahmad, A.	2019		SI	SI	SI	SI		BCW Framework	[20]
A-23	A framework for assessing the insider threat in Parasta	Abuli, M.J.	2016	Questionnaires	SI	SI	SI	SI		Internal Threat framework	[14]
A-28	"A case analysis of securing organisations against inforr	Molok, N., Ahmad, A. and Chang, S.	2018	Interviews about the levels of maturity	SI	NO	NO	NO		Framework for organisatio	[6]
A-30	Unintentional Internal Threats: A Foundational Study	CERT	2013		SI	SI	SI	SI		Comprehensive UIT Featur	[7]
A-31	- Thesis -The Internal Threat	Jacinda L. Wunderlich	2011		SI	SI	SI	SI		Framework para mitigar e i	[50]
A-32	Managing internal Threat	Ernest and Yung		Interviews	SI	SI	SI	SI		Insider threat program mat	[49]
A-33	Review and insight on the behavioral aspects of cyberse	Maalem Lahcen Rachid Ait;Caulkins	2020	1) TPB (Theory of Planned Behavior)2)	SI	SI	SI	SI		Interdisciplinary framework	[15]
A-42	The inhospitable vulnerability	Chen, Hsiangting Shatina;Fiscus, J	2018		SI	SI	SI	SI			[60]
A-44	Employees Attitude towards Cyber Security and Risky C	Hadlington, Lee	2018	Cuestionario						Investigacion busca medir l	[31]
A-47	An Overview of Cybersecurity Regulations and Standar	Lechner, Nadica Hrgarek	2017		SI	SI	SI	SI		Framework de seguridad ci	[38]
A-50	Introduction to the special issue on insider threat model	Moore, Andrew P;Kennedy, Kirk A;	2016	Interviews						Metodos Combinados1) Ag	[40]
A-52	Cybersecurity risks, vulnerabilities and countermeasure	Conteh, Nabie Y;Schmick, Paul J	2016	Cuestionarios	NO	SI	NO	NO		Medidas de prevencion con	[26]
A-53	Detection and prediction of insider threats to cyber sec	Gheyas, Iffat A;Abdallah, Ali E	2016	Interviews and Questionaries						IDPA (insider threat detecti	[29]
A-56	DATA LOSS PREVENTION AND CONTROL: INSIDE AC	Tu, Manghui;Spoa-Harty, Kimberly;S	2015							1) The WDOA (Work Role-D	[51]

P2	¿De qué manera las actividades del personal interno de una organización sobre la infraestructura de TI, pueden considerarse una amenaza no intencional a la ciberseguridad?
Cadena de busqueda	(Insider Threats Cyber Security) AND (unintentional OR "human error" OR unintended) AND (public sector OR public organization OR public administration)
Total de Articulos	265
Aplico criterios de inclusion/exclusion	34
Articulos para la Pregunta 2	10

ID	Titulo	Autor	Año de publicación	Se identifica IS-CHEC como técnica para detectar causas de UIT en las actividades del personal	Se identifica otras técnicas para detectar causas de UIT en las actividades del personal	Se identifican UIT en el área de Negocios	Se identifican UIT en el área de soporte	Se identifican UIT en el área de investigación y desarrollo	Se identifican UIT en otras áreas de la organización	Roles del personal interno sobre infraestructura de TI	Tipo de actividades del personal interno	Referencia
A-03	Real-Time Information Security Incident Management:	MARK EVANS , YING HE , CUNJIN LI	2019	SI		SI	NO	NO			GISAT	[11]
A-04	Evaluating information security core human error cause	Evans M., He Y., Maglaras L., Yevse	2019	SI		SI	SI	SI				[12]
A-07	An investigation into information security threats from	Chinyemba M.K., Phiri J.	2018	NO	Encuestas	SI	SI	SI	Recursos Humanos	Security Manager/Direc		[8]
A-09	"An Investigation into Cyber Security Threats by Insider	Melissa K. Chinyemba	2019	NO	Cuestionarios	SI	SI	SI	TI/Recursos Humanos			[10]
A-11	"An Investigation of Information Security Threats from	MK Chinyemba, J Phiri	2018	NO	EntrevistasCuestionarios	SI	SI	SI	TI			[9]
A-23	A framework for assessing the insider threat in Parasta	Abuli, M.J.	2016	NO	Marco de trabajo	NO	NO	NO				[14]
A-24	An analysis of insider dysfunctional behavours in an acc	Mat Roni, M.S.	2015	NO	TPB (Teoria del compor	NO	NO	NO				[13]
A-28	"A case analysis of securing organisations against inforn	Molok, N., Ahmad, A. and Chang, S.	2018	NO	Entrevistas	NO	NO	NO		IT AssistantSystem Anal	OSN Functions	[6]
A-30	Unintentional Internal Threats: A Foundational Study	CERT	2013	NO	Comprehensive UIT Fea	NO	NO	NO				[7]
A-33	Review and insight on the behavioral aspects of cyberse	Maalem Lahcen Rachid Ait;Caulkins	2020	NO	Social Cognition Theory	NO	NO	NO				[15]

P3	¿Cuáles han sido los factores de éxito para definir modelos, marcos o medidas para identificar amenazas no intencionales por personal interno en instituciones públicas y en qué buenas prácticas se han basado?
Cadena de busqueda	(Insider Threats Cyber Security) AND (unintentional OR "human error" OR unintended) AND (public sector OR public organization OR public administration)
Total de Articulos	265
Aplico criterios de inclusion/exclusion	34
Articulos para la Pregunta 3	21

ID	Titulo	Autor	Año de publicación	Programa de amenazas internas CERT	ISO 27001 (ISMS)	Identificación de otras buenas prácticas en el modelo	Se identifican factores de riesgo organizacionales	Se identifican factores de riesgo humano	Se identifican factores de riesgo psicosocial y demográfico	Se identifican otro tipo de factores de riesgo	Referencia
A-01	Protecting Information with Cybersecurity	John M. BorkyThomas H. Bradley	2019	NO	NO		SI	SI	SI	Cybersecurity Risk Mana	[62]
A-04	Evaluating information security core human error cause	Evans M., He Y., Maglaras L., Yevsey	2019				SI	NO	NO		[12]
A-05	Framework for digital data access control from internal	Halim H., Yusof M.M.	2019	NO	SI			SI			[32]
A-07	An investigation into information security threats from	Chinyemba M.K., Phiri J.	2018	NO	SI						[8]
A-08	The enemy has passed through the gate: Insider threats	Fischbacher-Smith D.	2015				SI	SI	SI		[28]
A-11	"An Investigation of Information Security Threats from	MK Chinyemba, J Phiri			SI						[9]
A-13	Towards a Taxonomy of Information Security Managem	Alshaikh, M., Ahmad, A., Maynard, S.	2014		NO	Taxonomía de practicas de gestion de seguridad de la informacion					[18]
A-18	"Strategies to Mitigate Knowledge Leakage Risk caused	Agudelo Serna, C., Bosua, Ahmad an	2017	NO	NO	ISO 27005	SI	SI	SI	Factores Tecnologicos	[17]
A-19	"Exploring Knowledge Leakage Risk in Knowledge-Intens	Alkuruni, H., Maynard, S., Alshaikh,	2019	NO	NO		SI	SI	SI	Factores Tecnologicos	[63]
A-28	"A case analysis of securing organisations against inforn	Molok, N., Ahmad, A. and Chang, S.	2018							1) Integration of OSN pa	[6]
A-30	Unintentional Internal Threats: A Foundational Study	CERT	2013	NO	SI	Auto (Automated Secur	SI	SI	SI		[7]
A-31	- Thesis - The Internal Threat	Jacinda L. Wunderlich	2011	NO	NO	Politicas y conciencia sobre la seguridad de la informacion por parte de organizaciones					[50]
A-32	Managing Internal Threat	Ernest and Yung		SI	1)National Security Alla						[49]
A-33	Review and insight on the behavioral aspects of cyberse	Maalem Lahcen Rachid Ait;Caulkins	2020	NO	NO	NIST	SI	SI	SI		[15]
A-38	Aspects of human weaknesses in cyber security	Moinescu, Radu;Răcuciu, Ciprian;G	2019	NO	NO	Security Policy	NO	SI	NO		[56]
A-39	Mitigating cyber attacks through the measurement of no	Carlton, Melissa;Levy, Yair;Ramim,	2019	NO	NO	Herramienta de CSI	NO	SI	NO		[23]
A-41	Human-centered strategies for cyber-physical systems	Ceesay, E N;Myers, K;Watters, P A	2018	NO	NO	Implementing a Holistic	NO	SI	NO		[61]
A-42	The inhospitable vulnerability	Chen, Hsiangting Shatina;Fiscus, Jo	2018	NO	NO	NIST					[60]
A-47	An Overview of Cybersecurity Regulations and Standard	Lechner, Nadicia Hrgarek	2017	NO	NO	NIST					[38]
A-53	Detection and prediction of insider threats to cyber secu	Sheyas, Iffat A;Abdallah, Ali E	2016				SI	SI	SI		[29]
A-57	Unintentional Insider Threat: Contributing Factors, Obse	Greitzer, Frank L.;Strozer, Jeremy;Co	2014	NO	NO		SI	SI	SI		[71]

Anexo C: Informe de Hoja de Ruta

Informe de hoja de ruta del Diseño de un modelo para identificar amenazas no intencionales de ciberseguridad en instituciones públicas generadas por personal interno a partir de su comportamiento sobre la infraestructura de TI (MANIC)

Basándose en Hevner y Chatterjee (2010), se pueden identificar las siguientes fases de la metodología de Ciencia del Diseño:

1. Conciencia del problema
2. Propuesta de solución
3. Desarrollo del artefacto
4. Evaluación del artefacto
5. Conclusión del proyecto

Se desarrollará cada uno de ellos en detalle aplicados al proyecto de tesis en los siguientes puntos.

1. Conciencia del Problema

De acuerdo con la problemática desarrollada, se ha contextualizado el problema en dos aproximaciones principales:

- Ausencia de un modelo que identifique distintas amenazas no intencionales de Ciberseguridad dentro de organizaciones públicas para que pueda tener medidas de control, detección y tratamiento de los riesgos afectó a la probabilidad de ocurrencia de dichas amenazas.
- Ausencia de estándares y buenas prácticas enfocadas en amenazas no intencionales de Ciberseguridad

El conocimiento del problema conduce a la necesidad de contar con un modelo para la identificación de amenazas no intencionales de Ciberseguridad en instituciones públicas generadas por personal interno en la infraestructura de TI.

Como resultado de este estudio, se puede apreciar que existe concordancia con la revisión del estado que muestra la ausencia de este modelo que propone diseñar.

2. Propuesta de solución

En esta fase, se pretende diseñar un modelo basado en componentes que permitan proponer medidas para tratar los riesgos a causa de amenazas no intencionales de Ciberseguridad que puedan ser identificadas dentro de la organización producto de la existencia de vulnerabilidades generadas por parte del personal interno.

La construcción del modelo tendrá en consideración una matriz de gestión de riesgos y un análisis previo de la organización con la finalidad de plantearse objetivos alcanzables y medibles que el modelo pueda ayudar a cumplir. La propuesta del modelo y sus componentes está basada en las buenas prácticas y normativas internacionales a fin de tener una mayor validez en la ejecución del mismo dentro de una organización pública.

3. Desarrollo del artefacto

En esta fase, se procede con la definición del modelo, que de acuerdo con las 5 fases se le conoce como el artefacto. El diseño del modelo está basado en buenas prácticas internacionales sobre gestión de riesgos, seguridad de la información y adicionalmente se ha empleado la revisión sistemática para el diseño de ciertos componentes.

La estructura del modelo será la siguiente:

Tabla 1: Estructura de los componentes del modelo (MANIC)

Modelo de Detección de Amenazas No Intencionales Internas de Ciberseguridad (MANIC) para instituciones públicas			
	Nombre	**Descripción**	**Estándares principales**
COMPONENTES	**1. Análisis situacional**	Herramienta de análisis GAP que va a permitir determinar el estado actual (AS-IS) de la organización en lo referente a Ciberseguridad	ISO 27002, ISO 27032, ISO 27103, Normas NIST
	2. Objetivos de Ciberseguridad	Corresponde a los objetivos (TO-BE) de Ciberseguridad que van a ser cubiertos por la aplicación del marco MANIC en cualquier entidad del estado	Estado del arte
	3. Métricas e indicadores	Indicadores que miden si el objetivo ha sido alcanzado o no	Propia autoría
	4. Lista de patrones de comportamiento	Patrones de comportamiento que se pretenden detectar en la institución estatal.	Estado del arte
	5. Matriz de gestión de riesgos de Ciberseguridad	Implica desde la identificación de riesgos, análisis, evaluación de riesgos, tratamiento de riesgos y proposición de controles: • Procesos de negocio • Activos de información digital involucrados • Vulnerabilidades • Amenazas <- Internas no intencionales • Riesgos • Impacto para la organización • Probabilidad de ocurrencia del riesgo • Tratamiento del riesgo o Propuesta de controles	ISO 31000, ISO 27005
	6. Guía de aplicación del modelo	Guía de pasos mediante la cual se va a aplicar el modelo en cualquier institución del estado	Propia autoría

4. Evaluación del artefacto

Una vez construido el artefacto se procede con la validación del modelo en una institución pública. El modelo deberá pasar por la evaluación de un especialista que pueda brindar sus observaciones de manera documentada con la finalidad de tener la aprobación y preparar el modelo para una futura implementación. Estas observaciones deberán tener las consideraciones de cada componente con el fin de proponer una mejora o eliminación si en caso fuera necesario.

5. Conclusiones del proyecto

En esta fase y de acuerdo con la teoría de la Ciencia del Diseño, no solo se debe documentar y consolidar los resultados, sino que se debe categorizar el conocimiento adquirido y poner en evidencia el aprendizaje que se pudo obtener del proyecto y del modelo diseñado.

Anexo D: Matriz de Análisis Situacional

La Matriz de Análisis Situacional se encuentra en el siguiente link:

https://drive.google.com/file/d/1JyWLXVMlvGUbef-D-283-w9hygSt0KtS/view?usp=sharing

Análisis Situacional aplicando normas ISO 27103, ISO 27002:2013 y NIST Framework

SECCIÓN	REQUERIMIENTO ISO 27103/27002:2013/NIST Framework 1.1	NIST 1.1 (Referencia)	ESTADO	DOCUMENTO /EVIDENCIA	COMENTARIOS /OBSERVACIONES	DOCUMENTO /EVIDENCIA DESEADA
1	**Objetivos de Negocio, Gestión de Activos Digitales y Riesgos**					
1.1	**Gestión de Activos Digitales**					
	La organización debe identificar y mantener un inventario de sus activos digitales o activos que soportan servicios o información digital	ID.AM-1				Se espera recibir un documento que pueda mostrar la importancia y el ciclo de vida del activo (creación, procesamiento, almacenamiento, transmisión y eliminación). Los documentos deben estar actualizados y deben ser coherentes con otros inventarios
	La organización debe identificar y mantener un inventario de sus plataformas y aplicaciones de software	ID.AM-2				Se espera recibir un documento que pueda mostrar la importancia y el ciclo de vida del activo (creación, procesamiento, almacenamiento, transmisión y eliminación). Los documentos deben estar actualizados y deben ser coherentes con otros inventarios
	La organización debe tener políticas, procedimientos y controles para la transferencia de datos a través de medios de comunicación oficiales	ID.AM-3				Se espera recibir un documento que pueda mostrar las políticas, procedimientos y controles para transferir información. (ej. Procedimientos para proteger información, detección y protección contra malware, protección de documentos adjuntados, uso de técnicas criptográficas, uso adecuado de contestadores y reenvío automáticos, requisitos legales, etc.)
	La organización debe tener medidas de seguridad e identificación al trabajar con activos digitales externos	ID.AM-4				Se espera recibir un documento que pueda mostrar el control adecuado, ubicación, modo de uso y cadena de custodia al transferir el activo
	Los recursos de la organización (ej. hardware, dispositivos, datos, personal y softwares) deben ser priorizados basados en su clasificación, criticidad y valor en el negocio	ID.AM-5				Se espera recibir un documento que pueda mostrar la clasificación de los recursos de acuerdo a las necesidades del negocio, accesos, prioridades, procesos, restricciones,

						almacenamiento, requisitos legales, etc.
1.2	**Ambiente de Negocio**					
	La organización debe comunicar e identificar su rol en la cadena de suministro cibernético	ID.BE-1				Se espera recibir un documento que pueda mostrar las políticas necesarias en relación con los proveedores y su rol especifico de la organización dentro de la cadena de suministro
	La organización debe comunicar su lugar dentro de la infraestructura crítica y el sector industrial al que corresponde	ID.BE-2				Se espera recibir un documento que pueda demostrar la comunicación
	La organización debe establecer y comunicar las prioridades para la misión, los objetivos y las actividades de la organización.	ID.BE-3				Se espera recibir un documento que pueda demostrar que la organización tiene claro los objetivos y que sean comunicados adecuadamente
	La organización debe identificar las funciones críticas y dependencias de servicios prestados ya sean públicos o privados	ID.BE-4				Se espera recibir un documento que pueda mostrar las medidas tanto preventivas, de mantenimiento y de detección de las funciones criticas dependientes de las organizaciones (ej. electricidad, telecomunicaciones, suministro de agua, gas, etc.)
	La organización debe definir requerimientos de resiliencia ante eventualidades por parte de servicios críticos prestados en todos los estados de sus operaciones	ID.BE-5				Se espera recibir un documento que demuestre los requerimientos necesarios de acción ante eventualidades
1.3	**Gobernanza**					
	La organización debe establecer y comunicar sus políticas de Ciberseguridad	ID.GV-1				Se espera recibir un documento que muestre las políticas de seguridad de la información que sea validado y aprobado por la gerencia, así como pruebas aprobadas de cómo se comunican esas políticas a los usuarios previstos o las partes interesadas que se espera que cumplan con las políticas (por ejemplo, planes de concientización, registro de asistencia a la capacitación, recibo policial firmado)
	La organización debe alinear los roles de Ciberseguridad con los roles internos y externos	ID.GV-2				Se espera recibir un documento/evidencia que muestre la alineación de roles asignados
	La organización debe conocer los reglamentos y requisitos relacionados a la Ciberseguridad, como también la privacidad y libertad civil, las cuales deben ser gestionadas	ID.GV-3				Se espera recibir un documento/evidencia que definan los controles específicos y las responsabilidades individuales para cumplir con estos requisitos.
	La organización debe involucrar los riesgos de Ciberseguridad dentro de su	ID.GV-4				Se espera recibir un documento/evidencia que

	proceso de gobernanza y gestión de riesgos					involucren estos riesgos de Ciberseguridad y las responsabilidades individuales para cumplirlo
1.4	**Gestión de Riesgos**					
	La organización debe identificar y documentar las vulnerabilidades de los activos digitales	ID.RA-1				Se espera recibir un documento/ evidencia para cumplir este requisito
	La organización debe considerar el intercambio de fuentes de información relacionado a la inteligencia de las amenazas de ciberseguridad	ID.RA-2				Se espera recibir un documento/ evidencia para cumplir este requisito
	La organización debe identificar y documentar las amenazas internas y externas	ID.RA-3				Se espera recibir un documento/ evidencia para cumplir este requisito
	La organización debe identificar los impactos en el negocio y sus probabilidades	ID.RA-4				Se espera recibir un documento/ evidencia para cumplir este requisito
	La organización debe determinar el riesgo en base a las amenazas, vulnerabilidades, impactos y probabilidades	ID.RA-5				Se espera recibir un documento/ evidencia que demuestre una gestión de riesgos adecuada
	La organización debe priorizar las respuestas al riesgo identificado	ID.RA-6				
	La organización debe establecer un proceso de gestión de riesgos	ID.RM-1				
	La organización debe determinar la tolerancia al riesgo organizacional y ser claramente expresado	ID.RM-2				
	La organización debe identificar, establecer, evaluar y gestionar el proceso de gestión de riesgos de la cadena de suministro cibernético	ID.SC-1				
	La organización debe implementar medidas apropiadas, establecidas en el contrato, para cumplir con los objetivos de Ciberseguridad de la organización y el plan de gestión de riesgos de la cadena de suministros cibernético	ID.SC-3				
2	**Control de Accesos, Políticas de seguridad, Mantenimiento y Protección de Información**					
2.1	**Control de Accesos y Gestión de Identidad**					
	La organización debe administrar, verificar, revocar y auditar las identidades y credenciales solo para dispositivos, usuarios y procesos autorizados	PR.AC-1				Se espera recibir un documento/ evidencia que demuestre la gestión adecuada de accesos para los usuarios
	La organización debe gestionar y proteger los accesos físicos a los activos digitales	PR.AC-2				
	La organización debe gestionar el acceso remoto a la organización	PR.AC-3				
	La organización debe gestionar los permisos de acceso de acuerdo con funciones y privilegios	PR.AC-4				
	La organización debe proteger la integridad de la red mediante una segmentación, segregación, etc.	PR.AC-5				Se espera recibir un documento/ evidencia que demuestre controles, procesos y accesos a la red
2.2	**Conciencia y Capacitación**					
	La organización debe informar y capacitar a su personal	PR.AT-1				Se espera recibir un documento/ evidencia que permita establecer un plan de capacitación que incluya
	La organización debe concientizar y motivar a su personal					

	Los usuarios de la organización tanto privilegiados, personal físico personal de Ciberseguridad, altos ejecutivos, partes interesadas y terceros deben entender sus roles y responsabilidades	PR.AT-2 PR.AT-3 PR.AT-4 PR.AT-5				manuales, guías aplicativas, charlas, campañas, cursos, etc.
2.3	**Seguridad de Datos**					
	La organización debe proteger los datos en reposo	PR.DS-1				Se espera recibir un documento/ evidencia que establezca la protección, disponibilidad, cuidado de los datos
	La organización debe proteger los datos en transito	PR.DS-2				
	La organización debe gestionar formalmente la configuración inicial, puesta en uso, transferencia, eliminación y disposición de sus activos	PR.DS-3				
	La organización debe tener la capacidad para mantener la disponibilidad de los sistemas y de los datos	PR.DS-4				
	La organización establece medidas de protección ante fuga de datos	PR.DS-5				
	La organización establece mecanismos de verificación de la integridad del software, firmware e información	PR.DS-6				
	La organización debe separar entornos de desarrollo con los de producción, asi como también los ambientes de prueba deben estar separados en caso tenga sistemas desarrollados	PR.DS-7				Se espera recibir un documento/ evidencia de la diferenciación de los entornos
2.4	**Procesos y Procedimientos de protección de la Información**					
	La organización debe mantener una configuración básica de las tecnologías de información y sistemas de control mediante principios de seguridad	PR.IP-1				Se espera recibir un documento/ evidencia que muestre el uso de procesos y procedimientos de protección de la información
	La organización debe implementar un ciclo de vida del desarrollo del sistema para gestionar sistemas	PR.IP-2				
	La organización debe tener un proceso de control de cambios de configuración	PR.IP-3				
	La organización debe realizar, mantener y probar sus backups de Información	PR.IP-4				
	La organización establece políticas para la eliminación de datos	PR.IP-6				
	La organización debe mejorar sus procesos de protección constantemente	PR.IP-7				
	La organización debe establecer planes de respuesta antes Incidentes y Continuidad de Negocio	PR.IP-9				
	La organización debe establecer planes de recuperación ante desastres e incidentes					
	La organización debe probar sus planes de respuesta y recuperación	PR.IP-10				
	La organización debe aplicar politicas de Ciberseguridad en las prácticas de RRHH (ej. selección de personal, des aprovisionamiento, etc.)	PR.IP-11				
	La organización debe desarrollar e implementar un plan de gestión vulnerabilidades	PR.IP-12				
2.5	**Mantenimiento**					
	La organización mantiene y repara los activos de la organización siguiendo procesos y herramientas aprobados	PR.MA-1				Se espera recibir un documento/ evidencia de las herramientas o procesos utilizados para el mantenimiento de activos
	La organización mantiene y repara remotamente los activos de la organización siguiendo procesos y protección ante accesos no autorizados	PR.MA-2				
2.6	**Tecnología de Protección**					

	La organización determina, documenta, revisa e implementa los registros de auditoría de acuerdo con las políticas	PR.PT-1				Se espera recibir un documento/ evidencia que muestre las políticas adecuadas en cuanto a las auditorías realizadas
	La organización debe establecer políticas y procedimientos para la gestión de medios extraíbles según su clasificación hecha por la institución (ej. USB, discos, laptops, etc.)	PR:PT-2				Se espera recibir un documento/ evidencia que presenta las políticas o procedimientos en cuanto al uso de medios extraíbles
	La organización debe proteger las redes de comunicación y control	PR.PT-4				Se espera recibir un documento/ evidencia de medidas de protección de las redes de comunicación
3	**Detección de Anomalías, Eventos y Monitoreo**					
3.1	**Anomalías y Eventos**					
	La organización debe establecer una línea base de operaciones de red, flujo de datos, usuarios y sistemas ante posibles eventos o anomalías ocasionados por amenazas de Ciberseguridad	DE.AE-1				Se espera recibir un documento/ evidencia de plan de acción ante eventos y anomalías detectadas desde su identificación, impacto y usuarios involucrados
	La organización debe analizar los eventos o anomalías producidos por una amenaza de Ciberseguridad para entender el objetivo del ataque y los métodos aplicados	DE.AE-2				
	La organización debe determinar el impacto del evento	DE.AE-4				
	La organización debe establecer umbrales de alerta para cada aspecto	DE.AE-5				
3.2	**Monitoreo continuo de Seguridad**					
	La organización debe monitorear la red para detectar potenciales eventos de ciberseguridad	DE.CM-1				Se espera recibir un documento/ evidencia que muestre un plan de monitoreo de la red, entorno físico, códigos y vulnerabilidades
	La organización debe monitorear el entorno físico para detectar potenciales eventos de ciberseguridad	DE.CM-2				
	La organización debe detectar códigos maliciosos	DE.CM-4				
	La organización debe detectar código móvil no autorizado	DE.CM-5				
	La organización debe realizar la exploración de vulnerabilidades	DE.CM-8				
3.3	**Procesos de Detección**					
	La organización tiene definido los roles y responsabilidades para la detección de eventos y anomalías	DE.DP-1				Se espera recibir un documento/ evidencia que muestre los roles y responsabilidades definidas antes un evento detectado para su debida acción
	La organización prueba sus procesos de detección	DE.DP-3				Se espera recibir un documento/ evidencia que muestra la efectividad de los procesos de detección después de utilizarlos
	La organización comunica la información de los eventos detectados a las partes involucradas	DE.DP-4				Se espera recibir un documento/ evidencia que presente como el registro obligatorio de hacer efectiva la comunicación ante un evento detectado
	La organización mantiene una constante mejora de sus procesos de detección	DE.DP-5				Se espera recibir un documento/ evidencia que muestre que existe una mejora continua en la detección de eventos

4	**Plan de Respuestas**					
4.1	**Planificación de Respuesta**					
	La organización debe ejecutar un plan de respuestas durante y después del incidente	RS.RP-1				Se espera recibir un documento/ evidencia que presente un plan de respuesta ante la ocurrencia de algún incidente
4.2	**Comunicación**					
	El personal de la organización conoce sus roles y orden de operaciones cuando una respuesta es necesaria	RS.CO-1				Se espera recibir un documento/ evidencia que presente un plan de respuesta ante la ocurrencia de algún incidente
	La organización debe reportar los incidentes de acuerdo con los criterios establecidos	RS.CO-2				
	La organización debe compartir la información de acuerdo con los planes de respuesta	RS.CO-3				
	La organización coordina con las partes interesadas de acuerdo con los planes de respuesta	RS.CO-4				
	La organización comparte voluntariamente información y viceversa con las partes interesadas externas para generar conciencia sobre la situación de Ciberseguridad	RS.CO-5				
4.3	**Análisis**					
	La organización investiga las notificaciones de los sistemas de detección	RS.AN-1				Se espera recibir un documento/ evidencia que presente un plan de respuesta ante la ocurrencia de algún incidente
	La organización entiende el impacto del incidente	RS.AN-2				
	La organización realiza análisis forenses	RS.AN-3				
	La organización clasifica los incidentes de acuerdo con los planes de respuesta	RS.AN-4				
4.4	**Mitigación**					
	La organización contiene y resuelve los incidentes	RS.MI-1 RS.MI-2				Se espera recibir un documento/ evidencia que presente un plan de respuesta ante la ocurrencia de algún incidente
4.5	**Mejoras**					
	La organización incorpora las lecciones aprendidas a los planes de respuesta	RC.RP-1				Se espera recibir un documento/ evidencia que presente un plan de respuesta ante la ocurrencia de algún incidente
	La organización actualiza sus estrategias de respuesta	RC.RP-2				
5	**Plan de Recuperación**					
5.1	**Planificación de Recuperación**					
	La organización ejecuta un plan de recuperación durante o después del incidente de Ciberseguridad	RC.RP-1				Se espera recibir un documento/ evidencia que presente un plan de recuperación ante algún incidente
5.2	**Mejoras**					
	La organización incorpora las lecciones aprendidas a los planes de recuperación	RC.IM-1				Se espera recibir un documento/ evidencia que presente un plan de recuperación ante algún incidente
	La organización actualiza sus estrategias de recuperación	RC.IM-2				
5.3	**Comunicación**					

	La organización gestiona las relaciones públicas	RC.CO-1				Se espera recibir un documento/ evidencia que presente un plan de recuperación ante algún incidente
	La organización repara su reputación después de resolver el incidente.	RC.CO-2				
	La organización comunica sus actividades de recuperación al personal interno, externo, ejecutivos y equipos de gestión	RC.CO-3				
6	**Recursos Humanos y partes intereses**					
6.1	**Personal, Proveedores y Partes interesadas**					
	La organización debe establecer los roles y responsabilidades de Ciberseguridad para el personal y las partes interesadas de terceros (ej. proveedores, clientes, etc.)	ID.AM-6				Se espera recibir un documento/evidencia que muestre los roles de Ciberseguridad asignados
	La organización debe identificar, priorizar y evaluar a sus proveedores, socios de sistemas de información, componentes y servicios mediante su proceso de gestión de riesgos de la cadena de suministros cibernética	ID.SC-2				Se espera recibir un documento/ evidencia este requerimiento dentro de la gestión de riesgos para la cadena de suministros
	La organización debe monitorear la actividad del personal ante potenciales eventos de ciberseguridad	DE.CM-3				Se espera recibir un documento/ evidencia de políticas de seguridad dentro del área de trabajo en relación con el personal, proveedores, personal no autorizado
	La organización debe monitorear la actividad de proveedores de servicios externos ante potenciales eventos de Ciberseguridad	DE.CM-6				
	La organización debe monitorear al personal no autorizado, conexiones, dispositivos y softwares	DE.CM-7				
6.2	**Ciudadano, Instituciones relacionadas y Cumplimiento regulatorio**					
	La organización debe cumplir con el marco regulatorio del estado respetando los principios rectores de la Ley de Protección de datos personales N° 29733 del ciudadano utilizando su información solo con su consentimiento y para fines determinados que deberán ser informados	LEY-29733				Se espera recibir un documento/evidencia que muestre el cumplimiento del marco regulatorio relacionado a la Ley N° 29733
	La organización debe cumplir con el marco regulatorio del estado respetando los principios rectores de la Ley de Protección de datos personales N° 29733 de sus empleados utilizando su información solo con su consentimiento y para fines determinados que deberán ser informados	LEY-29733				Se espera recibir un documento/evidencia que muestre el cumplimiento del marco regulatorio relacionado a la Ley N° 29733
	La organización debe cumplir con el marco regulatorio del estado que permite la interoperabilidad entre instituciones públicas mediante el uso de un Marco de Interoperabilidad del Estado, en base a la Ley de Gobierno Digital N° 1412	LEY-1412				Se espera recibir un documento/evidencia que muestre el cumplimiento del marco regulatorio relacionado a la Ley N° 1412

Resultados de la Matriz de Análisis Situacional				
Clasificación Matriz	Estado	Significado	Total	Porcentaje de requerimientos por estado (%)
Nivel 0	No Aplica	El requisito no es aplicable en la organización	0	
Nivel 1	Incompleto	El requisito no muestra evidencia de su ejecución o los documentos presentados no sustentan la conformidad del requisito evaluado	0	
Nivel 2	En proceso	El requisito se ejecuta parcialmente o la documentación presentada evidencia su ejecución, pero a un mínimo nivel de conformidad	0	
Nivel 3	Ejecutado	El requisito se ejecuta conforme a la entidad, se presentan los documentos que sustentan su aplicación	0	
Nivel 4	Optimizado	El requisito se ejecuta conforme a la entidad, presenta los documentos necesarios para su validación y existe mejora continua en su aplicación	0	
Total			**0**	

SECCIÓN	REQUERIMIENTO ISO 27103/27002:2013/NIST Framework 1.1	Total	No Aplica	Incompleto	En proceso	Ejecutado	Optimizado
1	**Objetivos de Negocio, Gestión de Activos Digitales y Riesgos**	**24**	**0**	**0**	**0**	**0**	**0**
1.1	**Gestión de Activos Digitales**	5	0	0	0	0	0
1.2	**Ambiente de Negocio**	5	0	0	0	0	0
1.3	**Gobernanza**	4	0	0	0	0	0
1.4	**Gestión de Riesgos**	10	0	0	0	0	0
2	**Control de Accesos, Políticas de seguridad, Mantenimiento y Protección de Información**	**31**	**0**	**0**	**0**	**0**	**0**
2.1	**Control de Accesos y Gestión de Identidad**	5	0	0	0	0	0
2.2	**Conciencia y Capacitación**	3	0	0	0	0	0
2.3	**Seguridad de Datos**	7	0	0	0	0	0
2.4	**Procesos y Procedimientos de protección de la Información**	11	0	0	0	0	0
2.5	**Mantenimiento**	2	0	0	0	0	0
2.6	**Tecnología de Protección**	3	0	0	0	0	0
3	**Detección de Anomalías, Eventos y Monitoreo**	**13**	**0**	**0**	**0**	**0**	**0**
3.1	**Anomalías y Eventos**	4	0	0	0	0	0
3.2	**Monitoreo continuo de Seguridad**	5	0	0	0	0	0
3.3	**Procesos de Detección**	4	0	0	0	0	0
4	**Plan de Respuestas**	**13**	**0**	**0**	**0**	**0**	**0**
4.1	**Planificación de Respuesta**	1	0	0	0	0	0
4.2	**Comunicación**	5	0	0	0	0	0
4.3	**Análisis**	4	0	0	0	0	0
4.4	**Mitigación**	1	0	0	0	0	0
4.5	**Mejoras**	2	0	0	0	0	0
5	**Plan de Recuperación**	**6**	**0**	**0**	**0**	**0**	**0**
5.1	**Planificación de Recuperación**	1	0	0	0	0	0
5.2	**Mejoras**	2	0	0	0	0	0
5.3	**Comunicación**	3	0	0	0	0	0
6	**Recursos Humanos y partes intereses**	**8**	**0**	**0**	**0**	**0**	**0**
6.1	**Personal, Proveedores y Partes interesadas**	5	0	0	0	0	0
6.2	**Ciudadano, Instituciones relacionadas y Cumplimiento regulatorio**	3	0	0	0	0	0

Anexo E: Matriz de Trazabilidad para la construcción de los Patrones de Comportamiento

	Tipo de Amenazas	UIT-HACK				DISC		PHYS		PORT		
		Robo de ID/Acceso no autorizado	Phishing	Aplicaciones maliciosas/ Malware	Ingeniería Social	Enviar información sensible por correo o fax accidentalmente	Divulgación de datos a través de internet, social media, cloud o móviles	Información sensible física en escritorios o lugares inseguros	Eliminación de información sensible de forma incorrecta	Robo de equipos portables	Pérdida de equipos portables	Robo de unidades de respaldo
Factores Causales	**Factores Organizacionales generales**											
	Requerimientos de proceso de negocio (BPR)	•			•	•	•	•	•			
	Flujo de datos				•	•		•	•			
	Escenario de trabajo	•	•	•	•	•		•	•		•	
	Planificación/Control del trabajo		•	•	•	•	•	•	•			
	Factores Humanos											
	Fatiga o somnolencia				•		•	•				
	Carga de trabajo mental		•	•	•		•	•				
	Falta de conciencia de la situación (SA)		•	•	•	•	•			•		•
	Mente distraída		•		•	•	•				•	
	Sesgos cognitivos		•		•	•	•	•	•		•	
	Factores Psicosociales, Socioculturales y otros											
	Cultura	•					•					
	Estado de ánimo					•	•	•	•			
	Edad	•					•	•	•			
	Influencia de Drogas/Hormonas/Enfermedades		•	•	•		•					

Anexo F: Acta de Validación de los especialistas

Acta de Validación de la especialista Jennifer Ayllón

Perfil del Experto:

Ingeniero Electrónico, con 18 años de experiencia en Tecnologías de la Información y los últimos 11 años como especialista en Ciberseguridad, Seguridad de la Información y Continuidad de Negocio. Con estudios concluidos de Maestría de Seguridad en Informática y un MBA Gerencial de CENTRUM. Certificada en Gestión de Servicios de TI, Seguridad de Información, Continuidad de Negocio, Ciberseguridad, Anti-Soborno, CBCI, Scrum Master, ITIL, TOGAF. Con estudios en Gestión de Procesos, Sistemas de Control Interno, Gestión de Riesgos, entre otros.

Acta de Validación:

Lima, 30 de septiembre del 2020

Validación de Componentes del Modelo MANIC

Por medio de la presente acta se hace constar que **Jennifer Jacinta Ayllón Bulnes** ha revisado el proyecto de tesis titulado **"DISEÑO DE UN MODELO PARA IDENTIFICAR AMENAZAS NO INTENCIONALES DE CIBERSEGURIDAD EN INSTITUCIONES PÚBLICAS GENERADAS POR PERSONAL INTERNO A PARTIR DE SU COMPORTAMIENTO SOBRE LA INFRAESTRUCTURA DE TI"** del alumno **Anderson Jesús Castillo Lopez**, alumno de la especialidad de Ingeniería Informática en la Pontificia Universidad Católica del Perú. Se realizó la validación y revisión de los componentes del Modelo de Amenazas No intencionales de Ciberseguridad (MANiC) correspondiente a los resultados esperados RE1, RE2, RE3, RE4 y parte del RE7 con el compromiso por parte del tesista de corregir y mejorar las observaciones hechas por el especialista.

Atentamente.

Jennifer Jacinta Ayllón Bulnes

Lima, 27 de octubre del 2020

Validación de Componentes del Modelo MANIC

Por medio de la presente acta se hace constar que <NOMBRE COMPLETO DEL VALIDADOR> que se ha revisado el proyecto de tesis titulado **"DISEÑO DE UN MODELO PARA IDENTIFICAR AMENAZAS NO INTENCIONALES DE CIBERSEGURIDAD EN INSTITUCIONES PÚBLICAS GENERADAS POR PERSONAL INTERNO A PARTIR DE SU COMPORTAMIENTO SOBRE LA INFRAESTRUCTURA DE TI"** del alumno **Anderson Jesús Castillo Lopez**, alumno de la especialidad de Ingeniería Informática en la Pontificia Universidad Católica del Perú. Se realizó la validación y revisión de los componentes del Modelo de Amenazas No intencionales de Ciberseguridad (MANIC) correspondiente a los resultados esperados RE5, RE6, RE7, RE8 con el compromiso por parte del tesista de corregir y mejorar las observaciones hechas por el especialista.

Atentamente.

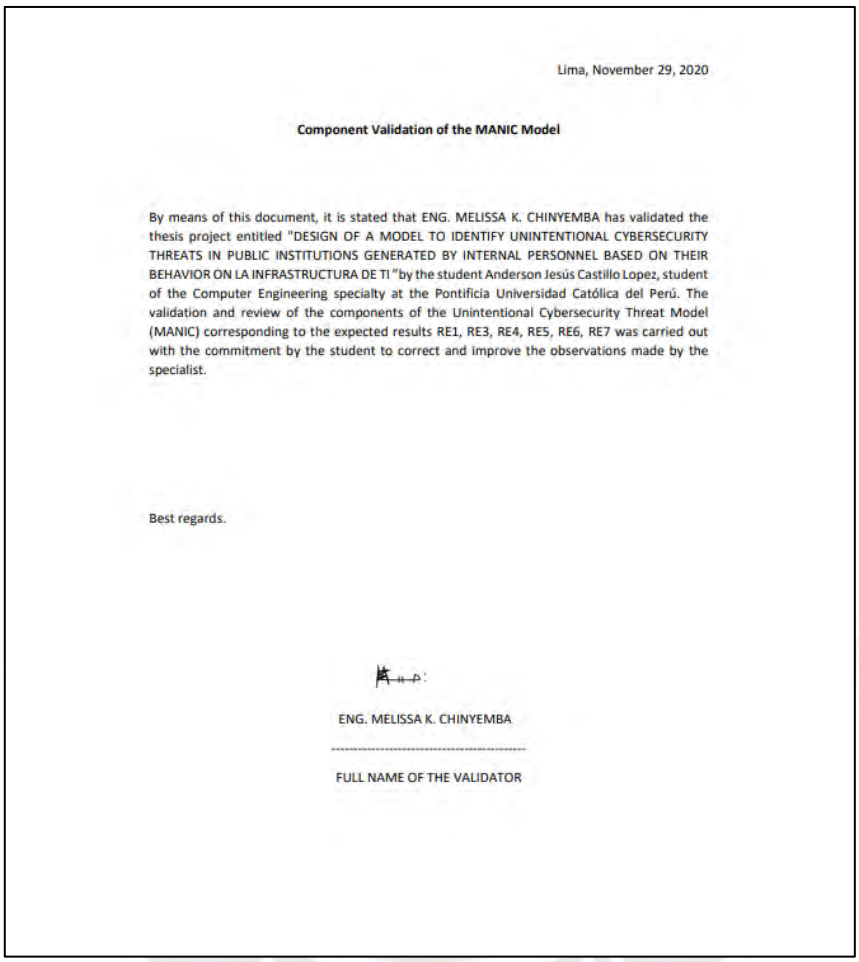
Jennifer Jacinta Ayllón Bulnes

Acta de Validación de la especialista Melissa K. Chinyemba

Perfil del Experto:

University of Zambia | UNZA · Department of Electrical and Electronic Engineering. Master of Engineering - ICT Security and CyberSecurity specialist.

Acta de Validación:



Lima, November 29, 2020

Component Validation of the MANIC Model

By means of this document, it is stated that ENG. MELISSA K. CHINYEMBA has validated the thesis project entitled "DESIGN OF A MODEL TO IDENTIFY UNINTENTIONAL CYBERSECURITY THREATS IN PUBLIC INSTITUTIONS GENERATED BY INTERNAL PERSONNEL BASED ON THEIR BEHAVIOR ON LA INFRASTRUCTURA DE TI "by the student Anderson Jesús Castillo Lopez, student of the Computer Engineering specialty at the Pontificia Universidad Católica del Perú. The validation and review of the components of the Unintentional Cybersecurity Threat Model (MANIC) corresponding to the expected results RE1, RE3, RE4, RE5, RE6, RE7 was carried out with the commitment by the student to correct and improve the observations made by the specialist.

Best regards.

ENG. MELISSA K. CHINYEMBA

FULL NAME OF THE VALIDATOR

Anexo G: Control de cambios de los componentes del modelo

En esta sección se presentan solo los componentes originales que sufrieron cambios en base a las observaciones realizadas por los especialistas: Cada cambio será resaltado de color anaranjado para identificar los cambios realizados

1. Análisis Situacional

Para el análisis situacional, por el tamaño de la matriz de análisis situacional, herramienta utilizada para el análisis, se presenta solo los puntos que sufrieron cambios en base a las observaciones

SECCIÓN	REQUERIMIENTO ISO 27103/27002:2013/NIST Framework 1.1	NIST 1.1 (Referencia)
1	**Objetivos de Negocio, Gestión de Activos y Riesgos**	
1.1	**Gestión de Activos**	
	Los recursos de la organización (ej. hardware, dispositivos, datos, personal y softwares) deben ser priorizados basados en su clasificación, criticidad y valor en el negocio	ID.AM-5
1.2	**Ambiente de Negocio**	
	La organización debe comunicar e identificar su rol en la cadena de suministro	ID.BE-1
1.3	**Gobernanza**	
	La organización debe establecer y comunicar sus políticas de Ciberseguridad	ID.GV-1
1.4	**Gestión de Riesgos**	
	La organización debe determinar el riesgo en base a las amenazas, vulnerabilidades y probabilidades	ID.RA-5
	La organización debe priorizar las respuestas al riesgo	ID.RA-6
	La organización debe determinar y expresar una tolerancia al riesgo	ID.RM-2
2	**Control de Accesos, Políticas de seguridad, Mantenimiento y Protección de Información**	
2.2	**Conciencia y Capacitación**	
	La organización informa y capacita a sus usuarios	PR.AT-1
	Los usuarios de la organización tanto privilegiados, personal, altos ejecutivos y partes interesadas deben entender sus roles y responsabilidades	PR.AT-2 PR.AT-3 PR.AT-4
2.3	**Seguridad de Datos**	
	La organización debe gestionar formalmente la transferencia, eliminación y disposición de sus activos	PR.DS-3
	La organización debe separar entornos de desarrollo con los de producción en caso tenga sistemas desarrollados	PR.DS-7
2.4	**Procesos y Procedimientos de protección de la Información**	
	La organización debe mantener una configuración básica de las tecnologías de información y sistemas de control industrial mediante principios de seguridad	PR.IP-1
	La organización debe aplicar la Ciberseguridad en las prácticas de RRHH (ej. selección de personal, des aprovisionamiento, etc.)	PR.IP-11
3	**Detección de Anomalías, Eventos y Monitoreo**	
3.1	**Anomalías y Eventos**	

	La organización debe establecer una línea de operaciones de red, flujo de datos, usuarios y sistemas ante posibles eventos	DE.AE-1
	La organización debe analizar los eventos detectados para entender el objetivo del ataque y los métodos aplicados	DE.AE-2
	La organización debe determinar el impacto del evento	DE.AE-4
	La organización debe establecer un umbral de alerta	DE.AE-5
4	**Plan de Respuestas**	
4.2	**Comunicación**	
	La organización debe compartir la información de forma consistente y con planes de respuesta	RS.CO-3
4.3	**Análisis**	
	La organización realiza forenses	RS.AN-3
	La organización clasifica los incidentes de acuerdo con los planes de respuesta	RS.AN-4
4.4	**Mitigación**	
	La organización contiene y mitiga los incidentes	RS.MI-1 RS.MI-2
5	**Plan de Recuperación**	
5.3	**Comunicación**	
	La organización repara su reputación después de reparar el incidente.	RC.CO-2

2. Objetivos y Métricas de Ciberseguridad

	Métricas por Objetivo	Unidad de medida	Propósito de métrica	Mecanismo para medir la métrica	Frecuencia de medición de la métrica	Responsable de la medición de la métrica
Objetivos del Modelo	**Objetivo 1: Crear conciencia de las amenazas intencionales y no intencionales de Ciberseguridad dentro y fuera de la organización.** **Objetivo 2:** Capacitar a los empleados en reconocimiento de phishing, ransomware y otros vectores de amenazas en las redes sociales.					
	M1. Evaluaciones periódicas de los colaboradores sobre Ciberseguridad	Nota de evaluación	Identificar los colaboradores con notas desaprobatorias y las causas de sus resultados	Evaluación realizada por medio del área de TI	Mensual	Área de TI/ RRHH
	M2. Cursos a manera de evaluación y capacitación sobre Ciberseguridad	Compromiso de aplicación de conceptos	Comprometer al colaborador con aplicar los conocimientos aprendidos dentro de la organización mediante la aceptación de un compromiso digital	Documento digital de compromiso hecho por el área de TI o consultoría	Mensual	Área de TI o consultoría
	Objetivo 3: Entrenar y desarrollar conciencia en los empleados sobre los sesgos cognitivos que puedan perjudicar sus actividades diarias.					
	M3. Evaluaciones psicológicas de los empleados	Resultados cualitativos de la evaluación	Conocer el comportamiento de los colaboradores y posibles factores	Evaluación digital realizado por un especialista	Mensual	Área de RRHH

			que puedan afectar su trabajo habitual	de gestión humana o psicólogo		
	M4. Evaluaciones del nivel de satisfacción dentro de la organización	Resultados cualitativos	Conocer el nivel de satisfacción del empleado al trabajar en la organización	Encuestas realizadas por el área de RRHH	Mensual	Área de RRHH
	Objetivo 4: Proteger los activos digitales de la organización mediante una gestión de activos de Ciberseguridad.					
	M5. Número de incidentes de seguridad relacionado con la pérdida, eliminación, corrupción de activos digitales	Número de incidentes de seguridad agrupado por áreas	Identificar las áreas con mayor número de incidentes de seguridad y averiguar las causas	Registros por medio de mesa de ayuda	Diario	Mesa de ayuda
	M6. Reporte de incumplimiento de las políticas de seguridad de la información relacionado a los activos digitales	Número de incidentes por incumplimiento agrupado por áreas	Identificar las áreas con mayor número de incumplimientos de políticas y averiguar las causas	Registros por medio de mesa de ayuda	Diario	Mesa de ayuda
	Objetivo 5: Controlar los accesos y permisos de cada empleado de la organización.					
	M7. Número de incidentes de seguridad relacionados con la pérdida de confidencialidad de datos personales en la organización	Número de incidentes de seguridad agrupado por áreas	Identificar las áreas con mayor número de incidentes de seguridad y averiguar las causas	Registros por medio de mesa de ayuda	Diario	Mesa de ayuda
	M8. Monto total de multas por incumplimiento de la ley de datos personales aplicados en un período anual	Número de multas por incumplimiento por áreas	Identificar las áreas con mayor número de multas por incumplimiento de la ley	Registros por medio de mesa de ayuda	Diario	Mesa de ayuda
	Objetivo 6: Mejorar la usabilidad del Sistema de Información para reducir la probabilidad de errores humanos.					
	M9. Nivel de usabilidad de los softwares de la organización	Nivel de satisfacción del usuario	Identificar qué softwares tienen un nivel bajo de satisfacción en cuanto a usabilidad	Sistema de escalas de usabilidad	Quincenal	Área de TI

3. Patrones de comportamiento

	Tipo de Amenazas	UIT-HACK				DISC		PHYS		PORT		
		Robo de ID/Acceso no autorizado	Phishing	Aplicaciones maliciosas/ Malware	Ingeniería Social	Enviar información sensible por correo o fax accidentalmente	Divulgación de datos a través de internet, social media, cloud o móviles	Información sensible física en escritorios o lugares inseguros	Eliminación de información sensible de forma incorrecta	Robo de equipos portables	Pérdida de equipos portables	Robo de unidades de respaldo
Factores Causales	**Factores Organizacionales generales**											
	Requerimientos de proceso de negocio (BPR)	●			●	●	●	●	●			
	Flujo de datos				●	●		●	●			
	Escenario de trabajo	●	●	●	●	●		●	●		●	
	Planificación/Control del trabajo		●	●	●	●	●	●	●			
	Factores Humanos											
	Fatiga o somnolencia				●		●	●				
	Carga de trabajo mental		●	●	●		●	●				
	Falta de conciencia de la situación (SA)		●	●	●	●	●			●		●
	Mente distraída		●		●	●	●				●	
	Sesgos cognitivos		●		●	●	●	●	●		●	
	Factores Psicosociales, Socioculturales y otros											
	Cultura	●					●					
	Estado de ánimo					●	●	●	●			
	Edad	●					●	●	●			
	Influencia de Drogas/Hormonas/Enfermedades		●	●	●		●					

4. Matriz de gestión de riesgos

Se hizo una modificación del diseño de la tabla para la medición del riesgo. Más allá de ese cambio, no hubo modificaciones en la matriz de gestión de riesgos.

Nivel de Riesgo		
1 (poner cabeceras)	2 (poner cabeceras)	Bajo
3	6	Medio
8	10	Alto
12	16	Muy Alto

5. Guía de implementación del modelo

Para la guía de implementación se agregó los siguientes puntos:

- Se agregó un acápite que indique qué personal debería formar parte del equipo de trabajo que ejecute la guía y las competencias debe tener el personal que realice estos trabajos.
- Se agregaron las fórmulas para la evaluación del nivel de riesgo en base al impacto y probabilidad del riesgo. En esta sección se describe cómo se evalúa cada riesgo y las condiciones respectivas.

Anexo H: Resultados de la validación de los especialistas

Los resultados validados por los especialistas junto con sus comentarios, nivel de pertinencia y sugerencias, en caso lo considere pertinente, se encuentran en el siguiente link: https://drive.google.com/folderview?id=1PptaFBPlOWRvqRA4SyklfZTenNOkEotG