MAESTRÍA EN CIBERSEGURIDAD

PROYECTO DE GRADUACIÓN

Sometido al Tribunal Examinador de Postgrados para optar por el grado de Maestría en Ciberseguridad

Título del Proyecto

Elaboración De Un Modelo De Mitigación De Riesgos Basado Iso31000 Para El Uso Seguro De Redes Wi-Fi Públicas En Centros Comerciales De La Zona Pacífico Norte

AUTOR

Juan Ezequiel Peña Álvarez

TUTOR

Randall Artavia Delgado

LECTOR

Irvin Argenis Sáenz Córdoba

Perez Zeledón, Costa Rica

Diciembre, 2025

UNIVERSIDAD SAN ISIDRO DEL LABRADOR
MAESTRÍA EN CIBERSEGURIDAD

TRIBUNAL EXAMINADOR

Lic. Ruddy Rodríguez Acuña
Director de Maestría

Msc. Randall Artavia Delgado
Tutor

Msc. Irvin Argems Sáenz Córdoba
Lector

DECLARACIÓN JURADA

Yo, Juan Ezequiel Peña Alvarez, mayor, casado, egresado de la carrera de Maestría Profesional en Ciberseguridad de la Universidad San Isidro Labrador, domiciliado en la ciudad de Liberia, Guanacaste, portador(a) de la cédula de identidad número 155802422722, en este acto, debidamente apercibido y entendido de las penas y consecuencias con las que se castiga, en el Código Penal, el delito del perjurio, ante quienes se constituyen en el Tribunal Examinador de mi Trabajo Final de Graduación para optar por el título de maestría, juro solemnemente que mi trabajo final de graduación titulado "**Elaboración De Un Modelo De Mitigación De Riesgos Basado Iso31000 Para El Uso Seguro De Redes Wi-Fi Públicas En Centros Comerciales De La Zona Pacífico Norte**" es una obra original que ha respetado todo lo preceptuado por las Leyes Penales así con la Ley de Derechos de Autor y Derechos Conexos, número 6683 de 14 de octubre de 1982 y sus reformas, publicada en la Gaceta número 226 de 25 de noviembre de 1982; incluyendo el numeral 70 de dicha ley que advierte: artículo 70°: Es permitido citar a un autor transcribiendo los pasajes pertinentes siempre que estos no sean tantos y seguidos, que puedan considerarse como una producción simulada y sustancial, que redunde en perjuicio del autor y de la obra original. Asimismo, quedo advertido que la Universidad San Isidro Labrador se reserva el derecho de protocolizar este documento ante Notario Público. En fe de lo anterior firmo en la ciudad de Liberia, Guanacaste, al ser el seis del mes de diciembre del año dos mil veinticinco.

Juan Ezequiel Peña Álvarez

Cédula: 155802422722

DEDICATORIA

Al cerrar este capítulo tan importante de mi vida, no puedo evitar sentir una profunda gratitud y humildad por todo lo que he logrado. Esta Maestría en Ciberseguridad no es solo un logro personal, sino un reflejo del apoyo y amor incondicional que he recibido a lo largo del camino.

A Dios, por ser mi guía constante, dándome fuerzas en cada momento de duda y desánimo, y por iluminarme con sabiduría para enfrentar cada desafío. A mi esposa, el pilar fundamental de mi vida, cuya paciencia, amor y comprensión han sido el motor que me ha impulsado a seguir adelante. A mis hijos, por su alegría infinita, por recordarme que la verdadera esencia de la vida está en la simplicidad y el amor que compartimos cada día.

A mis padres, por su ejemplo de esfuerzo, sacrificio y dedicación. Gracias por darme las alas para volar y los cimientos sobre los que hoy me sostengo. A mis hermanos, por su constante apoyo y por recordarme, siempre, que en la vida no hay éxito verdadero sin unidad y familia.

Este logro no es solo mío, es el reflejo de todos ustedes. ¡Gracias por estar a mi lado en cada paso de este arduo viaje! Esta Maestría no es solo un título, sino una promesa de seguir creciendo, aprendiendo y, sobre todo, honrando a quienes han creído en mí. ¡Lo logramos juntos!

AGRADECIMIENTOS

Al concluir este ciclo de estudios, quiero tomar un momento para expresar mi más sincero agradecimiento a todas las personas que han sido parte fundamental de este viaje. Cada uno de ustedes ha dejado una huella indeleble en este proceso.

A Dios, por su presencia constante en mi vida. No solo me ha brindado la fortaleza para superar obstáculos, sino que también ha guiado mis decisiones, mostrándome siempre el camino cuando la incertidumbre me rodeaba.

A mi esposa, mi compañera de vida, quien con su amor y apoyo incondicional ha sido mi refugio en los momentos de cansancio. Gracias por ser mi constante motivación, por siempre creer en mí y por compartir mis sueños como si fueran nuestros.

A mis hijos, quienes con su energía y sonrisas me recordaron que el equilibrio entre esfuerzo y amor es lo que da sentido a todo. Ustedes son la razón por la que cada día me esfuerzo más.

A mis padres, cuyo sacrificio y dedicación me han permitido estar donde estoy hoy. Son el fundamento sobre el cual se construye mi éxito, y por eso siempre les estaré agradecido. Gracias por enseñarme el valor del trabajo arduo y la importancia de la educación.

A mis hermanos, por su apoyo, sus palabras de aliento y por ser un equipo en todo momento. En cada uno de ustedes he encontrado fuerza y respaldo cuando más lo necesitaba.

Este logro no sería el mismo sin el amor, la comprensión y la paciencia de todos ustedes. Gracias por hacer de mi camino un sendero lleno de apoyo, risas y esperanza. ¡Este título también es suyo!

CARTA DE AUTORIZACIÓN DEL TUTOR

Pérez Zeledón, 06 de diciembre de 2025

Licenciado
Ruddy Rodríguez Acuña
Director de la Escuela de Ingeniería de Sistemas
Universidad San Isidro Labrador

Estimado señor:

Yo, Randall Mauricio Artavia Delgado, mayor, Ingeniero en Informática, con domicilio en la Trinidad de Moravia, San José, portador de la cédula de identidad número 2-0574-0823, en mi condición de tutor del Proyecto de Graduación titulado "Elaboración De Un Modelo De Mitigación De Riesgos Basado Iso31000 Para El Uso Seguro De Redes Wi-Fi Públicas En Centros Comerciales De La Zona Pacífico Norte", propuesta por el estudiante Juan Ezequiel Peña Álvarez, manifiesto lo siguiente:

1. Que el proceso de trabajo final de graduación culmina satisfactoriamente.
2. Que se ha incorporado en el documento final las sugerencias hechas por el Tribunal Examinador.
3. Que he cumplido con el acompañamiento encomendado por la Universidad en forma y fondo.
4. Que considero que el documento final responde a las exigencias académicas establecidas por la Universidad.

Atentamente,

M.Sc. Randall Mauricio Artavia Delgado
Tutor

CARTA DE APROBACIÓN DEL LECTOR

Pérez Zeledón, 06 de diciembre de 2025

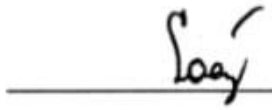
Licenciado
Ruddy Rodríguez Acuña
Director de la Escuela de Ingeniería de Sistemas
Universidad San Isidro Labrador

Estimado señor:

Yo, Irvin Argenis Sáenz Córdoba, mayor, Ingeniero en Informática, con domicilio en Río Danta de Guápiles, portador de la cédula de identidad número 7-0197-0839, en mi condición de lector del Proyecto de Graduación titulado "Elaboración De Un Modelo De Mitigación De Riesgos Basado Iso31000 Para El Uso Seguro De Redes Wi-Fi Públicas En Centros Comerciales De La Zona Pacífico Norte", propuesta por el estudiante Juan Ezequiel Peña Álvarez, manifiesto lo siguiente:

1. Que la lectura del trabajo final de graduación concluye satisfactoriamente.
2. Que he leído el documento final y he hecho mis observaciones en el mismo.
3. Que he cumplido con las labores de lector encomendadas por la Universidad en forma y fondo.
4. Que considero que el documento final responde a las exigencias académicas establecidas por la Universidad.

Atentamente,



M.Sc. Irvin Argenis Sáenz Córdoba
Lector

TABLA DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

LISTA DE PALABRAS CLAVES

- Gestión de riesgos
- ISO 31000
- Redes Wi-Fi públicas
- Centros comerciales
- Ciberseguridad
- Seguridad de la información
- Vulnerabilidades
- Amenazas digitales
- Controles de seguridad
- Mitigación de riesgos
- Usuarios móviles
- Protección de datos

RESUMEN EJECUTIVO

La investigación aborda la problemática de la exposición a riesgos de ciberseguridad en redes Wi-Fi públicas ofrecidas en centros comerciales, tomando como caso de estudio el Mall Centro Plaza Liberia, ubicado en la zona Pacífico Norte. Se parte del reconocimiento de que estos servicios inalámbricos se han convertido en un componente clave de la experiencia del visitante, pero suelen gestionarse con un énfasis mayor en la continuidad del servicio que en una gestión preventiva y sistemática de riesgos. El objetivo general fue desarrollar un modelo de mitigación de riesgos basado en la norma ISO 31000 que fortalezca el uso seguro de la red Wi-Fi pública del mall, mediante la identificación, evaluación y tratamiento de las amenazas asociadas a su operación. Para ello, se plantearon objetivos específicos orientados a analizar el contexto interno y externo del centro comercial, identificar amenazas y vulnerabilidades, evaluar los riesgos según probabilidad e impacto, diseñar el modelo de mitigación y validar su pertinencia con expertos.

Metodológicamente, el estudio se enmarca en una investigación de tipo básico con orientación aplicada y nivel descriptivo, apoyada en un enfoque cualitativo guiado por la teoría fundamentada. Se trabajó con un estudio de caso centrado en el Mall Centro Plaza Liberia, considerando como población a los usuarios de la red Wi-Fi pública y al personal técnico y administrativo responsable de su gestión. Se utilizó un muestreo no probabilístico por conveniencia, aplicando entrevistas semiestructuradas y grupos focales con usuarios, así como entrevistas con personal técnico y de administración, complementadas con observación de la red y revisión de documentos internos y normativos. La información recabada se procesó mediante análisis temático, construyendo categorías relativas al contexto tecnológico y organizacional, a las prácticas de uso y a los riesgos percibidos, las

cuales se articularon con las etapas del proceso de gestión de riesgos definido por ISO 31000.

Los resultados muestran que el Mall Centro Plaza Liberia opera en un entorno de creciente conectividad, con infraestructura interna cifrada pero fragmentada y sin una red pública oficial claramente señalizada, lo que favorece la confusión de los usuarios y la aparición de redes no autorizadas. Se identificaron amenazas y vulnerabilidades de origen técnico (suplantación de puntos de acceso, captura de tráfico, secuestro de sesiones) y humano-organizacional (exceso de confianza en cualquier red disponible, desconocimiento de buenas prácticas, ausencia de campañas de sensibilización), que fueron evaluadas cualitativamente en función de su probabilidad, impacto y controles existentes, construyendo una matriz que permitió priorizar los riesgos más críticos. A partir de este diagnóstico se diseñó un modelo de mitigación de riesgos basado en ISO 31000, estructurado en etapas de gobernanza, establecimiento de contexto, identificación, análisis, evaluación, tratamiento, comunicación y monitoreo, que integra medidas técnicas y acciones educativas. La validación mediante juicio de expertos evidenció que el modelo es pertinente, claro y factible de implementar, concluyéndose que constituye una herramienta útil para fortalecer la seguridad del servicio de Wi-Fi público en el mall y un referente replicable para otros centros comerciales de la zona Pacífico Norte.

CAPITULO I. INTRODUCCIÓN

1.1 Planteamiento del tema de estudio

El uso de redes Wi-Fi públicas se ha consolidado como un servicio casi imprescindible en centros comerciales, aeropuertos y otros espacios de alta afluencia, con el propósito de mejorar la experiencia de los visitantes y fomentar la interacción digital con marcas y servicios. No obstante, desde la perspectiva de la Ciberseguridad, estas redes constituyen un vector crítico de exposición, al comprometer potencialmente la confidencialidad, integridad y disponibilidad de los datos transmitidos, especialmente cuando se emplean configuraciones básicas o se carece de controles avanzados de protección (Scarfone y Souppaya, 2010). En escenarios donde convergen grandes volúmenes de personas y dispositivos, como los malls, la superficie de ataque se incrementa de forma significativa y se ve agravada por prácticas de uso inseguras y por la percepción errónea de que, por encontrarse en un entorno "formal", las redes son intrínsecamente confiables (Conti et al., 2016).

En el contexto de Costa Rica y de la región latinoamericana, el crecimiento sostenido del acceso inalámbrico gratuito ha estado acompañado por un aumento de incidentes asociados a redes abiertas o deficientemente protegidas, entre ellos la suplantación de puntos de acceso (Evil Twin), la interceptación de comunicaciones, el secuestro de sesiones y el robo de credenciales (OAS, 2020). Organismos nacionales como el MICITT y el CSIRT han advertido sobre la necesidad de robustecer los esquemas de seguridad en redes de acceso público, alineando su gestión con marcos normativos y con los principios de la legislación en protección de datos personales, de manera que se resguarde adecuadamente la información de los usuarios y se reduzca la exposición a ciberamenazas emergentes.

En este contexto se ubica el Mall Centro Plaza Liberia, en la región Pacífico Norte, que ofrece una red Wi-Fi pública como servicio de valor agregado para sus visitantes. Sin embargo, desde una mirada de Maestría en Ciberseguridad, se identifica que el centro comercial no dispone de un modelo formal de gestión de riesgos que permita identificar, evaluar y tratar de manera sistemática las amenazas asociadas a la operación de dicha red. Las prácticas existentes se limitan, principalmente, a configuraciones básicas de seguridad y a un monitoreo ocasional, sin un proceso estructurado que asegure continuidad, prevención, trazabilidad de incidentes ni alineamiento con estándares internacionales. Esta brecha incrementa la probabilidad de afectación a la privacidad de los usuarios, de interrupciones del servicio, de daños reputacionales para el establecimiento y de eventuales incumplimientos regulatorios.

El ISO 31000 se presenta como un marco de referencia reconocido internacionalmente para la gestión integral de riesgos, al proponer etapas claras de identificación, análisis, evaluación y tratamiento ajustables al contexto de cada organización (International Organization for Standardization, 2018). No obstante, su aplicación concreta a redes Wi-Fi públicas en centros comerciales como el Mall Centro Plaza Liberia no se encuentra estandarizada ni documentada. Frente a este escenario problemático, surge la necesidad académica y profesional, propia de un trabajo sometido al Tribunal Examinador de Postgrados para optar por el grado de Maestría en Ciberseguridad, de desarrollar un modelo de mitigación de riesgos basado en ISO 31000, específicamente orientado a la red Wi-Fi pública del mall, que permita reducir las vulnerabilidades técnicas y organizacionales, fortalecer la seguridad del servicio y aumentar la confianza de los usuarios que lo utilizan.

Problema central:

El Mall Centro Plaza Liberia carece de un modelo formal de gestión de riesgos basado en ISO 31000 para la identificación, evaluación y tratamiento de amenazas asociadas al uso de su red Wi-Fi pública, lo que incrementa la exposición a incidentes de seguridad y limita la capacidad de ofrecer un servicio confiable y seguro.

Entonces, se plantea la pregunta general: ¿Cómo desarrollar un modelo de mitigación de riesgos, basado en ISO 31000, que fortalezca el uso seguro de la red Wi-Fi pública del Mall Centro Plaza Liberia mediante la identificación, evaluación y tratamiento de las amenazas asociadas a su operación?

1.2 Antecedentes del tema

A escala internacional, las redes Wi-Fi públicas se han generalizado como servicios complementarios en centros comerciales, aeropuertos, hoteles y otros espacios de gran afluencia, con el objetivo de mejorar la experiencia del usuario y fomentar la interacción digital. No obstante, diversos estudios coinciden en que estos entornos se encuentran entre los más expuestos a amenazas de ciberseguridad, debido a su alta accesibilidad, la diversidad de dispositivos conectados y la frecuente ausencia de controles avanzados de protección (Scarfone y Souppaya, 2010; Conti et al., 2016). Entre las vulnerabilidades más comunes se reportan la creación de puntos de acceso falsos, el uso de cifrados débiles o inexistentes, mecanismos de autenticación insuficientes y la facilidad para interceptar, modificar o redirigir el tráfico de datos.

En América Latina, informes especializados señalan que los centros comerciales y otros espacios de acceso libre han sido objeto de ataques orientados a la obtención de credenciales, el secuestro de sesiones y el engaño a usuarios mediante técnicas como Evil Twin o Man-in-the-Middle (OAS, 2020). Este panorama se agrava por la heterogeneidad de los dispositivos utilizados, muchos de ellos sin configuraciones seguras por defecto, y

por el desconocimiento de buenas prácticas de seguridad en la población, lo que incrementa la probabilidad de incidentes y dificulta su detección temprana.

En Costa Rica, entidades como el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT), la Superintendencia de Telecomunicaciones (SUTEL) y el CSIRT han documentado vulnerabilidades recurrentes en redes abiertas o de configuración básica, enfatizando la necesidad de implementar esquemas consistentes de gestión del riesgo en servicios de acceso público (MICITT, 2022). Paralelamente, el marco legal encabezado por la Ley 8968 de Protección de la Persona frente al Tratamiento de sus Datos Personales establece obligaciones explícitas para los responsables de servicios digitales, entre ellas garantizar condiciones adecuadas de seguridad para los datos que se transmiten a través de redes inalámbricas.

En este contexto, los centros comerciales de la zona Pacífico Norte, y en particular el Mall Centro Plaza Liberia, comparten los retos descritos. Si bien se han adoptado medidas técnicas básicas para ofrecer conectividad inalámbrica a los visitantes, no se evidencia la existencia de un proceso formal de gestión de riesgos que permita identificar amenazas, evaluar impactos y definir estrategias de mitigación de manera sistemática y continua. La gestión de la red tiende a centrarse en la disponibilidad del servicio, más que en un enfoque integral de ciberseguridad, lo que abre brechas que pueden afectar la privacidad de los usuarios, la continuidad operativa y la reputación institucional.

Frente a esta situación, los marcos internacionales de gestión de riesgos, como la norma ISO 31000, se han consolidado como referentes para estructurar procesos de identificación, análisis, evaluación y tratamiento de riesgos en organizaciones de distintos sectores (ISO, 2018). Sin embargo, no se han identificado estudios nacionales que documenten la aplicación de ISO 31000 específicamente al uso seguro de redes Wi-Fi

públicas en centros comerciales de la zona Pacífico Norte, lo que revela un vacío de conocimiento práctico. Esta ausencia respalda la pertinencia de elaborar un modelo de mitigación de riesgos basado en dicho estándar, adaptado al contexto local, que fortalezca la seguridad de la conectividad inalámbrica y la confianza de los usuarios en estos entornos.

1.3 Justificación

El uso de redes Wi-Fi públicas en centros comerciales se ha convertido en un servicio casi indispensable para mejorar la experiencia de los visitantes, facilitar transacciones digitales y apoyar las estrategias comerciales de los establecimientos. Sin embargo, desde la perspectiva de la Ciberseguridad, este tipo de redes expone a usuarios y organizaciones a riesgos que pueden comprometer la confidencialidad, integridad y disponibilidad de la información, especialmente en entornos de alta concurrencia y con una gran diversidad de dispositivos conectados, donde el control efectivo del entorno inalámbrico se vuelve más complejo (Scarfone & Souppaya, 2010). Esta realidad es particularmente relevante en los centros comerciales de la zona Pacífico Norte, donde la oferta de conectividad gratuita crece más rápido que la adopción de esquemas formales de gestión de riesgos.

En el caso concreto del Mall Centro Plaza Liberia se evidencia que, si bien se han implementado ciertas medidas técnicas básicas, no existe un modelo estructurado de gestión del riesgo que permita identificar, evaluar y tratar de manera sistemática las amenazas asociadas al uso de su red Wi-Fi pública. Esta situación no solo limita la capacidad de anticipar y mitigar incidentes de seguridad, sino que también genera vulnerabilidades que pueden afectar la privacidad de los usuarios, la continuidad del servicio y la reputación del establecimiento. Además, el marco legal costarricense,

particularmente la Ley 8968 sobre protección de datos personales y su reglamento, impone la obligación de adoptar medidas efectivas para proteger la información que se transmite a través de servicios digitales, lo que hace aún más apremiante contar con un modelo formal alineado a dichas exigencias (PRODHAB, 2015).

La adopción de la norma ISO 31000 se justifica porque ofrece principios y directrices reconocidas internacionalmente para la gestión del riesgo, aplicables a organizaciones de cualquier tamaño y sector. Este estándar permite establecer un proceso continuo y dinámico de identificación, análisis, evaluación y tratamiento de riesgos, adaptable al contexto específico de las redes Wi-Fi públicas en centros comerciales (ISO, 2018). Asimismo, su enfoque es compatible con investigaciones de tipo cualitativo, ya que facilita integrar la percepción de expertos, el análisis del contexto local y la participación de actores relevantes (administración del centro comercial, personal técnico, comercios y usuarios) en la construcción del modelo de mitigación.

Desde el punto de vista académico, este trabajo contribuye al campo de la gestión de riesgos en entornos tecnológicos, al proponer una aplicación concreta y contextualizada de un estándar internacional en un ámbito poco documentado a nivel nacional. En el plano práctico, el modelo propuesto busca fortalecer la seguridad del servicio de Wi-Fi público en el Mall Centro Plaza Liberia y ofrecer una referencia replicable para otros centros comerciales de la zona Pacífico Norte, incrementando la confianza de los usuarios, mejorando la toma de decisiones operativas y apoyando el cumplimiento de las obligaciones regulatorias vigentes.

1.4 Objetivos

1.4.1 Objetivo general

Desarrollar un modelo de mitigación de riesgos basado en ISO 31000 que permita fortalecer el uso seguro de la red Wi-Fi pública del Mall Centro Plaza Liberia, mediante la identificación, evaluación y tratamiento de las amenazas asociadas a su operación.

1.4.2 Objetivos específicos

Analizar el contexto interno y externo del Mall Centro Plaza Liberia para comprender las condiciones tecnológicas, operativas y organizacionales que influyen en la gestión de riesgos de su red Wi-Fi pública.

Identificar las amenazas, vulnerabilidades y riesgos asociados al uso de la red Wi-Fi pública mediante la recopilación y análisis de información técnica y cualitativa proveniente de especialistas y actores relevantes.

Evaluar los riesgos identificados considerando su probabilidad, impacto y controles existentes, con el fin de establecer criterios que permitan priorizar su tratamiento dentro del modelo propuesto.

Diseñar un modelo de mitigación de riesgos basado en ISO 31000, estructurado en etapas y orientado a mejorar la gestión del servicio de Wi-Fi público del centro comercial.

Validar la pertinencia y aplicabilidad del modelo propuesto mediante la revisión y retroalimentación de expertos en redes inalámbricas, seguridad informática y gestión de riesgos.

1.5 Alcances

Figura 1

Modelo de Mitigación de Riesgos ISO 31000 para Redes Wi-Fi Públicas en Centros Comerciales

Nota. Obtenido de techsafety.ca

Este trabajo abarca el diseño, validación y presentación de un modelo de mitigación de riesgos basado en la norma ISO 31000, orientado a fortalecer el uso seguro de las redes Wi-Fi públicas en centros comerciales de la región Pacífico Norte de Costa Rica. El estudio considera un proceso estructurado que incluye el diagnóstico de vulnerabilidades, la elaboración del modelo, su validación mediante una experiencia piloto y la sistematización de los hallazgos en un conjunto de recomendaciones aplicables para la gestión de redes inalámbricas en entornos comerciales.

El alcance comprende la identificación de vulnerabilidades técnicas y organizacionales, el análisis del cumplimiento normativo asociado a la operación de redes inalámbricas públicas y la evaluación del nivel de conciencia de los usuarios respecto a los riesgos de seguridad digital. Para ello, se emplean técnicas de corte cualitativo, entrevistas,

encuestas y análisis documental, que permiten comprender el contexto específico, recoger la percepción de actores clave y fundamentar la propuesta del modelo de mitigación de riesgos.

Además, la investigación se circunscribe al caso del Mall Centro Plaza Liberia, centro comercial representativo de la región Pacífico Norte, donde se desarrollan las actividades de diagnóstico, recolección de información, validación y análisis que sustentan el modelo propuesto. Si bien los resultados pueden servir como referencia para otros centros comerciales o espacios con características similares, su aplicación en otros contextos dependerá de las particularidades regulatorias, tecnológicas y culturales de cada entorno.

En consecuencia, el proyecto no se limita a la formulación de un modelo técnico, sino que también incorpora la definición de lineamientos estratégicos y operativos orientados a fortalecer la seguridad digital, mejorar la confianza de los usuarios en el servicio de Wi-Fi público y sentar bases para futuras adaptaciones y ampliaciones del modelo en escenarios más amplios dentro de la región Pacífico Norte y, potencialmente, en otros contextos nacionales o regionales.

1.6 Limitaciones

La presente investigación contempla varias limitaciones que deben ser consideradas al momento de interpretar los resultados. En primer lugar, el estudio se desarrolla exclusivamente en el Mall Centro Plaza Liberia, por lo que los hallazgos y el modelo propuesto se construyen a partir de las condiciones tecnológicas, organizacionales y operativas propias de este caso. Si bien la propuesta puede servir como referencia para otros centros comerciales de la zona Pacífico Norte o de contextos similares, su

aplicabilidad en diferentes entornos requerirá ajustes y adaptaciones según las particularidades de cada realidad.

Asimismo, debido a restricciones de acceso, recursos y tiempo, no se incluyeron pruebas técnicas avanzadas, como evaluaciones de penetración de mayor alcance, monitoreo continuo del tráfico inalámbrico o simulaciones extendidas de incidentes de ciberseguridad. En consecuencia, el análisis se centra principalmente en la identificación cualitativa de riesgos, el diagnóstico de vulnerabilidades visibles y la percepción de actores clave, sin incorporar mediciones instrumentales detalladas ni análisis forenses especializados.

Por otra parte, la validación del modelo se realizó mediante una prueba piloto y la retroalimentación de un grupo acotado de especialistas, lo que restringe la amplitud de la evaluación. La disponibilidad de personal técnico, el nivel de participación de los usuarios y las condiciones operativas del centro comercial influyeron de manera directa en la profundidad y extensión del proceso de recolección de datos.

Finalmente, el alcance de este trabajo se limita a la elaboración y validación preliminar de un modelo de mitigación de riesgos basado en ISO 31000. La implementación completa del modelo en el Mall Centro Plaza Liberia, su seguimiento longitudinal, la medición sistemática de sus efectos y su eventual escalamiento a otros centros comerciales quedan fuera del alcance de la presente investigación y se plantean como líneas de trabajo futuras.

1.7 Cronograma de actividades

Tabla 1

Cronograma de actividades

NOMBRE DE LA TAREA	DURACIÓN	INICIO	FINAL
Trabajo de investigación final	94 días	Miércoles 03/09/25	Sábado 06/12/25
Matrícula TFG	1 día	Miércoles 03/09/25	Miércoles 03/09/25
Lectura manual de TFG y anotación de dudas	3 días	Jueves 04/09/25	Sábado 06/09/25
Reunión con el tutor	1 día	Domingo 07/09/25	Domingo 07/09/25
Planeación del trabajo	5 días	Lunes 08/09/25	Viernes 12/09/25
Definición del título	1 día	Lunes 08/09/25	Lunes 08/09/25
Definición de objetivos	1 día	Martes 09/09/25	Martes 09/09/25
Creación del cronograma	1 día	Miércoles 10/09/25	Miércoles 10/09/25
Creación bitácora de trabajo	2 días	Jueves 11/09/25	Viernes 12/09/25
Entrega del plan de trabajo al tutor	1 día	Sábado 13/09/25	Sábado 13/09/25
Desarrollo del Capítulo I	10 días	Domingo 14/09/25	Martes 23/09/25
Creación de estructura del TFG	2 días	Domingo 14/09/25	Lunes 15/09/25
Planteamiento del tema	2 días	Martes 16/09/25	Miércoles 17/09/25
Justificación del trabajo	2 días	Jueves 18/09/25	Viernes 19/09/25
Definición de alcances	2 días	Sábado 20/09/25	Domingo 21/09/25
Definición de limitaciones	2 días	Lunes 22/09/25	Martes 23/09/25
Envío Capítulo I a tutor	1 día	Miércoles 24/09/25	Miércoles 24/09/25

Desarrollo del Capítulo II	12 días	Jueves 25/09/25	Lunes 06/10/25
Desarrollo de marco teórico	12 días	Jueves 25/09/25	Lunes 06/10/25
Envío Capítulo II a tutor	1 día	Martes 03/10/25	Martes 03/10/25
Desarrollo del Capítulo III	12 días	Miércoles 04/10/25	Domingo 15/10/25
Tipo de Investigación	2 días	Miércoles 04/10/25	Jueves 05/10/25
Administración y abordaje	2 días	Viernes 06/10/25	Sábado 07/10/25
Sujetos y fuentes	3 días	Domingo 08/10/25	Martes 10/10/25
Diseño de técnicas e instrumentos para recolección de información	5 días	Miércoles 11/10/25	Domingo 15/10/25
Envío Capítulo III a tutor	1 día	Lunes 16/10/25	Lunes 16/10/25
Desarrollo del Capítulo IV	9 días	Martes 17/10/25	Miércoles 25/10/25
Introducción a la propuesta	4 días	Martes 17/10/25	Viernes 20/10/25
Propuesta	5 días	Sábado 21/10/25	Miércoles 25/10/25
Envío Capítulo IV a tutor	1 día	Jueves 26/10/25	Jueves 26/10/25
Desarrollo del Capítulo V	13 días	Viernes 27/10/25	Miércoles 08/11/25
Desarrollo conclusiones	5 días	Viernes 27/10/25	Martes 31/10/25
Desarrollo recomendaciones	4 días	Miércoles 01/11/25	Sábado 04/11/25
Resumen ejecutivo	2 días	Domingo 05/11/25	Lunes 06/11/25
Anexos	2 días	Martes 07/11/25	Miércoles 08/11/25
Envío Capítulo V a tutor	1 día	Jueves 09/11/25	Jueves 09/11/25
Cierre Trabajo Final	15 días	Viernes 10/11/25	Sábado 25/11/25

Revisión por parte del Tutor	5 días	Viernes 10/11/25	Martes 14/11/25
Correcciones sugeridas por Tutor	4 días	Miércoles 15/11/25	Sábado 18/11/25
Entrega borrador al Lector	1 día	Domingo 19/11/25	Domingo 19/11/25
Revisión por parte del Lector	4 días	Lunes 20/11/25	Jueves 23/11/25
Correcciones sugeridas por Lector	3 días	Viernes 24/11/25	Domingo 26/11/25
Envío al Filólogo	1 día	Lunes 27/11/25	Lunes 27/11/25
Revisión del Filólogo	3 días	Martes 28/11/25	Jueves 30/11/25
Correcciones Trabajo Final	3 días	Viernes 01/12/25	Domingo 03/12/25
Empaste documento Final	1 día	Lunes 04/12/25	Lunes 04/12/25
Entrega documento a Universidad	1 día	Sábado 06/12/25	Sábado 06/12/25
Trabajo Final – Tesis	1 día	Sábado 06/12/25	Sábado 06/12/25

Nota. Elaboración propia

1.8 Producto esperado del TFG

Tabla 2

Productos esperados por cada objetivo específico

Objetivos específicos	Entregables	Formato
Analizar el contexto interno y externo del Mall Centro Plaza Liberia para comprender las condiciones tecnológicas, operativas y organizacionales que influyen en la gestión de riesgos de su red Wi-Fi pública.	Informe de diagnóstico del contexto interno y externo del Mall Centro Plaza Liberia, que incluya la descripción de la infraestructura de red, los procesos organizacionales vinculados al servicio de Wi-Fi, el marco normativo aplicable y un análisis sintético de actores y entorno.	Documento digital en formato PDF con texto descriptivo, esquemas de la infraestructura, tablas de síntesis y, de ser necesario, anexos gráficos.
Identificar las amenazas, vulnerabilidades y riesgos asociados al uso de la red Wi-Fi pública mediante la recopilación y análisis de información técnica y cualitativa proveniente de especialistas y actores relevantes.	Informe técnico–cualitativo que contenga el inventario de amenazas, vulnerabilidades y riesgos identificados para la red Wi-Fi pública del centro comercial, elaborado a partir de entrevistas, observación y revisión documental.	Documento digital en formato PDF con tablas de amenazas y vulnerabilidades, descripciones narrativas, citas textuales de informantes clave y anexos de apoyo.
Evaluar los riesgos identificados considerando su probabilidad, impacto y controles existentes, con el fin de establecer criterios que permitan priorizar su tratamiento dentro del modelo propuesto.	Matriz de evaluación y priorización de riesgos, en la que se consignen probabilidad, impacto, controles existentes y nivel de riesgo resultante, así como los criterios utilizados para su categorización.	Documento digital en formato PDF que incluya tablas de evaluación, posibles representaciones gráficas (p. ej., mapa de calor) y explicación metodológica de la valoración.
Diseñar un modelo de mitigación de riesgos basado en ISO 31000, estructurado en etapas y orientado a mejorar la gestión del servicio de Wi-Fi público del centro comercial.	Propuesta formal del modelo de mitigación de riesgos basado en ISO 31000 para redes Wi-Fi públicas en centros comerciales de la zona Pacífico Norte, con definición de etapas, actividades, roles, flujos de trabajo y lineamientos operativos.	Documento digital en formato PDF tipo “manual/propuesta de modelo”, con diagramas de proceso, cuadros resumen por etapas y anexos con procedimientos sugeridos.
Validar la pertinencia y aplicabilidad del modelo propuesto mediante la revisión y retroalimentación de expertos en redes inalámbricas, seguridad informática y gestión de riesgos.	Informe de validación del modelo, que incluya las matrices de juicio de expertos, principales observaciones y ajustes realizados, así como la versión final del modelo de mitigación recomendada para su implementación.	Documento digital en formato PDF con síntesis de la validación, tablas de evaluación de expertos, descripción de mejoras incorporadas y versión final esquematizada del modelo.

Nota. Elaboración propia

El desarrollo del presente Trabajo Final de Graduación generará una serie de productos claramente alineados con los objetivos específicos planteados. Entre ellos se consideran el diagnóstico del contexto interno y externo del Mall Centro Plaza Liberia, informes técnico–cualitativos sobre amenazas, vulnerabilidades y riesgos, matrices de evaluación y priorización de riesgos, así como la propuesta formal de un modelo de mitigación basado en la norma ISO 31000 y su validación preliminar mediante el juicio de expertos.

Cada uno de estos entregables se constituye en un insumo clave para la construcción del modelo final y su adecuada adaptación al contexto particular del Mall Centro Plaza Liberia y, potencialmente, a otros centros comerciales de la zona Pacífico Norte. En el Cuadro 1 se detallan los productos esperados del TFG, junto con sus respectivos entregables y formatos de presentación.

CAPÍTULO II. MARCO TEÓRICO

2.1 Introducción

El presente capítulo expone los fundamentos conceptuales, normativos y contextuales que sustentan la investigación sobre el uso seguro de redes Wi-Fi públicas en centros comerciales del Pacífico Norte de Costa Rica. Se revisan estudios relacionados con ciberseguridad en redes abiertas, se analiza el marco teórico de la gestión de riesgos a partir de ISO 31000, se abordan características de las redes Wi-Fi públicas, y se incorpora el enfoque cualitativo como metodología base del estudio. Además, se presenta la contextualización nacional y local que influye en el diseño del modelo de mitigación de riesgos propuesto.

2.2 Antecedentes de la investigación

2.2.1 Estudios internacionales

La literatura internacional evidencia de manera consistente que las redes Wi-Fi públicas presentan vulnerabilidades significativas debido a su carácter abierto y a la facilidad con la que un atacante puede interceptar, manipular o monitorear el tráfico de los usuarios. Entre los ataques más frecuentes se encuentran la interceptación de datos, la suplantación de puntos de acceso (Evil Twin), el secuestro de sesiones y los ataques de intermediario (Man-in-the-Middle), los cuales permiten obtener credenciales, modificar información o redirigir al usuario hacia servicios maliciosos (Conti et al., 2016).

En la misma línea, guías técnicas como el NIST SP 800-153 advierten que las redes inalámbricas abiertas o mal configuradas suelen carecer de cifrado robusto y de mecanismos confiables de autenticación, lo que incrementa de forma considerable la superficie de ataque y, en consecuencia, la exposición de los usuarios (Scarfone & Souppaya, 2010). A partir de estos estudios se coincide en la necesidad de adoptar controles técnicos más sólidos, como autenticación reforzada, cifrado avanzado,

segmentación de tráfico y monitoreo continuo, complementados con estrategias de educación al usuario.

Este cuerpo de evidencia internacional resulta particularmente relevante para la presente investigación, pues respalda la pertinencia de contar con un modelo de mitigación de riesgos estructurado, como el que propone ISO 31000, aplicado al contexto específico de las redes Wi-Fi públicas en centros comerciales.

2.2.2 Estudios latinoamericanos

A nivel latinoamericano, diversos análisis realizados por organismos regionales han identificado que la región enfrenta niveles elevados de incidentes de ciberseguridad, especialmente en redes públicas y servicios compartidos. Informes conjuntos de la OEA y el BID señalan que los usuarios latinoamericanos presentan, en general, prácticas débiles de protección digital y una alta exposición a fraudes, robo de datos y ataques dirigidos mediante redes inalámbricas abiertas (OAS/BID, 2020).

Asimismo, estudios regionales destacan que una proporción importante de usuarios desconoce los riesgos asociados a conectarse a un Wi-Fi público y confía en exceso en la mera disponibilidad del servicio, sin considerar aspectos de autenticidad del punto de acceso o de cifrado de la información (UIT, 2021). Estos hallazgos no solo reflejan una brecha en competencias digitales, sino que también ponen en evidencia la ausencia de marcos claros de gestión de riesgos en muchos escenarios de conectividad pública.

En este contexto, la elaboración de un modelo de mitigación de riesgos basado en ISO 31000 para centros comerciales de la zona Pacífico Norte se alinea con las recomendaciones regionales, al aportar una herramienta metodológica que articula controles técnicos, organizacionales y educativos para reducir la exposición a incidentes.

2.2.3 Estudios costarricenses

En Costa Rica, la investigación académica sobre redes Wi-Fi públicas continúa siendo limitada; sin embargo, distintos informes técnicos aportan evidencia significativa sobre el estado de la seguridad en servicios de conectividad. El MICITT (2022) documenta riesgos en redes de acceso público y subraya que distintos entornos comerciales y recreativos carecen de modelos formales de gestión de seguridad, lo que deriva en configuraciones básicas, ausencia de monitoreo sistemático y respuestas reactivas ante incidentes.

Por su parte, el CSIRT-CR (2021) reporta incidentes recurrentes de acceso no autorizado, intentos de suplantación de puntos de acceso y vigilancia de tráfico en redes abiertas, lo que confirma que las amenazas descritas en la literatura internacional también están presentes en el país. A ello se suma el marco legal costarricense en materia de protección de datos personales, especialmente la Ley 8968 y su reglamento, que asigna a los administradores de servicios digitales responsabilidades directas sobre la confidencialidad y seguridad de la información tratada (PRODHAB, 2015).

Estos antecedentes revelan una brecha entre las obligaciones normativas y las prácticas operativas en muchos espacios de conectividad pública, entre ellos los centros comerciales. Precisamente, esa brecha justifica la necesidad de desarrollar un modelo de mitigación de riesgos alineado con ISO 31000, que oriente de manera sistemática la gestión de redes Wi-Fi públicas en el contexto costarricense.

2.2.4 Vacío de investigación

A pesar de la evidencia internacional y regional sobre los riesgos asociados a las redes Wi-Fi públicas, y de los reportes técnicos emitidos a nivel nacional, no se identifican

investigaciones en Costa Rica que apliquen de forma explícita un modelo formal de gestión de riesgos basado en ISO 31000 a redes Wi-Fi públicas en centros comerciales.

En particular, no se han encontrado estudios que aborden la elaboración, validación y aplicación de un modelo de mitigación de riesgos orientado al uso seguro de redes Wi-Fi en centros comerciales de la zona Pacífico Norte, considerando de manera integrada el contexto tecnológico, organizacional, normativo y las percepciones de los usuarios. Este vacío evidencia la oportunidad y pertinencia de la presente investigación, cuyo propósito es desarrollar un modelo contextualizado que responda a las necesidades del Mall Centro Plaza Liberia y que, al mismo tiempo, pueda servir como referencia metodológica para otros centros comerciales y entornos similares en la región.

2.3 Fundamentación teórica

2.3.1 Norma ISO 31000: Gestión de Riesgos

La ISO 31000 es un estándar internacional que establece principios y directrices para gestionar riesgos en organizaciones de cualquier sector. Define el riesgo como el efecto de la incertidumbre sobre los objetivos y propone un proceso sistemático que incluye la identificación, análisis, evaluación, tratamiento, monitoreo y comunicación del riesgo (International Organization for Standardization, 2018). Este enfoque permite que las decisiones se adopten con base en una comprensión explícita de las exposiciones y oportunidades, en lugar de depender únicamente de la intuición o de respuestas reactivas ante incidentes ya ocurridos.

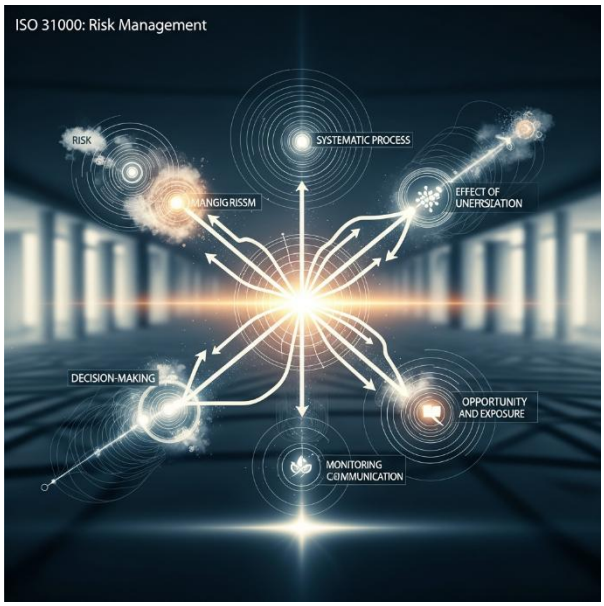
Además del proceso, la ISO 31000 plantea una serie de principios que orientan la gestión del riesgo, tales como su integración en todos los procesos organizacionales, su carácter estructurado y exhaustivo, la adaptación al contexto, la inclusividad de los actores, la naturaleza dinámica y basada en la mejor información disponible, así como la

consideración de factores humanos y culturales. Estos principios son especialmente relevantes en entornos tecnológicos como las redes Wi-Fi públicas, donde convergen distintos actores (administración del centro comercial, personal técnico, comercios y usuarios) con percepciones y responsabilidades diversas frente al riesgo.

La norma también distingue entre el marco de referencia de gestión del riesgo (risk management framework) y el proceso de gestión del riesgo. El primero se relaciona con los elementos organizacionales necesarios para que la gestión del riesgo sea sostenible en el tiempo (políticas, roles, recursos, comunicación interna), mientras que el segundo se centra en las etapas operativas de identificación, análisis, evaluación y tratamiento. Esta distinción resulta clave para el presente trabajo, ya que el modelo de mitigación propuesto no solo pretende describir pasos técnicos, sino también ofrecer lineamientos para que el centro comercial incorpore la gestión de riesgos en su cultura y estructura de gobierno de TI.

Figura 2

Norma ISO 31000: Gestión de Riesgos



Nota. Elaboración propia

En el contexto de las redes Wi-Fi públicas en centros comerciales de la zona Pacífico Norte, la ISO 31000 proporciona un marco flexible que puede adaptarse a las particularidades tecnológicas y normativas de Costa Rica. Al establecer el contexto, es posible delimitar el alcance de la red (zonas de cobertura, servicios ofrecidos, tipos de usuarios), definir criterios de riesgo acordes con las obligaciones regulatorias y las expectativas de los visitantes, y seleccionar estrategias de tratamiento acordes con las capacidades técnicas y organizacionales del Mall Centro Plaza Liberia. De esta manera, la norma se convierte en un eje articulador entre la ciberseguridad operativa y la gestión estratégica del riesgo.

2.3.2 Ciberseguridad en redes Wi-Fi públicas

La ciberseguridad en redes Wi-Fi públicas constituye un área crítica debido a las vulnerabilidades inherentes a su diseño y operación. Según la literatura especializada, estas redes son especialmente susceptibles a ataques de interceptación, suplantación de puntos de acceso, análisis pasivo de tráfico y diversas modalidades de intrusión que permiten a los atacantes capturar credenciales, manipular datos o instalar software malicioso en los dispositivos de los usuarios (Grimes, 2017; Conti et al., 2016). En muchos casos, la facilidad de conexión y la ausencia de barreras visibles generan una falsa sensación de seguridad entre quienes utilizan el servicio.

La complejidad aumenta en entornos con usuarios heterogéneos, como los centros comerciales, donde la alfabetización digital y la experiencia previa en seguridad informática varían ampliamente. En tales escenarios, los riesgos no solo dependen de la infraestructura técnica, tipo de cifrado, configuración de los puntos de acceso, segmentación de redes, sino también de factores humanos y organizacionales: políticas internas, procedimientos de respuesta a incidentes, canales de comunicación con los

usuarios y cultura de seguridad de la organización. La investigación ha demostrado que la percepción de seguridad de los usuarios influye significativamente en su comportamiento, condicionando decisiones como conectarse a cualquier red disponible, reutilizar contraseñas o acceder a servicios sensibles desde redes abiertas (UIT, 2021).

Por ello, las medidas de seguridad técnicas (como el uso de protocolos robustos de cifrado y autenticación, la segmentación de redes o la implementación de sistemas de detección de intrusos inalámbricos) deben complementarse con prácticas educativas y estrategias de comunicación dirigidas a los usuarios para lograr una mitigación efectiva. Campañas informativas, avisos visibles sobre el uso seguro del Wi-Fi y la promoción de hábitos básicos de protección (por ejemplo, evitar el acceso a banca en línea en redes públicas sin medidas adicionales) son componentes esenciales de un enfoque integral de ciberseguridad.

En el contexto específico de centros comerciales de la zona Pacífico Norte, la ciberseguridad en redes Wi-Fi públicas adquiere un matiz adicional: estos espacios funcionan como nodos de actividad económica y social, donde los visitantes realizan compras, interactúan con servicios digitales y consumen contenidos en línea. Un incidente de seguridad no solo compromete datos individuales, sino que puede afectar la reputación del centro comercial, la confianza en sus servicios y, en consecuencia, la fidelidad de los clientes. Esto refuerza la necesidad de gestionar la red inalámbrica no solo como un recurso tecnológico, sino como un activo estratégico vinculado a la experiencia del usuario.

Precisamente, la elaboración de un modelo de mitigación de riesgos basado en ISO 31000 permite articular estas dimensiones técnicas, humanas y organizacionales en un esquema coherente. Al identificar y evaluar los riesgos específicos de la red Wi-Fi pública

del Mall Centro Plaza Liberia, el modelo propone tratamientos que van desde la mejora de configuraciones de seguridad y la definición de un SSID oficial, hasta la implementación de protocolos de respuesta y la planificación de acciones formativas para usuarios y personal. De esta forma, la ciberseguridad en redes Wi-Fi públicas se integra en un sistema de gestión del riesgo más amplio y alineado con estándares internacionales.

2.3.3 Enfoque cualitativo y teoría fundamentada

El enfoque cualitativo permite explorar fenómenos complejos considerando las interpretaciones, experiencias y comportamientos de los participantes (Denzin & Lincoln, 2018). En esta investigación, resulta especialmente pertinente para comprender cómo distintos actores, usuarios, personal técnico, administración del centro comercial, significan la seguridad de la red Wi-Fi pública y cómo estas percepciones influyen en sus prácticas cotidianas. La teoría fundamentada funciona como guía metodológica para construir categorías analíticas emergentes a partir de entrevistas, observación y revisión documental, permitiendo que el modelo propuesto se derive de manera inductiva del contexto real estudiado.

La teoría fundamentada es especialmente útil para comprender cómo usuarios y administradores perciben la seguridad en redes Wi-Fi públicas, identificar patrones de comportamiento y relacionar estos hallazgos con la gestión del riesgo propuesta por ISO 31000 (Corbin & Strauss, 2015). Mediante procesos de codificación abierta, axial y selectiva, es posible organizar la información en categorías que reflejen tanto las vulnerabilidades técnicas como los factores humanos y organizativos que inciden en la seguridad de la red. Estas categorías, a su vez, sirven como puente entre la evidencia empírica y el diseño del modelo de mitigación.

Adicionalmente, el enfoque cualitativo favorece la comprensión del contexto local en toda su complejidad. No se trata únicamente de registrar configuraciones técnicas o listar amenazas, sino de analizar cómo se toman decisiones, qué prioridades se establecen en la gestión del servicio, qué barreras perciben los responsables para implementar controles más robustos y cómo los usuarios valoran la disponibilidad frente a la seguridad. Este tipo de comprensión contextual resulta difícil de capturar mediante enfoques exclusivamente cuantitativos y es fundamental para adaptar la ISO 31000 a un caso concreto como el del Mall Centro Plaza Liberia.

Por último, la teoría fundamentada contribuye a asegurar que el modelo resultante tenga relevancia práctica y coherencia interna, al construirse desde los datos y no imponerse de forma puramente teórica. La constante comparación entre casos, la búsqueda de saturación teórica y la reflexión sistemática sobre las categorías emergentes permiten afinar las etapas y componentes del modelo de mitigación de riesgos, de modo que respondan efectivamente a las necesidades del centro comercial y puedan, al mismo tiempo, servir como referencia para otros centros comerciales de la zona Pacífico Norte. De este modo, el enfoque cualitativo y la teoría fundamentada se integran como soportes metodológicos esenciales de la propuesta.

2.4 Definición y operacionalización de categorías clave

2.4.1 Gestión de Riesgos

La gestión de riesgos es un proceso continuo y sistemático que permite a una organización identificar, evaluar, y mitigar los riesgos que puedan afectar el logro de sus objetivos. Según la ISO 31000 (2018), este proceso incluye diversas etapas, como la identificación de los riesgos, el análisis de su impacto y probabilidad, y la implementación de medidas para reducirlos. En el contexto de la gestión de redes Wi-Fi públicas, la ISO

31000 establece un enfoque estructurado para abordar los riesgos asociados a la seguridad de la red, garantizando la confidencialidad, integridad y disponibilidad de los datos transmitidos a través de estas redes (International Organization for Standardization, 2018).

De acuerdo con Aven (2015), la gestión de riesgos debe ser entendida no solo como la aplicación de estrategias para mitigar riesgos ya conocidos, sino como un proceso dinámico que se adapta a la evolución de los riesgos, así como a los cambios en el entorno organizacional y tecnológico. En el caso de las redes Wi-Fi públicas, la identificación de amenazas potenciales (como la suplantación de puntos de acceso o el "man-in-the-middle") y la evaluación de su impacto, se vuelven cruciales para el diseño de estrategias de mitigación efectivas (Conti, Dragoni, & Lesyk, 2016).

En este estudio, la gestión de riesgos se opera de acuerdo con las directrices establecidas por la ISO 31000 (2018) y está orientada a comprender cómo se reconocen los riesgos asociados al uso de la red Wi-Fi pública en el Mall Centro Plaza Liberia. Este proceso busca evaluar las vulnerabilidades y las amenazas específicas que pueden comprometer la seguridad de los usuarios y la infraestructura tecnológica del centro comercial. El modelo de mitigación de riesgos debe proporcionar un enfoque integral que contemple tanto los riesgos técnicos como los humanos, así como las necesidades específicas del entorno comercial.

Operacionalización de la categoría "Gestión de Riesgos": Para abordar la gestión de riesgos en el contexto de las redes Wi-Fi públicas, se adoptará un enfoque cualitativo. Esto implica realizar entrevistas y grupos focales con los administradores de la red y con los usuarios para identificar las amenazas percibidas, las vulnerabilidades, y las prácticas de mitigación que ya se encuentran en práctica en el Mall Centro Plaza Liberia. Además, se

utilizarán herramientas de evaluación del riesgo como matrices de impacto y probabilidad para priorizar las amenazas y definir un plan de tratamiento de riesgos.

Figura 3

Gestión de Riesgos

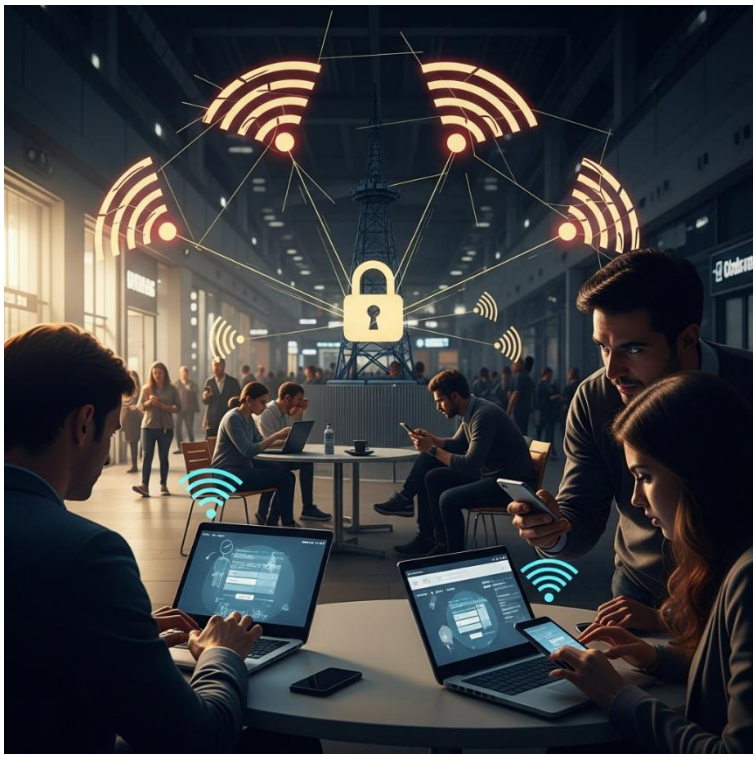
Nota. Elaboración propia

2.4.2 Redes Wi-Fi Públicas

Las redes Wi-Fi públicas representan un escenario altamente vulnerable debido a su naturaleza abierta. Estas redes permiten el acceso de una gran cantidad de usuarios, quienes frecuentemente desconocen los riesgos asociados al uso de redes no seguras (Scarfone & Souppaya, 2010). Según Scarfone y Souppaya (2010), las redes Wi-Fi públicas carecen de las medidas de seguridad robustas presentes en redes privadas, como el uso de cifrados avanzados y autenticación fuerte. Como consecuencia, son susceptibles a diversos tipos de ataques cibernéticos, tales como la interceptación de datos y la suplantación de puntos de acceso.

Figura 4

Redes Wi-Fi Públicas



Nota. Elaboración propia

El concepto de redes Wi-Fi públicas en este estudio se refiere a aquellas redes de acceso inalámbrico que están disponibles para el uso gratuito o por suscripción en lugares públicos, como centros comerciales, aeropuertos y hoteles. Según Conti, Dragoni y Lesyk (2016), estas redes representan un entorno de alto riesgo, ya que permiten la conexión de múltiples dispositivos sin las salvaguardias adecuadas. Las amenazas más comunes en redes Wi-Fi públicas incluyen el secuestro de sesiones, la suplantación de identidad (Evil Twin) y el espionaje del tráfico de datos (Man-in-the-Middle) (Conti et al., 2016).

Operacionalización de la categoría "Redes Wi-Fi Públicas": Para operacionalizar esta categoría en el estudio, se realizará un análisis técnico de las redes Wi-Fi en el Mall Centro Plaza Liberia. Este análisis incluirá la identificación de las configuraciones de seguridad existentes, como los protocolos de cifrado (WPA2, WPA3) y la segmentación de

redes. Además, se analizarán las políticas de acceso y las prácticas de seguridad que se comunican a los usuarios, con el fin de evaluar su efectividad en la prevención de amenazas.

2.4.3 Percepción de Seguridad

La percepción de seguridad es un factor crucial en la gestión de riesgos de redes Wi-Fi públicas, ya que influye directamente en el comportamiento de los usuarios. Según Grimes (2017), la percepción de seguridad de los usuarios no siempre coincide con la realidad de los riesgos técnicos presentes, lo que puede llevarlos a tomar decisiones imprudentes, como conectarse a redes inseguras o no tomar medidas preventivas para proteger su información personal. En el contexto de redes Wi-Fi públicas, esta percepción se ve fuertemente influenciada por la confianza que los usuarios depositan en el proveedor del servicio y la falta de educación en ciberseguridad (Grimes, 2017).

Figura 5

Percepción de Seguridad

Nota. Elaboración propia

En el Mall Centro Plaza Liberia, se espera que los usuarios confíen en la red Wi-Fi disponible, especialmente cuando es ofrecida por un establecimiento reconocido, lo que puede llevarlos a subestimar los riesgos asociados a su uso. La percepción de seguridad no solo abarca la confianza en la red, sino también la disposición de los usuarios para adoptar prácticas de seguridad, como el uso de conexiones cifradas o la evitación de realizar transacciones sensibles en redes públicas (Conti et al., 2016).

Operacionalización de la categoría "Percepción de Seguridad": La percepción de seguridad será evaluada mediante entrevistas y grupos focales con usuarios del Mall Centro Plaza Liberia. Las preguntas estarán diseñadas para identificar cómo los usuarios perciben la confiabilidad de la red Wi-Fi pública y qué medidas de seguridad consideran necesarias. Además, se utilizarán encuestas para evaluar el nivel de conocimiento sobre los riesgos de seguridad en redes Wi-Fi públicas.

2.4.4 Modelo de Mitigación

El modelo de mitigación de riesgos es un conjunto de estrategias y procedimientos diseñados para reducir la probabilidad e impacto de los riesgos identificados. Según Aven (2015), este modelo debe ser dinámico y flexible, permitiendo su adaptación a nuevas amenazas y cambios en el entorno. El modelo propuesto en este estudio se basa en el enfoque estructurado de la ISO 31000, que proporciona una metodología clara para la identificación, evaluación, y tratamiento de riesgos, a través de un proceso continuo de revisión y mejora (International Organization for Standardization, 2018).

El modelo de mitigación de riesgos se diseñará para abordar específicamente las vulnerabilidades técnicas y organizacionales de las redes Wi-Fi públicas en el Mall Centro Plaza Liberia. Esto incluirá estrategias como la implementación de autenticación robusta, el cifrado de datos y la segmentación de la red, así como la educación de los usuarios sobre

buenas prácticas de seguridad. Además, se establecerán procedimientos de monitoreo y revisión continua para evaluar la efectividad del modelo y adaptarlo a nuevas amenazas (Aven, 2015).

Operacionalización de la categoría "Modelo de Mitigación de Riesgos": El modelo será desarrollado en base a los principios de ISO 31000 (2018), integrando tanto medidas técnicas como organizacionales. La validación del modelo se llevará a cabo mediante la revisión por expertos en redes Wi-Fi y gestión de riesgos, quienes proporcionarán retroalimentación sobre la aplicabilidad y efectividad del enfoque propuesto.

Figura 6

Modelo de mitigación

Nota. Elaboración propia

2.5 Contextualización nacional y local

2.5.1 Marco legal costarricense

En Costa Rica, el marco normativo relacionado con la protección de datos personales y la ciberseguridad es un componente fundamental para garantizar la seguridad en entornos como las redes Wi-Fi públicas. La Ley 8968, conocida como la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales, establece las condiciones bajo las cuales los responsables de redes públicas deben garantizar la confidencialidad, integridad y disponibilidad de la información personal de los usuarios (PRODHAB, 2015). Esta legislación refuerza la obligación de las entidades que ofrecen servicios de conectividad, como los centros comerciales, de implementar medidas de seguridad adecuadas para proteger los datos personales de los usuarios de las redes Wi-Fi públicas.

La Ley 8279 sobre ciberseguridad, también conocida como la Ley General de Ciberseguridad, promueve la creación de políticas y marcos de gestión del riesgo en infraestructuras críticas y servicios digitales, incluyendo redes públicas (Gobierno de Costa Rica, 2020). Esta ley es fundamental, ya que establece principios para la protección de la infraestructura tecnológica, la seguridad de la información y la cooperación interinstitucional en la prevención de delitos informáticos.

Aunque estas leyes son un avance significativo, su aplicación en redes Wi-Fi públicas aún no es completamente explícita, lo que deja espacio para la implementación de estándares internacionales como ISO 31000 para la gestión de riesgos, adaptados a los desafíos específicos de los servicios de conectividad en espacios comerciales.

2.5.2 Zona Pacífico Norte: características tecnológicas y sociales

La región Pacífico Norte de Costa Rica ha experimentado un notable crecimiento en términos de infraestructura tecnológica, especialmente en áreas relacionadas con el acceso a Internet y la conectividad inalámbrica. Este crecimiento ha sido impulsado por el

aumento de la actividad comercial, turística y residencial, que ha llevado a una mayor demanda de servicios de conectividad, incluyendo las redes Wi-Fi públicas en lugares como centros comerciales, hoteles y restaurantes.

A pesar de estos avances, la región enfrenta ciertos desafíos en términos de seguridad cibernética. La infraestructura tecnológica en la zona es heterogénea, lo que significa que las redes de los diferentes proveedores pueden variar en términos de calidad y nivel de protección. Algunos centros comerciales han comenzado a ofrecer acceso Wi-Fi gratuito para atraer clientes, pero no siempre se implementan prácticas de seguridad adecuadas o no se percibe una educación digital integral para los usuarios, lo que incrementa la vulnerabilidad a ataques (MICITT, 2022).

En este contexto, el Mall Centro Plaza Liberia se presenta como un espacio representativo de las dinámicas comerciales de la zona, en el que la afluencia constante de personas de diversas partes del país y el extranjero genera una compleja interacción entre usuarios y la infraestructura de red. Este centro comercial, como muchos otros en la región, no solo es un punto de intercambio económico, sino también un espacio socialmente diverso, con visitantes que varían en sus niveles de conocimiento tecnológico y en su comprensión de los riesgos asociados con el uso de redes Wi-Fi públicas (SUTEL, 2021).

Operacionalización de la categoría "Zona Pacífico Norte": Para contextualizar esta categoría, se realizará un análisis detallado de las características socioeconómicas de la región, identificando las tendencias de conectividad, los servicios ofrecidos y los principales actores involucrados en la infraestructura de redes Wi-Fi. Este análisis incluirá datos sobre el acceso a la tecnología, la prevalencia de redes públicas y los factores sociales que afectan la percepción de seguridad de los usuarios. La información obtenida

ayudará a adaptar el modelo de mitigación de riesgos propuesto a las condiciones específicas del Mall Centro Plaza Liberia y otros centros comerciales de la región.

2.5.3 Mall Centro Plaza Liberia: descripción y relevancia

El Mall Centro Plaza Liberia, ubicado en la región Pacífico Norte de Costa Rica, es uno de los principales centros comerciales de la zona. Su ubicación estratégica, cercana a puntos turísticos importantes y rodeada de una creciente actividad comercial, lo convierte en un lugar de alta afluencia, tanto para residentes como para turistas. Este centro comercial ha comenzado a ofrecer servicios de Wi-Fi público como una ventaja competitiva, mejorando la experiencia de los visitantes y atrayendo a más clientes.

Sin embargo, la seguridad de la red Wi-Fi pública en el Mall Centro Plaza Liberia aún presenta vacíos significativos en su gestión de riesgos. A pesar de las medidas básicas de protección, como el cifrado WPA2 en algunas redes, no existe un modelo formal de gestión de riesgos que permita identificar y mitigar de manera efectiva las amenazas que podrían afectar la privacidad de los usuarios y la integridad de los datos que circulan por la red (SUTEL, 2021). Esta deficiencia es crítica, especialmente en un entorno comercial donde las expectativas de los consumidores en cuanto a seguridad son cada vez mayores.

Operacionalización de la categoría "Mall Centro Plaza Liberia": En esta categoría, se realizará un análisis detallado de la infraestructura de red del Mall Centro Plaza Liberia, observando las configuraciones de seguridad actuales y evaluando los riesgos asociados a la falta de un modelo formal de gestión. Además, se examinarán las políticas internas del centro comercial respecto al acceso público a Internet, así como la percepción de los usuarios sobre la seguridad de la red Wi-Fi. La información recopilada permitirá diseñar un modelo de mitigación de riesgos adaptado a las condiciones locales.

La selección de este entorno como caso de estudio permite contextualizar de manera precisa la aplicación de ISO 31000 y orienta el desarrollo de un modelo de mitigación funcional y aplicable a otros espacios comerciales con condiciones similares.

2.6 Relación entre categorías y modelo conceptual

La relación entre las categorías definidas en este estudio y el modelo conceptual propuesto es clave para comprender cómo los elementos teóricos y empíricos se interrelacionan para abordar los riesgos de seguridad en las redes Wi-Fi públicas. El modelo conceptual está fundamentado en la gestión de riesgos según ISO 31000 (2018) y tiene como objetivo proporcionar una visión integral de la seguridad de las redes inalámbricas públicas. Este modelo se articula a partir de las categorías de gestión de riesgos, redes Wi-Fi públicas, percepción de seguridad y modelo de mitigación de riesgos, permitiendo una comprensión holística de la problemática y facilitando el diseño de estrategias efectivas para mitigar los riesgos identificados.

Además, la interacción entre estas categorías permite enlazar de forma lógica el diagnóstico del contexto, la identificación de vulnerabilidades técnicas y humanas, y la formulación de respuestas organizacionales. Así, la gestión de riesgos opera como eje articulador; las redes Wi-Fi públicas representan el escenario donde el riesgo se materializa; la percepción de seguridad refleja cómo ese riesgo es interpretado por los usuarios; y el modelo de mitigación integra los aprendizajes para proponer acciones concretas. Esta estructura refuerza la coherencia interna del trabajo y garantiza que el modelo conceptual no sea una construcción abstracta, sino el resultado de un proceso de integración entre teoría, evidencia empírica y necesidades específicas del Mall Centro Plaza Liberia y de centros comerciales de la zona Pacífico Norte.

2.6.1 Gestión de Riesgos

La gestión de riesgos constituye el eje central del modelo conceptual. Según la ISO 31000 (2018), la gestión de riesgos debe involucrar un proceso iterativo que contemple la identificación, análisis, evaluación y tratamiento de los riesgos. Esta categoría organiza el proceso de intervención y guía las decisiones sobre cómo abordar las amenazas específicas en el contexto de las redes Wi-Fi públicas del Mall Centro Plaza Liberia. De acuerdo con Aven (2015), la gestión de riesgos debe ser flexible y adaptable a medida que surgen nuevas amenazas y cambios en el entorno, lo que implica que el modelo propuesto no debe ser estático, sino que debe incluir mecanismos de retroalimentación continua.

En el modelo conceptual planteado, la categoría de gestión de riesgos también cumple la función de vincular los requisitos normativos, las capacidades técnicas disponibles y las expectativas de los usuarios. A través de ella se definen los criterios de riesgo (por ejemplo, en términos de impacto sobre confidencialidad, integridad y disponibilidad), se establecen prioridades de tratamiento y se delimitan responsabilidades dentro de la organización. De esta forma, la gestión de riesgos no se reduce a un ejercicio puntual de evaluación, sino que se configura como un proceso de gobernanza que orienta la toma de decisiones en el centro comercial respecto a la operación y mejora continua de su red Wi-Fi pública.

2.6.2 Redes Wi-Fi Públicas

La categoría de redes Wi-Fi públicas define el entorno donde se manifiestan los riesgos. Estas redes son inherentemente vulnerables debido a su naturaleza abierta y a la diversidad de usuarios y dispositivos conectados. Según Scarfone y Souppaya (2010), estas redes presentan una exposición significativa a ataques de ciberseguridad, especialmente en lugares de alta afluencia como los centros comerciales. Por lo tanto, la categoría de redes Wi-Fi públicas está directamente vinculada con la identificación de vulnerabilidades en el

entorno del Mall Centro Plaza Liberia, permitiendo que el modelo conceptual contemple medidas para reforzar la seguridad técnica de la red, como el cifrado de datos y la autenticación robusta.

Complementariamente, esta categoría permite incorporar al modelo conceptual aspectos operativos y de diseño de la infraestructura inalámbrica, tales como la segmentación de redes, la delimitación de zonas de cobertura, la definición de un SSID oficial y las políticas de acceso para visitantes y comercios. De este modo, la red Wi-Fi pública no se concibe solo como un soporte tecnológico neutro, sino como un sistema socio-técnico cuya configuración incide directamente en el nivel de riesgo. Al integrar estas variables en el modelo conceptual, se facilita la formulación de recomendaciones específicas y realistas para el Mall Centro Plaza Liberia y otros centros comerciales de la zona Pacífico Norte.

2.6.3 Percepción de Seguridad

La percepción de seguridad de los usuarios influye significativamente en su comportamiento y decisiones sobre el uso de las redes Wi-Fi públicas. Grimes (2017) señala que la confianza de los usuarios en la red, y su disposición a tomar medidas preventivas, están estrechamente relacionadas con su percepción de seguridad. Esta categoría se integra en el modelo conceptual para asegurarse de que, además de las medidas técnicas, se incorporen estrategias educativas y comunicativas que modifiquen la percepción de seguridad de los usuarios, fomentando hábitos más responsables en el uso de redes públicas.

En este sentido, la percepción de seguridad actúa como un puente entre la gestión de riesgos y la conducta efectiva de los usuarios. Un modelo técnicamente sólido puede verse debilitado si los usuarios continúan conectándose a redes no oficiales, reutilizando

contraseñas o accediendo a servicios sensibles sin precauciones. Por ello, el modelo conceptual incorpora esta categoría para justificar la inclusión de campañas de sensibilización, mensajes claros en el portal de acceso, señalización visible del SSID oficial y otras acciones que contribuyan a alinear la percepción de seguridad con el riesgo real. De esta manera, se refuerza el componente humano del modelo de mitigación y se mejora la probabilidad de que las medidas propuestas tengan impacto en la práctica.

2.6.4 Modelo de Mitigación de Riesgos

El modelo de mitigación de riesgos actúa como el producto final del proceso de gestión de riesgos. Este modelo debe ser flexible y debe contemplar tanto medidas técnicas como organizacionales, siguiendo las directrices de ISO 31000 (2018). La relación entre las categorías anteriores permite la construcción de un modelo adaptado a las características del Mall Centro Plaza Liberia, y que pueda ser implementado en otros contextos similares. El modelo propuesto no solo responde a las vulnerabilidades técnicas, sino también a las necesidades operativas y a las percepciones de los usuarios, lo que lo convierte en una solución integral y viable.

Así, el modelo de mitigación sintetiza los aportes de la gestión de riesgos (proceso), de las redes Wi-Fi públicas (escenario), y de la percepción de seguridad (dimensión humana) en un conjunto de etapas y acciones concretas. Entre ellas se incluyen la definición del contexto, la elaboración de un registro de riesgos, la priorización de amenazas, la selección de tratamientos y el monitoreo de resultados. Al integrarse en el modelo conceptual, esta categoría asegura que el resultado de la investigación no se limite a un diagnóstico descriptivo, sino que se materialice en una propuesta operativa que el centro comercial pueda adoptar, evaluar y mejorar con el tiempo.

2.7 Síntesis y conclusión del marco teórico

El marco teórico desarrollado en este estudio proporciona una base sólida para comprender los factores que influyen en la gestión de riesgos de redes Wi-Fi públicas, especialmente en centros comerciales como el Mall Centro Plaza Liberia. A través de la revisión de la literatura, se han identificado las principales vulnerabilidades de las redes Wi-Fi públicas, como la falta de cifrado robusto, la suplantación de puntos de acceso y los ataques de intermediarios, que representan riesgos significativos para la seguridad de los usuarios (Conti et al., 2016; Scarfone & Souppaya, 2010).

La ISO 31000 (2018) ha sido utilizada como el marco central para la gestión de riesgos, proporcionando una metodología estructurada para abordar las amenazas en las redes Wi-Fi públicas. Este enfoque permite no solo la identificación y evaluación de los riesgos, sino también la implementación de medidas de mitigación que integran tanto soluciones técnicas como organizacionales. Aven (2015) destaca que la gestión de riesgos debe ser un proceso continuo y adaptativo, lo que refuerza la necesidad de un modelo dinámico que se ajuste a los cambios en el entorno y a la evolución de las amenazas. En ese sentido, la propuesta de un modelo de mitigación basado en ISO 31000 responde a la necesidad de dotar al Mall Centro Plaza Liberia de una herramienta que trascienda acciones aisladas y se consolide como un sistema de gestión.

En cuanto a la percepción de seguridad, se ha demostrado que este factor influye en gran medida en el comportamiento de los usuarios, quienes, a menudo, subestiman los riesgos asociados al uso de redes Wi-Fi públicas (Grimes, 2017). Este hallazgo subraya la importancia de incorporar estrategias educativas que ayuden a modificar las actitudes y comportamientos de los usuarios, promoviendo un uso más responsable y seguro de las redes. Al integrar esta dimensión en el marco teórico, se reconoce que la seguridad no

depende únicamente de configuraciones técnicas, sino también de la forma en que los usuarios comprenden y gestionan su propia exposición al riesgo.

El estudio también ha evidenciado que la falta de un modelo formal de gestión de riesgos en el Mall Centro Plaza Liberia es una de las principales deficiencias en la seguridad de su red Wi-Fi pública. La implementación de un modelo de mitigación basado en ISO 31000 es esencial para reducir la exposición a los riesgos, mejorar la seguridad de los usuarios y aumentar la confianza en el servicio ofrecido. Esta carencia de modelos formalizados se conecta con el vacío identificado en la literatura nacional, reforzando la pertinencia académica y práctica de la investigación.

En conclusión, este marco teórico ha permitido establecer una comprensión integral de los riesgos asociados a las redes Wi-Fi públicas y la necesidad de un enfoque estructurado y adaptativo para su gestión. La combinación de los principios de la ISO 31000, el análisis de vulnerabilidades técnicas y la atención a la percepción de seguridad de los usuarios proporciona las bases para el desarrollo de un modelo de mitigación de riesgos efectivo y viable. A partir de esta fundamentación, el trabajo empírico buscará transformar dichos aportes teóricos en un modelo contextualizado para centros comerciales de la zona Pacífico Norte, con especial énfasis en el caso del Mall Centro Plaza Liberia.

CAPITULO III. MARCO METODOLÓGICO

3.1 Tipo, nivel, enfoque y diseño de investigación

3.1.1. Tipo de investigación

La investigación de tipo teórica o básica se orienta principalmente a generar y profundizar conocimientos, conceptos y marcos explicativos sin perseguir de manera inmediata la solución de un problema práctico concreto. Su finalidad es ampliar el cuerpo teórico de una disciplina, construir o refinar modelos y aportar principios generales que permitan comprender mejor la realidad, más que intervenir directamente sobre ella (Bernal, 2010). En este tipo de estudios, el énfasis está en el desarrollo conceptual y metodológico, así como en la sistematización de saberes existentes para proponer nuevas interpretaciones o estructuras teóricas.

En cambio, la investigación de tipo aplicada utiliza los conocimientos y teorías ya existentes para abordar problemas específicos de la realidad, con el propósito de diseñar soluciones, métodos, procedimientos o tecnologías que puedan implementarse en contextos concretos. Su valor se mide, sobre todo, por la utilidad práctica de sus resultados y por su capacidad de mejorar situaciones reales en organizaciones, sectores o comunidades, a través de propuestas directamente operativas o intervenciones evaluables (Cerda, 2011). En este enfoque, el componente teórico sigue siendo importante, pero se subordina al objetivo de transformar o resolver un problema delimitado.

En el caso del presente trabajo, se adopta la investigación de tipo teórica o básica, porque el objetivo principal es elaborar un modelo conceptual de mitigación de riesgos sustentado en la norma ISO 31000 y en la revisión de la literatura sobre gestión de riesgos y seguridad de la información. Es decir, el estudio se centra en analizar, estructurar y proponer un modelo referencial que aporte al conocimiento sobre cómo gestionar los

riesgos en redes Wi-Fi públicas, más que en implementar y evaluar empíricamente dicho modelo en un centro comercial específico.

3.1.2. Alcance de investigación

La investigación exploratoria se utiliza cuando el tema o problema de estudio ha sido poco abordado o no se cuenta con información suficiente, de modo que su finalidad principal es "preparar el terreno", familiarizar al investigador con el fenómeno, generar primeras ideas y orientar estudios posteriores de mayor profundidad. Hernández-Sampieri et al. (2014) señalan que los estudios exploratorios se efectúan, por lo general, cuando el objetivo es examinar un tema poco estudiado o novedoso, evaluando su pertinencia, posibles enfoques y futuras preguntas de investigación.

La investigación descriptiva se centra en detallar y caracterizar de manera sistemática un fenómeno, grupo o situación tal como se presenta en un momento determinado, sin manipular variables ni establecer relaciones causales. Albán (2020) indica que este tipo de estudios busca describir las características fundamentales de conjuntos homogéneos de fenómenos, utilizando criterios ordenados que permitan establecer su estructura o comportamiento y ofrecer información sistemática y comparable. En otras palabras, su interés principal es responder a la pregunta "cómo es" o "cómo se manifiesta" el objeto de estudio.

La investigación correlacional tiene como propósito examinar el grado de relación que existe entre dos o más variables, mediante procedimientos estadísticos como coeficientes de correlación, sin que ello implique necesariamente una relación de causa-efecto. Bernal (2016), retomando a Salkind, explica que la investigación correlacional busca mostrar o examinar la relación entre variables o resultados de variables, identificando asociaciones positivas o negativas, pero sin afirmar que una variable sea

causa directa de la otra. Su aporte principal es predecir tendencias y comportamientos en función de esas asociaciones.

La investigación explicativa se orienta a responder a la pregunta "¿por qué?" de los fenómenos, intentando ir más allá de la simple descripción o correlación para establecer relaciones de causa-efecto entre variables. Abreu (2012) señala que la investigación explicativa tiene como objetivo fundamental responder por qué ocurren los hechos, probando hipótesis y buscando las causas de los fenómenos mediante diseños que permiten inferir relaciones causales, ya sean experimentales o no experimentales. Este nivel constituye uno de los alcances más profundos, pues pretende explicar los mecanismos que subyacen al comportamiento observado.

En el presente trabajo, el alcance que mejor se ajusta es el descriptivo. La investigación se orienta a caracterizar el contexto de uso de las redes Wi-Fi públicas en centros comerciales, describir los riesgos presentes, los controles existentes y las prácticas de los usuarios y de la administración, para luego, a partir de esa descripción, estructurar un modelo de mitigación de riesgos alineado con ISO 31000. No se pretende medir estadísticamente la relación entre variables, sino más bien ofrecer una visión detallada de la situación actual y de los elementos que deben considerarse en el modelo. Por ello, el estudio se inscribe en la lógica de la investigación descriptiva, tal como la conciben Albán (2020) y otros autores, al centrarse en describir sistemáticamente las características del fenómeno para sustentar una propuesta de mejor.

3.1.3. Enfoque de investigación

En el nivel macro, el objeto de análisis son las condiciones estructurales del entorno económico e institucional que afectan de manera agregada a los sectores productivos y a las empresas. Desde la perspectiva de la competitividad sistémica, el nivel macro incluye

la estabilidad macroeconómica, la política fiscal y monetaria, el sistema financiero, la apertura comercial y el marco regulatorio general que determinan los incentivos y riesgos para la actividad empresarial (Labarca, 2007).

También, el nivel meta se sitúa por encima del macro y se refiere a factores socioculturales e institucionales de largo plazo que configuran la capacidad de una sociedad para sostener estrategias de desarrollo y competitividad. Esser et al. (1996) definen este nivel como el ámbito de los valores compartidos, la cultura política, la cohesión social y la orientación de largo plazo del país, elementos que influyen en la forma en que el Estado, las empresas y la ciudadanía conciben la innovación, el riesgo y la cooperación.

De la misma manera, el nivel meso corresponde al espacio intermedio entre el contexto nacional y la empresa individual, e incluye tanto a los sectores, regiones y cadenas de valor como a las políticas e instituciones de apoyo específicas. Desde el modelo de competitividad sistémica, en este nivel se ubican los programas sectoriales, los centros tecnológicos, las agencias de fomento productivo y las infraestructuras especializadas que buscan complementar y multiplicar los esfuerzos de las firmas (Esser et al., 1996).
Por su parte, el nivel micro se centra en la empresa y en las redes inmediatas en las que

participa, abarcando la gestión interna, los recursos, las capacidades y los procesos que inciden directamente en su desempeño. Ferrer (2005) subraya que la competitividad micro se basa en la interacción y el aprendizaje dentro de la organización, especialmente en la gestión de la innovación, la calidad, la logística y la cooperación con proveedores y clientes. En la misma línea, Ibarra, González y Demuner (2017) muestran que las dimensiones de planeación estratégica, operaciones, sistemas de información y capital humano determinan el nivel de competitividad de las pymes manufactureras, destacando

que la adopción de tecnologías de información y prácticas de gestión modernas es un componente clave del desempeño en este nivel.

En el presente trabajo, el nivel de análisis predominante es el micro. El estudio se orienta a diseñar un modelo de gestión de riesgos aplicable a organizaciones específicas y se concentra en sus procesos internos de seguridad de la información, en la identificación de amenazas, vulnerabilidades y controles, así como en las capacidades técnicas y procedimentales de cada entidad para gestionar el riesgo en redes Wi-Fi públicas. Aunque el trabajo reconoce que las políticas nacionales de ciberseguridad o la cultura digital de la sociedad forman parte de los niveles macro y meta, la unidad de análisis concreta es la organización y sus sistemas, lo que coincide con la definición de competitividad y gestión en el nivel micro como el ámbito donde se toman decisiones operativas y estratégicas sobre tecnologías, procesos y recursos internos

3.1.4. Diseño de investigación

La investigación cualitativa se orienta a comprender en profundidad cómo las personas interpretan su realidad, explorando significados, percepciones y experiencias en su contexto natural. No busca medir variables numéricamente, sino captar la riqueza de los discursos, las prácticas y las interacciones a través de técnicas como entrevistas, grupos focales, observación o análisis documental (Patton, 2015).

La investigación cuantitativa, en cambio, se centra en la medición objetiva de variables y en el análisis estadístico de datos numéricos con el fin de describir tendencias, comparar grupos o comprobar hipótesis. Babbie (2016) señala que este enfoque se apoya en instrumentos estandarizados, muestras definidas y procedimientos estadísticos que permiten evaluar la magnitud de los fenómenos y la relación entre variables.

La investigación de enfoque mixto integra, en un mismo diseño, componentes cualitativos y cuantitativos, de modo que los datos numéricos y narrativos se combinan para ofrecer una comprensión más completa del problema. Johnson, Onwuegbuzie y Turner (2007) definen los métodos mixtos como la clase de investigación en la que el investigador mezcla o integra técnicas, datos y análisis cuantitativos y cualitativos en un solo estudio o en un programa de investigación.

En el presente trabajo se adopta un enfoque mixto, porque el objetivo es tanto describir y medir ciertos aspectos del problema como comprender en profundidad las percepciones y prácticas de los actores involucrados. Por un lado, se recopilan datos cuantitativos mediante encuestas estructuradas a usuarios y personal de los centros comerciales, permitiendo estimar niveles de uso, percepción de riesgo y presencia de controles de seguridad. Por otro lado, se desarrollan técnicas cualitativas para interpretar cómo se gestionan realmente las redes Wi-Fi y qué barreras existen para aplicar la norma ISO 31000.

3.2 Administración y abordaje del proyecto objeto

3.2.1 Descripción de supuestos

Para el desarrollo de esta investigación, se han establecido los siguientes supuestos:

Los usuarios de redes Wi-Fi públicas no están completamente informados sobre los riesgos asociados con su uso, lo que puede llevar a comportamientos imprudentes, como conectarse a redes inseguras o no proteger adecuadamente su información.

Existen vulnerabilidades técnicas y organizacionales en la red Wi-Fi pública del Mall Centro Plaza Liberia que no han sido abordadas adecuadamente por la administración del centro comercial, lo que aumenta la exposición a posibles ataques.

La implementación de un modelo de gestión de riesgos basado en ISO 31000 puede reducir significativamente los riesgos de seguridad asociados con el uso de la red Wi-Fi pública, al proporcionar un enfoque estructurado y sistemático para la identificación, evaluación y mitigación de los riesgos.

3.2.2 Restricciones y riesgos

Entre las principales restricciones de esta investigación se encuentran:

Acceso limitado a datos históricos de incidentes de seguridad en la red Wi-Fi pública del Mall Centro Plaza Liberia, ya que no existe un sistema formal de gestión de riesgos que registre y clasifique los incidentes pasados. Esto limita el análisis cuantitativo de los incidentes de seguridad previos y puede afectar la precisión del diagnóstico de vulnerabilidades.

Variabilidad en el comportamiento de los usuarios frente a las recomendaciones de seguridad. La adopción de buenas prácticas de seguridad por parte de los usuarios puede ser limitada por su nivel de conocimiento y comprensión de los riesgos asociados al uso de redes Wi-Fi públicas.

En las infraestructuras tecnológicas de otros centros comerciales de la región. La implementación del modelo en el Mall Centro Plaza Liberia puede no ser completamente aplicable a otros centros comerciales con características técnicas y organizacionales diferentes.

En cuanto a los riesgos, se destacan:

Resistencia organizacional a adoptar el modelo de mitigación propuesto. Los responsables de la gestión de la red Wi-Fi pueden mostrar resistencia a implementar cambios, especialmente si implican inversiones adicionales en infraestructura o modificaciones operativas.

Evolución rápida de las amenazas de ciberseguridad. Los modelos de mitigación de riesgos podrían quedar obsoletos rápidamente a medida que surgen nuevas técnicas de ataque. Esto resalta la necesidad de un enfoque de gestión de riesgos continuo y adaptativo, que se revise periódicamente.

3.3 Sujetos y fuentes de información

3.3.1 Sujetos de Información

Los sujetos de información de la investigación se organizan en dos grandes grupos. El primero está conformado por los usuarios de las redes Wi-Fi públicas del Mall Centro Plaza Liberia, incluyendo a personas mayores de 18 años que se conectan voluntariamente a la red durante su visita al centro comercial. En este grupo se considerarán diversos perfiles en función de la edad (jóvenes, adultos y adultos mayores), género, nivel educativo, ocupación (estudiantes, trabajadores, comerciantes, entre otros), experiencia en el uso de tecnologías digitales y frecuencia de uso de redes Wi-Fi públicas (usuarios ocasionales, frecuentes e intensivos). Asimismo, se tomará en cuenta el tipo de dispositivo utilizado y el principal propósito de conexión (uso de redes sociales, mensajería instantánea, trabajo o estudio remoto, operaciones bancarias y compras en línea), con el fin de obtener una visión amplia y representativa de las percepciones y prácticas de seguridad digital.

El segundo grupo de sujetos de información está integrado por los responsables de la gestión y seguridad de la red Wi-Fi dentro del centro comercial. En este grupo se incluye al personal técnico encargado de la infraestructura de red (administradores de red, especialistas en soporte TI o representantes del proveedor del servicio de internet) y a los administradores o jefaturas vinculadas con la toma de decisiones sobre políticas de seguridad, experiencia del cliente y servicios digitales del mall. De estos participantes se

registrarán aspectos como el cargo que desempeñan, los años de experiencia en el área, el nivel de formación en ciberseguridad, el grado de conocimiento de la norma ISO 31000 y sus funciones específicas en relación con la operación y el control de la red Wi-Fi pública.

En términos de frecuencia por perfil, se proyecta trabajar, por ejemplo, con 100 participantes en total, de los cuales aproximadamente 90 corresponderán a usuarios de la red Wi-Fi pública, permitiendo analizar distintos perfiles de uso y percepciones de riesgo, mientras que alrededor de 10 pertenecerán al personal vinculado a la gestión de la red, distribuidos entre responsables técnicos y administradores del centro comercial. Esta distribución prioriza la voz de los usuarios finales sin dejar de incorporar la perspectiva técnica y de gestión, necesaria para comprender las decisiones y criterios que sustentan la seguridad de la red Wi-Fi en el Mall Centro Plaza Liberia.

3.3.2 Fuentes de información

Las fuentes primarias son aquellos documentos u objetos que contienen información original, es decir, resultados directos de una investigación, de una observación o de una creación intelectual. Incluyen artículos científicos que reportan estudios empíricos, tesis, actas, encuestas aplicadas por el propio investigador, entrevistas, registros administrativos, bases de datos originales, obras literarias, leyes, entre otros materiales producidos en el momento en que ocurre el fenómeno que se estudia (Hernández-Sampieri & Mendoza, 2018).

Las fuentes secundarias reúnen, organizan, interpretan o sintetizan información procedente de fuentes primarias. En esta categoría se encuentran los artículos de revisión, libros de texto, capítulos de libros que analizan varios estudios, metaanálisis y estados del arte (Booth, Colomb & Williams, 2016).

Por último, las fuentes terciarias son instrumentos de consulta que ayudan a localizar y acceder a fuentes primarias y secundarias; no desarrollan contenidos de investigación en profundidad, sino que cumplen un papel de guía o índice. Dentro de esta categoría se encuentran los catálogos de bibliotecas, bases de datos bibliográficas, enciclopedias generales, directorios de revistas, motores de búsqueda académicos y repertorios temáticos (Badke, 2017).

Entonces, las fuentes de información primarias serán las siguientes:

Entrevistas y grupos focales con usuarios: A través de entrevistas semiestructuradas y grupos focales, se obtendrá información sobre la percepción de seguridad de los usuarios, sus comportamientos al utilizar la red Wi-Fi pública y las medidas de seguridad que adoptan.

Entrevistas con personal técnico y administrativo: Estas entrevistas proporcionarán datos sobre las prácticas actuales de seguridad de la red, las vulnerabilidades conocidas y las políticas de gestión de riesgos existentes.

Las fuentes de información secundarias incluirán:

Informes de seguridad internos del Mall Centro Plaza Liberia, si están disponibles, que podrían proporcionar detalles sobre incidentes pasados.

Literatura académica y profesional sobre la gestión de riesgos en redes Wi-Fi públicas y las mejores prácticas en ciberseguridad.

3.4 Muestreo

3.4.1 Población y muestreo

La población en una investigación se entiende como el conjunto total de unidades de análisis (personas, organizaciones, documentos, eventos, etc.) que comparten una o más características definidas por el investigador y sobre las cuales se pretende emitir

conclusiones. Es decir, la población está formada por todos los elementos que cumplen los criterios de inclusión del estudio, aunque no necesariamente todos sean observados de manera directa (Hernández-Sampieri & Mendoza, 2018).

Entonces, la población de estudio está compuesta por los usuarios que frecuentan el Mall Centro Plaza Liberia y utilizan la red Wi-Fi pública. El tamaño de la muestra se determinará a partir de la disponibilidad y disposición de los participantes para participar en entrevistas y grupos focales.

3.4.2 Tipo de muestreo

El muestreo no probabilístico por conveniencia es una técnica de selección de participantes en la que los sujetos se eligen porque están disponibles, son accesibles o se considera que pueden aportar información relevante, sin que todos los miembros de la población tengan la misma probabilidad conocida de ser incluidos. En este tipo de muestreo, el investigador escoge a los casos que tiene “más a mano” o que resulta más factible contactar, por razones de tiempo, recursos o contexto, por lo que se reconoce que la muestra no será representativa en sentido estadístico, aunque sí puede ser útil para estudios exploratorios, descriptivos o aplicados (Otzen & Manterola, 2017).

Se empleará un muestreo no probabilístico por conveniencia, dado que la selección de los participantes se basará en su disponibilidad y disposición para participar en las entrevistas y grupos focales. Este tipo de muestreo es apropiado para estudios cualitativos en los que no se requiere que la muestra sea representativa de toda la población, sino que se busca obtener perspectivas detalladas sobre el tema de estudio (Creswell, 2014).

3.5 Diseño de técnicas e instrumentos para recolectar información

3.5.1 Detalle de técnica e instrumentos de aplicación

Las principales técnicas de recolección de datos serán:

Entrevistas semiestructuradas: La entrevista semiestructurada es una técnica de recolección de datos cualitativos que se basa en una guía de temas o preguntas previamente elaborada, pero que permite flexibilidad para profundizar, formular preguntas emergentes y adaptar el orden según el curso de la conversación. De esta manera, combina elementos estructurados y abiertos, favoreciendo la obtención de información comparable entre participantes, pero sin perder la riqueza del discurso individual (Kvale & Brinkmann, 2015).

Entonces, se llevarán a cabo entrevistas con los usuarios de la red Wi-Fi y con el personal técnico del centro comercial. Las entrevistas semiestructuradas permitirán explorar en profundidad las experiencias, percepciones y prácticas de seguridad de los participantes.

Grupos focales: Los grupos focales consisten en entrevistas colectivas con un grupo reducido de participantes que comparten ciertas características, convocados para discutir un tema específico bajo la conducción de un moderador. Esta técnica busca explorar percepciones, opiniones y significados que surgen de la interacción grupal, aprovechando el intercambio entre los participantes para profundizar en el fenómeno estudiado (Krueger & Casey, 2015).

Se realizarán grupos focales con los usuarios para obtener información sobre sus preocupaciones y comportamientos comunes al usar redes Wi-Fi públicas, promoviendo la discusión entre los participantes sobre sus experiencias de conectividad y seguridad.

Los instrumentos de recolección incluirán:

Guías de entrevistas: Las guías de entrevistas son instrumentos escritos que organizan los temas, preguntas iniciales y posibles preguntas de sondeo que el entrevistador utilizará durante la entrevista. No constituyen un cuestionario rígido, sino una hoja de ruta que ayuda a asegurar que se aborden los aspectos centrales de la investigación, manteniendo al mismo tiempo la flexibilidad necesaria para seguir las respuestas del entrevistado y explorar cuestiones emergentes (Merriam & Tisdell, 2016).

Estas guías estarán diseñadas para explorar temas específicos relacionados con la seguridad de las redes Wi-Fi públicas, la percepción de los usuarios y las prácticas de gestión de riesgos.

Protocolos de discusión para grupos focales: Los protocolos de discusión para grupos focales son documentos que estructuran el desarrollo de la sesión grupal, incluyendo la secuencia de actividades, las preguntas clave, las reglas de participación, el rol del moderador y los tiempos aproximados. Su finalidad es garantizar que todos los temas relevantes sean tratados, que se mantenga un clima de respeto y participación equilibrada, y que la información obtenida sea coherente con los objetivos de la investigación (Guest, Namey & Mitchell, 2013; Krueger & Casey, 2015).

Se utilizarán para guiar las conversaciones en los grupos focales, asegurando que los temas relevantes sean cubiertos de manera adecuada.

3.5.2 Detalle de la aplicación de técnicas e instrumentos

El trabajo de campo se desarrollará principalmente a través de entrevistas semiestructuradas y grupos focales, aplicados de manera planificada y sistemática. En el caso de las entrevistas, se coordinará previamente una cita con cada participante, explicándole el objetivo del estudio, el carácter voluntario de su participación y las

condiciones de confidencialidad de la información brindada. Las entrevistas se llevarán a cabo en un ambiente privado y tranquilo dentro o en las inmediaciones del centro comercial, para evitar interrupciones y facilitar que la persona se sienta cómoda al compartir sus experiencias sobre el uso de redes Wi-Fi públicas. Cada sesión tendrá una duración aproximada de 30 a 45 minutos y se apoyará en una guía de preguntas, lo que permitirá abordar los temas centrales de la investigación y, al mismo tiempo, profundizar en aspectos relevantes que puedan surgir de manera espontánea durante la conversación.

En cuanto a los grupos focales, se conformarán equipos de entre 5 y 8 participantes que compartan el rasgo de ser usuarios de redes Wi-Fi públicas en centros comerciales, procurando diversidad en edad, experiencia tecnológica y frecuencia de uso. Estas sesiones se desarrollarán en un espacio adecuado para la interacción grupal, donde los participantes puedan verse, escucharse y dialogar con comodidad. El moderador seguirá un protocolo de discusión que incluirá preguntas detonantes, dinámicas breves de presentación y normas de convivencia, con el objetivo de promover un clima de confianza y respeto. La duración estimada de cada grupo focal será de aproximadamente una hora, tiempo durante el cual se recogerán opiniones, percepciones, prácticas habituales y propuestas de mejora relacionadas con la seguridad en el uso de la red Wi-Fi pública.

Tanto en las entrevistas como en los grupos focales, se solicitará autorización para grabar el audio de las sesiones, a fin de asegurar la fidelidad de la información y facilitar su posterior análisis. Una vez finalizada la recolección de datos, se procederá a la transcripción de los registros y a su organización en una matriz de análisis cualitativo. A partir de estas transcripciones se aplicará un enfoque de análisis temático, identificando categorías, subcategorías, patrones de respuesta y temas recurrentes vinculados con riesgos percibidos, prácticas de seguridad, nivel de conocimiento de los usuarios y gestión de la

red por parte del centro comercial. De esta forma, la aplicación de las técnicas e instrumentos permitirá construir un panorama detallado y coherente sobre la seguridad del uso de redes Wi-Fi públicas, que servirá de base para el diseño del modelo de mitigación de riesgos.

3.6 Determinación de variables

3.6.1 Clasificación

a) Variable cualitativa

Una variable cualitativa se define como aquella que expresa atributos, categorías o cualidades que no se representan mediante números, sino a través de nombres o clasificaciones (por ejemplo, tipo de protocolo de seguridad o nivel percibido de seguridad) y que permiten describir características de los sujetos u objetos estudiados (Salkind, 2017).

En este estudio, las variables cualitativas permiten clasificar a los participantes y a la configuración de la red según categorías de seguridad, percepción y comportamiento sin asignarles un valor numérico directo (Martínez-González et al., 2014).

Variables técnicas

Se consideran variables técnicas las que describen características de la infraestructura y configuración de la red Wi-Fi, como el tipo de cifrado utilizado, la presencia de portal cautivo, los protocolos de autenticación y la existencia de políticas formales de seguridad, las cuales se categorizan cualitativamente según su nivel de robustez o implementación.

- **Variables humanas**

Se consideran variables humanas aquellas relacionadas con los usuarios y su interacción con la red, tales como la percepción de seguridad, el nivel de conocimiento sobre riesgos y los patrones de comportamiento (por ejemplo, si realizan operaciones bancarias o compras en línea al conectarse), que se expresan en categorías o niveles de respuesta.

b) Variable cuantitativa

Una variable cuantitativa se entiende como aquella que representa una cantidad o magnitud susceptible de medirse numéricamente, sobre la cual es posible realizar operaciones aritméticas como sumas, promedios o porcentajes (Martínez-González et al., 2014).

En el contexto de esta investigación, las variables cuantitativas permiten medir, por ejemplo, el número de incidentes de seguridad, la cantidad de dispositivos conectados o el tiempo de conexión a la red Wi-Fi pública, facilitando el análisis estadístico descriptivo (Triola, 2018).

Variables cuantitativas discretas

Una variable cuantitativa discreta es aquella que solo puede asumir valores enteros, generalmente resultado de un conteo, como el número de incidentes de seguridad reportados, la cantidad de dispositivos conectados simultáneamente o el número de controles de seguridad implementados (Freund, Perles & Miller, 2014).

En esta investigación, las variables discretas permiten contabilizar eventos o elementos (por ejemplo, incidentes o medidas de seguridad) y facilitan el cálculo de frecuencias y proporciones para describir el nivel de riesgo y protección de la red.

Variables cuantitativas continuas

Una variable cuantitativa continua puede tomar cualquier valor dentro de un intervalo, incluidos decimales, ya que proviene de mediciones como tiempo, intensidad o proporciones (Triola, 2018).

Aplicado al estudio, son variables continuas el tiempo de conexión a la red (en minutos), el ancho de banda promedio utilizado o el porcentaje de uso de la red en determinadas franjas horarias, lo que permite analizar variaciones más finas en el comportamiento de uso y desempeño de la red Wi-Fi.

3.6.2 Definición

Variables técnicas: Factores que incluyen la calidad de la infraestructura de la red Wi-Fi pública, como el cifrado de datos, el uso de protocolos de seguridad, la autenticación de usuarios y la segmentación de la red.

Variables humanas: Factores subjetivos relacionados con la percepción de seguridad de los usuarios, como su conocimiento sobre los riesgos asociados con el uso de redes públicas, su confianza en la red y su cumplimiento con las recomendaciones de seguridad.

3.6.3 Cuadro o matriz de las variables

Tabla 3

Matriz de variables

Objetivo	Variable	Variable conceptual	Variable operacional	Variable instrumental
Analizar el contexto interno y externo del Mall Centro Plaza Liberia para comprender las condiciones tecnológicas, operativas y organizacionales que influyen en la gestión de riesgos de su red Wi-Fi pública.	Diagnóstico del contexto de la red Wi-Fi pública	Proceso sistemático de recopilación y análisis de información tecnológica, organizacional, normativa y de usuarios que describe la situación actual de la red Wi-Fi pública y su entorno de gestión de riesgos.	Elaboración de una matriz de contexto que sintetice infraestructura de red, forma de gestión del servicio, marco normativo aplicable y perfiles de usuarios, a partir de entrevistas, observación y revisión documental.	Matriz de diagnóstico del contexto interno y externo (hoja de cálculo), más fichas de observación y registros de entrevistas en documentos Word/PDF.
Identificar las amenazas, vulnerabilidades y riesgos asociados al uso de la red Wi-Fi pública mediante la recopilación y análisis de información técnica y cualitativa proveniente de especialistas y actores relevantes.	Identificación de amenazas, vulnerabilidades y riesgos	Proceso de reconocimiento sistemático de eventos potenciales, condiciones de vulnerabilidad y escenarios de riesgo que pueden comprometer la confidencialidad, integridad y disponibilidad de la información que circula por la red Wi-Fi pública.	Registro en matrices de identificación de riesgos de las amenazas, vulnerabilidades y activos afectados, clasificándolos según su origen, tipo de impacto y elementos de la infraestructura o de la gestión involucrados.	Matriz de identificación de riesgos (Excel) complementada con transcripciones y resúmenes de entrevistas y grupos focales en documentos Word/PDF.
Evaluar los riesgos identificados considerando su probabilidad, impacto y controles existentes, con el fin de establecer criterios que permitan priorizar su	Evaluación y priorización de riesgos	Proceso de valoración de los riesgos identificados en función de su probabilidad de ocurrencia, el impacto potencial y los controles existentes, con el propósito de determinar su nivel de	Construcción de matrices de evaluación en las que se consignen probabilidad, impacto, controles existentes, nivel de riesgo resultante y prioridad de	Matriz de evaluación y priorización de riesgos (hoja de cálculo o PDF con tablas y, en su caso, mapas de calor).

tratamiento dentro del modelo propuesto.		criticidad y el orden de atención.	tratamiento para cada riesgo.	
Diseñar un modelo de mitigación de riesgos basado en ISO 31000, estructurado en etapas y orientado a mejorar la gestión del servicio de Wi-Fi público del centro comercial.	Modelo de mitigación de riesgos basado en ISO 31000	Propuesta estructurada de etapas, acciones, roles y lineamientos operativos que adapta el ciclo de gestión de riesgos de ISO 31000 al contexto de la red Wi-Fi pública del Mall Centro Plaza Liberia, para reducir la probabilidad e impacto de los riesgos identificados.	Definición y documentación de las etapas del modelo (gobernanza, contexto, identificación y análisis, evaluación, tratamiento, comunicación y monitoreo), con sus actividades, productos esperados, responsables y flujos de trabajo.	Documento digital tipo "manual/propuesta de modelo" (Word/PDF) con diagramas de proceso, cuadros resumen por etapas y anexos técnicos.
Validar la pertinencia y aplicabilidad del modelo propuesto mediante la revisión y retroalimentación de expertos en redes inalámbricas, seguridad informática y gestión de riesgos.	Validación del modelo de mitigación de riesgos	Proceso de valoración del modelo por parte de expertos y actores clave según criterios de claridad, coherencia con ISO 31000, pertinencia para el contexto del mall, factibilidad de implementación e integración de dimensiones técnicas y humanas.	Aplicación de matrices de juicio de expertos, sistematización de sus valoraciones cualitativas y cuantitativas, y registro de los ajustes incorporados al modelo a partir de sus observaciones.	Matrices de juicio de expertos y reporte de validación del modelo (documentos Word/PDF con tablas de evaluación y síntesis de observaciones).

Nota. Elaboración propia

CAPÍTULO IV. ANÁLISIS DE RESULTADOS

4.1. Resultados según objetivos específicos

4.1.1. Resultados del objetivo específico 1

Del análisis del contexto externo se corroboró que el Mall Centro Plaza Liberia se inserta en la región Pacífico Norte de Costa Rica, caracterizada por un crecimiento sostenido de la infraestructura de conectividad y una alta presencia de redes inalámbricas públicas en espacios comerciales y turísticos. Este entorno de expansión tecnológica convive con desafíos en materia de ciberseguridad y heterogeneidad en los niveles de protección entre proveedores, lo que incrementa la exposición a riesgos cuando no se acompaña de prácticas de gestión y educación digital adecuadas.

En el contexto interno, la observación de campo permitió identificar múltiples redes inalámbricas asociadas a distintos locales y servicios del centro comercial. En todas las redes observadas se constató el uso de cifrado WPA2, considerado una fortaleza desde el punto de vista técnico. Sin embargo, no se identificó una red pública oficial claramente señalizada para los visitantes, lo que genera un escenario de fragmentación del servicio y potencial confusión en el momento de elegir a qué red conectarse.

Desde la perspectiva organizacional, las entrevistas con el personal técnico y administrativo evidenciaron que la gestión de la red se orienta principalmente a garantizar disponibilidad y continuidad del servicio para los comercios, mientras que la gestión sistemática del riesgo (alineada a marcos como ISO 31000) aún no está formalmente integrada como proceso transversal. Aunque se reconocen responsabilidades en materia de protección de datos y cumplimiento normativo, estas se operacionalizan de manera más reactiva que preventiva, dependiendo en gran medida de las configuraciones por defecto del equipamiento y de recomendaciones puntuales de proveedores o reguladores.

Finalmente, en términos de perfil y prácticas de los usuarios, se constató que estos asumen que, por estar dentro de un centro comercial formal, las redes disponibles son "confiables" y legítimas, tendiendo a conectarse a aquella que tenga mejor señal o aparezca primero en la lista, sin verificar detalladamente el nombre del SSID ni la legitimidad del emisor.

Esta combinación de contexto externo dinámico, infraestructura interna cifrada pero poco señalizada, y percepción de confianza generalizada configura el marco en el que se deberán gestionar los riesgos de la red Wi-Fi pública.

Tabla 4

Contexto interno y externo relacionado con la gestión de riesgos de la red Wi-Fi pública del Mall Centro Plaza Liberia

Dimensión de análisis	Hallazgos empíricos principales	Implicaciones para la gestión de riesgos
Entorno tecnológico regional (externo)	Crecimiento acelerado de la conectividad y oferta de redes Wi-Fi públicas en espacios comerciales y turísticos.	Mayor presión para ofrecer Wi-Fi como servicio estándar, con riesgo de priorizar la disponibilidad sobre la seguridad integral.
Marco normativo y de políticas (externo)	Existencia de políticas nacionales de ciberseguridad y normativa de protección de datos personales (p. ej., Ley 8968).	Obliga al centro comercial a incorporar criterios de protección de datos y gestión de riesgo en el diseño de su servicio Wi-Fi.
Infraestructura inalámbrica en el mall (interno)	Identificación de múltiples redes internas con cifrado WPA2 y ausencia de redes abiertas visibles.	El nivel de cifrado reduce ciertos riesgos técnicos, pero la multiplicidad de redes puede dificultar el control centralizado.
Señalización y oferta de Wi-Fi (interno)	No se identificó una red pública oficial claramente señalizada para los visitantes.	Aumenta la probabilidad de que usuarios se conecten a redes no oficiales o no previstas por la administración del mall.
Perfil y percepción de usuarios (interno)	Los usuarios asumen que, por estar en un mall, las redes son confiables y revisan poco el nombre del SSID.	Eleva la vulnerabilidad frente a redes maliciosas o mal configuradas en un entorno con múltiples SSIDs visibles.

Organización interna y procesos (interno)	La gestión se centra en la continuidad del servicio; la gestión formal de riesgos no se ha institucionalizado plenamente.	Se requiere evolucionar desde un enfoque reactivo hacia un modelo sistemático de gestión de riesgos alineado con ISO 31000.

Nota. Elaboración propia

4.1.2. Resultados del objetivo específico 2

A partir del análisis de las entrevistas con usuarios y personal técnico, junto con la observación del entorno inalámbrico, se identificó un conjunto de amenazas potenciales asociadas tanto a factores técnicos como humanos y organizacionales. Desde la perspectiva del usuario, emergieron prácticas que incrementan la exposición al riesgo, tales como conectarse a la primera red disponible sin verificar el nombre completo del SSID, asumir que toda red dentro del mall es legítima, y no aplicar medidas básicas como el uso de VPN, la desactivación de conexiones automáticas o la actualización periódica de contraseñas.

En el ámbito técnico, el personal reconoció la posibilidad de ataques como la suplantación de puntos de acceso (evil twin), la captura de tráfico en redes legítimas, el secuestro de sesiones y el acceso no autorizado a equipos conectados, aun cuando no se han registrado incidentes graves visibles durante el periodo de observación.

Además, se señalaron como vulnerabilidades la ausencia de una red pública unificada bajo control directo de la administración del centro comercial, cierta dependencia de las configuraciones por defecto de los equipos de red, y la falta de protocolos formales documentados para la gestión de incidentes.

En el plano organizacional, se identificó que la comunicación hacia usuarios sobre buenas prácticas de uso de Wi-Fi es limitada: no se observaron campañas visibles de sensibilización ni materiales informativos en zonas comunes. Ello refuerza un escenario en el que, aunque la infraestructura utilice cifrado robusto, la combinación de hábitos de los usuarios, ausencia de señalización clara y falta de lineamientos unificados genera un

conjunto de riesgos latentes que pueden materializarse si aparecen actores maliciosos o si se relajan los controles existentes.

Tabla 5

Amenazas, vulnerabilidades y tipo de riesgo asociadas al uso de redes Wi-Fi en el Mall Centro Plaza Liberia

Amenaza principal	Vulnerabilidades asociadas	Tipo de riesgo predominante	Fuente principal de evidencia
Conexión de usuarios a redes no oficiales o no previstas	Ausencia de una red pública oficial señalizada; múltiples SSIDs visibles; baja verificación del nombre de la red.	Humano / organizacional	Observación de campo y entrevistas a usuarios.
Suplantación de puntos de acceso (evil twin)	Confianza excesiva en cualquier red dentro del mall; inexistencia de campañas de alerta sobre este tipo de ataque.	Técnico / humano	Entrevistas con personal técnico.
Captura de tráfico en redes legítimas	Uso de aplicaciones sensibles (banca, correo) en Wi-Fi público sin medidas adicionales (VPN, cifrado de extremo a extremo).	Técnico / humano	Entrevistas con usuarios y personal técnico.
Secuestro de sesiones y robo de credenciales	Sesiones abiertas en redes públicas; reutilización de contraseñas; desconocimiento de buenas prácticas.	Técnico / humano	Entrevistas a usuarios.
Acceso no autorizado a dispositivos conectados	Falta de configuración de firewalls personales en dispositivos; redes invitado no segmentadas adecuadamente.	Técnico	Entrevistas a personal técnico.
Gestión reactiva de incidentes	Ausencia de procedimientos formales documentados para detectar, registrar y responder a incidentes.	Organizacional	Entrevistas a personal técnico y revisión interna.
Incumplimiento de expectativas normativas	Desconexión entre marcos legales de protección de datos y prácticas concretas de sensibilización a usuarios.	Organizacional / legal	Revisión documental y entrevistas con administración.

Nota. Elaboración propia

4.1.3. Resultados del objetivo específico 3

La evaluación de riesgos se realizó mediante una matriz cualitativa que combinó tres criterios: probabilidad de ocurrencia, impacto potencial sobre la confidencialidad, integridad y disponibilidad de la información de los usuarios y del centro comercial, y controles existentes. Se empleó una escala cualitativa de tres niveles (bajo, medio, alto) para cada criterio, a partir del juicio experto del equipo investigador, la evidencia empírica recopilada y la experiencia del personal técnico.

Los resultados muestran que, pese a la ausencia de redes abiertas y de indicios visibles de actividad maliciosa durante la observación de campo, algunos riesgos mantienen una prioridad de tratamiento alta, principalmente aquellos vinculados a la confusión de SSID y a la falta de señalización clara de una red oficial, así como a la posible suplantación de puntos de acceso. Ello se debe a que la probabilidad de que los usuarios se conecten a redes no oficiales es elevada, dada su baja revisión del nombre de la red y la confianza generalizada en el entorno del mall.

Otros riesgos, como la captura de tráfico o el secuestro de sesiones, se ubicaron en un nivel de riesgo medio, pues, aunque el impacto sería alto en caso de materializarse, cuentan con mitigaciones parciales proporcionadas por el uso de cifrado WPA2 en las redes observadas y por las propias medidas de seguridad de ciertas aplicaciones (p. ej., cifrado extremo a extremo en mensajería).

Finalmente, algunos riesgos organizacionales, como el manejo reactivo de incidentes, se ubicaron en un nivel medio con probabilidad moderada, pero con impacto relevante en términos reputacionales y de cumplimiento normativo si se produjera un incidente sin respuesta adecuada.

Tabla 6

Evaluación cualitativa de los riesgos de seguridad en la red Wi-Fi pública

Riesgo evaluado	Probabilidad estimada	Impacto estimado	Controles existentes principales	Nivel de riesgo resultante	Prioridad de tratamiento
Conexión a redes no oficiales o no previstas	Alta	Alto	Cifrado WPA2 en redes internas; ausencia de redes abiertas visibles.	Alto	Alta
Suplantación de puntos de acceso (evil twin)	Media	Alto	Buen nivel de cifrado en redes legítimas; monitoreo básico del personal.	Alto	Alta
Captura de tráfico en redes legítimas	Media	Alto	Cifrado WPA2; aplicaciones con cifrado extremo a extremo.	Medio	Media
Secuestro de sesiones y robo de credenciales	Media	Alto	Políticas de seguridad de aplicaciones; recomendaciones generales.	Medio	Media
Acceso no autorizado a dispositivos conectados	Baja	Alto	Segmentación parcial; configuraciones estándar de routers.	Medio	Media
Gestión reactiva de incidentes de seguridad	Media	Medio	Experiencia empírica del personal; apoyo eventual de proveedores.	Medio	Media
Desalineación con marcos normativos de protección de datos	Baja	Alto	Conocimiento general de la normativa; políticas corporativas generales.	Medio	Media/Baja

Nota. Elaboración propia

4.1.4. Resultados del objetivo específico 4

El modelo de mitigación diseñado se estructura explícitamente a partir del ciclo de gestión de riesgos propuesto por la norma ISO 31000, adaptado al contexto específico del Mall Centro Plaza Liberia y a la naturaleza de los riesgos identificados en su entorno Wi-Fi. El diseño integra cinco grandes etapas: (a) establecimiento del contexto, (b)

identificación y análisis de riesgos, (c) evaluación y priorización, (d) tratamiento del riesgo, y (e) comunicación–consulta y monitoreo–revisión, concebidas como un proceso iterativo y dinámico.

En la etapa de establecimiento del contexto, el modelo propone formalizar la caracterización del entorno tecnológico, organizacional y regulatorio del centro comercial, incorporando de manera explícita las particularidades de la región Pacífico Norte, el marco normativo costarricense y los perfiles de usuarios que frecuentan el mall.
Sobre esta base se estructura la etapa de identificación y análisis de riesgos, en la que se consolidan las amenazas y vulnerabilidades detectadas (tanto técnicas como humanas y organizacionales) a partir de entrevistas, observación y revisión documental.

La etapa de evaluación y priorización articula los criterios de probabilidad, impacto y controles existentes para determinar qué riesgos requieren atención inmediata, cuáles pueden ser tolerados bajo vigilancia y cuáles demandan planes de mejora gradual, siguiendo la lógica ya sintetizada en la matriz de riesgos.

A partir de esta priorización, la etapa de tratamiento del riesgo define acciones concretas para el Mall Centro Plaza Liberia, entre las que destacan: la creación de una red Wi-Fi pública oficial con SSID claramente identificable y señalización visible; el refuerzo de la segmentación de redes; la implementación de procedimientos documentados para la gestión de incidentes; y el despliegue de campañas de sensibilización dirigidas a usuarios.

Finalmente, el modelo incorpora de forma transversal la comunicación y consulta con usuarios, comercios y personal técnico, así como un componente de monitoreo y revisión que contempla la evaluación periódica del funcionamiento de los controles, la actualización de la matriz de riesgos y la incorporación de experiencias derivadas de

incidentes o pruebas piloto, en coherencia con los principios de mejora continua de ISO 31000.

Tabla 7

Etapas del modelo de mitigación de riesgos basado en ISO 31000 para la red Wi-Fi del Mall Centro Plaza Liberia

Etapa del modelo (ISO 31000 adaptada)	Objetivo en el contexto del mall	Actividades principales propuestas	Actores clave involucrados	Productos esperados
Establecimiento del contexto	Delimitar el entorno tecnológico, organizacional y normativo del servicio Wi-Fi.	Mapeo de redes y SSIDs; revisión de políticas internas; análisis de marco legal y lineamientos nacionales de ciberseguridad.	Administración del mall; personal técnico.	Informe de contexto y alcance de la gestión.
Identificación y análisis de riesgos	Reconocer amenazas, vulnerabilidades y escenarios de riesgo relevantes.	Entrevistas y grupos focales; observación de la infraestructura; consolidación de amenazas técnicas, humanas y organizacionales.	Equipo de TI; usuarios clave; investigador.	Registro estructurado de riesgos.
Evaluación y priorización de riesgos	Estimar probabilidad–impacto y jerarquizar riesgos para decidir acciones.	Asignación cualitativa de probabilidad e impacto; análisis de controles existentes; definición de niveles de riesgo y prioridades.	Equipo de TI; administración; asesor externo.	Matriz de evaluación y mapa de prioridades.
Tratamiento del riesgo	Diseñar e implementar medidas técnicas y organizativas para reducir	Creación de SSID público oficial; refuerzo de cifrado y segmentación; protocolos de incidentes; guías	Administración; TI; comercios; proveedor de red.	Plan de tratamiento y procedimientos.

	riesgos priorizados.	de uso seguro para usuarios.		
Comunicación y consulta + monitoreo y revisión	Mantener informados a los actores y asegurar mejora continua del modelo.	Campañas de sensibilización; paneles informativos; revisión periódica de incidentes; actualización anual de la matriz de riesgos.	Administración; TI; comunicaciones ; comercios.	Reportes de seguimiento y ajustes al modelo.

Nota. Elaboración propia

4.1.5. Resultados del objetivo específico 5

La validación del modelo se realizó mediante juicio de expertos, convocando a especialistas en redes inalámbricas, ciberseguridad y gestión de riesgos, así como a un representante de la administración del Mall Centro Plaza Liberia. Estos expertos revisaron la propuesta de modelo, la matriz de riesgos y los procedimientos de implementación, emitiendo valoraciones cualitativas sobre criterios de claridad, coherencia con ISO 31000, pertinencia para el contexto del centro comercial, factibilidad de implementación y contribución a la experiencia de usuario.

En términos generales, los expertos consideraron que el modelo es pertinente y aplicable al contexto del mall, destacando positivamente la traducción de los principios de ISO 31000 a procedimientos concretos (p. ej., creación de un SSID oficial; protocolos de incidentes; campañas de sensibilización). Señalaron como fortalezas la integración de dimensiones técnicas y humanas y la inclusión de un componente explícito de comunicación con los usuarios. No obstante, recomendaron prestar especial atención a dos aspectos: (a) asegurar el compromiso sostenido de la administración del centro comercial para dotar de recursos y tiempo al proceso, y (b) coordinar las acciones con los distintos

comercios que gestionan redes propias para evitar solapamientos o mensajes contradictorios.

Como parte de la validación, se realizó además una prueba piloto limitada de algunas acciones propuestas, centrada en la señalización de la red oficial y la difusión de recomendaciones básicas de seguridad en puntos estratégicos del mall. Los expertos resaltaron que, aunque el alcance de la prueba fue acotado, permitió evidenciar que los usuarios identificaban con mayor facilidad la red legítima, mostraban mayor cautela al conectarse y valoraban positivamente la presencia de información visible sobre seguridad. Estos resultados reforzaron la viabilidad del modelo, a la vez que mostraron la necesidad de consolidar mecanismos de monitoreo y retroalimentación continua una vez que se implemente de forma completa.

Tabla 8

Síntesis de la valoración de expertos sobre el modelo de mitigación de riesgos

Criterio de validación	Valoración cualitativa global	Comentarios y observaciones recurrentes de los expertos
Claridad y estructura del modelo	Alta	El modelo presenta etapas bien definidas y lógica interna consistente, fácil de seguir por el personal.
Coherencia con ISO 31000	Alta	Se reconocen claramente las fases del ciclo de gestión de riesgos y su adaptación al contexto Wi-Fi.
Pertinencia para el contexto del mall	Alta	Responde a problemas identificados en el Mall Centro Plaza Liberia y es adaptable a otros centros.
Factibilidad de implementación	Media-alta	Requiere coordinación con comercios y asignación de recursos, pero se considera viable en fases.
Integración de dimensiones técnica y humana	Alta	Se valora la inclusión de acciones técnicas (cifrado, segmentación) y educativas (campañas a usuarios).
Contribución a la experiencia de usuario	Alta	La señalización del SSID oficial y las recomendaciones visibles aumentan la sensación de confianza.

Potencial de mejora continua	Media-alta	La propuesta de monitoreo y revisión anual es adecuada, pero se sugiere definir indicadores concretos.

Nota. Elaboración propia

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

Objetivo específico 1

En relación con el primer objetivo específico, se concluye que el Mall Centro Plaza Liberia opera en un entorno de alta expansión de la conectividad, con infraestructura interna cifrada pero fragmentada y sin una red pública oficial claramente señalizada, lo que evidencia una gestión de la red centrada en la continuidad del servicio más que en una gestión preventiva y sistemática de los riesgos.

Objetivo específico 2

En relación con el segundo objetivo específico, se concluye que las principales amenazas, vulnerabilidades y riesgos asociados al uso de la red Wi-Fi pública responden a una combinación de factores técnicos (posible suplantación de puntos de acceso, captura de tráfico, secuestro de sesiones) y humanos–organizacionales (confusión de SSID, confianza excesiva del usuario y ausencia de campañas de sensibilización).

Objetivo específico 3

En relación con el tercer objetivo específico, se concluye que la evaluación cualitativa de los riesgos, considerando probabilidad, impacto y controles existentes, permitió construir una matriz que jerarquiza los riesgos, destacando como prioritarios aquellos vinculados a la conexión a redes no oficiales y a la suplantación de puntos de acceso, los cuales requieren tratamiento inmediato por su alta probabilidad e impacto potencial.

Objetivo específico 4

En relación con el cuarto objetivo específico, se concluye que el modelo de mitigación de riesgos diseñado logra adaptar coherentemente las etapas de ISO 31000, establecimiento del contexto, identificación, análisis, evaluación, tratamiento,

comunicación y monitoreo, al servicio de Wi-Fi público del centro comercial, traduciéndolas en acciones concretas y comprensibles para la gestión operativa del mall.

Objetivo específico 5

En relación con el quinto objetivo específico, se concluye que la validación mediante juicio de expertos y prueba piloto limitada confirmó la pertinencia, claridad y factibilidad del modelo propuesto, a la vez que evidenció la necesidad de asegurar un compromiso institucional sostenido y la coordinación con los comercios para garantizar su implementación eficaz.

Objetivo general

En relación con el objetivo general, se concluye que fue posible desarrollar un modelo de mitigación de riesgos basado en ISO 31000, pertinente y aplicable al contexto del Mall Centro Plaza Liberia, que integra la identificación, evaluación y tratamiento de las amenazas asociadas a la red Wi-Fi pública y ofrece una guía estructurada para fortalecer el uso seguro de este servicio.

5.2 Recomendaciones

En correspondencia con el objetivo general, se recomienda que la administración del Mall Centro Plaza Liberia adopte formalmente el modelo de mitigación de riesgos basado en ISO 31000 como marco rector para la gestión de la red Wi-Fi pública, asignando recursos específicos y estableciendo su aplicación como parte de las políticas internas de seguridad de la información.

En correspondencia con el primer objetivo específico, se recomienda institucionalizar un proceso periódico de análisis del contexto interno y externo de la red Wi-Fi, designando un responsable de seguridad que coordine la información tecnológica, organizacional y normativa para orientar la toma de decisiones en materia de riesgos.

En correspondencia con el segundo objetivo específico, se recomienda implementar un mecanismo sistemático de identificación y registro de amenazas y vulnerabilidades —incluyendo un inventario actualizado de puntos de acceso y SSID— que permita detectar configuraciones inseguras y apoyar el diseño de acciones preventivas sobre la red Wi-Fi pública.

En correspondencia con el tercer objetivo específico, se recomienda utilizar y actualizar regularmente la matriz de evaluación de riesgos como herramienta de apoyo para priorizar las acciones de seguridad, de manera que la asignación de recursos y esfuerzos se enfoque en los riesgos de mayor nivel identificados en el análisis.

En correspondencia con el cuarto objetivo específico, se recomienda implementar de forma progresiva las etapas del modelo diseñado, iniciando por la creación y señalización de un SSID oficial para la red pública y por la formalización de los protocolos de tratamiento de incidentes, para luego avanzar hacia acciones complementarias de segmentación, monitoreo y sensibilización.

En correspondencia con el quinto objetivo específico, se recomienda mantener un esquema permanente de revisión y mejora del modelo a través de la retroalimentación periódica de expertos y actores clave, incorporando sus observaciones en la actualización de procedimientos y controles para asegurar la vigencia y eficacia de la gestión de riesgos en la red Wi-Fi pública.s.

BIBLIOGRAFÍA

Abreu, J. L. (2012). *Hipótesis, método y diseño de investigación*. *Daena: International Journal of Good Conscience, 7*(2), 187–197.

Albán, G. P. G. (2020). *Metodologías de investigación educativa: descriptivas, experimentales, participativas y de investigación-acción*. *RECIMUNDO, 4*(3), 163–173.

Arias, F. G. (2012). *El proyecto de investigación* (6.ª ed.). Editorial Episteme. Recuperado de https://abacoenred.org/wp-content/uploads/2019/02/El-proyecto-de-investigaci%C3%B3n-F.G.-Arias-2012-pdf-1.pdf

Aven, T. (2015). *Risk analysis: Assessing uncertainties beyond expected values and probabilities*. John Wiley & Sons. Recuperado de https://bookis.com/no/books/terje-aven-risk-analysis-assessing-uncertainties-beyond-expected-2015

Babbie, E. (2016). *The practice of social research* (14th ed.). Cengage Learning.

Badke, W. (2017). *Research strategies: Finding your way through the information fog* (6th ed.). iUniverse.

Bernal Torres, C. A. (2010). *Metodología de la investigación: Administración, economía, humanidades y ciencias sociales* (3.ª ed.). Pearson Educación.

Bernal Torres, C. A. (2016). *Metodología de la investigación* (4.ª ed.). Pearson Educación.

Bernal-Ruiz, F., et al. [No incluido completamente en la lista original]

Bisquerra, R. (2009). *Metodología de la investigación educativa* (2.ª ed.). La Muralla. Recuperado de https://www.dykinson.com/libros/metodologia-de-la-investigacion-educativa/9788471337778/

Booth, W. C., Colomb, G. G., & Williams, J. M. (2016). *The craft of research* (4th ed.). University of Chicago Press.

Cerda Gutiérrez, H. (2011). *Los elementos de la investigación: Cómo reconocerlos, diseñarlos y construirlos*. Editorial Magisterio.

Conti, M., Dragoni, N., & Lesyk, V. (2016). A survey of man-in-the-middle attacks. *IEEE Communications Surveys & Tutorials, 18*(3), 2027–2051. https://doi.org/10.1109/COMST.2016.2544939

Corbin, J., & Strauss, A. (2015). *Basics of qualitative research: Techniques and procedures for developing grounded theory* (4th ed.). SAGE Publications. Recuperado de https://us.sagepub.com/en-us/nam/basics-of-qualitative-research/book235578

Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches* (4th ed.). SAGE Publications. Recuperado de https://us.sagepub.com/en-us/nam/research-design/book246125

Denzin, N. K., & Lincoln, Y. S. (Eds.). (2018). *The SAGE handbook of qualitative research* (5th ed.). SAGE Publications. Recuperado de https://us.sagepub.com/en-us/nam/the-sage-handbook-of-qualitative-research/book245951

Esser, K., Hillebrand, W., Messner, D., & Meyer-Stamer, J. (1996). Competitividad sistémica: Nuevo desafío para las empresas y la política. *Revista de la CEPAL, 59*, 39–52.

Estela Paredes, R. (2020). *Investigación propositiva. Módulo 1. Investigación aplicada IV*. Instituto de Educación Superior Pedagógico Público Indoamérica. https://es.calameo.com/read/006239239f8a941bec906

Ferrer, J. (2005). Competitividad sistémica: Niveles analíticos para el desarrollo industrial. *Revista Venezolana de Gerencia, 10*(31), 469–492.

Freund, J. E., Perles, B. M., & Miller, I. (2014). *Estadística matemática con aplicaciones* (8.ª ed.). Pearson.

Grimes, R. A. (2017). *Hacking the hacker: Learn from the experts who take down hackers*. Wiley. Recuperado de https://www.wiley.com/en-us/Hacking+the+Hacker%3A+Learn+From+the+Experts+Who+Take+Down+Hackers-p-9781119396213

Guest, G., Namey, E., & Mitchell, M. (2013). *Collecting qualitative data: A field manual for applied research*. SAGE.

Guevara Albán, G. P., Verdesoto Arguello, A. E., & Castro Molina, N. E. (2020). *Metodologías de investigación educativa (descriptivas, experimentales, participativas, y de investigación-acción)*. *RECIMUNDO, 4*(3), 163–173. https://www.recimundo.com/index.php/es/article/view/860

Hadi Mohamed, M. M., Martel Carranza, C. P., Huayta Mamani, F., Rojas Apaza, R., & Arias Gallegos, W. L. (2023). *Metodología de la investigación: Guía para el proyecto de tesis* (1.ª ed. digital). Instituto Universitario de Innovación Ciencia y Tecnología Inudi Perú. https://doi.org/10.35622/inudi.b.073

Hernández Sampieri, R., Collado Fernández, C., & Lucio Baptista, P. (2006). *Metodología de la investigación* (4.ª ed.). McGraw-Hill/Interamericana Editores. Recuperado de https://www.mheducation.com.mx

Hernández, R., Fernández, C., & Baptista, P. (2014). *Metodología de la investigación* (6.ª ed.). McGraw-Hill Education. Recuperado de https://dialnet.unirioja.es/servlet/libro?codigo=571687

Hernández-Sampieri, R., Fernández-Collado, C., & Baptista-Lucio, M. del P. (2014). *Metodología de la investigación* (6.ª ed.). McGraw-Hill.

Hernández-Sampieri, R., & Mendoza, C. P. (2018). *Metodología de la investigación: Las rutas cuantitativa, cualitativa y mixta*. McGraw-Hill.

Ibarra, M. A., González, L., & Demuner, M. (2017). Competitividad empresarial de las pequeñas y medianas empresas manufactureras de Baja California. *Estudios Fronterizos, 18*(35), 107–130. https://doi.org/10.21670/ref.2017.35.a06

International Organization for Standardization. (2018). *ISO 31000:2018: Risk management—Guidelines*. ISO. https://www.iso.org/standard/65694.html

International Telecommunication Union. (2021). *Global Cybersecurity Index 2020 (GCI)*. ITU. Recuperado de https://www.telecomunicaciones.gob.ec/wp-content/plugins/download-monitor/download.php?force=1&id=5337

Johnson, R. B., Onwuegbuzie, A. J., & Turner, L. A. (2007). Toward a definition of mixed methods research. *Journal of Mixed Methods Research, 1*(2), 112–133. https://doi.org/10.1177/1558689806298224

Kerlinger, F. N., & Lee, H. B. (2000). *Foundations of behavioral research* (4th ed.). Harcourt College Publishers. Recuperado de https://openlibrary.org/books/OL53085M/Foundations_of_behavioral_research

Krueger, R. A., & Casey, M. A. (2015). *Focus groups: A practical guide for applied research* (5th ed.). SAGE.

Kvale, S., & Brinkmann, S. (2015). *InterViews: Learning the craft of qualitative research interviewing* (3rd ed.). SAGE.

Labarca, N. (2007). Consideraciones teóricas de la competitividad empresarial. *Omnia, 13*(2), 158–184.

Martínez, M. (2018). *Investigación cualitativa: Teoría y práctica* (2.ª ed.). Editorial UOC. Recuperado de https://www.editorialuoc.cat

Martínez-González, M. Á., Sánchez-Villegas, A., & Fajardo, J. F. (2014). *Bioestadística amigable* (3.ª ed.). Díaz de Santos.

Medina-Romero, M. Á., Hurtado Tiza, D. R., Muñoz Murillo, J. P., Ochoa Cervantez, D. O., & Izundegui Ordóñez, G. (2023). *Método mixto de investigación: Cuantitativo y cualitativo*. Instituto Universitario de Innovación Ciencia y Tecnología Inudi Perú. https://doi.org/10.35622/inudi.b.105

Merriam, S. B., & Tisdell, E. J. (2016). *Qualitative research: A guide to design and implementation* (4th ed.). Jossey-Bass.

MICITT. (2022). *Política Nacional de Ciberseguridad 2022–2027*. Ministerio de Ciencia, Tecnología y Telecomunicaciones de Costa Rica. Recuperado de https://www.micitt.go.cr

Organization of American States. (2020). *Ciberseguridad en América Latina y el Caribe* [Sitio web de programa]. Organización de los Estados Americanos. Recuperado de https://www.oas.org/ext/es/seguridad/prog-ciber

Organization of American States, & Inter-American Development Bank. (2020). *Ciberseguridad: Riesgos, avances y el camino a seguir en América Latina y el Caribe*. OAS & BID. Recuperado de https://es.slideshare.net/slideshow/reporte-ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-amrica-latina-y-elcaribe/237394241

Otzen, T., & Manterola, C. (2017). Técnicas de muestreo sobre una población a estudio. *International Journal of Morphology, 35*(1), 227–232. https://doi.org/10.4067/S0717-95022017000100037

Patton, M. Q. (2015). *Qualitative research & evaluation methods: Integrating theory and practice* (4th ed.). SAGE.

PRODHAB. (2015). *Ley N.° 8968: Protección de la persona frente al tratamiento de sus datos personales*. Agencia de Protección de Datos de los Habitantes. Recuperado de https://www.prodhab.go.cr

Rojas Soriano, L. (2016). *La investigación cualitativa y su aplicación en el ámbito social*. Editorial Universitaria.

Sabino, C. (2014). *El proceso de investigación* (4.ª ed.). Editorial Panapo. Recuperado de https://abacoenred.org/wp-content/uploads/2019/02/EL-PROCESO-DE-INVESTIGACION-SABINO-pdf.pdf

Salkind, N. J. (2017). *Statistics for people who (think they) hate statistics* (6th ed.). SAGE.

Scarfone, K., & Souppaya, M. (2010). *Guidelines for securing wireless local area networks (WLANs)* (NIST Special Publication 800-153). National Institute of Standards and Technology. Recuperado de https://csrc.nist.gov/publications/detail/sp/800-153/final

SUTEL. (2021). *Estudio sobre ciberseguridad en Costa Rica y sus retos*. Superintendencia de Telecomunicaciones de Costa Rica. Recuperado de https://www.sutel.go.cr

Triola, M. F. (2018). *Estadística* (13.ª ed.). Pearson.

Vizcaíno Zúñiga, P. I., Cedeño Cedeño, R. J., & Maldonado Palacios, I. A. (2023). *Metodología de la investigación científica: Guía práctica*. *Ciencia Latina Revista Científica Multidisciplinar,* *7*(4), 9723–9762. https://doi.org/10.37811/cl_rcm.v7i4.7658

ANEXOS

Anexo 1. Modelo De Mitigación De Riesgos Basado Iso31000

El modelo de mitigación de riesgos propuesto se basa en los principios y el proceso de gestión de riesgos establecidos por la norma ISO 31000 y se adapta al contexto de los centros comerciales de la zona Pacífico Norte, tomando como caso de referencia el Mall Centro Plaza Liberia. El propósito es proporcionar una estructura clara y replicable que permita identificar, evaluar y tratar los riesgos asociados al uso de redes Wi-Fi públicas, integrando dimensiones técnicas, organizacionales y humanas, con énfasis en la percepción de seguridad de los usuarios.

El modelo se organiza en seis componentes principales:

1. Marco de gobernanza y responsabilidades.
2. Establecimiento del contexto.
3. Identificación y análisis de riesgos.
4. Evaluación y priorización de riesgos.
5. Tratamiento de riesgos (técnico, organizacional y educativo).
6. Comunicación, monitoreo y mejora continua.

A continuación, se desarrolla cada componente.

1. Marco de gobernanza y responsabilidades

El primer componente del modelo define la estructura mínima de gobernanza necesaria para que la gestión de riesgos no dependa solo de acciones aisladas del personal técnico, sino que quede integrada en la gestión general del centro comercial.

Objetivo general del componente

- Asegurar que exista una estructura organizativa, con roles y responsabilidades definidos, que respalde la implementación y sostenibilidad del modelo de mitigación de riesgos en la red Wi-Fi pública.

Elementos clave

- Comité o responsable de gestión de riesgos de TI:
    - Designar una persona o equipo responsable de coordinar la gestión de riesgos vinculada a la red Wi-Fi pública.
    - Incluir representación de:
        - Administración del centro comercial.
        - Personal técnico / proveedor de servicios de red.
        - Área legal o de cumplimiento (cuando exista).
- Política de seguridad de la red Wi-Fi pública:
    - Documento breve que establezca:
        - Objetivo de la red Wi-Fi pública.
        - Alcance (áreas de cobertura, tipo de usuarios).
        - Principios de seguridad (confidencialidad, integridad, disponibilidad).
        - Compromisos de cumplimiento normativo.
- Asignación de responsabilidades:
    - Quién configura y administra la red.
    - Quién monitorea eventos e incidentes.
    - Quién coordina la respuesta ante incidentes de seguridad.
    - Quién se encarga de la comunicación interna y externa sobre temas de seguridad.

2. Establecimiento del contexto

Esta etapa define el entorno en el que opera la red Wi-Fi pública y los criterios que se utilizarán para valorar los riesgos. Constituye la base para que las decisiones posteriores sean coherentes con la realidad del centro comercial y de la zona Pacífico Norte.

Objetivo de la etapa

- Comprender el contexto tecnológico, organizacional, normativo y de usuarios en el que se presta el servicio de Wi-Fi público, y establecer los criterios de evaluación de riesgos.

Acciones principales

- Contexto tecnológico:
    - Describir la infraestructura de red:
        - Número y ubicación de puntos de acceso.
        - Esquema de red (segmentación entre red pública y redes internas).
        - Protocolos de cifrado y autenticación utilizados.
    - Identificar proveedores de servicio de Internet y acuerdos de nivel de servicio.
- Contexto organizacional:
    - Analizar cómo se gestiona actualmente el servicio:
        - Procedimientos formales (si existen).
        - Prácticas informales del personal técnico.
        - Grado de documentación de configuraciones y cambios.
- Contexto normativo y regulatorio:
    - Identificar obligaciones mínimas:
        - Protección de datos personales.
        - Disposiciones de ciberseguridad relevantes.
- Contexto de usuarios:
    - Caracterizar el tipo de usuarios:
        - Visitantes locales y turistas.
        - Comercios instalados en el centro.
        - Personal interno.
    - Mapear necesidades de conectividad y posibles usos (consultas, redes sociales, transacciones, etc.).
- Criterios de riesgo:
    - Definir las dimensiones de impacto a considerar:
        - Impacto sobre los datos de los usuarios.
        - Impacto sobre la disponibilidad del servicio.
        - Impacto reputacional para el centro comercial.
        - Impacto legal o regulatorio.

3. Identificación y análisis de riesgos

En esta etapa se identifican de manera sistemática las amenazas, vulnerabilidades y escenarios de riesgo que afectan a la red Wi-Fi pública, así como los controles existentes. El modelo propone combinar información técnica y cualitativa.

Objetivo de la etapa

- Identificar los riesgos relevantes asociados a la red Wi-Fi pública, considerando factores técnicos, humanos y organizacionales.

Acciones principales

- Levantamiento de información técnica:
    - Revisar configuraciones de la red:
        - Tipo de cifrado (WPA2, WPA3, abierto, etc.).
        - Segmentación entre redes (administrativa, comercial, público).
        - Mecanismos de autenticación (portal cautivo, usuario/contraseña, sin autenticación).
    - Recopilar registros básicos (logs) si están disponibles.
- Identificación de amenazas típicas:
    - Ejemplos:
        - Puntos de acceso falsos (Evil Twin).
        - Ataques Man-in-the-Middle.
        - Sniffing del tráfico sin cifrar.
        - Secuestro de sesión.
        - Accesos no autorizados a segmentos internos.
- Identificación de vulnerabilidades:
    - Cifrado débil o inexistente.
    - Ausencia de segmentación adecuada.
    - Falta de actualización de firmware de los dispositivos.
    - Ausencia de políticas de uso aceptable.
- Consideración de factores humanos:
    - Baja percepción de riesgo por parte de los usuarios.
    - Conductas inseguras (conectarse a cualquier SSID, uso de contraseñas débiles, acceso a banca en línea sin medidas adicionales).

- Análisis preliminar:
    - Describir, para cada riesgo:
        - Fuente (amenaza).
        - Vulnerabilidad explotada.
        - Activos afectados (datos de usuarios, reputación, continuidad del servicio).

4. Evaluación y priorización de riesgos

A partir de los riesgos identificados, el modelo propone asignarles una valoración en términos de probabilidad e impacto, considerando los controles ya existentes. Esto permite focalizar los esfuerzos en los riesgos más críticos.

Objetivo de la etapa

- Clasificar y priorizar los riesgos para decidir qué tratamiento corresponde a cada uno.

Acciones principales

- Definir escalas cualitativas:
    - Probabilidad:
        - Baja, media, alta.
    - Impacto:
        - Bajo, moderado, alto, crítico (sobre datos, servicio, reputación).
- Construir una matriz de probabilidad–impacto:
    - Ubicar cada riesgo en la matriz.
    - Determinar nivel de riesgo:
        - Aceptable.
        - Tolerable con control.
        - No aceptable (requiere acciones inmediatas).
- Revisión de controles existentes:
    - Identificar qué riesgos ya tienen controles parciales:
        - Por ejemplo, cifrado WPA2 activado, pero sin segmentación.

    - Evaluar si esos controles son suficientes o deben reforzarse.
- Priorización final:
    - Elaborar un listado de riesgos priorizados, indicando:
        - Riesgos de intervención inmediata.
        - Riesgos a gestionar a mediano plazo.
        - Riesgos a monitorear.

5. Tratamiento de riesgos

El tratamiento de riesgos es el núcleo operativo del modelo. Aquí se definen las acciones concretas para reducir la probabilidad y/o el impacto de los riesgos priorizados. El modelo combina medidas técnicas, organizacionales y de sensibilización.

Objetivo de la etapa

- Diseñar e implementar medidas de mitigación alineadas con la magnitud de los riesgos y las capacidades del centro comercial.

Líneas de tratamiento

1. Medidas técnicas de seguridad de la red
    - Uso de un SSID oficial claramente identificado y comunicado.
    - Implementación de cifrado robusto (WPA2/WPA3) en la red pública, cuando sea viable.
    - Segmentación de la red:
        - Separar redes administrativas, de comercios y de visitantes.
    - Configuración de mecanismos de registro y monitoreo:
        - Activar registros de conexión, alertas básicas y supervisión periódica por parte del personal técnico o proveedor.
    - Actualización periódica de firmware y parches de seguridad de los equipos.
2. Medidas organizacionales y procedimentales
    - Elaboración de una política de uso aceptable de la red Wi-Fi pública:
        - Qué se permite y qué no.
        - Límites de responsabilidad del centro comercial.

- Definición de un procedimiento de respuesta a incidentes:
  - Detección y registro.
  - Análisis y contención.
  - Comunicación interna y, si corresponde, externa.
- Establecimiento de acuerdos con el proveedor de servicios:
  - Requisitos mínimos de seguridad.
  - Tiempos de respuesta ante incidentes.
  - Responsabilidades compartidas.

3. Medidas educativas y de sensibilización
   - Diseño de materiales informativos para usuarios:
     - Mensajes en el portal de acceso (portal cautivo).
     - Afiche o señalización visible con el SSID oficial y recomendaciones básicas.
   - Actividades breves de capacitación para:
     - Personal del centro comercial.
     - Encargados de locales comerciales, de manera que puedan orientar a los clientes.
   - Recomendaciones clave para usuarios:
     - Verificar el nombre de la red oficial.
     - Evitar transacciones sensibles en redes abiertas.
     - Mantener dispositivos actualizados y, de ser posible, usar conexiones seguras (HTTPS, VPN).

Cada medida de tratamiento debe quedar documentada en un plan de tratamiento de riesgos, indicando responsables, recursos requeridos y plazos de implementación.

6. Comunicación, monitoreo y mejora continua

El modelo no termina con la implementación inicial de controles; la gestión de riesgos debe revisarse de manera periódica para adaptarse a nuevas amenazas, cambios tecnológicos y variaciones en el perfil de los usuarios.

Objetivo de la etapa

- Mantener un ciclo permanente de comunicación, seguimiento y mejora, que garantice la vigencia y eficacia del modelo.

Acciones principales

- Comunicación y consulta:
    - Informar periódicamente a la administración sobre:
        - Principales riesgos.
        - Controles implementados.
        - Incidentes ocurridos y lecciones aprendidas.
    - Mantener canales para que usuarios y comercios reporten problemas o comportamientos sospechosos en la red.
- Monitoreo:
    - Definir indicadores simples, por ejemplo:
        - Número de incidentes detectados al mes.
        - Número de cambios de configuración documentados.
        - Participación en acciones de sensibilización (talleres, campañas).
    - Revisar con frecuencia la matriz de riesgos y los registros de la red.
- Revisión y actualización del modelo:
    - Evaluaciones periódicas (por ejemplo, anual o semestral) para:
        - Verificar si los riesgos han cambiado.
        - Incorporar nuevas amenazas o cambios normativos.
    - Ajustar políticas, procedimientos y mensajes a usuarios según los resultados del monitoreo.

Anexo 2. Guías de Entrevistas y Grupos Focales

Guía de Entrevista Semiestructurada a Usuarios de Redes Wi-Fi

- Objetivo: Obtener percepciones sobre la seguridad en el uso de redes Wi-Fi públicas.
- Preguntas:
    1. ¿Cuáles son las principales razones por las que decides conectarte a la red Wi-Fi pública en el Mall Centro Plaza Liberia?
    2. ¿Con qué frecuencia usas redes Wi-Fi públicas?
    3. ¿Qué medidas tomas para proteger tu información cuando te conectas a redes públicas?
    4. ¿Qué tan confiable consideras que es la red Wi-Fi pública en el Mall Centro Plaza Liberia?
    5. ¿Alguna vez has tenido problemas de seguridad relacionados con el uso de Wi-Fi público?
    6. ¿Qué medidas consideras necesarias para mejorar la seguridad en redes Wi-Fi públicas?

Guía de Entrevista a Personal Técnico

- Objetivo: Conocer las prácticas de gestión y seguridad de las redes Wi-Fi del centro comercial.
- Preguntas:
    1. ¿Qué medidas de seguridad implementa el centro comercial en su red Wi-Fi pública?
    2. ¿Qué protocolos de cifrado se utilizan en la red Wi-Fi pública del Mall Centro Plaza Liberia?

3. ¿Cuáles son los principales problemas de seguridad que han enfrentado en la red Wi-Fi?
4. ¿Existen procedimientos para detectar y mitigar incidentes de seguridad en la red Wi-Fi pública?
5. ¿Se realizan auditorías periódicas o pruebas de penetración en la red?

Anexo 3. Resultados de las Entrevistas y Grupos Focales

Transcripciones de Entrevistas a Usuarios

- Resumen: Transcripción completa de las entrevistas realizadas a los usuarios de la red Wi-Fi, donde se recogen sus percepciones y prácticas respecto a la seguridad de la red. Ejemplos representativos de citas de los usuarios:
    - "Cuando estoy en un mall, normalmente siento que puedo conectarme con confianza; asumo que las redes son confiables." (Usuario 4)
    - "No reviso mucho los nombres, solo veo que tenga buena señal." (Usuario 2)

Transcripciones de Entrevistas a Personal Técnico

- Resumen: Transcripción de entrevistas realizadas con el personal técnico encargado de la red Wi-Fi del centro comercial. Estas entrevistas brindan detalles sobre las prácticas de seguridad y los desafíos técnicos.

Códigos y Categorías del Análisis Cualitativo

- Proceso de Codificación: Detalles sobre la codificación utilizada en el análisis de las entrevistas, donde se identificaron las categorías emergentes relacionadas con la percepción de seguridad, las prácticas de los usuarios y las medidas de seguridad observadas.

Anexo 4. Resultados de Observación de la Red Wi-Fi

Detalles de la Infraestructura de Red Wi-Fi del Mall Centro Plaza Liberia

Descripción: Observación de las redes Wi-Fi identificadas en el centro comercial, incluyendo las configuraciones de seguridad y las características de las redes disponibles para los usuarios.

Ejemplo:

Redes como @Ruijie-b07A5, Presidencia, 425035_DO…C_LIBERIA, HUAWEI-2.4G-YwG3, entre otras, fueron identificadas durante la visita.

Fortaleza: Uso de cifrado WPA2 en todas las redes observadas, lo cual es una práctica positiva.

Oportunidad de mejora: No se identificó una red pública oficial claramente señalizada, lo que podría generar confusión para los usuarios.

Observaciones sobre la Seguridad de la Red

Conclusión: Durante la observación de campo, no se encontraron indicios de redes abiertas ni señales visibles de actividad maliciosa, como ataques de suplantación de puntos de acceso.

Anexo 5. Resultados de Evaluación de Riesgos y Modelo de Mitigación

Matriz de Riesgos de Seguridad en la Red Wi-Fi

Evaluación de Riesgos: Matriz que clasifica los riesgos identificados (como la suplantación de puntos de acceso, secuestro de sesiones, etc.) en función de su probabilidad de ocurrencia y el impacto que tendrían en la seguridad de los usuarios.

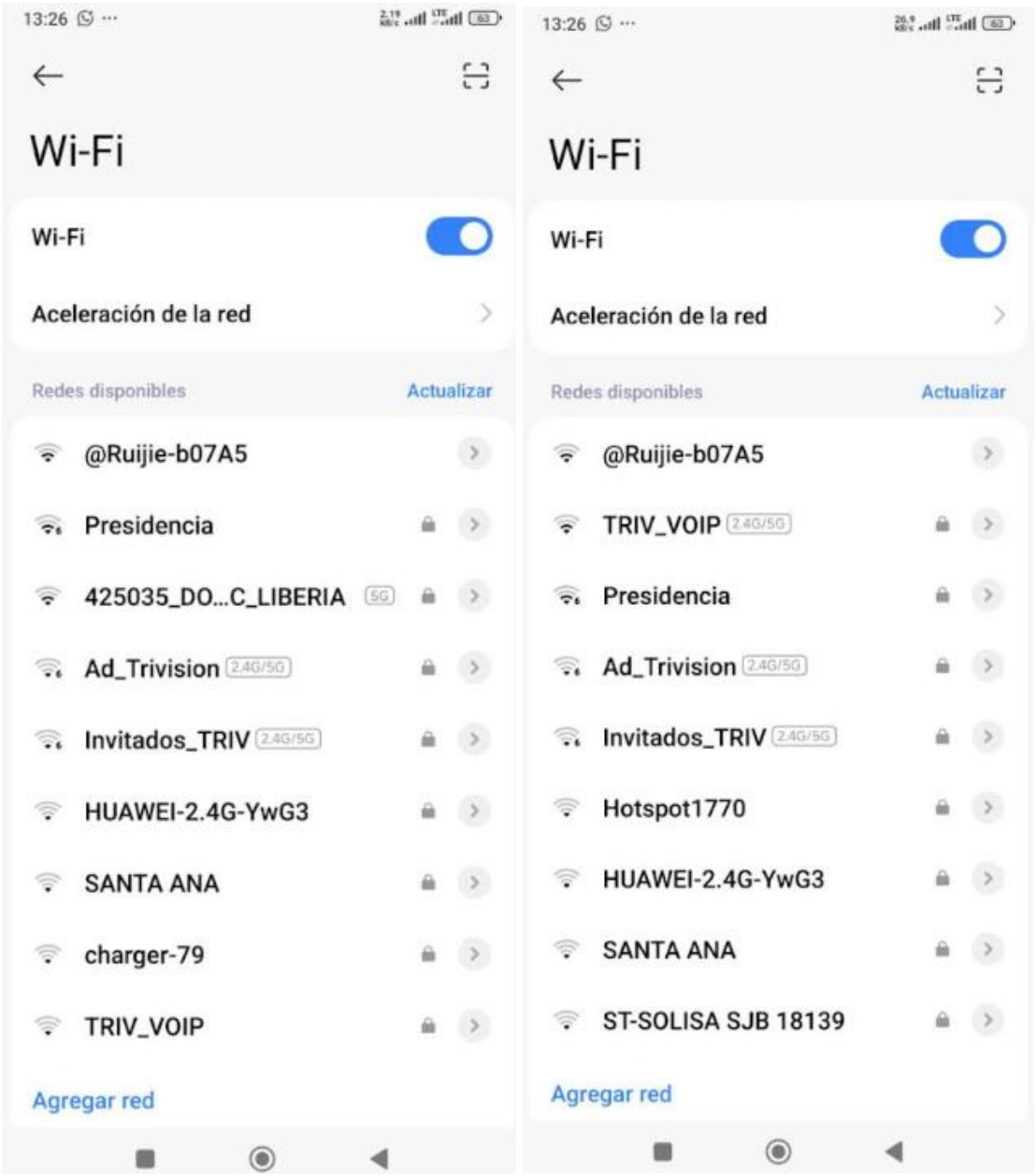
Modelo de Mitigación de Riesgos Basado en ISO 31000

Descripción del Modelo: Explicación detallada del modelo de mitigación propuesto, basado en la norma ISO 31000. Incluye las etapas de identificación, evaluación, tratamiento, monitoreo y revisión de los riesgos asociados a las redes Wi-Fi públicas.

Procedimientos de Implementación

Acciones Específicas: Detalles sobre las acciones recomendadas para mejorar la seguridad de la red Wi-Fi pública, tales como la implementación de autenticación reforzada, cifrado de datos, y la segmentación de la red.

Anexo 6. Redes Wi-Fi Públicas



Anexo 7. Documentos Normativos y Legales

Extractos de la Norma ISO 31000:2018

Norma ISO 31000: Incluir los principios y directrices clave de la norma ISO 31000 relacionados con la gestión de riesgos y cómo se aplican al contexto de redes Wi-Fi públicas.

Ley 8968 sobre Protección de Datos Personales en Costa Rica

Extractos Relevantes: Inclusión de los artículos clave de la ley 8968 que establecen la responsabilidad de los proveedores de redes Wi-Fi en cuanto a la protección de datos personales y las medidas de seguridad requeridas.

Anexo 8. Resultados de Validación del Modelo

Retroalimentación de expertos

La validación del modelo de mitigación de riesgos se realizó mediante el juicio de expertos en redes inalámbricas, ciberseguridad y gestión de riesgos. Los especialistas revisaron la estructura general del modelo, sus etapas, actividades y lineamientos operativos, evaluando su coherencia y pertinencia respecto al problema identificado en el Mall Centro Plaza Liberia.

En términos generales, la valoración fue favorable, destacándose la integración de medidas técnicas, organizacionales y educativas, así como la alineación explícita con los principios de la norma ISO 31000. Los expertos consideraron que el modelo es claro, aplicable y adaptable a otros centros comerciales con características similares.

Entre las principales sugerencias se recomendó reforzar la etapa de monitoreo y revisión, precisar los roles y responsabilidades de los actores involucrados y potenciar las estrategias de comunicación con los usuarios. Estas observaciones fueron incorporadas mediante ajustes en las etapas del modelo y en la definición de actividades específicas de seguimiento y sensibilización.

Prueba piloto del modelo de mitigación

La prueba piloto del modelo se llevó a cabo en el Mall Centro Plaza Liberia, con el propósito de comprobar su aplicabilidad práctica y detectar posibles ajustes operativos. Durante este ejercicio se aplicaron las etapas de diagnóstico, priorización de riesgos y adopción inicial de medidas técnicas y organizacionales.

Como parte de la prueba, se realizaron ajustes básicos en la configuración de la red Wi-Fi pública (revisión de cifrado, segmentación y uso de un SSID oficial), se clarificaron

procedimientos internos de respuesta ante incidentes y se probaron mensajes iniciales de orientación al usuario sobre el uso seguro de la red.

Los resultados mostraron que el modelo es factible de implementar y contribuye a ordenar la gestión de la red Wi-Fi pública, aunque requiere coordinación constante entre administración, personal técnico y proveedor del servicio. A partir de la experiencia piloto se identificaron oportunidades de mejora, especialmente en la formalización de indicadores de seguimiento y en la planificación de acciones de sensibilización continua, las cuales se integraron en la versión final del modelo.