Universidad de Costa Rica

Facultad de Ciencia Económicas

Escuela de Administración de Negocios

Proyecto seminario de graduación para optar por el grado de Licenciatura en Dirección de Empresas

Gestión del riesgo por fraude a través de medios digitales: La imagen corporativa del Banco de Costa Rica

Carlos Hernández Sibaja B33324

Hernán Cervantes Sanabria A71698

Ana Lucía Esquivel Salas B32460

Ciudad Universitaria Rodrigo Facio 2022

Artículo 6

El Presidente del Comité Evaluador comunicó en público el resultado de la deliberación y les declaró: *Licenciadas en Dirección de Empresas.*

Se les indicó la obligación de realizar las gestiones para el Acto de Juramentación más próximo. Luego se dio lectura al acta que firmaron los miembros del Comité y el grupo de estudiantes.

Arturo Méndez Arias
Representante Director, Escuela Administración de Negocios

Carlos Andrés Hernández Sibaja
Carné B33324

Silvia Chinchilla Sáenz
Tutor

José Hernán Cervantes Sanabria
Carné A71698

Ronny Meneses Fernández
Lector

Ana Lucía Esquivel Salas
Carné B32460

Edgar Humberto Hernández Cañas
Lector

Juan Carlos Arias Contreras
Secretario

Según lo establecido en el Reglamento de Trabajos Finales de Graduación, artículo 39 "... En caso de trabajos sobresalientes; si así lo acuerdan por lo menos cuatro de los cinco miembros del Comité, se podrá conceder una aprobación con distinción".

◯ Se aprueba con Distinción

Observaciones: _____

LHS

UNIVERSIDAD DE COSTA RICA
FACULTAD DE CIENCIAS ECONÓMICAS

Acta # 23-2022

Acta de la Sesión 23-2022 del Comité Evaluador de la Escuela de Administración de Negocios, celebrada el 01 de diciembre de 2022, por medio de la Plataforma Zoom, con el fin de proceder a la Exposición del Trabajo Final de Graduación de **Carlos Andrés Hernández Sibaja, carné B33324, José Hernán Cervantes Sanabria, carné A71698 y Ana Lucia Esquivel Salas, carné B32460,** quienes optaron por la modalidad de Seminario de Graduación.

Presentes: Arturo Méndez Arias, quien presidió; Silvia Chinchilla Sáenz, Tutor; Ronny Meneses Fernández y Édgar Humberto Hernández Cañas, lectores; Juan Carlos Arias Contreras, Representante del Sector Docente de la Escuela de Administración de Negocios, quien actuó como Secretario de la Sesión.

Artículo 1

El Presidente informa que los expedientes de las personas postulantes, contienen todos los documentos que el Reglamento exige. Declara que han cumplido con los requisitos del Programa de la Carrera de Licenciatura en Dirección de Empresas.

Artículo 2

Hicieron la exposición del Trabajo Final: ***Gestión del riesgo por fraude a través de medios digitales: La imagen corporativa del Banco de Costa Rica.***

Artículo 3

Terminada la disertación, los miembros del Comité Evaluador, interrogaron a quienes expusieron, en el tiempo reglamentario. Las respuestas fueron Satisfactorias, en opinión del Comité.

(satisfactorias/insatisfactorias)

Artículo 4

Concluido el interrogatorio, el Tribunal procedió a deliberar

Artículo 5

Efectuada la votación, el Comité Evaluador consideró el Trabajo Final de Graduación Satisfactorio, y lo declaró Aprobado .

(Satisfactorio /insatisfactorio) (Aprobado /no aprobado)

Ciudad Universitaria Rodrigo Facio

Escuela Administración de Negocios

2 de diciembre del 2022

A quien interese

Yo, Mag. Silvia Chinchilla Sáenz, cédula 106510036, en calidad de tutora del Trabajo Final de Graduación titulado “Gestión del riesgo por fraude a través de medios digitales: La imagen corporativa del Banco de Costa Rica”, presentado por los estudiantes: Carlos Hernández Sibaja, carné B33324; Hernán Cervantes Sanabria, carné A71698; Ana Lucía Esquivel, carné B32460, hago constar que el documento entregado es el definitivo y no tuvo correcciones necesarias.

Atentamente,

Carta de aprobación del filólogo

Cartago, 02 de diciembre de 2022

Los suscritos, Elena Redondo Camacho, mayor, casada, filóloga, incorporada a la Asociación Costarricense de Filólogos con el número de carné 0247, portadora de la cédula de identidad número 3-0447-0799 y, Daniel González Monge, mayor, casado, filólogo, incorporado a la Asociación Costarricense de Filólogos con el número de carné 0245, portador de la cédula de identidad número 1-1345-0416, ambos vecinos de Quebradilla de Cartago, revisamos el trabajo final de graduación que se titula: *Gestión del riesgo por fraude a través de medios digitales: La imagen corporativa del Banco de Costa Rica*, sustentado por Carlos Hernández Sibaja, Hernán Cervantes Sanabria y Ana Lucía Esquivel Salas.

Hacemos constar que se corrigieron aspectos de ortografía, redacción, estilo y otros vicios del lenguaje que se pudieron trasladar al texto. A pesar de esto, la originalidad y la validez del contenido son responsabilidad directa de la persona autora.

Esperamos que nuestra participación satisfaga los requerimientos de la Universidad de Costa Rica.

X

Elena Redondo Camacho
Filóloga - Carné ACFIL n.º 0247

X

Daniel González Monge
Filólogo - Carné ACFIL n.º 0245

Dedicatoria

Queremos expresar nuestras muestras de agradecimiento en primera instancia a Dios, por mantenernos siempre con salud y darnos esa guía para elaborar este proyecto en las mejores condiciones. También a nuestras familias, las cuales siempre han estado apoyándonos en todo momento y fueron ese sostén cuando la situación se complicaba. De igual manera, debemos agradecer a la tutora Silvia Chinchilla y lectores que siempre estuvieron con nosotros y nos dieron la orientación necesaria para seguir adelante, también es necesario agradecer a Gustavo Arias, encargado del Departamento de Prevención de Fraudes del BCR, quien nos ayudó a conseguir la información necesaria y siempre mostraba la mejor de las disposiciones. Por último, agradecemos a la Escuela de Administración de Negocios, la cual desarrolla estudiantes íntegros y brinda las herramientas necesarias para el desarrollo, tanto personal como laboral.

Contenido capitulario

Derechos de propiedad intelectual ii

Carta de aprobación del filólogo iii

Dedicatoria iv

Contenido capitulario v

Índice de tablas xi

Índice de figuras xii

Resumen ejecutivo xiv

Introducción 1

Justificación 3

Objetivos 4

Objetivo general 4

Objetivos específicos 4

Alcances 5

Limitaciones 5

Capítulo I. Fundamentación teórica y mejores prácticas 7

1.1. Marco conceptual 7

1.1.1. Fraude cibernético 7

1.1.1.1. Tipos de fraude cibernético 7

1.1.1.1.1. Fraude en segunda persona 8

1.1.1.1.2. Fraude en tercera persona 8
1.1.1.1.2.1. Ingeniería social 8
1.1.1.1.2.2. Suplantación de identidad (phishing) 9
1.1.1.1.2.3. Spear phishing 9
1.1.1.1.2.4. Suplantación de identidad (vishing) 9
1.1.1.1.2.5. Smishing 9
1.1.1.1.2.6. Secuestro de información (ransomware) 10
1.1.1.1.2.7. Skimming 10
1.1.1.1.2.8. Redes sociales/angler fishing 10
1.1.1.1.2.9. Pharming 10
1.1.1.1.2.10. Sitios fraudulentos 11
1.1.1.1.2.11. Baiting 11
1.1.1.1.2.12. Man in the Middle (MiTM) 11
1.1.1.1.2.13. Capturador de claves (key logger) 11
1.1.1.1.2.14. Sniffing 12
1.1.2. Gestión de riesgo 12
1.1.3. Tipos de mecanismos de seguridad 12
1.1.4. Imagen corporativa 17
1.1.5. Medios digitales 17
1.1.6. Definición de la banca 18

1.1.7. Modelos de gestión de riesgo.....19
1.1.7.1. COSO.....19
1.1.7.2. Modelo de las tres líneas de defensa.....21
1.1.7.2.1. Primera línea de defensa: la gestión operativa.....22
1.1.7.2.2. Segunda línea de defensa: Funciones de gestión de riesgo y cumplimiento.....22
1.1.7.2.3. Tercera línea de defensa: funciones de auditoría interna.....23
1.1.7.3. Modelo de las tres líneas.....24
1.1.7.3.1. Principios del modelo de las tres líneas del IIA.....25
1.1.7.3.2. Roles clave del modelo de las tres líneas del IIA.....26
1.2. Gestión del riesgo por fraude en el ámbito internacional a través de medios digitales.....28
1.3. Gestión del riesgo por fraude en el ámbito nacional a través de medios digitales.....33
1.4. Imagen corporativa en el sector bancario internacional.....35
1.5. Imagen corporativa en el sector bancario nacional.....36
Capítulo II. Situación actual del Banco de Costa Rica.....38
2.1. Descripción de la organización.....38
2.1.1. Reseña histórica.....38
2.1.2. Misión.....39
2.1.3. Visión.....39

2.1.4. Valores 39
2.1.5. Objetivos estratégicos 40
2.1.6. Productos y servicios 40
2.1.7. Recursos y estructura de la entidad 40
2.1.8. Principales competidores 41
2.2. Sistema de gestión integral de riesgo 44
2.2.1. Riesgos objeto de gestión 45
2.2.1.1. Financieros 45
2.2.1.2. No financieros 45
2.2.2. Principios y políticas 45
2.2.3. Modelos y metodologías 46
Capítulo III. Marco contextual 50
3.1. Situación actual de los fraudes digitales 50
Capítulo IV. Marco metodológico 53
4.1. Paradigma y enfoque 53
4.2. Fases de la investigación 54
4.3. Instrumentos y técnicas de recolección de datos 55
4.3.1. Revisión documental 56
4.3.2. Cuestionario 56
4.3.3. Entrevista 56

4.3.4. Entrevista dirigida o semiestructura 57

4.3.5. Entrevista en profundidad 57

4.3.6. Grupo focal 57

4.4. Fuentes de información (primarias y secundarias) 57

4.4.1. Población y muestra.....57

4.4.2. Tabulación y análisis de los resultados 58

4.4.2.1. Encuesta 59

4.4.2.1.1. Perfil de las personas encuestadas.....59

4.4.2.1.2. Análisis de uso de las plataformas digitales 62

4.4.2.1.3. Análisis de la comunicación bancaria con respecto a la prevención de fraude 68

4.4.2.1.4. Imagen corporativa del Banco de Costa Rica 70

4.4.2.2. Cuestionario 75

Capítulo V. Propuestas 82

5.1. Propuesta modelo de gestión de riesgo 82

5.2. Propuestas que se relacionan con los hallazgos de la gestión del riesgo ..90

5.2.1. Imagen corporativa.....90

5.2.2. Mejora continua.....91

5.2.3. Proveedores de datos 92

Capítulo VI. Conclusiones y recomendaciones.....94

6.1. Conclusiones 94

6.2. Recomendaciones 96

Referencias bibliográficas 98

Cronograma de actividades 107

Anexos 108

Encuesta 108

Cuestionario 118

Índice de tablas

Tabla 1 Principios del modelo de las tres líneas del IIA 25

Tabla 2 Roles clave del modelo de las tres líneas del IIA 27

Tabla 3 Hechos que se relacionan con la imagen corporativa del sector bancario costarricense.....36

Tabla 4 Integrantes del sistema bancario nacional 41

Tabla 5 Miembros del ABC.....42

Tabla 6 Propuesta gestión de riesgo por fraude.....84

Tabla 7 Recomendaciones para la mejora de la imagen corporativa 89

Tabla 8 Propuesta imagen corporativa.....90

Tabla 9 Propuesta mejora continua 91

Tabla 10 Propuesta fuentes de información para el análisis del fraude 92

Índice de figuras

Figura 1 Conceptos sobre medios digitales.....18

Figura 2 El modelo de las tres líneas de defensa.....21

Figura 3 El modelo de las tres líneas del IIA 24

Figura 4 Países latinoamericanos con estrategia nacional de ciberseguridad 30

Figura 5 Conglomerado Financiero BCR 41

Figura 6 Cálculo realizado para obtener una muestra significativa 58

Figura 7 Clientes actuales del Banco de Costa Rica 59

Figura 8 Personas que fueron clientes del banco de Costa Rica en el pasado, pero que actualmente no lo son.....60

Figura 9 Razones por las cuales dejaron de ser clientes del Banco de Costa Rica 60

Figura 10 Distribución por género 61

Figura 11 Distribución por edad.....61

Figura 12 Distribución por estado civil.....62

Figura 13 Distribución por lugar de residencia.....62

Figura 14 Utilización de plataformas digitales del Banco de Costa Rica.....63

Figura 15 Razones para no utilizar plataformas digitales del Banco De Costa Rica 63

Figura 16 Frecuencia con que se utilizan las plataformas virtuales del Banco de Costa Rica.....64

Figura 17 Porcentaje de uso de las plataformas del Banco de Costa Rica de acuerdo con el dispositivo.....64

Figura 18 Plataforma virtual que utilizan para ingresar al Banco de Costa Rica ...65

Figura 19 Tipo de transacciones más realizadas en la plataforma del Banco de Costa Rica ...66

Figura 20 Nivel de confianza en las plataformas virtuales del Banco de Costa Rica ...67

Figura 21 Porcentaje de la población que considera que la plataforma digital del Banco de Costa Rica es segura para realizar transacciones ...67

Figura 22 Razones por las cuales consideran que la plataforma digital del Banco de Costa Rica es segura para realizar transacciones...68

Figura 23 Porcentaje de la población que ha recibido información sobre cómo prevenir fraude por parte del Banco de Costa Rica ...69

Figura 24 Medios por los cuales la población ha recibido información sobre cómo prevenir fraude por parte del Banco de Costa Rica ...69

Figura 25 Porcentaje de la población que considera que es importante recibir información sobre cómo prevenir fraude...70

Figura 26 Porcentaje de la población que considera que la percepción sobre una organización es un factor importante en el momento de elegir una institución financiera ...71

Figura 27 Porcentaje de la población que posee cuentas con otros bancos.....72

Figura 28 Institución financiera preferida ...72

Figura 29 Razones de preferencia de la institución financiera ...73

Figura 30 Evaluación de la imagen corporativa del Banco de Costa Rica.....74

Figura 31 Opinión sobre el servicio que recibe del Banco de Costa Rica.....74

Figura 32 Aspectos que se consideran relevantes a cambiar en el BCR.....75

Resumen ejecutivo

El fraude digital ha venido en aumento con el paso de los años. Esto hace que cada día sean más importantes las gestiones que realizan las organizaciones para prevenirlo. Debido a esto, en el ámbito mundial se han desarrollado muchos programas y directrices sobre gestión del riesgo que cada vez toman mayor fuerza e importancia en las instituciones de cualquier sector.

Estadísticamente, se determinó que las instituciones financieras son las que sufren un 300 % más los ataques digitales comparadas con organizaciones de otra índole. Al mismo tiempo, tratan de persuadir a las personas para que entreguen información sensible y, de este modo, logren entrar y cometer el crimen informático.

Internacionalmente, se realizan esfuerzos para que las instituciones financieras tomen consciencia sobre la importancia de la gestión de fraude en medios digitales, ya que algunos estudios demuestran que en la región latinoamericana no se cuenta con procesos y sistemas robustos para contener la gran cantidad de delitos informáticos que han aparecido y que seguirán creciendo.

El Banco de Costa Rica es una institución financiera sólida que tiene 145 años de existencia y se creó con el fin de impulsar el desarrollo económico y social de Costa Rica. Es importante resaltar, que ha logrado adaptarse a los cambios del mercado durante el paso de los años y siempre ha estado en la vanguardia como uno de los bancos más importantes en el país.

Debido a la historia e importancia que tiene el Banco en el país se fundó la necesidad de investigar sobre la gestión por fraudes digitales que se realizan en la actualidad, para determinar sus condiciones y respuestas ante los ataques cibernéticos. De igual manera, se busca definir la afectación que estos delitos puedan tener sobre la imagen corporativa de la institución, ya que la imagen un factor primordial para la diferenciación en el sector bancario.

Para el estudio, la población encuestada fue una muestra representativa de la población económicamente activa de Costa Rica y también se realizó un cuestionario

dirigido a las personas colaboradoras del Departamento de Prevención de Fraudes del BCR. El propósito principal de estos instrumentos fue indagar sobre la percepción que tiene la ciudadanía de la imagen corporativa del BCR y también conocer la gestión por riesgo que utilizan en la actualidad, para desarrollar acciones que ayuden a mejorar y mantener sanos ambos aspectos.

Después de analizar de forma cualitativa y cuantitativa la información recolectada en los distintos instrumentos, se elaboró un nuevo mecanismo de gestión de fraude para los puntos débiles que se encontraron integrando los modelos que se utilizan, pero que se venían trabajando aparte. Esta propuesta incluye la integración de la metodología COSO con la nueva metodología de las Tres Líneas en aspectos como imagen corporativa, estandarización de procesos, tiempos de espera, falta de educación al cliente, nuevas fuentes de información y fortalecimiento en la oficina de prevención de fraudes. De igual forma, se desarrolló una propuesta que se enfoca solamente en los aspectos por mejorar en el BCR para aumentar la cantidad de personas que tengan una buena percepción de la entidad.

Por último, en el apartado de conclusiones y recomendaciones se resumen los principales hallazgos de la investigación y se presentan escenarios para que el BCR pueda mejorar su gestión y, de este modo, también su imagen corporativa.

Introducción

Un aspecto fundamental de las organizaciones en la actualidad es su imagen. Su importancia radica en que:

> La proyección y la protección de la imagen positiva de las marcas aparecen como una de las necesidades vitales y prioritarias de las empresas u organizaciones, pues la imagen tiene repercusiones -buenas o malas- sobre el rendimiento económico de las mismas y sobre el bienestar de la población a las que pretenden servir (Karounga, 2006, p. 27).

El sector bancario ofrece en el mercado productos y servicios similares, por lo tanto, resulta importante la diferenciación mediante la imagen corporativa. Esta imagen es favorable cuando se logra posicionar, de manera positiva, en la mente de las personas consumidoras. Lo anterior es un factor vital para que las entidades bancarias logren obtener la confianza por parte de sus clientes y se consoliden en el tiempo.

En la banca nacional, el Banco de Costa Rica (BCR) en el que se realiza el estudio, con 143 años de existencia y que demuestra gran solidez en el país, se ha visto afectado al igual que muchas otras entidades por el aumento constante de los crímenes cibernéticos viéndose amenazada su imagen. Ante esta realidad y, aunque el Banco de Costa Rica, como otras entidades financieras, ha fortalecido sus mecanismos de control y seguridad, el gran auge en medios digitales ocasiona que en el ámbito nacional se siga registrando diariamente gran cantidad de personas afectadas por fraudes. Por lo tanto, se observa la oportunidad de evaluar si estos mecanismos y comunicación corporativa pueden mejorarse y adaptarse a la realidad nacional, de forma que la imagen del Banco no se vea afectada debido a estas situaciones fraudulentas.

En la actualidad, el Departamento de Prevención de Fraudes del Banco de Costa Rica realiza una gestión de riesgo en tiempo real, lo cual indica que trata de evitar el fraude en el momento que sucede. Sin embargo, son conscientes de que

se debe mejorar el proceso preventivo y detectivo, de forma tal que disminuya la cantidad de personas afectadas. Como respuesta al problema, se proponen mejoras al proceso de gestión de riesgo asociado con el fraude a través de medios digitales, con el fin de fortalecer las etapas preventivas en tiempo real y las consecuencias, lo que permite mantener y hasta optimizar la imagen y confianza de la organización ante sus clientes.

El BCR utiliza una clasificación de riesgo con base en el objeto de interés, con el fin de subdividir cada riesgo y mitigarlo, de forma específica. El riesgo asociado con el fraude electrónico se cataloga como un riesgo operativo tecnológico según la metodología general de valoración cualitativa de riesgos. Esta metodología se aplica para identificar, analizar, evaluar, gestionar, documentar y comunicar los riesgos relevantes asociados con procesos, proyectos estratégicos e infraestructura de tecnología de información, proponiendo planes para gestionar los eventos con un nivel de riesgo medio o alto.

En el presente trabajo se realiza una encuesta a una muestra representativa de clientes del banco de Costa Rica, así como un cuestionario a todas las personas funcionarias del Departamento de Fraudes. Con los hallazgos que se obtienen se crea una propuesta para la gestión del riesgo por fraude para mejorar la imagen del Banco.

El presente trabajo se divide en cinco capítulos que se describen a continuación:

- En el Capítulo I se define el fraude cibernético y sus tipos. Incluye varios conceptos como gestión de riesgo, imagen corporativa, medios digitales y banca. Por último, se describen los modelos de gestión del riesgo que utilizan las instituciones financieras.
- En el Capítulo II se describen los aspectos generales del Banco de Costa Rica, así como su contexto actual. Este contiene su modelo de gestión de riesgo y metodologías.

- En el Capítulo III se detalla el marco metodológico, así como los resultados de los instrumentos de recolección de datos aplicados a clientes y colaboradores del Banco de Costa Rica.
- El Capítulo IV contiene la propuesta de gestión del riesgo por fraude a través de medios digitales y de mejoramiento de la imagen corporativa con base en los hallazgos de la investigación.
- El Capítulo V abarca las conclusiones y recomendaciones que se obtienen de la investigación.

Justificación

La gestión del riesgo por fraude es primordial en las entidades bancarias para asegurar una protección adecuada del patrimonio e información de sus clientes y, a la vez, para fortalecer la confianza de los usuarios hacia la institución. El fraude evoluciona a través del tiempo y, por ende, la gestión de este no puede ser estática, por lo que se deben establecer procesos y directrices internas orientadas a identificar, valorar y mitigar la posible afectación para la persona usuaria.

Sin embargo, en la actualidad, los crímenes se presentan cada vez más en plataformas digitales, ya que el Internet proporciona anonimato para el delincuente. El BCR recibe denuncias diarias por fraudes informáticos por parte de sus clientes y, en su mayoría, son personas que no están educadas en temas de prevención de fraude. No obstante, en mayo de 2020 hubo una filtración de 900.000 tarjetas por parte del grupo cibercriminal Maze, lo que generó pánico y un impacto negativo en la imagen corporativa del BCR. Por lo tanto, es de gran interés el identificar las oportunidades de mejora en la gestión del riesgo por fraude a través de medios digitales presentes en el BCR que impactan su imagen corporativa.

En la actualidad, el BCR dispone de mecanismos para permitir al cliente utilizar los servicios digitales con seguridad y evitar ser víctima de fraude, como la clave dinámica, el certificado digital, controles de acceso del territorio desde donde se puede acceder a la página web, frase de seguridad y código de identificación. No obstante, después de la filtración de datos del 2020 el BCR ha adoptado nuevos

mecanismos de seguridad como la detección biométrica de rostro, clave dinámica digital y el envío de correos electrónicos al cliente con cada transacción que haga.

Sin embargo, este tipo de herramientas que ha adoptado el banco en los últimos meses son equivalentes a los mecanismos que ya otras entidades bancarias poseían con anterioridad, lo que demuestra un desfase con respecto a la industria y, de esta manera, afecta su imagen corporativa. Por lo tanto, investigar el manejo de otras instituciones sobre la gestión de fraude con énfasis en la imagen corporativa se prevé de gran valor para fortalecer los procesos en el BCR.

Con estas oportunidades de mejora, la investigación propuesta se torna pertinente y necesaria para ampliar el conocimiento en los procesos de gestión preventiva del fraude en medios digitales y su consecuente efecto en la imagen corporativa del Banco de Costa Rica.

Objetivos

Objetivo general

Fortalecer la imagen corporativa del Banco de Costa Rica por medio de una propuesta de gestión del riesgo por fraude en medios digitales a través del análisis y evaluación de su control actual.

Objetivos específicos

1. Determinar la teoría sobre los tipos de fraude a través de medios digitales y buenas prácticas que se implementan por parte del sector bancario nacional e internacional, con respecto a la gestión del riesgo asociado y el efecto en su imagen corporativa.
2. Describir el contexto del Banco de Costa Rica en el sector bancario nacional, así como su gestión del riesgo por fraude a través de medios digitales y el impacto en su imagen corporativa.

3. Identificar las oportunidades de mejora en la gestión del riesgo por fraude a través de medios digitales presentes en el Banco de Costa Rica que impactan su imagen corporativa.
4. Elaborar lineamientos de gestión del riesgo por fraude a través de medios digitales, que coadyuven al fortalecimiento de la imagen corporativa del Banco de Costa Rica.
5. Establecer conclusiones y recomendaciones para que se mejore la gestión del riesgo por fraude a través de medios digitales que coadyuven al fortalecimiento de la imagen corporativa del Banco de Costa Rica.

Alcances

La presente investigación tiene como alcance el análisis de la gestión del riesgo por fraude a través de los medios digitales en el Banco de Costa Rica y su impacto en la imagen corporativa, así como identificar opciones de mejora en la gestión para desarrollar una propuesta que fortalezca esta imagen. Esta investigación aborda estos temas, con el fin de fortalecer la imagen de la entidad por medio de una propuesta que incluye los mecanismos que puede implementar para una gestión correcta del riesgo por fraude en medios digitales en su fase preventiva, de detección en tiempo real y de seguimiento posterior al hecho.

Cabe destacar que en la investigación no se aborda el *onboarding* digital, ya que son mecanismos de seguridad mucho más avanzados que no se utilizan en el país para la banca como la tecnología biométrica para reconocimiento óptico y la videoidentificación para la solicitud de servicios. Al finalizar la investigación, se le entrega al banco la propuesta que se mencionó orientada a mejorar la gestión por riesgo a través de medios digitales.

Limitaciones

Con respecto a las limitaciones que pueden presentarse durante la investigación, se interponen:

- Al ser una entidad bancaria, se rige bajo regulaciones estrictas en el manejo de la información. Por lo tanto, cierta parte de la información puede no ser compartida.
- La implementación de la viabilidad de la propuesta es determinada por el Departamento de Prevención de Fraudes.
- Por la naturaleza del objeto de estudio, la información puede resultar cambiante a través del tiempo.
- Debido a la coyuntura actual de la pandemia de la COVID-19 se pueden presentar limitaciones en el momento de aplicar los instrumentos y técnicas de recolección de datos.

Capítulo I. Fundamentación teórica y mejores prácticas

El presente capítulo detalla un panorama general del fraude cibernético y sus tipos. Asimismo, se definen varios conceptos como gestión de riesgo, imagen corporativa, medios digitales y banca. Por último, se describen los modelos de gestión del riesgo que utilizan las instituciones financieras.

1.1. Marco conceptual

1.1.1. Fraude cibernético

El fraude cibernético (también conocido como fraude electrónico o fraude digital) se define como un engaño que se lleva a cabo deliberadamente para asegurar una ganancia injusta o ilegal, en la cual alguna parte de la comunicación entre la víctima y el defraudador es por medio de una red computacional, o alguna acción se realiza en una red computacional (Bergman, 2005).

A la vez, el Centro de Denuncias de Crímenes por Internet define el crimen por Internet como cualquier actividad ilegal que involucra uno o más componentes del Internet, como sitios web, grupos de *chat* o correos electrónicos. El crimen por Internet involucra su uso para comunicar representaciones falsas o fraudulentas a las personas consumidoras (IC3, 2020). De acuerdo con los conceptos descritos y para efectos de esta investigación, se define fraude electrónico como el acto de defraudar a una persona a través de cibermedios, con el fin de obtener una ganancia ilegal o injusta.

1.1.1.1. Tipos de fraude cibernético

Primero, se detallan los dos grandes grupos en que se separan los tipos de fraudes cibernéticos, con base en quién provee el objeto de valor de la transacción y, seguidamente, se clasifican los métodos que se utilizan que son objeto del estudio.

1.1.1.1.1. Fraude en segunda persona

Este tipo de crimen se da cuando es: “La misma persona defraudada, quien en virtud del engaño que obra sobre ella, entrega al defraudador la cosa objeto del delito” (Centro de Información Jurídica en Línea, 2009, s. p.), es decir, a través de algún tipo de promesa la persona usuaria del banco envía libremente sus fondos a otra cuenta sin que haya de por medio un punto en el que el estafador tenga acceso a la cuenta del ofendido. En meses recientes ha tomado auge un ejemplo de este tipo de fraude llamado estafa por Sinpe Móvil que:

> Consiste en la falsificación del comprobante de pago [de algún artículo o servicio que tuviera a la venta], el cual es mostrado por el estafador al beneficiario del pago, quien confía y no verifica el ingreso de fondos a su cuenta bancaria (Banco Central de Costa Rica, 2021, s. p.).

1.1.1.1.2. Fraude en tercera persona

Este se refiere a cuando: “El cliente legítimo no tiene ningún conocimiento de la actividad fraudulenta […]. El estafador se hace pasar por su identidad y utiliza sus datos de la vida real para engañar a su banco o cualquier otra entidad” (Feedzai, 2022, s. p.). Para llegar a este punto, el criminal requiere tener acceso a la cuenta e información del cliente y para conseguirlo usa varios métodos que a continuación se detallan:

1.1.1.1.2.1. Ingeniería social

Esta consiste en: “Obtener información confidencial a través de la manipulación de usuarios legítimos […]. El principio que sustenta la ingeniería social es que en cualquier sistema los usuarios son el eslabón débil” (Banco Nacional, 2021, s. p.).

La ingeniería social es una forma de engaño que se utiliza por personas con un alto grado de convencimiento, que al igual que en la mayoría de las estafas seleccionan una víctima y estudian detalles sobre ella, como el lugar de residencia, trabajo, familiares, gustos, preferencias y planean cómo convencerlas para que les

faciliten información o realicen actividades. Todo esto con el fin de ejecutar un fraude.

1.1.1.1.2.2. Suplantación de identidad (phishing)

El Banco de Costa Rica (2021) lo define como la creación de sitios fraudulentos en Internet que son copias del sitio oficial de una institución financiera, por ejemplo, un banco. Usualmente, se distribuyen correos electrónicos que incluyen un enlace (*link*) al sitio fraudulento y motivan al usuario a que ingrese, ya sea utilizando mensajes amenazantes o motivantes para de esta forma obtener información confidencial del usuario.

1.1.1.1.2.3. Spear phishing

De acuerdo con Kaspersky (2020):

> El spear phishing es una estafa de correo electrónico o comunicaciones dirigida a personas, organizaciones o empresas específicas. Aunque su objetivo a menudo es robar datos para fines maliciosos, los cibercriminales también pueden tratar de instalar malware en la computadora de la víctima (s. p.).

1.1.1.1.2.4. Suplantación de identidad (vishing)

Este se refiere a una variante del phishing que:

> Consiste en el uso del Protocolo Voz sobre IP (VoIP) y de la ingeniería social para engañar personas y obtener información delicada como puede ser información financiera o información útil para el robo de identidad. El término es una combinación del inglés *voice* (voz) y *phishing* (Grupo UTE, 2016, s. p.).

1.1.1.1.2.5. Smishing

Según el Banco de Costa Rica (2021) este consiste en el envío de mensajes de texto por medio del cual se solicita y convencen a los usuarios de entregar información confidencial como número de cuenta, PIN, clave de acceso, código de seguridad y otros con los cuales posteriormente pueden efectuar el fraude.

Recientemente, tomó mucho auge que se envían estos mensajes a través de plataformas como WhatsApp.

1.1.1.1.2.6. Secuestro de información (ransomware)

El *ransomware* es:

> Un programa que se transmite como un troyano o gusano y provoca que el usuario afectado tenga acceso restringido a partes o archivos del sistema infectado. El creador del ransomware solicitará entonces un pago para proporcionar acceso a dichos datos (Banco Nacional, 2021, s. p.).

1.1.1.1.2.7. Skimming

Este tipo de fraude requiere la clonación física de una tarjeta de crédito. Lo cual:

> Se realiza a través de un dispositivo que contiene un chip el cual permite copiar la información de las bandas magnéticas simplemente arrastrando la tarjeta a través de él. Dicho dispositivo recibe el nombre de skimmer. Mediante él, los datos se traspasan a un computador y son copiados a una tarjeta virgen, lo que se conoce como Skimming (Yopo Díaz, 2012, s. p.).
>
> Este tipo de fraude puede entrar en la categoría de cibernético si la información de la tarjeta clonada se utiliza a través de medios digitales.

1.1.1.1.2.8. Redes sociales/angler fishing

Según el Banco Nacional (2021) el fraude a través de redes sociales se ha intensificado con el paso de los años y este consiste en el uso de la ingeniería social en las redes sociales para obtener información de sus usuarios, con el fin de utilizarla de manera fraudulenta.

1.1.1.1.2.9. Pharming

Se trata de un *malware* que, cuando la persona usuaria digita la dirección oficial del banco, redirige a un sitio fraudulento (Banco de Costa Rica, 2021).

1.1.1.1.2.10. Sitios fraudulentos

Este consiste en:

La creación de páginas de internet fraudulentas que pueden o no mostrarse como publicidad en páginas oficiales con el fin de engañar al usuario y generar que caiga en error para que ingrese a ellas y en las cuales se utiliza el engaño para pedir información sensible de los usuarios, a cambio de un premio o remuneración inexistente (Banco Nacional, 2021, s. p.).

1.1.1.1.2.11. Baiting

De acuerdo con Cortés Hernández (2019):

Consiste en dejar dispositivos de almacenamiento extraíble (CD, DVD, USB) conteniendo algún software infectado en algún lugar a la vista (por ejemplo, baños públicos, ascensores, aceras, etc.), esperando a que alguien los recoja y conecte a su dispositivo. De esta forma un software malicioso se instalará y permitirá que el hacker obtenga los datos personales del usuario (p. 3).

1.1.1.1.2.12. Man in the Middle (MiTM)

En español se traduce como *hombre en el medio*. Según Malenkovich (2013), en este tipo de fraude el atacante se sitúa entre las dos partes que intentan comunicarse, interceptando los mensajes enviados e imitando al menos a una de ellas, pasando totalmente desapercibido para alcanzar con éxito la meta de obtener información confidencial para cometer después un delito.

1.1.1.1.2.13. Capturador de claves (key logger)

Se define como un tipo de *software* o un dispositivo *hardware* específico que se encarga de registrar las pulsaciones que se realizan en el teclado, para posteriormente memorizarlas en un archivo o enviarlas a través de Internet. Estos dispositivos suelen usarse en computadoras de uso público, como en un hotel o en los llamados café Internet (Banco Nacional, 2021).

1.1.1.1.2.14. Sniffing

Según Mendoza y Rodríguez (2010), este tipo de fraude consiste en escuchar los datos que atraviesan la red sin interferir con la conexión a la que corresponden, principalmente para obtener contraseñas o información confidencial.

1.1.2. Gestión de riesgo

Según García y Salazar, la gestión integral de los riesgos es un: "Proceso estructurado, consistente y continuo, implementado a través de toda la organización para identificar, evaluar, medir y reportar amenazas y oportunidades que afectan el poder alcanzar el logro de sus objetivos" (s. p.). Asimismo, explican que puede definirse como la: "Identificación, medición y evaluación colectiva de todos los riesgos que afectan el valor de la entidad financiera, así como la definición e implementación de una estrategia en el negocio y en la operación para gestionar efectivamente esos riesgos" (García y Salazar, 2005, s. p).

Para efectos de esta investigación, la gestión del riesgo se define como el procedimiento establecido para identificar, evaluar y reportar posibles riesgos o amenazas para una entidad, así como las posibles oportunidades de esta por implementar. La definición de medidas para tratarlos puede tomarse de la ISO 31000, la cual trata sobre una: "Norma internacional que ofrece las directrices y principios para gestionar el riesgo de las organizaciones" (ISOTools, 2020, s. p).

La norma anterior se basa en el COSO (Committee of Sponsoring Organization of Treadway Commission) y tiene por objetivo que las organizaciones, sin importar su tamaño, puedan gestionar los riesgos de estas, de una manera efectiva. Lo anterior se hace desarrollando, implementando y mejorando el proceso de gestión de riesgos en cada actividad que realiza la empresa.

1.1.3. Tipos de mecanismos de seguridad

Antes de brindar una definición y mencionar los distintos tipos de mecanismos de seguridad que van a tratarse en la investigación es importante definir seguridad informática. Para Baca Urbina (2016) se define como:

> La disciplina que, con base en políticas y norma internas y externas de la empresa, se encarga de proteger la integridad y privacidad de la información que se encuentra almacenada en un sistema informático, contra cualquier tipo de amenazas, minimizando los riesgos tanto físicos como lógicos, a los que está expuesta (p. 12).

Para establecer un sistema seguro, la información tiene que cumplir una serie de propiedades fundamentales como está indicado en el Marco de gestión y de negocio global para el gobierno y la gestión de las TI de la empresa (Cobit), entre las cuales menciona: integridad, eficacia, eficiencia, confidencialidad, disponibilidad, cumplimiento y confiabilidad. Baca Urbina (2016) da una definición a cada una de estas propiedades:

- Integridad: que la información que se recibe sea precisa y esté completa para lograr su procesamiento.
- Confidencialidad: en todas las etapas del procesamiento la información se encuentra protegida contra accesos que no se autorizan.
- Efectividad: toda la información que sea necesaria para desarrollar cualquiera de las tareas propuestas.
- Eficiencia: que la información se genere y se utilice con los recursos necesarios que posee la empresa.
- Disponibilidad: que la información esté a mano cuando se requiera.
- Cumplimiento/apego a estándares: al procesar la información se tienen que tomar en cuenta las leyes, acuerdos internos y contractuales a la que está sometida.
- Confiabilidad: que la información no ha sido alterada de ninguna forma.

Teniendo un acercamiento sobre la seguridad informática y las variables de la información, se puede entender con facilidad el concepto de mecanismos de seguridad, este es parte fundamental del trabajo de investigación. Está definición

práctica y sencilla la proporciona Guamán Sinchi (2014) que los define como: “Herramientas, técnicas o métodos utilizados para mantener la disponibilidad, confidencialidad y la integridad de un sistema informático” (p. 17).

Definido el concepto de mecanismos de seguridad, es importante resaltar la existencia de una norma que se relaciona con la seguridad informática, como la ISO 27000, la cual brinda una perspectiva general de los sistemas de gestión de seguridad de la información (SGSI). Los SGSI se definen como: “Una serie de políticas, procedimientos e instrucciones o directrices específicas para cada actividad o sistema de información que persiguen como objetivo la protección de los activos de información en una organización” (ISO 27000, 2018). Estos sistemas poseen un proceso sistemático detallado a continuación:

- Se planifica la seguridad de la información, estableciendo los procesos y objetivos por alcanzar.
- Se implementa la seguridad de la información en los procesos.
- Se mantienen estables los procesos establecidos para la seguridad de la información.
- Se miden los resultados.
- Se detalla la eficacia de los procesos.
- Se analizan los resultados para establecer nuevas metas.

En la actualidad, los SGSI resultan esenciales para todas las empresas, ya que la información desempeña un rol importante para obtener los objetivos y, al mismo tiempo, se encuentra expuesta a riesgos físicos o que se relacionan con la tecnología. Aunque en todas las compañías es relevante, resulta vital para las empresas que se dedican al comercio electrónico o la banca por la información confidencial de sus clientes.

Para la investigación es importante mencionar los tipos de mecanismos de seguridad existentes. Para Moreno Granados (2018) se divide en cuatro grandes

grupos: preventivos, detectores, correctivos y disuasivos, los cuales se detallan a continuación:

- Mecanismos preventivos: son los encargados de prevenir cualquier tipo de ataque informático y su función está dada en el monitoreo constante de la información. Un ejemplo de este mecanismo son los antivirus.

- Mecanismos detectivos: detectan todas las posibles amenazas para los bienes de una compañía o de un usuario. Deben actuar antes de que la amenaza se inicie. Un ejemplo de este mecanismo es el personal operativo del sistema.

- Mecanismos correctivos: son los encargados de corregir cualquier anormalidad o daño producto de un ataque en los sistemas.

- Mecanismos disuasivos: son los encargados de evitar a los ejecutores de los ataques para lograr un daño mínimo en los sistemas. Los ejemplos de estos mecanismos son identificación digital, contraseña de seguridad, biométrica, firma digital y llaves.

De los ejemplos mencionados entre los grupos de mecanismos de seguridad, es relevante definir algunos de más conocidos en el ámbito general. Aguilera (2010) da una definición sencilla:

- Control de acceso: la forma de ingresar a distintos sitios mediante nombres de usuario y contraseñas.

- Cifrado de datos: también llamada encriptación, en donde los datos se esconden bajo un algoritmo de encriptación y el emisor y receptor son los únicos conocedores de la clave para acceder a ellos.

- Antivirus: capaces de detectar y proteger los datos y sistemas de la entrada de virus y otros *software* maliciosos que tratan de acceder a datos confidenciales.

- Firewall: son dispositivos de *software* o *hardware* que impiden el acceso a los sistemas.
- Firma digital: su función es la identificación segura de la persona o al equipo, el cual se hace responsable del mensaje o documento.
- Certificados digitales: son documentos digitales que tienen respaldo de una institución que garantiza que la persona o empresa sea quien indica ser y, de este modo, se logre la integridad de la información.

Por último, es importante mencionar los mecanismos de seguridad con los que cuenta el Banco de Costa Rica y otras entidades en la actualidad:

- Control por lugar de acceso: este proceso limita el acceso a la banca en línea desde Costa Rica o el exterior.
- Frase de seguridad: es una frase de bienvenida para evitar que las personas ingresen a páginas clonadas del Banco.
- Código de identificación: para ingresar a la página web siempre se le solicitará la cédula y una clave de acceso.
- Clave dinámica: es una tarjeta impresa con valores distintos que son solicitados siempre al ingreso del sitio web del Banco.
- Firma digital: puede ingresar al sitio web utilizando la firma digital y con esto tener mejor control de acceso.
- Token o clave virtual: aplicación móvil que genera una clave de varios dígitos cada 30 o 60 segundos para realizar transacciones en las plataformas virtuales.
- Mensaje código confirmación: mensajes que se generan automáticamente en el momento que se haga una transacción con tarjetas de débito o crédito de las distintas entidades.

- Doble autenticación: metodología de autenticación que, además de requerir un nombre de usuario y contraseña, solicita el ingreso de un segundo factor, el cual puede ser un código de seguridad o un dato biométrico para que la autenticación sea exitosa (Corrales, 2014).

1.1.4. Imagen corporativa

Según Fodymanow (2016), la imagen corporativa es el: “Aspecto general de una corporación, empresa o negocio en la mente de clientes, inversores y empleados”. Asimismo, menciona que es: “Indispensable para cada negocio construir una identidad, para lograr objetivos de negocio” (Fodymanow, 2016, s. p.).

De acuerdo con Margulies (citado en Currás Pérez, 2010), la imagen corporativa se puede definir como: “Los mecanismos que una empresa elige para identificarse ante sus stakeholders, la comunidad, clientes, trabajadores y medios” (s. p.). Además, en el mismo texto citó a Abratt (citado en Currás Pérez, 2010), con la definición de imagen corporativa que es: “Lo que una audiencia puede reconocer de una empresa y distinguirla de las otras, y que puede ser utilizado para representar o simbolizar a la compañía” (s. p.).

Para efectos de esta investigación, se define imagen corporativa como la identidad ante la comunidad, clientes, trabajadores y medios, con relación a su compromiso y esfuerzos para asegurar una protección adecuada del patrimonio e información de sus clientes.

1.1.5. Medios digitales

Los medios digitales se consideran un medio de comunicación que tiene la misma función que los medios impresos, radiofónicos y televisivos. Además, se llama cibermedio, definido según Linares, Codrina y Pedraza (citados por Cabral Vargas, 2018) como: “Un medio de comunicación que utiliza una plataforma digital interactiva en línea, bien en forma de sitio web o bien en forma de aplicación para la web móvil” (p. 4). Asimismo, cabe destacar la recopilación de conceptos realizada por Cabral Vargas (2017) sobre el término de medios digitales:

Figura 1
Conceptos sobre medios digitales

Autores	Definiciones
(Moscoso 1998, 329).	Medios y bienes que permiten adquirir, precisar o comunicar conocimientos, con el fin de resolver una necesidad o llevar a cabo una empresa.
(Berestova 2016, 86).	Una forma de almacenamiento a largo plazo, es decir, una manera para replicar y transportar el significado expresado en caracteres legibles por el ser humano y por una máquina.
(Villaseñor 1998, 30).	Instrumentos que usa o crea el profesional de la información para satisfacer las demandas y necesidades informativas de los usuarios de cualquier unidad informativa, ya sea un archivo, una biblioteca o un centro de documentación.
(Soy I Aumatell 2012).	El concepto de recurso de información comprende fuentes formales o informales (un individuo, una organización o un documento), servicios y sistemas de información.

Fuente: Cabral Vargas (2017, p. 4).

Para efectos de esta investigación, se define como el medio o instrumento de almacenamiento y razón de la información para resolver necesidades del usuario, de forma remota.

1.1.6. Definición de la banca

La banca es una institución que se encarga de la intermediación financiera. Definida según Escoto Leiva (2001) como: “El servicio que se hace para contactar a los poseedores de recursos financieros (dinero, bienes de capital, captación de recursos, etc.) con aquellas personas físicas o jurídicas que necesitan dichos recursos financieros (préstamos) para utilizarlos y generar utilidades” (p. 32). En el caso específico de la banca en el ámbito de Costa Rica, Escoto Leiva (2001) la define como: “El establecimiento público o privado autorizado para ejercer las actividades bancarias con sus recursos propios o ajenos” (p. 31).

Al ser el Banco de Costa Rica el objeto de estudio es importante mencionar algunos puntos fundamentales que posee la Banca Estatal Costarricense, estos son para Escoto (2001):

- Colaboran para ejecutar la política monetaria, cambiaria, crediticia y bancaria.

- Procurar liquidez, solvencia y el buen funcionamiento del sistema bancario nacional.
- Custodiar y administrar los depósitos bancarios colectivos.
- Evitar que en el país existan medios de producción inactivos, tratando de llegar a los distintos sectores para ofrecer sus servicios.

1.1.7. Modelos de gestión de riesgo

1.1.7.1. COSO

González Martínez (s. f.) menciona que es un marco integrado de diseño, implementación y conducción del control interno, propuesto por el Comité de Organizaciones Patrocinadoras de la Comisión Treadway (COSO). Asimismo, este modelo surge para el mejoramiento del manejo de los recursos en cualquier tipo de organización como consecuencia de escándalos, fraudes y crisis financiera.

Se basa en 17 principios que son aplicables en el ámbito de entidad, operativo y funcional:

1. La organización demuestra compromiso con la integridad y los valores éticos.
2. El consejo de administración demuestra independencia de la dirección y ejerce la supervisión del desempeño del sistema de control interno.
3. La dirección establece con la supervisión del Consejo, las estructuras, líneas de reporte y los niveles de autoridad y responsabilidad apropiados para la consecución de los objetivos.
4. La organización demuestra compromiso para atraer, desarrollar y retener a profesionales competentes, en concordancia con los objetivos de la organización.
5. La organización define las responsabilidades de las personas a nivel de control interno para la consecución de los objetivos.
6. La organización define los objetivos con suficiente claridad para permitir la identificación y evaluación de los riesgos relacionados.

7. La organización identifica los riesgos para la consecución de sus objetivos en todos los niveles de la entidad y los analiza como base sobre la cual determina cómo se deben gestionar.
8. La organización considera la probabilidad de fraude al evaluar los riesgos para la consecución de los objetivos.
9. La organización idéntica y evalúa los cambios que podrían afectar significativamente al sistema de control interno.
10. La organización define y desarrolla actividades de control que contribuyen a la mitigación de los riesgos hasta niveles aceptables para la consecución de los objetivos.
11. La organización define y desarrolla actividades de control a nivel de entidad sobre la tecnología para apoyar la consecución de los objetivos.
12. La organización despliega las actividades de control a través de políticas que establecen las líneas generales del control interno y procedimientos.
13. La organización obtiene o genera y utiliza información relevante y de calidad para apoyar el funcionamiento del control interno.
14. La organización comunica la información internamente, incluidos los objetivos y responsabilidades que son necesarios para apoyar el funcionamiento del sistema de control interno.
15. La organización se comunica con los grupos de interés externos sobre los aspectos clave que afectan al funcionamiento del control interno.
16. La organización selecciona, desarrolla y realiza evaluaciones continuas y/o independientes para determinar si los componentes del sistema están presentes y funcionando.
17. La organización evalúa y comunica las deficiencias de control interno de forma oportuna a las partes responsables de aplicar medidas correctivas, incluyendo la alta dirección y el consejo, según corresponda (González Martínez, s. f., s. p.).

1.1.7.2. Modelo de las tres líneas de defensa

Este es uno de los modelos de riesgo más reconocidos y aceptados en la industria financiera. Evolucionó durante y después de los 90 cuando la industria del Internet expuso la amplitud y profundidad del panorama de riesgo. El modelo se desarrolló para identificar claramente los roles y responsabilidades de las unidades de negocio, practicar una constante gestión de riesgo y sostener actividades de gestión de riesgo (Telem, 2016).

El modelo gira en torno a tres líneas o grupos que en conjunto buscan mitigar o eliminar cualquier riesgo latente. Como se detalla en la imagen siguiente, la primera línea la lidera la Gerencia, la segunda se trata de los distintos aspectos definidos por la administración para el control del riesgo y en la última línea se presenta una auditoría interna que es independiente de las dos primeras líneas. Además de esto, el modelo también resalta la participación en el coaccionar y definición de tareas de las tres líneas a la alta gerencia y el gobierno corporativo, de forma tal que por su diseño pueda auditarse por organismos de control o auditores externos.

Figura 2
El modelo de las tres líneas de defensa

Adaptado de la Guía emitida por ECIIA/FERMA sobre la
8va Directiva de Derecho de Sociedades de la Unión Europea, artículo 41

Fuente: The Institute of Internal Auditors (IIA, 2013).

A continuación, se detalla en profundidad el proceder de cada una de las líneas de defensa:

1.1.7.2.1. Primera línea de defensa: la gestión operativa

Al tratarse la parte de la organización donde ocurren los procesos operativos (por ejemplo, interacción con los clientes, transferencia de fondos, manejo de inventario, etc.), la Gerencia operativa.

> Es responsable de mantener un control interno efectivo y de ejecutar procedimientos de control sobre los riesgos de manera constante en el día a día. La gerencia operativa identifica, evalúa, controla y mitiga los riesgos, guiando el desarrollo e implementación de políticas y procedimientos internos que aseguren que las actividades efectuadas son consistentes con las metas y objetivos. A través de una estructura de responsabilidad distribuida en cascada, los gerentes de nivel medio diseñan e implementan procedimientos detallados que sirven como controles y supervisan la ejecución de tales procedimientos por parte de sus empleados (IIA, 2013, p. 3).

1.1.7.2.2. Segunda línea de defensa: Funciones de gestión de riesgo y cumplimiento

Esta segunda línea vela por la implementación y cumplimiento a cabalidad de los controles de riesgos por parte de la Gerencia operacional (primera línea de defensa). Según el Instituto de Auditores Internos (IIA, 2013) las funciones específicas varían de acuerdo con la organización e industria, aunque las funciones típicas de esta segunda línea de defensa comprenden:

> • Una función de gestión de riesgos (y/o comité) que facilita y monitorea la implementación de prácticas efectivas de gestión de riesgos por parte de la gerencia operativa y que asiste a los propietarios del riesgo en la definición del objetivo de exposición al riesgo y en la presentación adecuada de información relacionada con riesgos a toda la organización.
> • Una función de cumplimiento para monitorear diversos riesgos específicos

tales como el incumplimiento de leyes y regulaciones aplicables. Con esta capacidad, esta función independiente reporta directamente a la alta dirección y en algunos sectores económicos, directamente a los organismos de gobierno corporativo.

• Una función de contraloría que monitorea riesgos financieros y la emisión de la información financiera (s. p.).

1.1.7.2.3. Tercera línea de defensa: funciones de auditoría interna

Al ver que la segunda línea de defensa trabaja relacionada con la primera para asegurarse de que se cumpla con los controles de gestión de riesgo, se vuelve necesaria una tercera línea que vele exclusivamente por verificar que la ejecución de la gestión se dé de manera correcta y en concordancia con las políticas de la alta gerencia y el gobierno corporativo.

De acuerdo con la IIA (2013), este aseguramiento que se reporta a los organismos de gobierno corporativo y alta dirección usualmente cubre:

• Un amplio rango de objetivos, incluyendo la eficiencia y efectividad de las operaciones, salvaguarda de activos, confiabilidad e integridad de los procesos de reporte, y cumplimiento con leyes, regulaciones, políticas, procedimientos y contratos.

• Todos los elementos de los marcos de gestión de riesgos y control interno, que incluyen: ambiente de control interno, todos los componentes del marco de gestión de riesgos de la organización (por ejemplo, identificación de riesgos, evaluación de riesgos y respuesta), información y comunicación, y monitoreo.

• La entidad en su conjunto, divisiones, subsidiarias, unidades operativas y funciones – incluyendo procesos de negocios, tales como ventas, producción, *marketing*, seguridad, funciones de clientes, y operaciones – como también funciones de soporte (por ejemplo, contabilización de ingresos y gastos, recursos humanos, adquisiciones, remuneraciones, presupuestos, gestión de infraestructura y activos, inventario, y tecnología de la información) (s. p.).

1.1.7.3. Modelo de las tres líneas

Este es un nuevo modelo para la gobernanza y gestión de riesgo lanzado en julio del año 2020 por el IIA. El modelo surge de la actualización del modelo mencionado de las tres líneas de defensa. La palabra *defensa* deja de ser parte del nombre del modelo al reconocerse que la toma de decisiones que se basa en riesgo no es solo para medidas defensivas, sino también sobre el aprovechamiento de las oportunidades, con el fin de apoyar a las organizaciones para que alcancen sus objetivos (Babinchak, 2020). Cabe mencionar también la inclusión en el modelo en un sentido más amplio y específico de las relaciones entre los roles participantes, la inclusión de principios para seguir y la definición de roles específicos fundamentales para su aplicación correcta.

Figura 3
El modelo de las tres líneas del IIA

Fuente: Fundación Latinoamericana de Auditores Internos (FLAI, 2020).

1.1.7.3.1. Principios del modelo de las tres líneas del IIA

El nuevo modelo innova al incorporar principios para describir su funcionamiento. Esto ayuda a que soporte coyunturas más dinámicas y variables que enfrentan las organizaciones en la actualidad, debido a la complejidad de estas y la alta volatilidad del riesgo.

Tabla 1
Principios del modelo de las tres líneas del IIA

Roles	Descripción
1. Gobierno	El gobierno de una organización requiere de estructuras y procesos apropiados para: • Rendición de cuentas a través de la integridad, liderazgo y transparencia a las partes interesadas que la supervisen. • Toma de acciones con base en riesgo y la aplicación de recursos para lograr los objetivos de la organización. • Aseguramiento y asesoramiento por parte de un rol de auditoría interna para proporcionar claridad y confianza
2. Roles del órgano de gobierno	• Se asegura que se han establecido estructuras y procesos adecuados para un gobierno eficaz y que los objetivos y actividades de la organización están alineados con los intereses prioritarios de las partes interesadas. • Delega la responsabilidad y proporciona recursos a la dirección para alcanzar los objetivos de la organización mientras que asegura que se cumplan las expectativas legales, regulatorias y éticas. • Establece y supervisa un rol de auditoría interna independiente, objetiva y competente para proporcionar claridad y confianza en el progreso hacia el logro de los objetivos.
3. Dirección y roles de primera y segunda línea	La responsabilidad de la dirección de alcanzar los objetivos organizativos comprende, tanto los roles de primera como los de segunda línea. • Los roles de primera línea se alinean más directamente con la entrega de productos o servicios a los clientes de la organización, lo que incluye los roles de soporte. • Los roles de segunda línea proporcionan asistencia en la

	gestión del riesgo. Los roles de primera y segunda línea pueden mezclarse o separarse. Los roles de segunda línea pueden centrarse en objetivos específicos de la gestión de riesgos, como el cumplimiento de las leyes, las regulaciones y el comportamiento ético aceptable; el control interno; la seguridad de la información y la tecnología; la sostenibilidad y el aseguramiento de la calidad.
4. Roles de tercera línea	La auditoría interna proporciona aseguramiento y asesoramiento independientes y objetivos sobre la adecuación y eficacia del gobierno y la gestión de riesgos. Informa de sus conclusiones a la Gerencia y al órgano de gobierno para promover y facilitar la mejora continua. Al hacerlo, puede considerar el aseguramiento de otros proveedores internos y externos.
5. Independencia de tercera línea	La independencia de la auditoría interna de las responsabilidades de la Gerencia es fundamental para su objetividad, autoridad y credibilidad. Se establece mediante la rendición de cuentas ante el órgano de gobierno, el acceso sin restricciones a las personas, los recursos y los datos necesarios para completar su trabajo y la ausencia de prejuicios o interferencias en la planificación y prestación de servicios de auditoría.
6. Creación y protección del valor	Todos los roles que trabajan juntos contribuyen colectivamente a la creación y protección del valor cuando están alineados entre sí y con los intereses prioritarios de las partes interesadas. La alineación de las actividades se logra mediante la comunicación, la cooperación y la colaboración. Esto asegura la fiabilidad, coherencia y transparencia de la información necesaria para la toma de decisiones basada en el riesgo.

Fuente: Elaboración propia con base en información de la Fundación Latinoamericana de Auditores Internos (FLAI, 2020).

1.1.7.3.2. Roles clave del modelo de las tres líneas del IIA

Otra gran mejora que se incluye en este nuevo modelo es la definición clara de los roles de varios líderes en la organización que incluye la supervisión por parte del gobierno corporativo, de líderes administrativos y operacionales de riesgo y cumplimiento (roles de primera y segunda línea) y el aseguramiento independiente

a través de la auditoría interna (tercera línea) y también define la posición de los proveedores de aseguramiento externo (Babinchak, 2020).

Tabla 2
Roles clave del modelo de las tres líneas del IIA

Principio	Descripción
1. El órgano de gobierno	• Acepta la rendición de cuentas a las partes interesadas por la supervisión de la entidad. • Se compromete con las partes interesadas para vigilar sus intereses y comunicarse, de forma transparente, sobre el logro de los objetivos. • Nutre una cultura que promueve el comportamiento ético y la rendición de cuentas. • Establece estructuras y procesos de gobierno, lo que incluye a los comités auxiliares, según sea necesario. • Delega la responsabilidad y proporciona recursos a la dirección para alcanzar los objetivos. • Determina el grado de aceptación del riesgo de la entidad y supervisa la gestión del riesgo (lo que incluye el control interno). • Supervisa el cumplimiento de las expectativas legales, reglamentarias y éticas. • Establece y supervisa un rol de auditoría interna independiente, objetiva y competente.
2. Dirección	Roles de primera línea ● Dirige y orienta las acciones (lo que incluye la gestión del riesgo) y la aplicación de recursos para alcanzar los objetivos de la organización. ● Mantiene un diálogo continuo con el órgano de gobierno e informa sobre los resultados previstos, reales y esperados que se vinculan con los objetivos de la organización y el riesgo. ● Establece y mantiene estructuras y procesos adecuados para la gestión de operaciones y riesgos (lo que incluye el control interno). ● Garantiza el cumplimiento de las expectativas legales, reglamentarias y éticas. Roles de segunda línea

	● Proporciona conocimientos especializados complementarios, apoyo, vigilancia y cuestionamientos que se relacionan con la gestión del riesgo, entre otros: ● El desarrollo, la implementación y la mejora continua de las prácticas de gestión de riesgos (lo que incluye el control interno) en el ámbito de procesos, sistemas y entidades. ● El logro de objetivos de gestión de riesgos, como cumplimiento de leyes, reglamentos y comportamiento ético aceptable, control interno, seguridad de la información y la tecnología, sostenibilidad y aseguramiento de calidad. ● Proporciona análisis e informes sobre la adecuación y eficacia de la gestión de riesgos (lo que incluye el control interno).
3. Auditoría interna	● Mantiene la rendición de cuentas primaria ante el órgano de gobierno y la independencia de las responsabilidades de la dirección. ● Comunica el aseguramiento y asesoramiento independientes y objetivos a la dirección y al órgano de gobierno sobre la adecuación y eficacia de la gobernanza y la gestión de riesgos (lo que incluye el control interno) para apoyar el logro de los objetivos de la organización y promover y facilitar la mejora continua. ● Informa al órgano de gobierno las deficiencias en la independencia y la objetividad y aplica las salvaguardas necesarias.
4. Proveedores de aseguramiento externo	Proporcionar aseguramiento adicional para: ● Satisfacer las expectativas legislativas y reglamentarias que sirven para proteger los intereses de las partes interesadas. ● Satisfacer las solicitudes de la dirección y del órgano de gobierno de complementar las fuentes internas de aseguramiento.

Fuente: Elaboración propia con base en información de la Fundación Latinoamericana de Auditores Internos (FLAI, 2020).

1.2. Gestión del riesgo por fraude en el ámbito internacional a través de medios digitales

Vivimos en una era donde la conectividad y anonimato que ofrece la estructura favorece un incremento constante de los delitos informáticos.

El crimen en línea ya supone, aproximadamente, la mitad de todos los delitos

> contra la propiedad que tienen lugar en el mundo. A nivel agregado, las cifras adquieren aún mayor magnitud pues los daños económicos de los ataques cibernéticos podrían sobrepasar el 1% del producto interno bruto (PIB) en algunos países (BID, 2020, s. p.).

De acuerdo con la Organización de Estados Americanos (Organización de Estados Americanos, 2019):

> La frecuencia con la que las empresas de servicios financieros aseguran sufrir incidentes de seguridad es un 300 % superior a la de las compañías de otros sectores. Lo anterior hace que los temas de ciberseguridad sean muy importantes en el sector financiero, toda vez que, si los clientes y empresas no ven el entorno digital como un espacio confiable y seguro para sus interacciones, la desconfianza afectaría el uso de los canales digitales y, por lo tanto, todas las inversiones realizadas en procesos de digitalización de la experiencia del cliente no generaría el impacto positivo esperado (s. p.).

Según un reporte del Banco Interamericano de Desarrollo (BID, 2020) la región de América Latina y el Caribe todavía no está suficientemente preparada para enfrentar los ataques que se producen en el ciberespacio. Únicamente 7 países cuentan con un plan de protección de su infraestructura crítica y 20 han establecido algún tipo de grupo de respuesta a incidentes.

El mismo informe señala que en un tercio de los países no existe un marco legal sobre los delitos informáticos y únicamente cinco países de la región se han adherido a la Convención de Budapest, que facilita la cooperación internacional en la lucha contra el crimen informático. Para un delito que no conoce fronteras, trabajar junto con otros países es un factor indispensable para el éxito y el reporte expande que, hasta principios de 2020, solo 12 países habían aprobado una estrategia nacional de ciberseguridad (ver Figura 4) y únicamente 10 países han establecido un organismo gubernamental central responsable de la gestión de la ciberseguridad. Uno de los factores que limita el progreso de la región en la materia es la ausencia de talento humano calificado. La brecha de profesionales en ciberseguridad se estima en 600.000 personas en la región.

Figura 4
Países latinoamericanos con estrategia nacional de ciberseguridad

Fuente: Desafíos del riesgo cibernético en el sector financiero para Colombia y América Latina (OEA).

Debido a lo anterior, la Secretaría General de la Organización de los Estados Americanos (OEA), a través del Programa de Ciberseguridad Adscrito a la Secretaría del Comité Interamericano contra el Terrorismo (CICTE), promueve la:

> Agenda sobre ciberseguridad digital para las Américas, que se estructura en torno a tres (3) pilares: (i) el desarrollo normativo, especialmente el apoyo en la formulación, discusión y socialización de políticas nacionales de ciberseguridad; (ii) el fortalecimiento de capacidades para disfrutar de las oportunidades que aportan el desarrollo de las Tecnologías de la Información y las Comunicaciones (TIC), pero también para hacer frente a los riesgos asociados; y (iii) la ejecución de actividades de investigación y gestión del conocimiento en ciberseguridad (OEA, 2019, s. p.).

En un estudio que se lleva a cabo por parte de la OEA (2019):

> Se analizaron datos de 191 entidades bancarias en 19 países de la región (17% grandes, 48% medianas y 35% pequeñas) […]. Con relación a la preparación y gobernanza, el estudio concluye que la ciberseguridad se considera como una preocupación de alto riesgo para las instancias de decisión (juntas/consejos directivos) en las entidades bancarias de la región. No obstante, se encuentra que en la mayoría de este tipo de organizaciones

convencer a la alta dirección de la organización es medianamente complejo. Este sector se esfuerza por encontrar el talento adecuado e incorporar expertos cibernéticos en sus organizaciones dados los complejos desafíos actuales.

• En promedio, en el 74% de las entidades se tiene una única área responsable por la seguridad digital.

• En promedio, en el 72% de las entidades la junta directiva recibe reportes periódicos acerca de indicadores y gestión de riesgos.

• En promedio, en el 41% de las entidades en la región existen dos niveles jerárquicos entre el CEO y el máximo responsable de la seguridad digital.

• En promedio, más del 60% de las entidades demuestra apoyo a la gestión del riesgo de seguridad digital, exigiendo la adopción de buenas prácticas de seguridad y fomentando la capacitación y sensibilización en seguridad digital.

• Los estándares, mejores prácticas y marcos metodológicos más implementados son las normas ISO 27001 y COBIT.

• En promedio, el número de miembros del equipo destinado a la seguridad digital es de diecisiete (17), para un banco típico de la región y el 82% considera adecuado que el equipo crezca (s. p.).

Además, este estudio señala que:

> Los eventos de i) *phishing*, ii) ingeniería social, y, iii) *software* espía (*malware* o troyanos) fueron los más frecuentes contra sus usuarios de servicios financieros […] y el presupuesto destinado a la seguridad digital por una entidad bancaria promedio en la región equivale aproximadamente al 2,09% del EBITDA del año anterior […] y en total el costo de respuesta y de recuperación ante incidentes de seguridad digital para una entidad bancaria promedio en la región supone aproximadamente el 1,52% del EBITDA del año anterior (OEA, 2019, s. p.).

Por último, el mismo estudio de la OEA (2019) señala las siguientes recomendaciones a las entidades bancarias analizadas:

• La necesidad de contar con una instancia u órgano de gobierno corporativo para liderar los temas de ciberseguridad, con respaldo y esquema de reporte a las máximas instancias de decisión de las instituciones y que cuente con recursos adecuados para gestionar los riesgos de seguridad digital.

• La relevancia de hacer revisión habitual de mejores prácticas en marcos de gobierno, seguridad y/o estándares internacionales, así como del marco regulatorio local e internacional aplicable a los diversos sectores y entidades/instituciones financieras, haciendo un proceso de mapeo y priorización para su adecuada aplicación.

• La necesidad de priorizar el desarrollo de capacidades usando tecnologías digitales emergentes, tales como Big Data, Inteligencia Artificial y sus relacionadas (tales como computación cognitiva y Machine Learning), que tienen un importante potencial en la optimización de recursos destinados a la detección y prevención de riesgos de seguridad digital.

• La relevancia de participar activamente en alianzas en las que se logre compartir las conclusiones y lecciones aprendidas sobre la gestión de eventos (ataques exitosos y ataques no exitosos), que faciliten la identificación y prevención de delitos, así como el desarrollo de soluciones holísticas para gestionar el riesgo cibernético.

• La importancia de disponer planes de capacitación con públicos objetivos y específicos (empleados internos, insourcing, proveedores, clientes, nivel ejecutivo, etc.) que se orienten a elevar la cultura de seguridad digital, el desarrollo de capacidades y la sensibilización (según sea el caso), garantizando su ejecución periódica y estableciendo evaluaciones a efecto de determinar su impacto.

• La relevancia de comunicar estratégicamente a la alta dirección y órganos de gobierno que los recursos destinados a seguridad digital no son un costo, sino realmente una inversión y que la protección contra incidentes digitales debe ser parte integral de la estrategia de negocio, dado el alto impacto y repercusión que se pueden derivar de su ocurrencia. Estimar una tasa interna de retorno de las inversiones efectuadas en seguridad digital (s. p.).

1.3. Gestión del riesgo por fraude en el ámbito nacional a través de medios digitales

- Las tecnologías de información se han convertido en un elemento de suma importancia para el desarrollo financiero en el ámbito nacional y de Latinoamérica. Sin embargo, este elemento solo puede verse materializado si se da una gestión correcta del riesgo de la seguridad digital.

- En el ámbito nacional, se ha tenido apoyo de la Organización de los Estados Americanos (OEA) para la implementación y mejora de estrategias nacionales en seguridad digital, ya que, según estudios realizados a distintos países de la zona, no existe un nivel de preparación adecuado. Cabe destacar que OCDE (2016) menciona que Costa Rica se encuentra entre los únicos 11 países de la zona que cuenta con una legislación penal en temas de ciberseguridad, lo anterior con la creación del CSIRT-CR 2012 del Decreto Ejecutivo n.º 37052 del MICIT.

Con respecto a la gestión del riesgo en el ámbito financiero, se analizaron los informes anuales del 2021 de las tres principales entidades financieras de Costa Rica (El Financiero, 2019), lo que coloca al Banco de Costa Rica, Banco Nacional y BAC Credomatic como las entidades con mayores utilidades en el 2020.

El Banco de Costa Rica tiene una clasificación de riesgos divididos en dos secciones: financieros y no financieros. Esta investigación se enfoca en los no financieros y dentro de este rubro se encuentra la seguridad de la información y TI. En el informe anual se detalla que la gestión de este riesgo se realiza con un plan anual de evaluaciones que se relacionan con procesos, contratos, aplicativos, estrategia, servicios, plataformas y seguridad de TI (Banco de Costa Rica, 2021). En la gestión de este riesgo también se revisan y proponen, de forma periódica, indicadores de riesgo, logrando un mejor control y monitoreo de los riesgos a los cuales están expuestos.

A continuación, se mencionan las mejoras obtenidas en la gestión de riesgo tecnológico mencionadas en el informe:

- Aprobación de una nueva metodología para la evaluación de riesgo tecnológico y ciberriesgo.
- Adquisición de una nueva herramienta para la gestión de riesgo tecnológico, llamada Delphos Continuum.
- Nuevos indicadores de riesgos que se relacionan con aplicativos críticos.
- Capacitaciones dentro de la institución.

Por otra parte, el Banco Nacional tiene un modelo de gestión de riesgo que se basa en las tres líneas de defensa. La primera línea son las actividades que generan una exposición a los riesgos, la segunda línea es el control, supervisión y cumplimiento de riesgos y la tercera línea es la evaluación periódica de políticas, métodos y procedimientos (Banco Nacional, 2021). Al igual que el BCR, el Banco Nacional divide los riesgos en dos grupos: los financieros y no financieros. Sin embargo, el riesgo tecnológico lo incluyen dentro de un riesgo financiero.

La gestión de riesgo de la seguridad de la información y riesgo digital mantiene un perfil muy conservador, lo que promueve políticas que disminuyan las posibles pérdidas financieras, reputacionales o confidencialidad e integridad de la información. Entre las prácticas realizadas en el BNCR para mitigar estos riesgos se mencionan dentro del informe (Banco Nacional, 2021):

- El envío de mensajes internos y externos (clientes), tanto semanales como de alertas emergentes.
- Certificación anual en temas de seguridad de la información para el BNCR.
- Participación en charlas con clientes externos.
- Ejecución de talleres teórico-prácticos para áreas críticas del BNCR y material de concientización para la Dirección Corporativa de Desarrollo Humano.
- Ejecución de ejercicios de simulación de phishing para el BNCR
- Ejecución de ejercicios de intrusión junto con la Dirección de Tecnología.

Los puntos anteriores, junto con las mejores prácticas internacionales como la ISO27000, ISO31000, Cobit y la legislación nacional Sugef 14-17, han llevado al BNCR a estar en un nivel estable en el indicador de riesgo digital.

Por último, el BAC Credomatic maneja también una gestión de riesgo que se basa en las tres líneas de defensa y también regulaciones nacionales estipuladas por las Sugef. Sin embargo, entre los riesgos que la entidad define como relevantes no se mencionan riesgos que tengan relación con la parte digital o de seguridad de la información, lo que sugiere que entre sus prioridades no se encuentra este tipo de gestión de riesgo. El único punto que menciona algo relacionado con la seguridad tecnológica es en los logros que se obtienen en el 2021 (BAC Credomatic, 2021):

- Aplicación de mejoras en las herramientas para los sistemas de detección, monitoreo y prevención de fraude.

Con este punto se puede determinar que se realizaron mejoras en los sistemas de la seguridad digital, pero no se da mayor detalle. Esto deja la incertidumbre de por qué este no es un riesgo relevante para la institución.

1.4. Imagen corporativa en el sector bancario internacional

La imagen corporativa es importante para el éxito empresarial de sectores competitivos como la banca (Bravo, 2016). Por consiguiente, alrededor del mundo las empresas bancarias realizan esfuerzos para que la imagen corporativa de cada uno de estos sea impecable. En resumen, como menciona Ries y Ries (citados en Bravo, 2016): “La gestión de la identidad corporativa resulta especialmente relevante en el sector servicios, donde la ausencia de aspectos tangibles con los que evaluar la oferta dificulta su diferenciación” (s. p.).

Al mismo tiempo, las diferentes crisis financieras que han sucedido desde los años 70, así como la crisis del 2007 en Estados Unidos, han debilitado el sector financiero de muchas regiones del mundo. Sin embargo: “Existen también cuestiones vinculadas a la percepción del cliente sobre las entidades bancarias que se constituyen elementos esenciales en la construcción de una imagen corporativa

fuerte" (Delgado, 2015, s. p). Por esto, no basta con solo los esfuerzos de índole económica y financiera de las entidades bancarias para poseer una cartera robusta de clientes que confíen en ellos.

1.5. Imagen corporativa en el sector bancario nacional

En la Tabla 3 se enlista una recopilación de hechos mencionados por Alcázar *et al*. (2019), desde una perspectiva de ética, imagen, credibilidad y confianza de la banca nacional:

Tabla 3
Hechos que se relacionan con la imagen corporativa del sector bancario costarricense

Aspecto	Hecho
Normativa	"En Costa Rica existen leyes, reglamentos y procedimientos de control de las operaciones bancarias que se realizan en el territorio nacional, el incumplimiento de esta normativa ha generado situaciones como las del Banco Anglo Costarricense, BICSA, Bancrédito y el Banco de Costa Rica, donde el común denominador ha sido la mala toma de decisiones por parte de los jerarcas, influenciadas por el clientelismo, favoritismo y amiguismo, por encima de las buenas prácticas del gobierno corporativo" (Alcázar, 2020, s. p).
Ética	"Si se retoman los hechos sucedidos en los últimos cuatro años, quedan en evidencia grandes deficiencias en el comportamiento moral de los individuos encargados de la toma de decisiones en los altos puestos de los bancos, lo cual ha producido pérdidas económicas considerables y ha deteriorado significativamente dos de los principales activos intangibles de las instituciones de intermediación financiera: la confianza y la imagen" (Alcázar, 2020, s. p).
Confianza	"Reciente, situaciones como las denunciadas por los medios de comunicación en los últimos tres años con respecto a movimientos y operaciones cuestionables (por ejemplo, el caso de la importación de cemento chino en el cual se involucraron los bancos estatales junto con sus gobiernos corporativos) dañaron la buena imagen que por muchos años han construido las instituciones financieras estatales y quebrantaron la confianza de la sociedad en sus transacciones y mecanismos de control. Situaciones como estas abren una y otra vez en la memoria colectiva el fantasma del cierre

	del Banco Anglo Costarricense en septiembre de 1994” (Alcázar, 2020, s. p).
	“La reputación es el activo intangible más importante de una organización, especialmente la de índole financiera, ya que es la base de la confianza de los clientes y se percibe como un indicador de la eficiencia con la cual se desarrollan las acciones de la institución” (Alcázar, 2020, s. p).

Fuente: Elaboración propia, 2022.

Capítulo II. Situación actual del Banco de Costa Rica

2.1. Descripción de la organización

2.1.1. Reseña histórica

Según el sitio oficial del Banco de Costa Rica (2021a), este:

> Fue fundado el 20 de abril de 1877 con el nombre de Banco de la Unión, el cual mantuvo hasta 1890, cuando lo varió por el actual. Nació con el propósito de ser una nueva opción bancaria entre las ya existentes y tuvo como funciones iniciales el prestar dinero, llevar cuentas corrientes, recibir depósitos y efectuar cobranzas, entre otras. A sólo siete años de su fundación el Banco de Costa Rica se convirtió en el único emisor de dinero y el primer administrador de las rentas públicas, mediante un contrato que se denominó Soto-Ortuño y que tuvo vigencia hasta el año 1896.
>
> Otros acontecimientos económicos se fueron sucediendo con los años hasta que en 1928 descentraliza sus servicios, con la creación de sus primeras sucursales en los puertos de Limón y Puntarenas.
>
> En 1948 la Junta Fundadora de la Segunda República decretó la nacionalización de la banca, por lo que el Banco de Costa Rica se integró a ella hasta la fecha. Se define como institución autónoma, de acuerdo con el Artículo 189 de la Constitución Política de la República de Costa Rica, de 1949.
>
> Durante los últimos años se ha preocupado adicionalmente por modernizar e innovar sus servicios y atención al público procurando mayor agilidad y comodidad, mediante el uso y aplicación de su moderna tecnología (BCR, 2021a, s. p.).

Además: “A finales del siglo XX, el BCR se destaca por la innovación tecnológica en el sector financiero, al instalar el primer cajero automático, emitir la primera tarjeta de débito y crear el primer autobanco” (La Nación, 2016, s. p).

Sumado a esto:

> Logró automatizar la gestión para la obtención y renovación de pasaportes y cédulas de residencia, y, en alianza con el Ministerio de Obras Públicas, facilitó la automatización de solicitudes y entregas de licencias de conducir. Con ello ha impulsado la inserción de sus clientes y público en general en la sociedad tecnológica contemporánea (La Nación, 2016, s. p.).

A continuación, se detalla la misión y visión, valores y objetivos estratégicos del Banco de Costa Rica según su sitio web:

2.1.2. Misión

"Impulsar el desarrollo social y económico, la competitividad y la sostenibilidad de Costa Rica, ofreciendo a sus clientes un conglomerado financiero público, innovador y seguro, así como un portafolio de excelencia en todos sus servicios" (BCR, 2021d, s. p.).

2.1.3. Visión

"Ser la opción financiera preferida y viable, que ofrece a sus clientes productos y servicios promotores del desarrollo del país, con estándares mundiales de calidad, innovación, precio y eficiencia" (BCR, 2021d, s. p.).

2.1.4. Valores

Según el BCR (2021d):

- Liderazgo: Actitud de servicio por medio de acciones ejemplares que inspiren una gestión proactiva basada en la interacción y la confianza.
- Innovación: Capacidad para sinergizar y generar una mejora constante de forma creativa.
- Respeto: Entendimiento mutuo entre personas para lograr un cumplimiento transparente.
- Responsabilidad: Compromiso personal en función de objetivos y resultados enfocados en la sostenibilidad y el cliente.
- Rendición de cuentas: Comportamiento íntegro de todas las personas

enfocado en hacer las cosas bien desde la primera vez para lograr buenos resultados.

• Credibilidad: Autenticidad en cada acción que permita crear relaciones justas y empáticas entre las personas a largo plazo (s. p.).

2.1.5. Objetivos estratégicos

- “Garantizar la solidez financiera del conglomerado.
- Apoyar el desarrollo del país” (BCR, 2021d, s. p.).

2.1.6. Productos y servicios

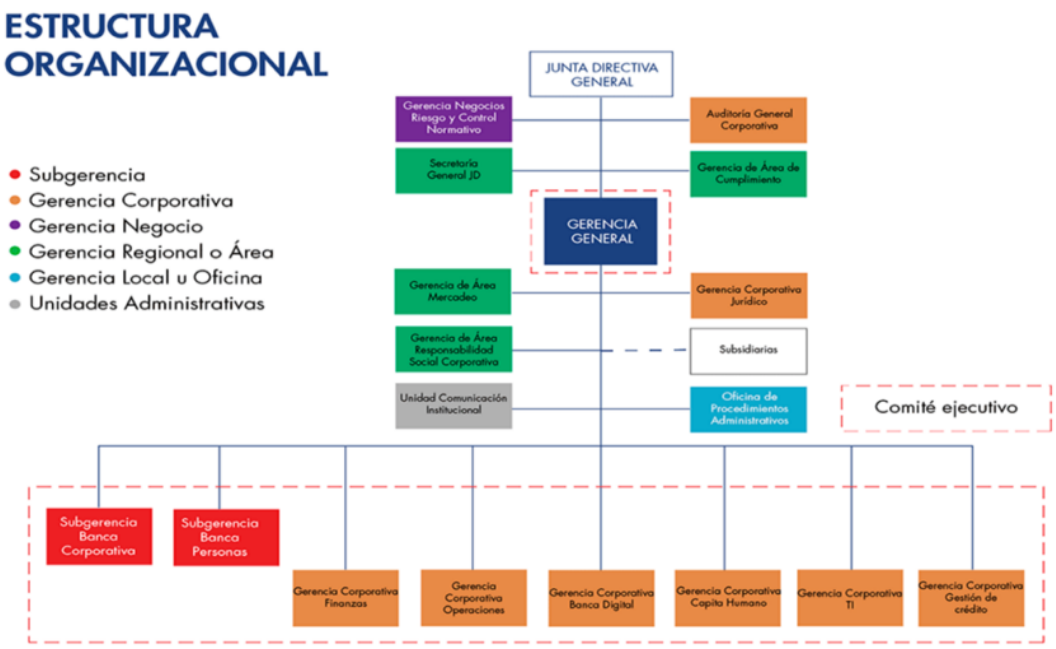
De acuerdo con la página oficial del BCR, algunos de los servicios son:

- Apertura de cuentas corrientes y de ahorro.
- Créditos hipotecarios, prendarios y fiduciarios.
- Depósitos a plazo.
- Tarjetas de débito y crédito.
- Red de cajeros automáticos.
- Banca por Internet y aplicaciones móviles.
- Planes de pensión.
- Fondos de inversión.
- Operaciones de bolsa.
- Correduría de seguros.
- Fideicomisos.

2.1.7. Recursos y estructura de la entidad

De acuerdo con la página web del BCR (2021c), el conglomerado financiero BCR se organiza de la siguiente manera.

Figura 5
Conglomerado Financiero BCR



Fuente: BCR (2021e).

2.1.8. Principales competidores

De acuerdo con el art. 1 de la Ley Orgánica del Sistema Bancario Nacional de Costa Rica (Ley n.º 1644, 1953), las entidades bancarias son las siguientes:

Tabla 4
Integrantes del sistema bancario nacional

Integrantes del sistema bancario nacional, art. 1 Ley Orgánica SBN
1) El Banco Central de Costa Rica.
2) El Banco Nacional de Costa Rica.
3) El Banco de Costa Rica.
4) (Derogado por el art. 1 de la Ley de Disolución del Banco Anglo Costarricense n.º 7471, de 20 de diciembre de 1994).

5) (Derogado por el art. 13 de la Ley n.º 9605, de 12 de setiembre de 2018, Fusión por absorción del Banco Crédito Agrícola de Cartago y el Banco de Costa Rica).

6) Cualquier otro banco del Estado que en el futuro llegara a crearse.

7) Los bancos comerciales privados, establecidos y administrados conforme con lo prescrito en el título VI de esta ley.

8) La sucursal bancaria domiciliada en Costa Rica de un banco extranjero.

Fuente: Elaboración propia con base en datos de la Ley n.º 1644 (1953).

Asimismo, cabe destacar los nombres de los miembros de la Asociación Bancaria Costarricense (ABC) que es una organización gremial que asocia a todos los bancos públicos y privados del Sistema para velar por los intereses del sector financiero nacional:

Tabla 5
Miembros del ABC

Nombre de la entidad	Descripción
Grupo Financiero BCT 	Se fundó en 1983 con un enfoque en el servicio de excelencia, buscando ofrecer asesoría y personalización en la oferta de productos financieros. En el año 2000, absorbió la Corporación Bancomer y en el 2007 adquirió la Compañía Financiera de Londres (Banco BCT, s. f.).
Grupo Financiero BAC Credomatic S. A.	Posee 70 años de experiencia, inició sus operaciones un 5 de julio de 1952 con la fundación del Banco de América en Nicaragua transformándose en un pionero del negocio de tarjetas de crédito en la región. De forma gradual, abrió operaciones en cada uno de los países, hasta que en la década de los 90 se convirtió en el primer grupo financiero con presencia en toda Centroamérica (BAC Credomatic, s. f.).
Conglomerado financiero Banco Nacional y	El Conglomerado Financiero Banco Nacional se fundó el 9 de octubre de 1914 con el nombre de Banco Internacional de Costa Rica para posteriormente, en 1936, llamarse Banco Nacional de Costa Rica.

Subsidiarias 	Pertenece al Estado costarricense y es el mayor banco de Costa Rica y Centroamérica (Banco Nacional, s. f.).
Grupo Financiero Davivienda	Parte del Grupo Empresarial Bolívar por más de 80 años. Es reconocido por el manejo único de su imagen a través de la comunicación convirtiéndose en una de las cinco marcas más valiosas y el primer banco en recordación publicitaria de Colombia (Davivienda, s. f.).
Grupo Financiero BNS de Costa Rica 	El Grupo BNS de Costa Rica es una subsidiaria de The Bank of Nova Scotia. Ingresó a Costa Rica en 1995 y ofrece al mercado nacional una amplia gama de productos y servicios financieros en sectores de banca de personas, banca comercial y corporativa, pymes, además de fondos de inversiones, *leasing*, seguros y banca privada (Scotiabank, s. f.).
Conglomerado Financiero Banco Popular y subsidiarias 	El Banco Popular se fundó en 1969 por el gobierno costarricense para fomentar el desarrollo económico. Desde 2000, el banco se ha convertido en un gran conglomerado financiero (la tercera mayor organización bancaria de Costa Rica) y oferta una gama completa de servicios bancarios, pensiones, valores bursátiles, fondos de inversión y seguros (TNI, 2017).
Conglomerado Financiero Banco de Costa Rica y Subsidiarias 	El Banco de Costa Rica se fundó el 20 de abril de 1877 con el nombre de Banco de la Unión, el cual mantuvo hasta 1890, cuando lo varió por el actual. Nació con el propósito de ser una nueva opción bancaria entre las existentes y tuvo como funciones iniciales el prestar dinero, llevar cuentas corrientes, recibir depósitos y efectuar cobranzas, entre otras (BCR, 2021a).
Banco Promerica 	Los orígenes del Grupo Promerica se remontan a noviembre de 1991, cuando Ramiro Ortiz Mayorga, junto con 133 socios provenientes de diversas actividades económicas en Nicaragua, fundó Banpro Grupo Promerica. A Banpro Grupo Promerica le siguieron Banco Promerica Costa Rica (1992), Banco Promerica El Salvador (1996), Banco Promerica República Dominicana, Banco Promerica Ecuador (2000), Banco Promerica

	Honduras (2001), St. Georges Bank Grupo Promerica en Panamá (2002), Banco Promerica Guatemala (2007) y St. Georges Bank Grupo Promerica en islas Caimán.
Grupo Financiero Lafise	Grupo LAFISE es un Holding empresarial moderno y diversificado fundado en 1985 para integrar y dinamizar los mercados de la región mediante una plataforma tecnológica de avanzada y un servicio ágil y amigable, de calidad mundial (Lafise, s. f.).
Grupo Financiero Cathay	Banco Cathay se fundó en 1998 para romper paradigmas, demostrando que los negocios y el desarrollo comercial entre Costa Rica y los países asiáticos era posible. Este es el único banco en Costa Rica con una estrecha conexión con la población de origen oriental radicada en el país, gracias a la existencia de personal con amplio dominio del idioma y la cultura en todas sus agencias (Banco Cathay, s. f.).
Banco CMB	Constituido como banco comercial privado, su actividad principal es el otorgamiento de préstamos, invertir en títulos valores por cuenta propia, emitir garantías de participación y cumplimiento, cuentas corrientes en dólares y colones, además de cartas de crédito, cobranzas y la captación de recursos por medio de la emisión de certificados de inversión para el sector corporativo. Adicionalmente, efectúa la compra y venta de divisas, transferencias de dinero a través del sistema Swift y otros servicios financieros (Banco CMB, s. f.).
Grupo Financiero Improsa	El Grupo Financiero Improsa inició sus operaciones en el año 1986 como Financiera Improsa. Nueve años después, la financiera se convirtió en Banco Improsa y en el año 2000 se estableció el Grupo Financiero Improsa, S. A. (Improsa, s. f.).

2.2. Sistema de gestión integral de riesgo

En la actualidad, el Banco de Costa Rica dispone de un Sistema Integral de Gestión de riesgo que le permite generar información para una adecuada toma de

decisiones y, a la vez, le permite producir un balance entre el riesgo que está dispuesto a asumir para lograr unos beneficios esperados en el tiempo.

2.2.1. Riesgos objeto de gestión

En el Banco de Costa Rica clasifican los riesgos por Financieros y No Financieros y a continuación se detallan:

2.2.1.1. Financieros

- Crédito.
- Mercado.
- Liquidez.

2.2.1.2. No financieros

- Estratégico.
- Operativo.
- Legal.
- Tecnología de información.
- Reputacional.
- Ambiental y social.
- Cumplimiento normativo.
- Legitimación de Capitales y Financiamiento al Terrorismo (Ley, 8204).

2.2.2. Principios y políticas

El BCR gestiona los riesgos mediante estudios cualitativos y cuantitativos dependiendo de la naturaleza y dificultad del riesgo, considerando siempre el impacto que vayan a ocasionar en los mercados financieros nacionales e

internacionales. Lo anterior lo realiza con una serie de principios y políticas que se detallan a continuación (BCR, 2021b):

- Gobierno corporativo que vela por el funcionamiento adecuado del sistema integral de riesgo.
- Estructura organizacional de riesgo con independencia funcional.
- Robusto marco normativo interno.
- Estrategia de gestión de riesgos efectiva, así como una declaratoria del apetito por riesgo adaptada a la realidad.
- Promoción constante de la cultura de gestión de riesgo en la entidad.
- Modelos y metodologías de acuerdo con la normativa prudencial y mejores prácticas internacionales.
- Herramientas y sistemas de información para la efectiva gestión de riesgos.
- Seguimiento y monitoreo constante del apetito y mitigadores de riesgo.
- Recurso humano competente y capacitado.

2.2.3. Modelos y metodologías

Para dar una explicación de los modelos y metodologías que se utilizan en el BCR para la gestión integral de riesgos es importante dividir las principales gestiones de riesgos efectuadas:

Gestión de riesgo de crédito:

- Modelo scoring: realiza una clasificación de los clientes para vivienda, consumo, pymes y tarjetas.
- Modelo riesgo empresarial: da una calificación de riesgo a los clientes corporativos.
- Modelo de riesgo de entidades financieras: da una calificación de riesgo a los clientes de naturaleza financiera.

- Metodología de capacidad de pago.
- Metodología de asignación de niveles de riesgo a actividades económicas.
- Metodología para la determinación de los límites de crédito.
- Metodología para el cálculo de la pérdida esperada en la cartera crediticia.
- Metodología de escenarios de estrés para la morosidad.

Gestión de riesgos de mercado y liquidez:

- Proyección de macroprecios: proyecta el movimiento de los macroprecios y flujos de efectivo.
- Sensibilidad de la posición propia en moneda extranjera: por movimientos en el cambio del dólar.
- Valor en riesgo Sugef 3-06: mide el impacto de la variación del precio sobre las inversiones sobre la suficiencia patrimonial.
- Valor en riesgo de la cartera de inversiones: determina la pérdida máxima en la cartera de inversiones por movimientos en precios.
- Sensibilidad del margen financiero por movimientos en tasas de interés.
- Cobertura de las inversiones líquidas: cuantifica la cobertura de los instrumentos de inversión líquida sobre los productos de captación puestos al público.
- Máxima variación esperada en las captaciones: pronostica la máxima salida esperada.
- Factor de renovación de CDP: mide la permanencia de los instrumentos a plazo del público.
- Permanencia de saldos de cuentas a la vista: mide la permanencia de los instrumentos a la vista.
- Concentración de las captaciones: mide las captaciones por tipo de público.

Gestión de riesgo operativo:

- Metodología cálculo valor de riesgo: mediante el método Montecarlo determina los niveles de pérdida de riesgo operacional.
- Metodología para la evaluación de riesgo: mide la frecuencia e impacto del riesgo que pueda afectar los objetivos del banco.
- Metodología para la evaluación de riesgo legal: evalúa el riesgo legal por eventos que causen pérdidas en el banco.

Gestión de riesgo tecnológico:

- Posee indicadores de riesgo tecnológico que miden los posibles efectos ante un siniestro.

Gestión de riesgo estratégico:

- Metodología para la evaluación de riesgo estratégico: evalúa riesgos estratégicos para evitar pérdidas o situaciones que lleguen a afectar el cumplimiento de objetivos.

Gestión de riesgo reputacional:

- Metodología para la evaluación del riesgo reputacional: evalúa riesgos reputacionales para evitar pérdidas o situaciones que afecten el cumplimiento de objetivos.

Gestión de riesgo en el ejercicio de las actividades como fiduciario:

- Metodología de categorización de los fideicomisos según complejidad: valora todas las características de los fideicomisos para darles una categoría.

Gestión de riesgo de legitimación de capitales:

- Metodología integral de valoración de riesgo de legitimación de capitales y financiamiento al terrorismo: evalúa el cumplimiento de la Ley n.º 8204.

- Modelo de riesgo a clientes: otorga a los clientes una categoría de riesgo de acuerdo con transacciones y perfiles del cliente.
- Modelo de zonas geográficas: asigna valores de riesgo, de forma nacional o internacional.
- Modelos corresponsales: evalúa corresponsales internacionales.

Gestión integral de los riesgos del conglomerado:

- Metodología para la determinación del capital económico: determina el capital económico del Banco para asignar una estimación de recursos mínimos ante eventualidades.

Gestión de continuidad de negocio.

Gestión de cumplimiento normativo.

Gestión de riesgos en las subsidiarias.

Capítulo III. Marco contextual

3.1. Situación actual de los fraudes digitales

En el ámbito global, se observa que la cantidad de fraudes bancarios cibernéticos ha ido en aumento en las entidades bancarias; una encuesta aplicada por KPMG (2019) concluyó que los fraudes que van en aumento desde el 2015 al 2018 son el robo de identidad, posesión de cuenta y ataques cibernéticos. De los fraudes anteriores, menos del 25 % de las personas o empresas recuperan lo perdido. De igual manera, entre todos los bancos encuestados, se obtuvo la conclusión de que el desafío más importante en el riesgo de fraude son los ciberataques. Según (2015), los define como: "Toda aquella acción ilegal que se da por vías informáticas o tiene como objetivo destruir y dañar ordenadores, medios electrónicos y redes de internet".

La Encuesta Nacional de Hogares realizada por el Instituto Nacional de Estadística y Censos (INEC, 2018) resalta que el robo y estafa de dinero por Internet va en aumento:

> El robo o estafa de dinero por internet pasó de 2 896 casos en el 2010 a 16 128 en el 2014 y creció vertiginosamente en los últimos 4 años con 55 296 casos reportados, siendo los hogares de mayores ingresos los más afectados con el 5,2%. (s. p).

Adicionalmente, señalan que la mayor parte de los casos suceden en el área urbana por encima del área rural:

> La ocurrencia de victimización es más alta en la zona urbana (21,3%) con respecto a la zona rural (14,2%), brecha que aumentó en los últimos diez años, mientras que en el 2014 la diferencia fue de 6.2 p.p., en el 2018 llegó a 7.1 p.p. (INEC, 2018, s. p).

Es importante detallar que la Encuesta Nacional de Hogares se realiza cada año. Sin embargo, los datos de robo y estafa se miden en un periodo de 4 años.

Datos que se obtienen del Organismo de Investigación Judicial (OIJ, 2019) señalan que entre el año 2018 y 2019 hubo un aumento del 21.8 % de fraudes en el país, lo que da como resultado que en promedio se realiza un fraude cada 37 minutos. De la cantidad total de fraudes realizados para el 2019 un 49 % corresponde a la provincia de San José, un 15 % en Alajuela, un 12 % en Heredia, un 7 % en Cartago, un 6 % en Puntarenas, un 6 % en Guanacaste y un 5 % en Limón. De los datos anteriores, el 4 % corresponde a estafas informáticas para el 2019 y en comparación con el año 2018 aumentaron en un 1 %. Los datos anteriores resultan alarmantes por la gran cantidad de personas que son estafadas en el país y el poco conocimiento existente para prevenir este tipo de ataques malintencionados.

La Banca en Costa Rica es un sector económico muy fuerte, la cual se caracteriza por sucursales físicas donde los clientes realizan las transacciones. Sin embargo, la era digital va en aumento en el sector. Chacón Jiménez (2017), que entrevistó al 92 % de las entidades financieras del país, señala que este sector apostará por la digitalización en la prestación de servicios y en 5 años se disminuirá considerablemente la cantidad de oficinas físicas. De la cantidad de entidades entrevistadas el 68 % indicó que las sucursales físicas tienen poco o nada de importancia en el futuro y el 89.5 % de las entidades indicó que las aplicaciones móviles son las que tendrán gran relevancia para los próximos años. Lo anterior resulta sumamente importante para lograr que conforme vaya afianzándose la era digital en la banca nacional, también vaya junto con las prácticas de seguridad y procesos para evitar los fraudes y vulnerabilidades cibernéticas.

En lo que respecta al Banco de Costa Rica, se ha caracterizado por ser una institución sólida financieramente y con respaldo estatal, lo que genera una mayor confianza entre los clientes. Para el año 2017, una entrevista de la República al gerente general interino de ese entonces Leonardo Acuña aseguraba que el patrimonio del Banco asciende a ₡509.117.000.000 y las utilidades acumuladas excedían los ₡30.347.000.000, logrando posicionarse como la segunda entidad más importante en el país (Arrieta, 2017).

Sin embargo, como toda entidad está expuesta a que los criminales usen su imagen corporativa para estafar a los clientes. Según una entrevista realizada al jefe de seguridad del BCR para el 2019, Giovanni Zamora (Vargas, 2020), indicó que diariamente al Banco entran entre 5 y 6 denuncias por fraude informático, esta es una cantidad preocupante para la organización. Otro factor importante, es que las entidades bancarias cuentan con hasta 120 días para resolver y brindar una respuesta a sus clientes como lo indicó en la misma entrevista el jefe de seguridad del Banco Nacional Raúl Lacayo, convirtiéndose en un factor controversial para que los clientes pierdan confianza en la entidad donde custodian su dinero.

Capítulo IV. Marco metodológico

Se presenta a continuación la estrategia metodológica, la cual incluye el paradigma, enfoque, tipo de investigación, así como las fuentes por utilizar para recolectar la información que aporta los insumos para la propuesta metodológica. Para recopilar la información pertinente y, como se ha descrito a lo largo de la investigación, el proyecto se desarrolla directamente en el Banco de Costa Rica, para analizar desde diferentes configuraciones la gestión de riesgo asociado con el fraude a través de medios digitales y su impacto en la imagen corporativa de la entidad.

4.1. Paradigma y enfoque

El paradigma seleccionado para la investigación corresponde a la combinación del paradigma positivista y el naturalista, a partir de las bondades, límites y posibilidades que cada uno plantea, puesto que ambos proporcionan diversas perspectivas de una misma realidad. El interés de la presente investigación es conocer desde la perspectiva naturalista, las formas para mitigar los intentos de crímenes informáticos a los que se enfrenta diariamente el BCR y que impactan su imagen corporativa. Es decir: “Se centra en el estudio de los significados de las acciones humanas y de la vida social” (Barrantes Echavarría, 2014, p. 82) y desde la visión positivista generalizar recomendaciones que estén disponibles para otras instituciones financieras que puedan estar siendo afectadas por estas mismas amenazas. Todo esto sin establecer, como bien lo indica Monje (2011), una separación tajante o dicotomía entre los dos enfoques metodológicos.

La persona investigadora debe: “Conocer los potenciales de cada paradigma, estar muy claro en sus preguntas de investigación y saber en cuál de ellos ubicarse para generar el conocimiento que quiere” (Monje, 2011, p. 50). Por lo tanto, la riqueza de combinar ambos paradigmas se reconoce en observar su complementariedad en el conocimiento, explicación y comprensión de la realidad social que se investiga y lograr una perspectiva más amplia y profunda del fenómeno.

Este es el caso de la presente investigación, donde se busca fortalecer la imagen corporativa del Banco de Costa Rica por medio de una propuesta de gestión, por lo que es necesario analizar los datos de una manera imparcial y enfocarse en interpretarla sin dejar que influyan creencias, sentimientos y tendencias en los resultados. Adicionalmente, es necesario escuchar e interactuar con las personas usuarias, para realizar una propuesta que se enfoca en sus necesidades y no otras, a partir de la comprensión de sus historias, gustos y posibilidades, formulando estrategias idóneas para la prevención del fraude a través de medios digitales.

Otra razón para utilizar un método mixto reside en la complejidad del problema de investigación, en el que coexisten dos realidades, una objetiva y la otra subjetiva. Por una parte, la lectura real y exacta del contexto del Banco de Costa Rica en el sector bancario nacional y su gestión del riesgo por fraude y, por otra, la respuesta oportuna a las necesidades de las personas usuarias para el fortalecimiento de su imagen corporativa. Es decir, no solamente se vuelve necesaria la participación de quien investiga, también parte de la relación sujeto-objeto, el sujeto forma parte indispensable de la realidad investigada y todas las relaciones que establece con su entorno son significativas para el análisis del fenómeno del que forma parte. Se examina: “El sujeto en su interacción con el entorno al cual pertenece y en función de la situación de comunicación de la cual participa” (Monje, 2011, p. 14).

4.2. Fases de la investigación

Entre los métodos mixtos se distinguen generalmente cuatro fases principales que se dan de manera paralela para ambos enfoques, en las que se aplican ambos métodos, de manera simultánea y concurrente: fase conceptual, fase empírica metodológica (método), fase empírica analítica (análisis de resultados) y fase inferencial (discusión). Hernández, Fernández y Baptista, (2014), indican las siguientes características:

- Se recolectan datos cuantitativos y cualitativos a varios niveles, de manera simultánea o en diferentes secuencias, a veces se combinan y transforman

los dos tipos de datos para arribar a nuevas variables y temas para futuras pruebas o exploraciones (Hernández-Sampieri y Mendoza, 2008).

• Se realizan análisis cuantitativos y cualitativos sobre los datos de ambos tipos durante todo el proceso. Se comparan variables y categorías cuantitativas con temas y categorías cualitativas y se establecen múltiples contrastes.

• Se pueden involucrar otros diseños específicos en el mismo estudio, por ejemplo, un experimento.

• Los resultados definitivos se reportan hasta el final, aunque pueden elaborarse informes parciales.

• El proceso es completamente iterativo.

• Son diseños para lidiar con problemas sumamente complejos.

• Los resultados se pueden generalizar y es factible al mismo tiempo desarrollar teoría emergente y probar hipótesis, explorar, etcétera (pp. 549-550).

4.3. Instrumentos y técnicas de recolección de datos

En el método mixto se tiene variedad de técnicas e instrumentos para la recolección de datos necesarios para responder al problema de investigación y los objetivos. “El proceso de recolección de datos para una investigación se lleva a cabo mediante la utilización de métodos e instrumentos, los cuales se seleccionan según se trate de información cuantitativa o cualitativa” (Monje, 2011, p. 133). Algunos de los métodos que se utilizan son directos como las entrevistas o la observación, las cuales se desarrollan *in situ* por la persona investigadora y otros son indirectos, como en el caso de los cuestionarios. El método que se utilice define los objetivos que se plantearon, el diseño de la investigación y la disponibilidad del personal, así como los recursos económicos (Monje, 2011).

Como factor importante Monje (2011) plantea que, dentro de la metodología para la recolección de datos, la intención de la persona investigadora debe ser producir información cuantitativa válida para medir con cierto grado de exactitud los fenómenos o el deseo de profundizar en la comprensión de estos desde el punto de vista cualitativo. De acuerdo con las variables y categorías de análisis que

median en la presente investigación, se seleccionaron instrumentos que promueven la interacción entre investigadores y personas participantes, potenciando espacios seguros, cómodos, de confianza y horizontales.

Es así como se propone el cuestionario: entrevista semiestructurada en profundidad, grupo focal, historias de vida y análisis de contenido. Cabe destacar que se respeta el distanciamiento social en la aplicación de cada uno de los instrumentos con el apoyo de herramientas tecnológicas que se utilizan en la actualidad.

4.3.1. Revisión documental

En la presente investigación se utiliza la revisión documental para el análisis de sistematizaciones que se relacionan con los modelos y prácticas que se implementan por parte del sector bancario nacional e internacional con respecto a la gestión del riesgo por fraude a través de medios digitales. Se pretende encontrar patrones de coincidencia y brechas entre diversas propuestas de modelos que se consideren relevantes como oportunidad para fortalecer la gestión actual.

4.3.2. Cuestionario

En la presente investigación se utiliza el cuestionario para recolectar la información que puedan brindar las personas funcionarias del Departamento de Gestión de Análisis y Prevención de Fraudes, con preguntas de respuesta cerrada que se relacionan con la gestión del riesgo actual ante situaciones que se presentan a través de medios digitales y su visión sobre la imagen corporativa.

4.3.3. Entrevista

En esta investigación, se utiliza la entrevista para recolectar la información que puedan brindar las personas funcionarias del Departamento de Gestión de Análisis y Prevención de Fraudes, con preguntas de respuesta abierta que se relacionan con la gestión del riesgo actual ante situaciones que se presentan a través de medios digitales.

4.3.4. Entrevista dirigida o semiestructura

Para la presente investigación se utiliza la entrevista semiestructurada, para recolectar la información que puedan brindar los clientes sobre sus experiencias en el Banco de Costa Rica sobre el tema de fraude y la visión que poseen sobre la imagen corporativa ante situaciones que se presentan a través de medios digitales.

4.3.5. Entrevista en profundidad

Se realiza una entrevista en profundidad sobre las experiencias de las personas participantes con respecto a la gestión del riesgo por fraude electrónico y el impacto sobre la imagen corporativa. En esta, se utiliza la entrevista en profundidad para recolectar la información que puedan brindar las personas funcionarias líderes o con rango de jefatura del Departamento de Gestión de Análisis y Prevención de Fraudes, con preguntas de respuesta abierta que se relacionan con la gestión del riesgo y la imagen corporativa del Banco de Costa Rica ante situaciones que se presentan a través de medios digitales.

4.3.6. Grupo focal

En esta investigación se utiliza el grupo focal para recolectar la información que puedan brindar las personas funcionarias del Departamento de Gestión de Análisis y Prevención de Fraudes, con una guía de conversación sobre las necesidades y lineamientos de gestión del riesgo para el fortalecimiento de su imagen corporativa. Es importante señalar que se realiza mediante medios digitales para respetar la coyuntura actual.

4.4. Fuentes de información (primarias y secundarias)

Las fuentes de información primarias son las personas participantes, mientras que las fuentes secundarias son los distintos materiales teóricos que se relacionan con el tema de investigación.

4.4.1. Población y muestra

Para la presente investigación las personas participantes se refieren a:

- La totalidad de las personas funcionarias del Departamento de Gestión de Análisis y Prevención de Fraudes del Banco de Costa Rica.
- La totalidad de las personas funcionarias líderes o con rango de jefatura del Departamento de Gestión de Análisis y Prevención de Fraudes del Banco de Costa Rica.
- Una muestra del total de la población económicamente activa, de acuerdo con la encuesta continua de empleo del INEC del primer trimestre del 2022.

4.4.2. Tabulación y análisis de los resultados

Para la recolección de los datos, se realizó una encuesta general y un cuestionario a las personas funcionarias del Departamento de Fraudes del Banco de Costa Rica. La cantidad de encuestas aplicadas fue de 391, las cuales corresponden a una muestra representativa de la cantidad total de la población económicamente activa del primer trimestre del 2022 según la encuesta continua del empleo (INEC, 2022). A continuación, se muestra el cálculo realizado para obtener una muestra significativa:

Figura 6
Cálculo realizado para obtener una muestra significativa

$$\frac{(1.96)^2(2430000)(0.5)(0.5)}{(0.05)^2(2430000-1)+(1.96)^2(0.5)(0.5)} = 384.0994356$$

Fuente: Elaboración propia, con un porcentaje de confianza de un 95 %.

Por otra parte, la cantidad de cuestionarios aplicados fueron 12, ya que es la cantidad total de personas que trabajan en este departamento. En este caso, se realizó un cuestionario para tener respuestas más amplias y una mejor percepción de los empleados hacia la institución.

El proceso de recolección de datos comenzó en mayo de 2022 y terminó en septiembre de ese mismo año. La forma de recolección fue mediante la herramienta de Google Forms, por la cual se logró conseguir la cantidad necesaria de personas

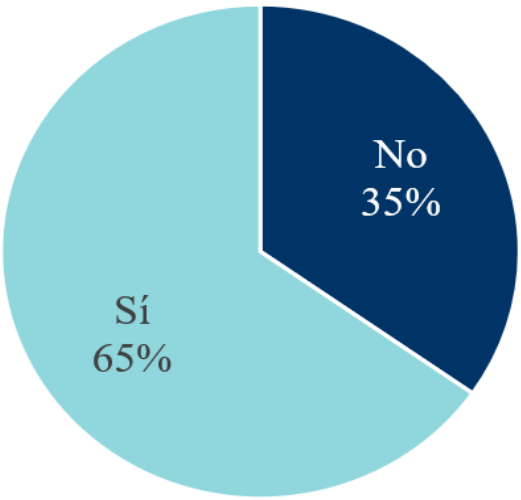
para abarcar la cantidad establecida y llegar de una manera más práctica a las personas funcionarias del Banco sin la necesidad de reunirse, de manera presencial, por los protocolos que actualmente tienen en el departamento.

4.4.2.1. Encuesta

4.4.2.1.1. Perfil de las personas encuestadas

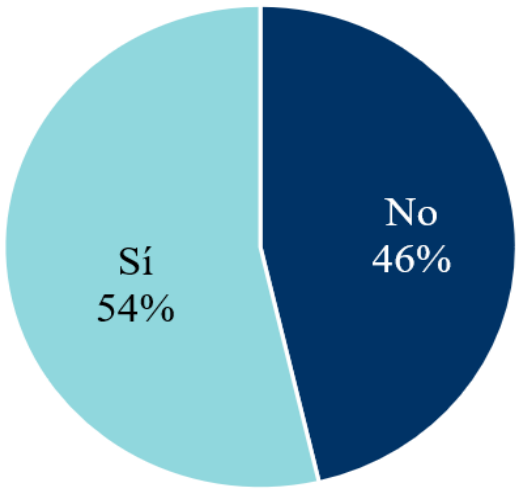
De acuerdo con los datos que se obtienen, la cantidad de personas que posee una cuenta con el BCR es el 65 % de la población, mientras que un 35 % no tiene una cuenta activa. Del anterior 35 % que no posee una cuenta activa, el 53 % tuvo una cuenta y un 47 % nunca ha tenido cuenta con esta institución. Del 53 % que tuvo una cuenta en el pasado, fueron muchos los factores que llevaron a cerrarla, sin embargo, el factor número uno fue que encontraron una institución bancaria mejor (ver Figura 9). Lo anterior, ayuda a interpretar que la institución tiene que trabajar en su imagen y servicio para retener este gran porcentaje de clientes.

Figura 7
Clientes actuales del Banco de Costa Rica



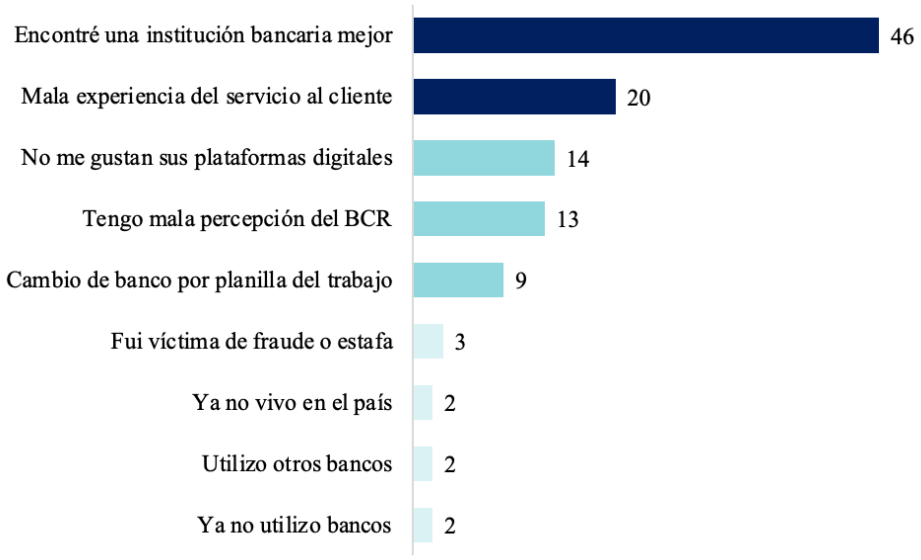
Fuente: Elaboración propia, 2022.

Figura 8
Personas que fueron clientes del banco de Costa Rica en el pasado, pero que actualmente no lo son



Fuente: Elaboración propia, 2022.

Figura 9
Razones por las cuales dejaron de ser clientes del Banco de Costa Rica

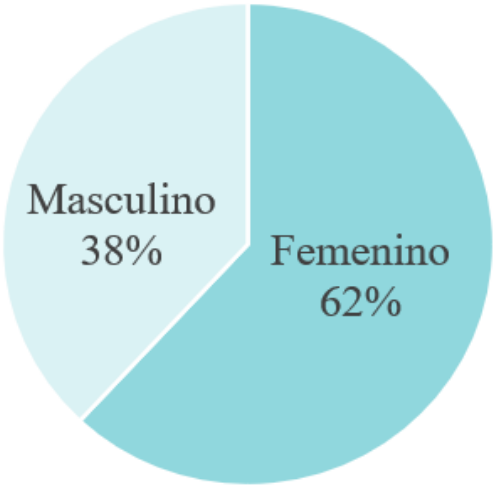


Fuente: Elaboración propia, 2022.

Con respecto al género, el 62 % de las personas encuestadas corresponde a mujeres y el 37 % hombres, de los cuales la mayoría está en un rango de edad

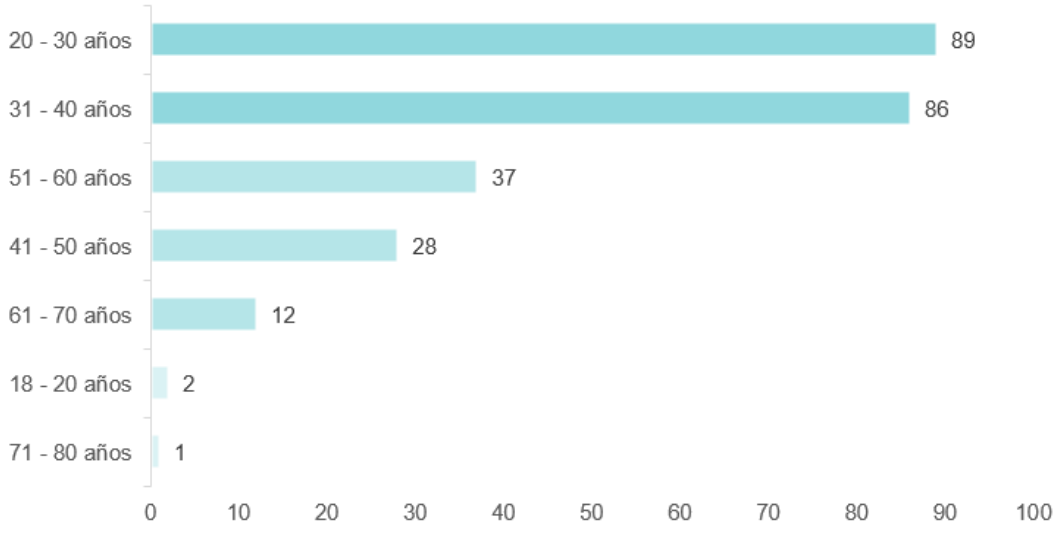
entre 20 y 30 años. El mayor porcentaje de las personas encuestadas es soltero y reside en la provincia de San José.

Figura 10
Distribución por género



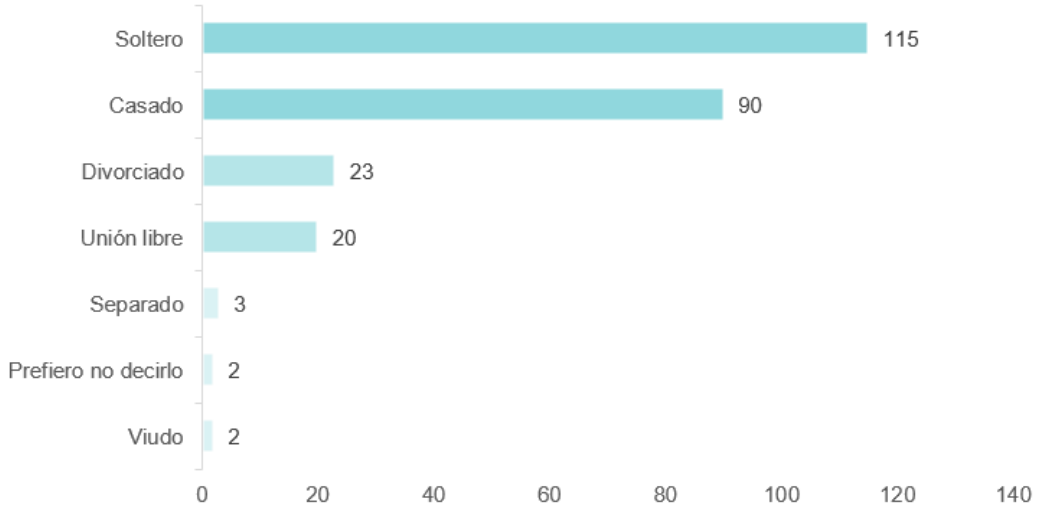
Fuente: Elaboración propia, 2022.

Figura 11
Distribución por edad



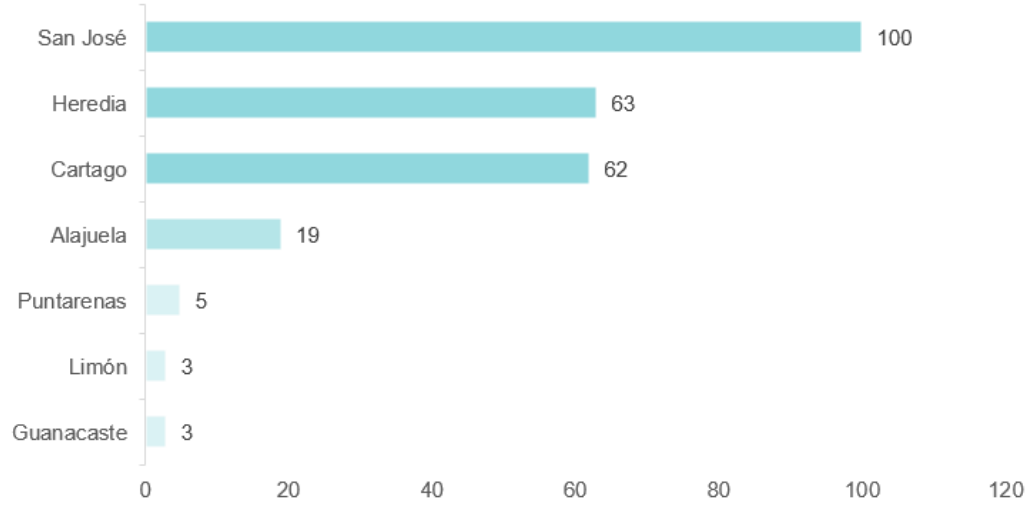
Fuente: Elaboración propia, 2022.

Figura 12
Distribución por estado civil



Fuente: Elaboración propia, 2022.

Figura 13
Distribución por lugar de residencia



Fuente: Elaboración propia, 2022.

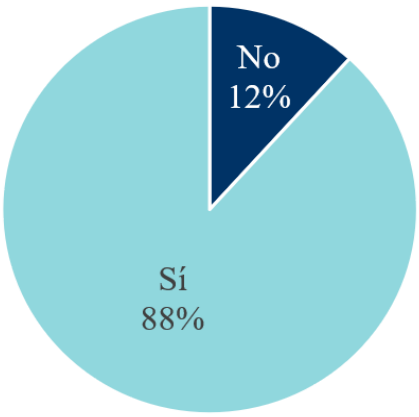
4.4.2.1.2. Análisis de uso de las plataformas digitales

Antes de conocer la percepción de las personas encuestadas sobre la seguridad de las plataformas digitales en el BCR, es valioso destacar la cantidad de

personas que la utilizan, periodicidad de uso, transacciones realizadas y plataformas que más se utilizan.

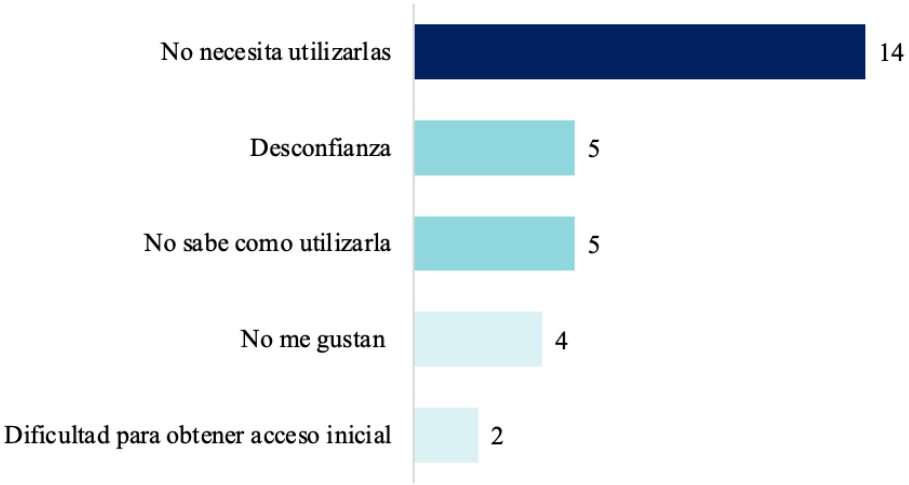
Con respecto al uso de las plataformas digitales del BCR, el 88 % de las personas encuestadas utiliza la plataforma digital y el porcentaje que no las usa justificó que era por no necesitar utilizarlas, por desconfianza y porque no les gusta.

Figura 14
Utilización de plataformas digitales del Banco de Costa Rica



Fuente: Elaboración propia, 2022.

Figura 15
Razones para no utilizar plataformas digitales del Banco De Costa Rica

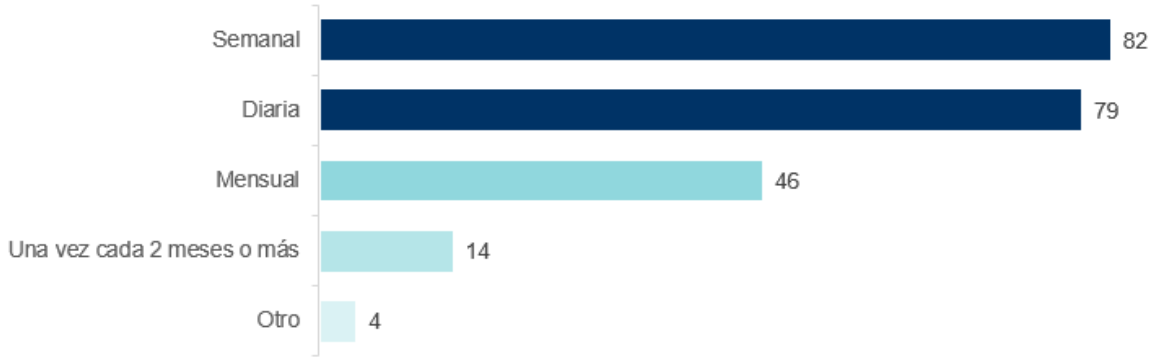


Fuente: Elaboración propia, 2022.

Del 88 % de personas que las utilizan, se logró conocer que la periodicidad con que usan las plataformas en mayor parte es de forma semanal con un 36 % y el celular es la herramienta de preferencia por la cual ingresan a las plataformas del BCR. Al consultar sobre el medio por el cual ingresan a sus datos, un 56 % de las personas encuestadas utiliza tanto la aplicación como la página web.

Figura 16

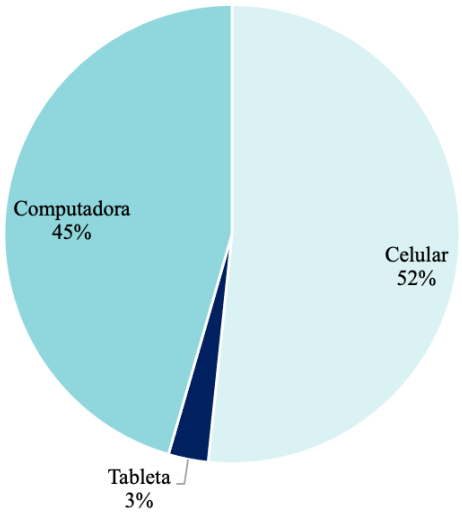
Frecuencia con que se utilizan las plataformas virtuales del Banco de Costa Rica



Fuente: Elaboración propia, 2022.

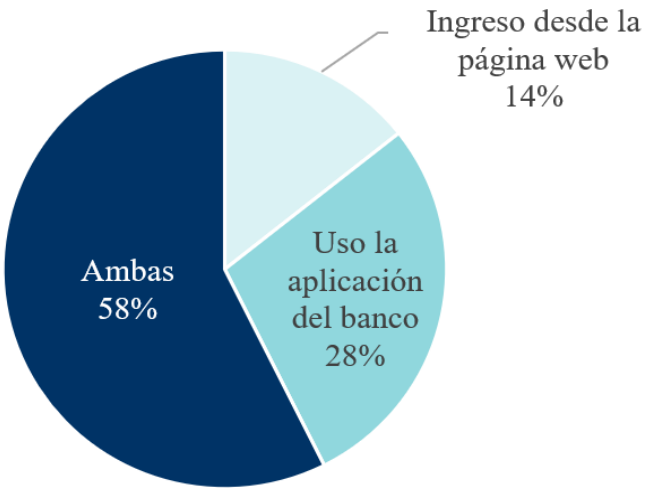
Figura 17

Porcentaje de uso de las plataformas del Banco de Costa Rica de acuerdo con el dispositivo



Fuente: Elaboración propia, 2022.

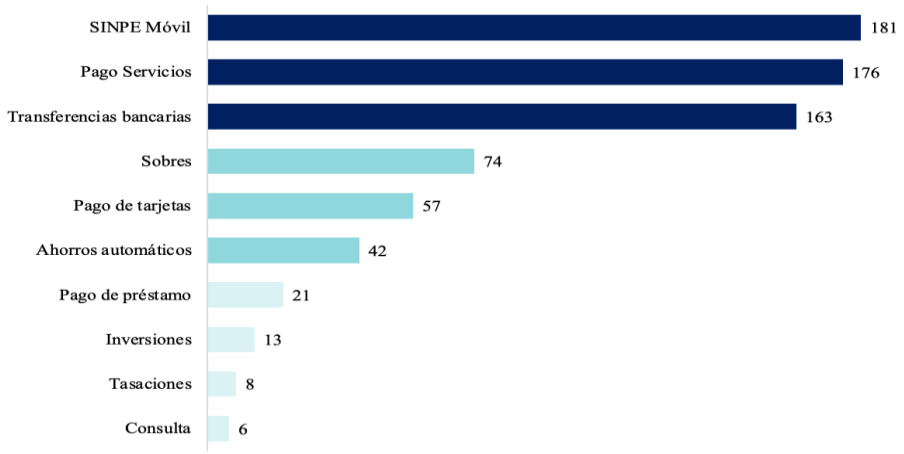
Figura 18
Plataforma virtual que utilizan para ingresar al Banco de Costa Rica



Fuente: Elaboración propia, 2022.

Entre las transacciones que más se realizan entre las plataformas del BCR están: Sinpe Móvil, transferencias bancarias y pago de servicios. Lo anterior resulta importante para conocer que las transacciones más frecuentes tienen que ver con el tránsito de dinero hacia otras instituciones o entes. Debido a lo anterior, la confianza hacia un banco es esencial para que las personas realicen sus transacciones con la mayor seguridad posible. Seguidamente, se les consultó si consideran que la percepción de las personas hacia una organización influye en el momento de adquirir un servicio financiero y el 96 % indica que es relevante.

Figura 19
Tipo de transacciones más realizadas en la plataforma del Banco de Costa Rica



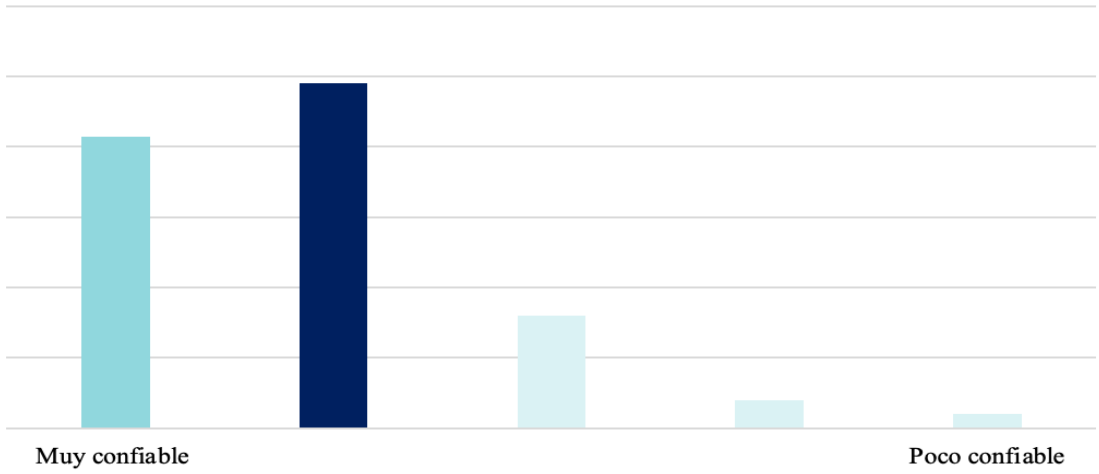
Fuente: Elaboración propia, 2022.

Con respecto a la confianza que poseen en las plataformas digitales del BCR, se observa que poseen un indicador de confianza alto para la población y el 92 % de las personas encuestadas considera que estas plataformas son seguras para realizar transacciones. Entre los puntos altos para considerarlas seguras estuvieron los mecanismos de seguridad que usan actualmente.

De igual forma, era importante conocer la opinión del 8 % de las personas encuestadas que no posee la confianza para utilizarlas y sus razones. Por lo tanto, se consultó sobre estas razones y todas las respuestas se relacionan con los fraudes, *hackers* y robos de dinero que se presentan en la institución, lo que da una alerta sobre la percepción que tienen algunos de sus clientes quienes son el eslabón que deben fortalecer en su imagen corporativa.

Figura 20

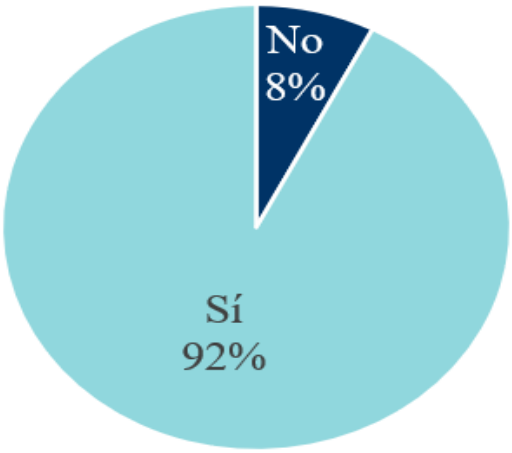
Nivel de confianza en las plataformas virtuales del Banco de Costa Rica



Fuente: Elaboración propia, 2022.

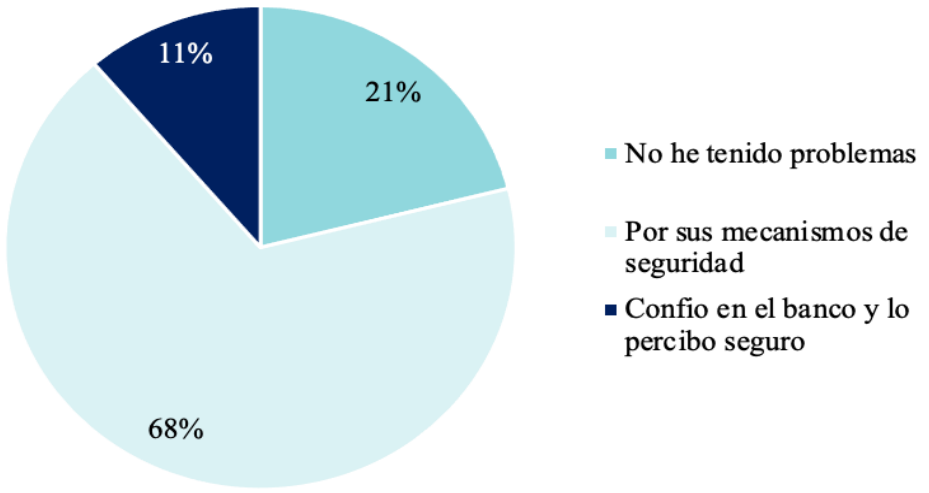
Figura 21

Porcentaje de la población que considera que la plataforma digital del Banco de Costa Rica es segura para realizar transacciones



Fuente: Elaboración propia, 2022.

Figura 22
Razones por las cuales consideran que la plataforma digital del Banco de Costa Rica es segura para realizar transacciones



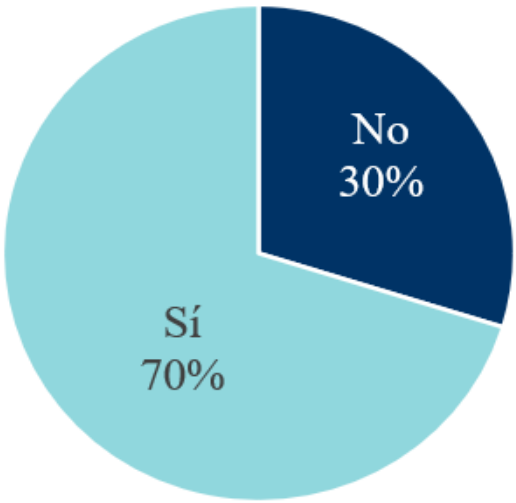
Fuente: Elaboración propia, 2022.

4.4.2.1.3. Análisis de la comunicación bancaria con respecto a la prevención de fraude

Con respecto a la comunicación que realiza el BCR sobre la prevención de fraudes, se les consultó a las personas encuestadas si reciben información de este tipo y un 70 % indicó que si han recibido información en algún momento y el medio por el que más comunican es el correo electrónico, siendo la opción que el 92 % de los encuestados votó. Un factor por considerar es que un 30 % de la población no recibe este tipo de información, es un porcentaje muy alto que eventualmente puede verse perjudicado por desconocimiento. Debido a lo anterior, el Banco debe investigar el motivo por el cual no reciben esa información y trabajar en reducir ese porcentaje, ya que el 98 % de la muestra indica que es importante recibirla. El 2 % que no lo considera relevante indica que, aunque se comunique, siguen siendo víctimas de fraudes y no confían en la entidad.

Figura 23

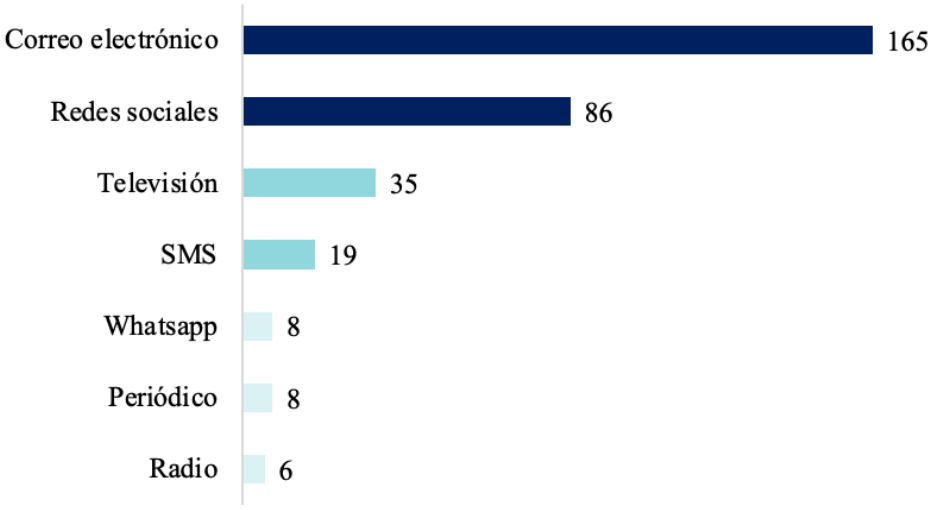
Porcentaje de la población que ha recibido información sobre cómo prevenir fraude por parte del Banco de Costa Rica



Fuente: Elaboración propia, 2022.

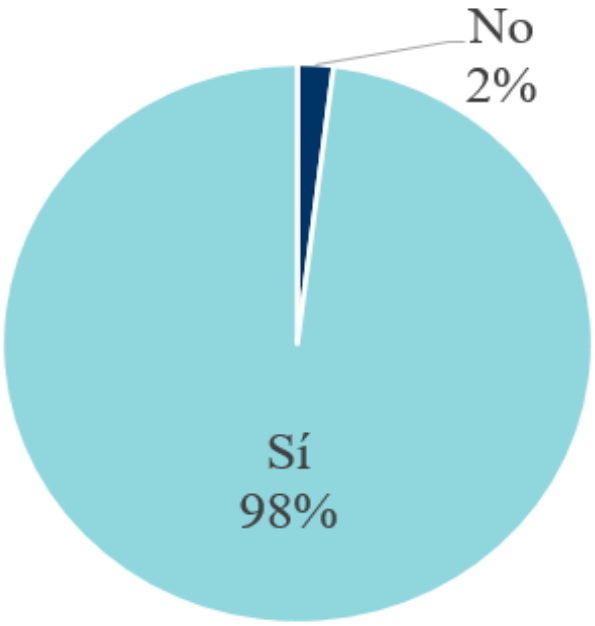
Figura 24

Medios por los cuales la población ha recibido información sobre cómo prevenir fraude por parte del Banco de Costa Rica



Fuente: Elaboración propia, 2022.

Figura 25
Porcentaje de la población que considera que es importante recibir información sobre cómo prevenir fraude

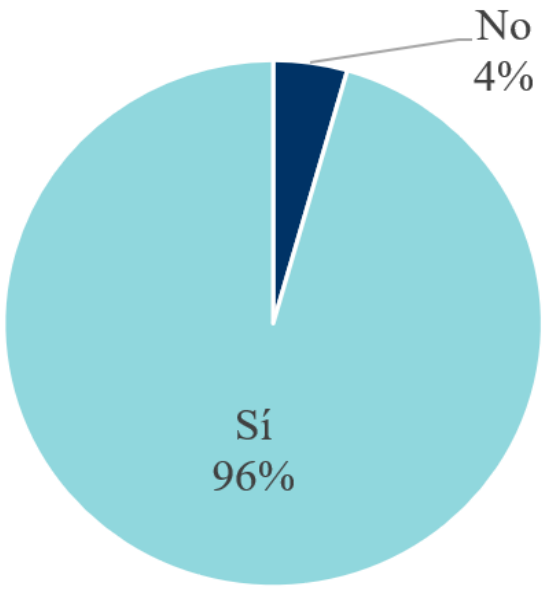


Fuente: Elaboración propia, 2022.

4.4.2.1.4. Imagen corporativa del Banco de Costa Rica

Antes de definir la percepción que tienen las personas sobre el BCR, resulta oportuno conocer si la percepción que se posea de una organización es un factor influyente en el momento de hacer una elección, el 96 % de los encuestados contestó que es relevante. Por lo tanto, en un mercado como el bancario que la diferenciación se da por el servicio al cliente y no por los productos al ser en todos los bancos similares, les da una gran responsabilidad por mantener una imagen corporativa buena para ser atractivos para los usuarios.

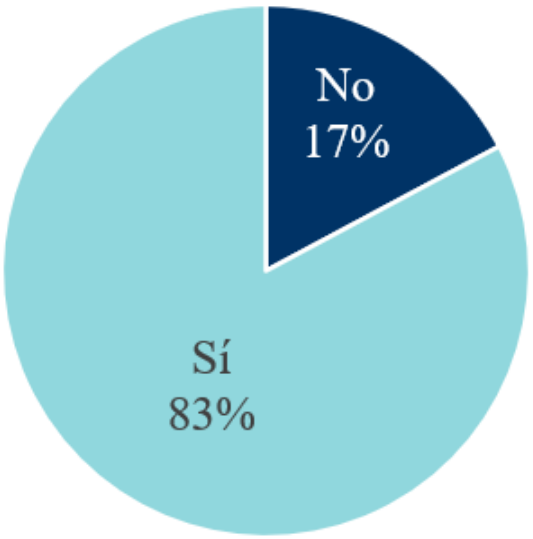
Figura 26
Porcentaje de la población que considera que la percepción sobre una organización es un factor importante en el momento de elegir una institución financiera



Fuente: Elaboración propia, 2022.

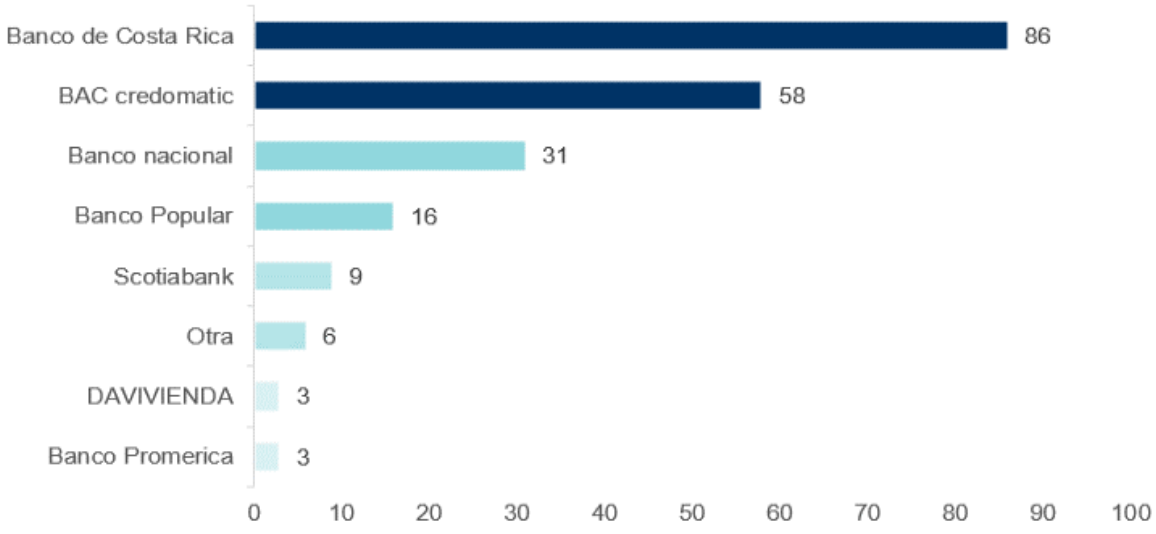
Al consultarles sobre si poseen cuentas en otros bancos, el 82 % de las personas encuestadas indica que sí, este es un dato fundamental al mostrar que las personas diversifican donde guardan el dinero y, a la vez, muestra la gran competencia que hay en este sector. Para el BCR es importante conocer que el 40 % de las personas encuestadas tiene como preferencia este banco, sin embargo, un 26 % prefiere el BAC Credomatic, un margen muy estrecho que se puede acortar según el manejo que se le dé a la entidad. Entre las preferencias que las personas encuestadas tienen hacia las entidades bancarias están: el servicio, la seguridad, la imagen institucional y la ubicación.

Figura 27
Porcentaje de la población que posee cuentas con otros bancos



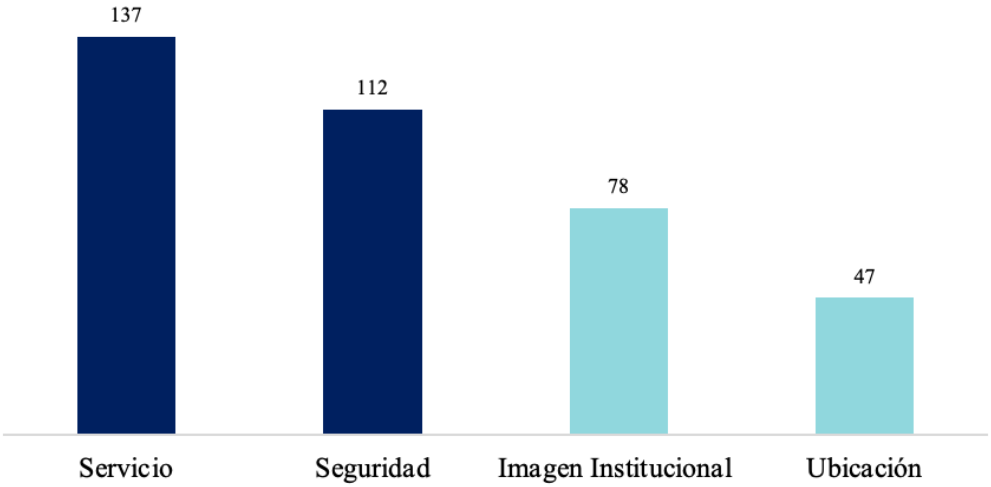
Fuente: Elaboración propia, 2022.

Figura 28
Institución financiera preferida



Fuente: Elaboración propia, 2022.

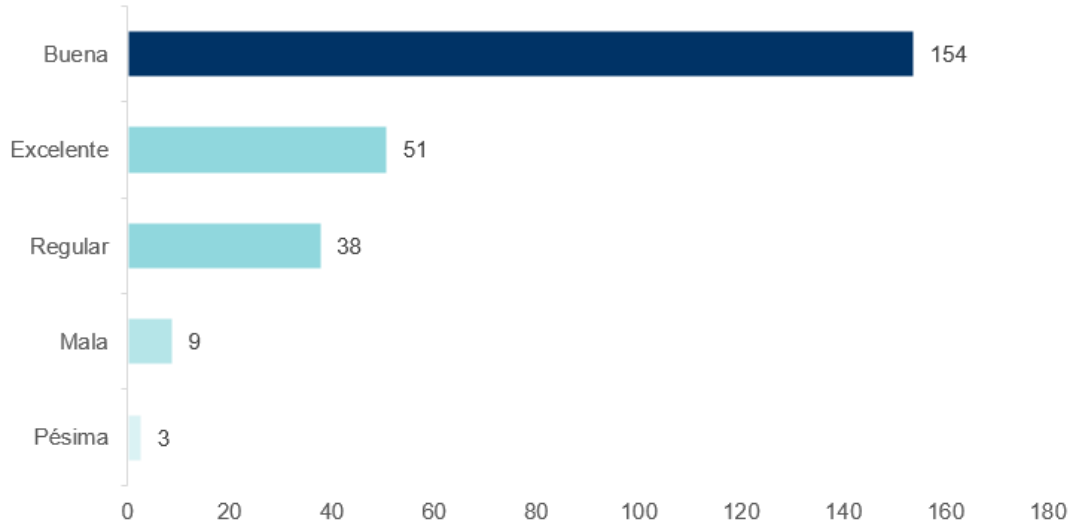
Figura 29
Razones de preferencia de la institución financiera



Fuente: Elaboración propia, 2022.

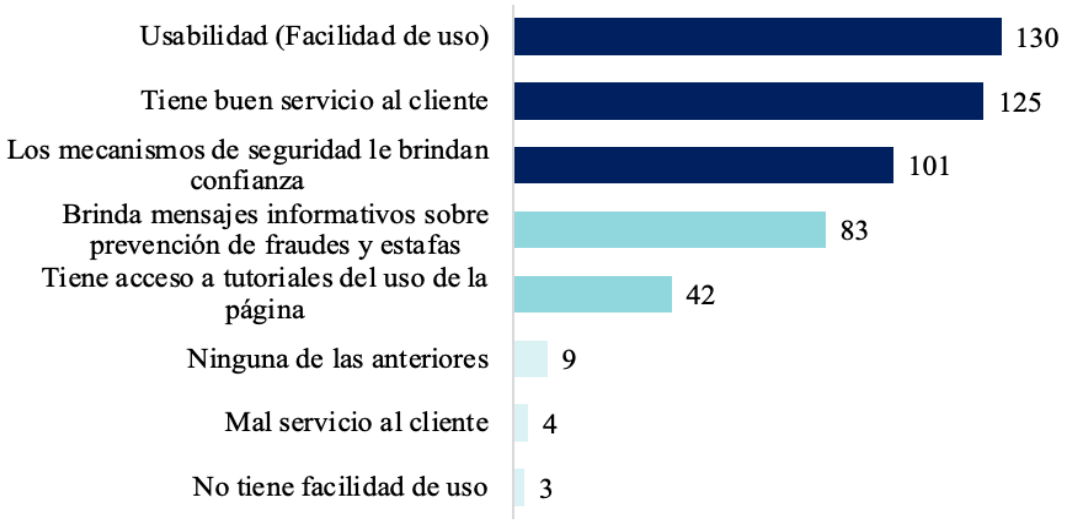
En lo que respecta al BCR, un 60 % de la muestra indica que la imagen corporativa del BCR es buena. Sin embargo, solo un 20 % indicó que es excelente y el restante 20 % lo ubica entre regular y pésima, por lo tanto, abre la posibilidad de que el Banco pueda seguir trabajando para que esta percepción que tienen los clientes aumente y logre consolidarse todavía más en el sector financiero. Para conocer sobre los aspectos en los cuales el BCR debe trabajar para mejorar la percepción de los clientes, se les consultó sobre el servicio al cliente que perciben por parte de la institución y la mayoría de los encuestados considera que brinda buen servicio, las plataformas digitales son fáciles de usar, tienen mecanismos óptimos de seguridad y envían mensajes sobre la prevención de fraudes. Estos son aspectos importantes sobre su imagen en la actualidad.

Figura 30
Evaluación de la imagen corporativa del Banco de Costa Rica



Fuente: Elaboración propia, 2022.

Figura 31
Opinión sobre el servicio que recibe del Banco de Costa Rica

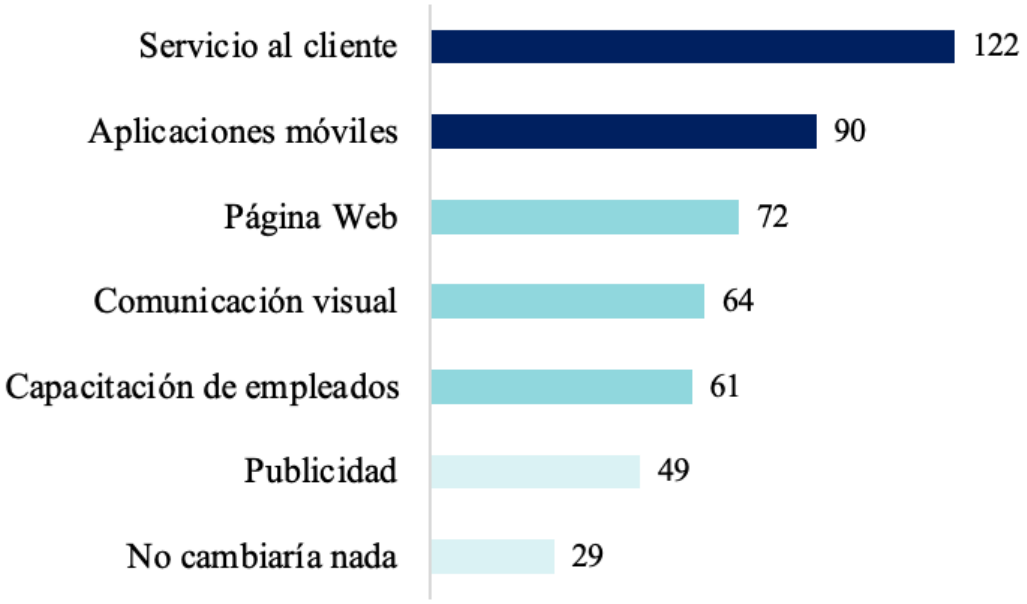


Fuente: Elaboración propia, 2022.

Por último, se preguntó sobre el aspecto que consideran importante rediseñar en la imagen del BCR y un 47 % de las personas encuestadas indicó que el servicio al cliente, un 35 % mejorar la aplicación móvil, un 28 % la página web, un 25 % capacitación de los empleados, entre otros. Resulta interesante que, por un

lado, las personas encuestadas consideran que el Banco tiene buen servicio al cliente, que las páginas digitales son fáciles de usar y que tienen mecanismos óptimos de seguridad, sin embargo, incluso así, son aspectos que también piden optimizar, por lo tanto, se puede definir que son características de constante cambio y que no se pueden dejar descuidadas para ser la institución financiera de preferencia en Costa Rica.

Figura 32
Aspectos que se consideran relevantes a cambiar en el BCR



Fuente: Elaboración propia, 2022.

4.4.2.2. Cuestionario

En primera instancia, se les consultó a las personas funcionarias del Departamento de Fraudes del BCR qué metodología de gestión de riesgo utilizan y 9 de las personas colaboradoras coincidieron en que se utiliza la metodología COSO Fraud Risk Management y esta se encuentra normada. De igual forma, utilizan otras metodologías de riesgo como la ISO 31000 y con estas logran desarrollar orientaciones de control interno, controlar el riesgo empresarial prevenir fraudes y mejorar el desempeño y supervisión organizacional. No obstante, tres colaboradores no

mencionan mecanismos de seguridad por lo que denotan no conocer qué es una metodología de riesgo ni cuál es la que el BCR utiliza.

Después de conocer la metodología de riesgo que se utiliza en la institución, se les consultó si tramitan o valorando incluir nuevos proyectos de gestión de riesgo, por lo que dos de las personas colaboradoras mencionaron que se encuentran con la actualización de la normativa bancaria en el tema de fraude, esto es importante para incluir nuevas metodologías. Por otro lado, tres colaboradores indicaron que se impartirán nuevas capacitaciones para conocer más sobre las metodologías de riesgo que se utilizan y cinco colaboradores mencionaron que crearán un nuevo centro de operación de seguridad (SOC) para integrar nuevas herramientas tecnológicas de monitoreo preventivo, anticorrupción y fraude interno. Por último, dos colaboradores no brindan una respuesta en concreto con respecto a los proyectos del banco.

Además, era importante conocer la opinión de las personas colaboradoras del Departamento de Prevención de Fraudes sobre los puntos fuertes de la gestión de riesgo que utilizan actualmente y, al preguntarles sobre estos, la mayoría indicó que los puntos más fuertes son la capacitación de las personas colaboradoras y el monitoreo constante de las transacciones. Por otra parte, otros aspectos que se mencionaron son control de riesgo, análisis forense de casos, análisis de seguimientos, la comunicación en el departamento y la prevención. Seguidamente, se les consultó sobre los mecanismos de seguridad con los que cuentan para la detección de fraudes y si consideran que son suficientes para la gestión adecuada del riesgo e indicaron que cuentan con un control y monitoreo físico de sitios en tiempo real con sistemas o aplicativos informáticos que ayudan al monitoreo constante de tarjetas y transacciones de las personas. Asimismo, indicaron que cuentan con un sistema propio de detección y otro tipo de mecanismos como:

- Las respuestas confidenciales
- Sistar (sistema de tarjetas)
- Salesforce (sistema de control de transacciones)

- VISA Risk Manager
- 3DS (3 dominios de seguridad de VISA, Mastercard y AMEX)

Con los sistemas antes expuestos, las personas colaboradoras indican que se eligieron porque todos son muy eficientes en la detección de patrones, auto-aprendizaje e inteligencia artificial y han dado buenos resultados en comparativa con otras instituciones financieras. Sin embargo, no coinciden en si son sistemas suficientes, ya que algunos indican que se pueden agregar más y otros piensan que no se necesitan más aplicativos.

Entrando en el tema específico de fraudes, se les consultó si se mantienen registros estadísticos de la cantidad de fraudes y la periodicidad en la que se efectúan; todos coincidieron que se realizan este tipo de estadísticas y que se gestiona y analiza por parte de la Jefatura del área. Al indicarse que se llevan estadísticas en el tema, se les preguntó sobre los tipos de fraude que más afectan a la institución, la mayoría de las respuestas que dieron coinciden en que la ingeniería social hacia el cliente juega un factor primordial para que se lleve a cabo el fraude y, de seguido, se mencionan en orden de afectación los fraudes electrónicos que más se utilizan:

1. Phishing.
2. Vishing.
3. Pharming.
4. Smishing.
5. Ransomware.
6. Spoofing.

Seguidamente, se consultó sobre la plataforma digital que más se utiliza para realizar los fraudes expuestos en la pregunta anterior y las personas colaboradoras indicaron que tanto la página web principal de personas como la aplicación móvil tienen una afectación similar y, en menor medida, el corresponsal llamado Tucán

(servicio para llevar a cabo transacciones bancarias en comercios de diferentes lugares) y la página web BCR comercial que se enfoca en las empresas. Asimismo, se consultó cuál de las dos plataformas (aplicación o móvil) es más segura contra fraudes; la mayoría coincide con que ambas son muy seguras. No obstante, un colaborador aclara que la aplicación es la más segura por poseer seguridad biométrica y no permitir el matricular cuentas bancarias para realizar depósitos.

Ante la interrogante de si existe algún control en tiempo real para la prevención de fraudes, todas las respuestas coincidieron en que sí poseen ese tipo de control con un sistema llamado Monitor Plus TI y tienen analistas que se encargan de ese monitoreo constante y el contacto inmediato con el cliente afectado. Siguiendo con el tema de la prevención de fraude, se les preguntó sobre cuál consideran que es el eslabón más débil en la cadena de seguridad del Banco, nueve funcionarios indicaron que el problema es el cliente o factor humano al brindar datos personales, sin embargo, dos funcionarios indicaron que el poco personal de la oficina de monitoreo en tiempo real y la forma reactiva de atender los fraudes son el eslabón débil.

Consultando sobre las medidas que han tomado para la educación de los clientes sobre fraudes, mencionan que han recurrido a comunicados, charlas, capacitaciones, inducciones, publicidad, campañas de prevención, entre otros. Sin embargo, también indican que las malas experiencias que les han pasado a los clientes y las noticias frecuentes en distintos medios de comunicación hacen que posean una mayor desconfianza de la institución y del sistema bancario en general.

Continuando con el tema, se les preguntó, si se está comunicando el tema de forma proactiva, por qué consideran que los casos y denuncias por fraude siguen en aumento, por lo que contestaron que uno de los factores principales es la confianza y falta de malicia que poseen los clientes sobre las llamadas, redes sociales y mensajes para que estos brinden datos sensibles sin darse cuenta y sean víctimas de fraude. De igual manera, mencionan que hay muchas instituciones en el aparato bancario costarricense que no trabajan de forma proactiva los fraudes y no invierten en sistemas avanzados para tener un método preventivo ante esta situación. Otra

respuesta que resaltar fue que no se mantiene un trabajo en conjunto e integración entre los distintos entes para que todos unan fuerzas y puedan disminuir la cantidad de casos. Por el contrario, todos trabajan de forma individual y la falta de políticas penales agresivas hace que todo se vuelva más complicado.

Para finalizar con el tema de fraudes, se les consultó sobre cómo se adaptan a las nuevas modalidades de fraudes y la mayoría de sus respuestas van en relación con los constantes estudios personales y capacitaciones sobre las nuevas modalidades y los fraudes que ya se llevan a cabo en otras latitudes para estar actualizados sobre la realidad mundial. Otra forma indicada es con la implementación de nuevos sistemas y mejoras en los sistemas actuales, con el fin de lograr un apoyo complementario en la prevención continua. Otra forma de adaptación que se mencionó es el estudio de patrones y el mapeo de oportunidades que puedan surgir según un proceso, cambio o generación que se dé en el ámbito nacional o regional.

A continuación, se les realizó consultas específicas de la institución y de su percepción como colaboradores. Por lo tanto, la primera consulta fue sobre si contaban con el personal suficiente dentro del área y el 66 % de las personas encuestadas indicó que contaban con suficiente personal, pero un 33 % indicó que no y que también tenían problemas de capacitación e integración. Lo anterior resulta preocupante por las deficiencias que se puedan presentar por este porcentaje del personal que está disconforme.

Al consultarle a las personas colaboradoras sobre el presupuesto que el BCR destina a la gestión de riesgo por fraude, el 100 % de las respuestas indica que desconocen el presupuesto. Sin embargo, mencionan que el BCR invierte en seguridad y cuenta con el presupuesto anual necesario.

Posteriormente, se les consultó sobre cuál es el proceso que tiene la institución en los casos de fraude y los tiempos de respuesta. Las personas funcionarias indicaron que el proceso siempre se tiene que realizar digitalmente en la página web del banco o directamente en la Contraloría de Servicios. Sobre los tiempos de respuesta siete de las personas funcionarias mencionan que desconocen el tiempo o todo depende del caso específico, tres funcionarios mencionan que los tiempos

se llevan de acuerdo con la ley y normativa interna y solo dos funcionarios indicaron tiempos específicos de 90 y 120 días de resolución.

Después de consultarles sobre el proceso y tiempos de espera, se les preguntó sobre los casos en los que el BCR se hace responsable por las pérdidas de los clientes y siete de las personas funcionarias indicaron que esto es un proceso que lleva el área de investigaciones y que ellos son los que determinan el resultado de la investigación. Un funcionario indicó que nunca se devuelven las pérdidas porque el cliente es el que comparte los datos personales y los restantes colaboradores indican que, si se determina que los clientes no tuvieron participación o el sistema de control de riesgos, las personas funcionarias, la normativa y la ley hayan sido vulneradas o fallaron se asume la responsabilidad como institución.

Por último, se les preguntó sobre la percepción que tienen del BCR en el manejo de los fraudes y de la percepción de la imagen corporativa que tienen los clientes de la institución. Con respecto a la primera consulta, once de las personas funcionarias indicaron que el manejo de los fraudes en el Banco se realizó de una manera excelente y que al poseer una plataforma robusta también cuentan con estadísticas de autoridades judiciales que los posiciona como una entidad líder en el manejo de fraude. Por el contrario, solo un funcionario indicó que el manejo es bueno, pero que puede mejorar para ser excelente. Con base en la segunda pregunta, también once de las personas funcionarias indicaron que la imagen corporativa del Banco es excelente y así se lo hacen saber los distintos clientes físicos y jurídicos, sin embargo, falta potenciar, observar y publicitar esos resultados a los clientes y la inversión en fraudes para que se logre una mejor percepción. El funcionario que indicó en la pregunta anterior que el manejo del fraude es bueno, pero se puede mejorar, mencionó lo mismo para esta consulta.

Además, se puede implementar un indicador de resultados clave para cada una de las personas que revisan en tiempo real las transacciones, que mida el porcentaje que reporta como fraudulentas del total que aprobaron y que las características se revisen tanto a nivel macro como de forma individual para detectar tendencias o patrones de fraude que puedan aumentar la pericia de estos analistas en el

futuro. Asimismo, esta información debe compartirse entre todas las entidades bancarias para que en conjunto puedan realizar una detección de fraude más amplia.

Capítulo V. Propuestas

5.1. Propuesta modelo de gestión de riesgo

Con base en los resultados de la investigación, se obtiene que la gestión de prevención de fraude del Banco de Costa Rica es robusta y utiliza estándares de prevención actualizados. Por lo tanto, la percepción que tienen los clientes de la institución es positiva hasta el punto de que el 80 % de las personas encuestadas la catalogan como buena o excelente.

Sin embargo, tomando como base los aspectos por mejorar que se desprenden de la investigación, se presenta una propuesta por medio de la integración de la metodología COSO con las tres líneas de defensa que se basa en el documento *Aprovechar el COSO en las Tres Líneas de defensa* (Anderson y Eubanks, 2015). La propuesta se relaciona con los hallazgos detectados y la actualización más reciente del modelo de las líneas de defensa ahora llamado el modelo de las tres líneas. Lo anterior ayuda a que los órganos de gobierno corporativo del Conglomerado Financiero BCR apliquen esta propuesta para fortalecer todavía más su gestión de fraude y, de este modo, influenciar positivamente la imagen corporativa.

De acuerdo con el Código de Gobierno Corporativo del BCR (2009), las líneas de defensa se estructuran de la siguiente manera:

- Primera línea de defensa: es la responsable de la gestión diaria de los riesgos, para efectos de esta investigación es el Departamento de Prevención de Fraudes.
- Segunda línea de defensa: es la encargada de supervisar los riesgos, que es el Departamento de Cumplimiento BCR.
- Tercera línea de defensa: encargados de evaluar internamente a la compañía, se traduce al Departamento de Auditoría Interna del BCR.

A continuación, se resume la integración que se mencionó, con base en los hallazgos que se obtienen. En primera instancia, se menciona el hallazgo, después

se desarrolla el rol o acción requerido para cada línea, así como el papel que desempeña la Junta Directiva del BCR en su administración correcta y, por último, se integra con el principio pertinente de la metodología COSO.

Tabla 6
Propuesta gestión de riesgo por fraude

Hallazgo	Primera línea (Gerencia de Banca Corporativa del BCR)	Segunda línea (Departamento de Prevención de Fraudes del BCR)	Tercera línea (Auditoría interna BCR)	Otro (Junta Directiva del BCR)	Principio(s) COSO
1. Promover la imagen corporativa, ya que es esencial para la gestión y crecimiento del banco[1].	• Recopilar los datos aportados por la oficina de prevención de fraudes para comunicar la gestión de riesgo efectuada en la organización. • Garantizar la confiabilidad e integridad de la información sobre los resultados de gestión de riesgo.	• Generar y almacenar los datos sobre la gestión de fraude.	• Evaluar la confiabilidad e integridad de los datos, de forma periódica	• Analizar la información que se recopiló para la toma de decisiones y anticipación de riesgos	• Principios de información y comunicación (14 y 15), puesto que se da una comunicación interna y externa. Asimismo, el uso de la información relevante.
2. Estandarizar procesos y conocimiento.[2]	• Compartir, de forma clara, información, procedimientos y objetivos necesarios	• Mantenerse informado sobre los procesos de gestión de riesgo	• Evaluar la coherencia de las evaluaciones con respecto a los	• Supervisar el desarrollo y evaluaciones de los componentes de control	• Principio 14: la organización comunica la información

[1] En la Tabla 8 se detalla una propuesta con soluciones específicas del hallazgo 1.
[2] En la Tabla 9 se detalla una propuesta con soluciones específicas de los hallazgos 2, 3, 4, 5 y 7.

	para realizar las labores de control de fraude a todo el personal del Departamento de Riesgos. • Realizar evaluaciones para monitorear el conocimiento de las personas colaboradoras sobre los procesos de gestión de fraude.	para cumplir con los objetivos y evaluaciones de la Gerencia.	procesos de negocio.	interno. • Recibir informes periódicos sobre el riesgo de la organización y las operaciones de gestión de riesgo.	internamente (incluidos los objetivos y las responsabilidades por el control interno) necesaria para respaldar el funcionamiento del control interno
3. Mejorar la eficiencia y los procesos para los tiempos de espera en la resolución de los casos.	• Comunicar a las personas colaboradoras del Departamento de Prevención de Fraudes los tiempos de resolución establecidos en normativa para que haya un mayor conocimiento de estos y, de esta forma, llevar un mejor control en la resolución final.	• Gestionar, de forma proactiva, los casos de fraude que llegan diariamente a la institución y velar porque se gestionen oportunamente	• Validar el cumplimiento de los tiempos estipulados en lo normativo.	• Revisar los informes de riesgos emitidos por el comité de riesgo y los informes de auditoría para determinar un buen manejo de las líneas de control.	• Principio 12 sobre las actividades de control a través de políticas que establecen los pasos y los procedimientos que transforman las políticas en acción.
4. Educar a la población vulnerable	• Enfocar su atención en la prevención y educación sobre el	• Monitorear las actividades de prevención	• Validar si los procedimientos para la	• Evaluar con base en los resultados de los informes	• Principio 10: la organización selecciona y

	fraude de las poblaciones más afectadas y que lideran los casos por el fraude que va en aumento	ejecutadas por la Gerencia y reforzar la educación en los clientes cuando sea posible	educación/concientización sobre fraude de la población vulnerable están diseñados correctamente y son efectivos en concordancia con los objetivos que se plantearon.	recibidos si la educación a las poblaciones más afectadas por los fraudes se traduce a una disminución de estos en concordancia con la misión del banco de impulsar el desarrollo social y económico de los costarricenses.	desarrolla actividades de control que contribuyen con mitigar los riesgos que se relacionan con el logro de los objetivos a niveles aceptables.
5. Evaluar la cantidad de personal ideal para el Departamento de Prevención de Fraudes	• Realizar un estudio de cargas de trabajo para determinar si las responsabilidades están establecidas claramente y distribuidas y se ejecutan de forma adecuada, oportuna y efectiva. • Definir y aplicar las acciones de mejora con base en los resultados del estudio.	• Suministrar la información necesaria de las funciones individuales de cada funcionario para que se determinen las cargas de trabajo y se lleve un esquema completo de funciones.	• Revisar la propuesta realizada por la primera línea, con el fin de que se adapte en lo normativo y no posea vicios.	• Constatar mediante los informes de gestión recibidos, los requerimientos de mejora de la gestión de prevención de fraudes y si aplica autorizar las plazas para la nivelación de las cargas de trabajo.	• Principio 4 la organización demuestra su compromiso para atraer, desarrollar y retener a los individuos competentes en coordinación con los objetivos.
6. Explorar	• Mantener	• Monitorear la	• Evaluar si los	• Supervisar que	• Principio 10:

nuevas fuentes de información y aprovechar en mayor medida las existentes	controles internos efectivos para la gestión y control de los riesgos. Su misión debe ser identificar, evaluar, controlar y mitigar los riesgos	aplicación adecuada de los controles definidos por la Gerencia. • Velar por la ejecución de los procesos y políticas para la prevención, detección y mitigación de riesgos por fraude. • Alertar cuando consideren que los sistemas que se utilizan no sean suficientes/óptimos para la gestión de fraude o se vuelvan obsoletos. • Utilizar información interna y externa que genere alertas para el análisis de riesgo por fraude potencial.	controles establecidos se ejecutan de manera correcta y apropiada para la gestión de riesgos y el cumplimiento de objetivos.	los sistemas de control interno sean adecuados para cumplir con los objetivos.	La organización define y desarrolla actividades de control que contribuyen con la mitigación de los riesgos hasta niveles aceptables para la consecución de los objetivos.

7. Fortalecimiento de la oficina de prevención de fraudes por medio de capacitaciones en el ámbito nacional e internacional[3]	• Establecer capacitaciones periódicas a las personas funcionarias del Departamento de Prevención de Fraudes para lograr un desarrollo adecuado de acuerdo con estándares internacionales y adecuados a la realidad global.	• Especializarse en temas de prevención de fraudes para que se adapten a los cambios constantes que se dan en el ámbito global y estar preparados ante eventuales ataques a la institución.	• Verificar que los programas y capacitaciones adquiridas cumplan con los requisitos establecidos.	• Establecer un mayor presupuesto en el área de prevención de fraudes para que puedan invertir en este tipo de capacitaciones.	• Principio 9 la organización identifica y analiza los cambios que pueden impactar significativamente en el control interno de la entidad.

Fuente: Elaboración propia, con datos de la presente investigación y de Anderson y Eubanks (2015).

[3] En la Tabla 10 se detalla una propuesta con soluciones específicas del hallazgo 6.

Aunado a los hallazgos de la propuesta de gestión de fraude, se encontró oportunidad de mejora desde la percepción de los clientes para la imagen corporativa del BCR. Por lo tanto, se presentan las siguientes recomendaciones:

Tabla 7
Recomendaciones para la mejora de la imagen corporativa

Propuesta de mejora
Servicio al cliente • Invertir en programas y guías a las personas colaboradoras que se encuentran frente al cliente, con el fin de desarrollar diferentes habilidades y con esto mejorar en los siguientes aspectos: o Profesionalismo: efectividad, eficacia y conocimiento sobre el trámite que se realiza. o Capacidad de respuesta: disposición hacia los clientes con un servicio rápido, oportuno y efectivo. o Comunicación: capacidad de transmitir ideas claras hacia el cliente. o Lenguaje corporal: deben siempre proyectar expresiones calmadas, interesadas y sinceras hacia la situación que pasa el cliente. Este lenguaje puede facilitar mucho la comunicación y ayuda a brindar un buen servicio. o Movimiento corporal: con los movimientos corporales pueden reflejar al cliente seguridad y una buena atención hacia la solicitud que se está tramitando. o Contacto visual: el contacto visual logra una buena conexión con el cliente. o Tono de voz: con el tono de voz se pueden calmar muchas situaciones y también darle un giro a distintos problemas que se tengan que solucionar. • Realizar encuestas de satisfacción con el servicio recibido por el funcionario del BCR para que con esto puedan llevar un control del servicio que se realiza y se puedan tomar decisiones que mejoren la experiencia del cliente
Aplicaciones móviles y página web • Disminuir el tiempo de respuesta del mecanismo de seguridad biométrico del rostro, para que se haga el reconocimiento facial sin fallas. • Diagramar la página web, esta posee mucha información y su jerarquía es deficiente, porque hay más información irrelevante para los usuarios en la página de inicio y la información relevante requiere de mayor búsqueda (más clics y navegación) en esta. • Redefinir el diseño de la página, de forma que no se sobrecargue con imágenes y *banners* y provoque distracción al usuario.

Comunicación visual • Mantener la línea de diseño, por medio del uso constante del libro de marca, para mantener un estándar.
Capacitación de empleados • Capacitaciones, refrescamientos mensuales sobre prevención de fraude y qué hacer en caso de verse afectado por los mismos al personal de primera línea. Esto con vistas a que los clientes reciban educación apropiada en todo momento sobre el tema, aunque el motivo de sus consultas sea por otras razones.
Publicidad • Enviar publicidad por distintos medios de comunicación para informar sobre la gestión correcta por fraude electrónico realizado en el BCR.

Fuente: Elaboración propia, 2022.

5.2. Propuestas que se relacionan con los hallazgos de la gestión del riesgo

5.2.1. Imagen corporativa

Tabla 8
Propuesta imagen corporativa

Hallazgo	Propuesta de mejora
Promover la imagen corporativa, ya que es esencial para la gestión y crecimiento del banco.	• Definir los datos relevantes para recolectar: o Cantidad de casos por denuncias sobre fraude. o Cantidad de quejas realizadas por redes sociales en las páginas oficiales del Banco. o Cantidad de casos en los que hubo vulnerabilidad de los sistemas del BCR. o Cantidad de casos en los que hubo responsabilidad del cliente (clasificarlos por tipos de fraude). • Asignar un encargado de desarrollar, mantener y actualizar los reportes sobre los datos recolectados en la gestión de riesgo. • Realizar reuniones de seguimiento semanales para exponer los datos recolectados de fraude. • Realizar boletines y actualizaciones mensuales en la página SOMOS BCR para mantener informadas a todas

	las personas colaboradoras del conglomerado sobre la gestión de fraude digital

5.2.2. Mejora continua

Tabla 9
Propuesta mejora continua

Hallazgo	Propuesta de mejora
Estandarizar procesos y conocimiento	• Realizar pruebas de conocimientos al Departamento de Prevención de Fraudes una vez al mes. En los casos en los que los resultados no sean los ideales, efectuar refrescamientos de la información. • Crear un centro de conocimiento (WIKI) que incluya los objetivos, políticas y los procedimientos para la gestión correcta del fraude electrónico y nombrar a un responsable de darle publicidad, seguimiento y mantenimiento.
Mejorar la eficiencia y los procesos para los tiempos de espera en la resolución de los casos.	• Implementar la plataforma de Microsoft Planner como herramienta principal de monitoreo de los casos de fraude. • Incluir cada caso individual de fraude en una tarea de Microsoft Planner con tiempos de resolución y clasificado por etapa del proceso (investigación interna y externa) para recibir alertas de vencimiento, orientadas a mejorar la eficiencia en la resolución de los casos. • Incluir un análisis estadístico de históricos sobre tiempos de resolución segmentados por etapa de proceso para identificar procesos de mejora con base en el tiempo.
Educar a la población vulnerable.	• Utilizar los recursos con los que se cuenta (demografía e historial transaccional de las personas que han denunciado ser víctimas de fraude y canales disponibles para compartir información) para definir los medios más eficaces por donde se pueda educar a esta población en temas de identificación y prevención de fraude. Lo anterior también resulta no solo en una mitigación del riesgo, sino en una

	oportunidad para crear valor en el BCR al generar más confianza en los clientes.
Evaluar la cantidad de personal ideal para el Departamento de Prevención de Fraudes.	• Implementar indicadores clave de rendimiento que midan aspectos como la velocidad, nivel de ocupación (tiempo efectivo de trabajo) y la calidad de la resolución de los casos de los analistas de fraude para nivelar las cargas de trabajo y eficacia entre estos. • Coordinar con el Departamento de Gestión de Procesos y Productividad sesiones de tomas de tiempo individuales para cada colaborador del Departamento de Fraudes para definir las cargas de trabajo y, por ende, el número de personas requeridas.
Fortalecer a la oficina de prevención de fraudes por medio de capacitaciones en el ámbito nacional e internacional.	• Aprovechar *webinars* (seminarios virtuales) sobre temas relevantes a la gestión de fraude y asignar tiempos específicos para educación de las personas colaboradoras.

5.2.3. Proveedores de datos

Tabla 10
Propuesta fuentes de información para el análisis del fraude

Hallazgo	Propuesta de mejora
Explorar nuevas fuentes de información y aprovechar en mayor medida las existentes.	• La gerencia puede accionar las siguientes ideas: A. Contratar proveedores de bases de datos especializadas u obtener información de otras entidades financieras (hay que sugerir que la información se comparta por medio de la Asociación Bancaria Costarricense) que ayuden, de manera redundante, a confirmar si existe riesgo de fraude en los perfiles de los clientes. Los datos por obtener al menos son: Dirección IP, ubicación actual, ubicaciones pasadas y reputación del dispositivo que se utiliza (por ejemplo, sistemas de enmascaramiento de ubicación, conexión sospechosa por IP o puntos de acceso con otros dispositivos asociados con fraude) para realizar la transacción (se puede utilizar la distancia en kilómetros del punto de acceso con respecto a la dirección registrada de la persona en el banco como un punto de información para medir si el

	comportamiento de la persona es normal o no). Evaluación del riesgo de la cuenta de correo electrónico del cliente registrado en el banco. Existen proveedores que evalúan el riesgo de las cuentas de correo electrónico con base en datos que se obtienen por diversas empresas registradas en su red. Una cuenta de correo que ha sido vulnerada puede identificarse y considerarse antes de que se realicen transacciones fraudulentas. B. Utilizar datos históricos de los clientes para detectar actividad irregular. Se puede tomar en cuenta para congelar una transacción y revisarla, de forma manual (incluso llamando al cliente de ser necesario), lo siguiente: Envíos de dinero por altos montos o alta frecuencia que no estén en concordancia con montos y frecuencia normal del cliente. Envío de dineros a cuentas (incluido Sinpe Móvil) que se relacionan con posible fraude según reportes de otros clientes. Tiempos de duración para realizar una transacción *cortos* para personas mayores de edad o que nunca hayan utilizado el servicio antes.

Fuente: Elaboración propia, 2022.

Con las propuestas de mejora anteriores, se pretende llevar a un nivel de aceptación todavía más alto a la gestión de riesgo que realiza el BCR al integrar a las líneas correspondientes de la institución por medio de los principios del COSO. De igual manera, se posicionaría de una mejor manera la imagen corporativa que tiene la institución actualmente para influenciar al 80 % de personas que la considera entre buena y pésima, con el fin de ampliar el 20 % restante que indica que es excelente.

Capítulo VI. Conclusiones y recomendaciones

Con base en lo realizado en el trabajo de investigación, se determinan las siguientes conclusiones y recomendaciones para la gestión de riesgo por fraude en el Banco de Costa Rica.

6.1. Conclusiones

- El personal del Departamento de Prevención de Fraudes debe estar más alineado con respecto al conocimiento, prácticas y políticas del Banco en cuanto a la mitigación y servicio al cliente en cuestiones de fraude electrónico. Lo anterior se debe a que las personas colaboradoras encuestadas no coinciden en sus respuestas sobre modelos de gestión del riesgo ni de sus puntos fuertes para la mitigación de este.

- El BCR está realizando esfuerzos por medio de comunicados, charlas, capacitaciones, inducciones, publicidad, campañas de prevención, entre otros, para que sus clientes conozcan cómo no ser parte de la estadística de víctimas del fraude electrónico. No obstante, deben fortalecer esta práctica para que sea una constante en la cultura del banco y que esta se traslade a todos sus clientes año tras año.

- La imagen corporativa es esencial para la diferenciación entre otras entidades bancarias, puesto que son empresas que brindan servicios estándar. No basta solamente enfocarse en esfuerzos de índole económica y financiera para contar con una cartera robusta de clientes que confíen en ellos. La imagen corporativa es el factor diferenciador para que los clientes perciban confianza, fortaleza y seguridad y prefieran utilizar sus servicios a diferencia de otras instituciones que no velan por su imagen corporativa.

- Durante el paso de los años, el fraude a nivel electrónico ha variado y se ha adaptado a las nuevas formas de prevención que aplican las instituciones. Por lo tanto, la gestión que apliquen las entidades bancarias tiene que estar en constante actualización para anticiparse al estudio de los delincuentes

sobre cómo evitar los mecanismos de seguridad. De esta forma, tener un mecanismo de respuesta oportuno para minimizar el impacto de los ataques. Por lo tanto, es importante que el BCR entienda que en temas de fraude electrónico no se trata de gestiones estáticas, por el contrario, gestiones dinámicas que se adapten al entorno donde operan y a las nuevas versiones y desarrollos tecnológicos.

- El Banco de Costa Rica cuenta con sistemas robustos para la prevención, detección y resolución del fraude. Por un lado, el Banco basa su gestión de riesgos global en el modelo de tres líneas de defensa, que integra la atención por parte de tres entes de la organización independientes que velan por el cumplimiento de los objetivos corporativos, a la vez que mitigan y controlan los riesgos asociados. Además, emplean la metodología COSO en su Departamento de Fraudes que se basa en 17 principios para la gestión de fraude.

- El Banco ha mantenido una buena gestión de fraude durante los años, sin embargo, esa gestión no la está percibiendo un 20 % de sus clientes según los resultados de la encuesta. Por lo tanto, se deben hacer más esfuerzos para brindar información respecto a los trabajos y solidez que poseen.

- El Banco de Costa Rica es una institución sólida que se ha mantenido financieramente estable durante su existencia. Sin embargo, debido a que el fraude se da por el descuido/ingenuidad de sus clientes, presenta entre 5 y 6 reclamos diarios por fraude. La tendencia nacional de reportes por fraude en las entidades financieras va en aumento. El tema de la educación y prevención en la persona usuaria es una oportunidad en especial para aquellos que no cuentan con conocimientos o recursos tecnológicos que es por donde usualmente se recibe esta información. Por lo tanto, se percibe una necesidad en este campo que todavía no se atiende a cabalidad por el BCR.

- Las nuevas tecnologías representan una gran oportunidad para el desarrollo bancario, sin embargo, tienen nuevos riesgos en el ámbito de fraude

electrónico. Por ejemplo, el Sinpe Móvil ha venido a facilitar las transacciones entre usuarios de distintas instituciones, de una manera nunca vista, no obstante, los cambios y desarrollos tecnológicos siempre traerán una contraparte que incluye un aumento en los riesgos de fraude mientras exista al menos el factor humano de por medio.

6.2. Recomendaciones

- Debe analizarse a la población que está reportando más fraudes para obtener cuáles son sus puntos en común/factores de riesgo. Estos usualmente incluyen a personas no familiarizadas con fraude y así desarrollar herramientas que logren educar a esta población con un enfoque fuerte en la identificación de situaciones en las que pueden estar siendo víctimas de ingeniería social, *software* maligno o estafas, entre otros.

- Deben mejorarse los sistemas y prácticas para la detección de fraude en tiempo real, ya que es claro que hay transacciones que no se están inspeccionando o deteniendo y terminan siendo fraude. Para esto, deben considerarse los históricos del tipo de cambio en la actividad, comportamiento del usuario, puntos de información (dispositivo que se utiliza, edad del usuario, tiempo de la transacción, ubicación, entre otros) de las transacciones fraudulentas y así identificar patrones que puedan mejorar el sistema de detección actual.

- Debido a que las entidades financieras presentan incidencias de seguridad en un 300 % a empresas de otros sectores la inversión tecnológica debe continuar. Usualmente, las nuevas tecnologías bancarias se dan primero en países desarrollados. El banco debe formar alianzas con bancos de estos países para identificar cuáles técnicas, sistemas y controles utilizan e implementan para la gestión de fraude y emularlos de acuerdo con la implementación de nuevas tecnologías bancarias en Costa Rica.

- Los modelos de las tres líneas de defensa del IIA en el 2020 evolucionaron al modelo de las tres líneas. Se eliminó la palabra defensa, ya que

consideraron que este modelo no debe solo enfocarse en la gestión de los riesgos para defenderse de estos, sino que también se pueden aprovechar las oportunidades que estos presentan para la consecución de los objetivos organizacionales. El BCR debe considerar la actualización de su metodología este nuevo pensamiento, pues puede ayudarle a ser más proactivo en la educación de las poblaciones afectadas diariamente por el fraude y que consecuentemente está impactando en su imagen corporativa.

- Según la normativa bancaria, el Banco dispone de 120 días para responder ante un caso de fraude presentado a un cliente. Por lo tanto, se recomienda que se valore este tiempo para que se pueda reducir y, de este modo, los clientes perciban que se trabaja de forma proactiva en los casos de delitos informáticos.

- El BCR actualmente mantiene un total de 12 colaboradores en el Departamento de Prevención de Fraudes. Sin embargo, se recomienda que la Junta Directiva haga un estudio del departamento para aumentar la cantidad de personal y pueda fortalecerlo, ya que algunos funcionarios consideran que no tienen el personal de trabajo adecuado y las cargas de trabajo están mal distribuidas. Asimismo, debe estandarizar su capacitación, puesto que sus colaboradores no poseen una coherencia entre los conocimientos de sus modelos de gestión de riesgo y cómo gestionarlo.

- Aumentar la comunicación institucional y externa sobre las gestiones y desarrollos que se realizan en la gestión de fraudes para que la imagen que poseen los clientes de la institución mejore y con esto la confianza aumente. Esta confianza es fundamental en las instituciones bancarias, ya que forma parte de un gran factor de diferenciación junto con el servicio al cliente.

- Consideramos que la integración de ambas metodologías (COSO y modelo de las tres líneas) fortalecerán, de una manera estructurada y detallada, los puntos de acción para la gestión del fraude del departamento.

Referencias bibliográficas

Aguilera, P. (2010). *Seguridad Informática*. EDITEX. https://books.google.es/books?hl=es&lr=&id=Mgvm3AYIT64C&oi=fnd&pg=PA1&dq=Seguridad+informatica+aguilera&ots=PqskU-CzIX3&sig=_N0l12FH8EbNv0si8PlWyaxjsXU#v=onepage&q&f=false

Alcázar, J. *et al.* (2019). *La banca costarricense y sus retos, desde una perspectiva de ética, imagen, credibilidad y confianza*. https://www.scielo.sa.cr/scielo.php?pid=S1659-49322020000100033&script=sci_arttext

Anderson, D. y Eubanks, G. (2015). *Aprovechar el COSO en las Tres Líneas de defensa*. FLAI. https://laflai.org/documentos/COSO_2015-3LOD-Thought-Paper-FULL_r3_ES.pdf

Arrieta, E. (2017). *Crisis del BCR golpea solo imagen*. La República. https://www.larepublica.net/noticia/crisis-del-bcr-golpea-solo-imagen

Babinchak, J. (2020). *IIA Issues Important Update to Three Línes Model*. Modernizing the Widely Used Approach to Governance, Risk. https://na.theiia.org/news/press-releases/Pages/IIA-Issues-Important-Update-to-Three-Lines-Model.aspx

BAC Credomatic. (2021). *Informe anual-Gestión integral de riesgo 2021*. https://www2.baccredomatic.com/es-cr/nuestra-empresa/informes-anuales-de-riesgos

BAC Credomatic. (s. f.). *Sobre nosotros*. https://www.baccredomatic.com/es-cr/nuestra-empresa/sobre-nosotros

Baca Urbina, G. (2016). *Introducción a la seguridad Informática*. Grupo Editorial Patria.

https://books.google.es/books?hl=es&lr=&id=IhUhDgAA-QBAJ&oi=fnd&pg=PP1&dq=mecanismos+de+seguridad++in-form%C3%A1ticos&ots=0WTz6BuhGs&sig=oWHhZSm_haLgz8cJi6-ZTdI7MGE#v=onepage&q=mecanismos%20de%20seguridad%20%20in-form%C3%A1ticos&f=false

Banco BCT. (s. f.). *Historia*. https://www.bancobct.com/acerca-de-bct-historia/

Banco Cathay. (s. f.). *Historia*. https://www.bancocathay.com/historia.html

Banco Central de Costa Rica. (2021). *BCCR alerta a la población sobre intentos de estafas con timo que se basa en Sinpe Móvil*. https://www.bccr.fi.cr/co-municacion-y-prensa/Docs_Comunicados_Prensa/CP-BCCR-026-2021-Alerta_intentos_estafas_timo_basado_Sinpe_Movil.pdf

Banco CMB. (s. f.). *Notas a los estados financieros*. https://www.citi-bank.com/icg/sa/latam/costa-rica/assets/docs/estados-financieros-2019/No-tas_a_los_estados_financieros_Banco_CMB_Jun_19.pdf

Banco de Costa Rica (BCR). (2009). *Código de Gobierno Corporativo*.

Banco de Costa Rica (BCR). (2021a). *Historia*. https://www.ban-cobcr.com/wps/portal/bcr/bancobcr/acerca-del-bcr/informacion_corpora-tiva/historia/

Banco de Costa Rica (BCR). (2021b). *Informe anual-Gestión integral de riesgo 2021*. https://www.bancobcr.com/wps/portal/bcr/bancobcr/acerca-del-bcr/transparencia/informes/gestionRiesgo/

Banco de Costa Rica (BCR). (2021c). *Nosotros*. https://www.ban-cobcr.com/wps/portal/bcr/bancobcr/acerca-del-bcr/informacion_corpora-tiva/mision_vision/

Banco de Costa Rica (BCR). (2021e). *Organización*. https://www.ban-cobcr.com/wps/portal/bcr/bancobcr/acerca-del-

bcr/informacion_corporativa/organizacion/

Banco de Costa Rica(BCR). (2021d). *Nuestros valores*. https://www.bancobcr.com/wps/portal/bcr/bancobcr/acerca-del-bcr/informacion_corporativa/valores/

Banco Interamericano de Desarrollo. (2020). *Ciberseguridad: Riesgos, avances y el camino por seguir en América Latina y el Caribe*. https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

Banco Nacional de Costa Rica. (2021). *Informe anual-Gestión integral de riesgo 2021*. https://www.bncr.fi.cr/_cache_551a/content/1609240000101242.pdf

Banco Nacional. (s. f.). *Conózcanos*. https://www.bncr.fi.cr/conozcanos

Barrantes Echavarría, R. (2014). *La investigación: un camino al conocimiento*. Euned.

Bergman, B. (2005). *E-fraud - State of art and Countermeasures* [Fraude electrónico - Lo último y contramedidas]. http://liu.diva-portal.org/smash/get/diva2:20140/FULLTEXT01

BID. (2020). *Estado de la Ciberseguridad en América Latina y El Caribe*. https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

Cabral Vargas, B. (2017). *Recursos y medios digitales de información Elementos teóricos y su uso desde la Bibliotecología*. UNAM. https://ru.iibi.unam.mx/jspui/handle/IIBI_UNAM/L219

Cabral Vargas, B. (2018). Consideraciones para el almacenamiento de archivos digitales en la nube informática en bibliotecas universitarias. *Investigación*

bibliotecológica, 32(2018) 55-75.

Centro de Información Jurídica en Línea. (2009). *La Estafa*. https://cijulenlinea.ucr.ac.cr/portal/descargar.php?q=MTEwMA==

Chacón Jiménez, K. (2017). *Así se perfila la Banca en Costa Rica en 5 años*. El Financiero. https://www.elfinancierocr.com/tecnologia/asi-se-perfila-la-banca-en-costa-rica-en-cinco-anos/JW2ZE56ODJE6NBV5WAGZ63VKPQ/story/Bureau

Corrales, G. (2014). *Welivesecurity*. ESET. https://www.welivesecurity.com/wp-content/uploads/2014/01/guia-autenticacion-eset.pdf

Cortés Hernández, A. M. (2019). *Ingeniería social: phishing y baiting*. Universidad Piloto de Colombia. http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6349/Ingenieria%20social%20Phishing%20y%20Baiting.pdf?sequence=1&isAllowed=n

Currás Pérez, R. (2010). *Identidad e imagen corporativas: revisión conceptual e interrelación*. https://www.redalyc.org/pdf/4561/456145285002.pdf

Davivienda. (s. f.). *Sobre nosotros*. https://www.davivienda.com/wps/portal/personas/nuevo/personas/quienes_somos/sobre_nosotros

Delgado, S. (2015). *Aplicación de los intereses pasivos y activos en el sistema bancario ecuatoriano y sus efectos macroeconómicos 2007-2013* (Tesis de maestría, Universidad de Guayaquil). http://repositorio.ug.edu.ec/bitstream/redug/7809/1/TESIS%20SILVIA%20DELGADO%2006-06-2015.pdf

Douglas A. y Eurobank, G. (2015). *Aprovechar el COSO en las Tres Líneas de defensa*. https://laflai.org/documentos/COSO_2015-3LOD-Thought-Paper-FULL_r3_ES.pdf

El Financiero. (2019). *La rentabilidad y el tamaño de la Banca en Costa Rica*.

https://www.larepublica.net/noticia/la-rentabilidad-y-el-tamano-de-la-banca-en-costa-rica

Escoto Leiva, R. (2001). *Banca comercial Euned*. https://books.google.co.cr/books?id=oDIBV4vO54IC&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

Feedzai. (2022). *Los tres principales desafíos del fraude en línea para los bancos*. https://feedzai.com/es/blog-delitos-financieros/los-tres-principales-desafios-del-fraude-en-linea-para-los-bancos/

Fodymanow, K. (2016). *Imagen corporativa*. Facultat de Belles Arts de Sant Carles. https://riunet.upv.es/bitstream/handle/10251/60607/FODYMANOW%20-%20IMAGEN%20CORPORATIVA.pdf?sequence=2

Fraud Magazine. (2016). *ACFE se asocia con COSO*. https://www.fraud-magazine.com/article.aspx?id=4294994631

Fundación Latinoamericana de Auditores Internos (FLAI). (2020). *El modelo de las tres líneas del IIA 2020*. *Una actualización de las tres líneas de defensa*. https://global.theiia.org/translations/PublicDocuments/Three-Línes-Model-Updated-Spanish.pdf

García, J. y Salazar, P. (2005). *Métodos de Administración y Evaluación de Riesgos*. http://repositorio.uchile.cl/tesis/uchile/2005/garcia_j2/sources/garcia_j2.pdf

González Martínez, R. (s. f.). *Marco Integrado de Control Interno, Modelo COSO III*. Manual del participante. https://docplayer.es/24887117-Marco-integrado-de-control-interno-modelo-coso-iii-manual-del-participante-autor-c-p-rafael-gonzalez-martinez-introduccion-2.html

Grupo UTE. (2016). *4 Técnicas de Auditoría - Flujo -Diagramación*. http://uteaudinfor.blogspot.com/2016/05/4-tecnicas-de-auditoria-flujo.html

Guamán Sinchi, B. (2014). *Anatomía de un ataque informático*. Universidad del Azuay. http://dspace.uazuay.edu.ec/handle/datos/5046

Hernández, R.; Fernández, C. Baptista, P. (2014). *Metodología de la investigación*. McGraw-Hill/Interamericana Editores, S. A. de C. V.

Improsa. (s. f.). *Historia*. https://www.grupoimprosa.com

Instituto Nacional de Estadística y Censos (INEC). (2018). *Encuesta Nacional de Hogares 2018*. https://www.inec.cr/noticia/crece-el-robo-y-las-estafas-de-dinero-por-internet

Instituto Nacional de Estadística y Censos (INEC). (2022). *Encuesta Continua de Empleo al primer trimestre del 2022*. https://www.inec.cr/sites/default/files/documetos-biblioteca-virtual/ece_i_t_2022.pdf

Internet Crime Complaint Center. (2020). *Frequently Asked Questions* (Preguntas Frecuentes). https://www.ic3.gov/faq/default.aspx

ISO 27000. (2018). *SGSI*. https://normaiso27001.es/referencias-normativas-iso-27000/#h31

ISOTools. (2020). *Sistemas de Gestión Normalizados*. *sistemas de gestión de riesgos y Seguridad*. https://www.isotools.org/normas/riesgos-y-seguridad/iso-31000/

Kapersky. (s. f.). *¿Qué es el spear phishing?* https://latam.kaspersky.com/resource-center/definitions/spear-phishing

KPMG. (2019). *Global Banking Fraud Survey* [Encuesta global de fraude bancario]. https://assets.kpmg/content/dam/kpmg/xx/pdf/2019/05/global-banking-fraud-survey.pdf

La Nación. (2016). Los 139 años del BCR. https://www.nacion.com/opinion/foros/los-139-anos-del-bcr/WCAIMC7G7NC4RMXAJTOTFQ6CSY/story/

Lafise. (s. f.). *Nuestra historia*. https://www.lafise.com/acerca-de-lafise/nuestra-historia

Ley n.º 1644. (1953). *Ley Orgánica del Sistema Bancario Nacional*. http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=9925

Malenkovich, S. (2013). *¿Qué es un ataque Man-in-the-Middle? Kapersky Daily*. https://www.kaspersky.es/blog/que-es-un-ataque-man-in-the-middle/648/

Monje, C. (2011). *Metodología de la investigación cuantitativa y cualitativa. Guía didáctica*. Universidad Surcolombiana. Facultad de Ciencias Sociales y Humanas. Programa de Comunicación Social y Periodismo. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwjotpTZu6vlAhUNy1kKHR_cCz0QFjAAeg-QIAhAC&url=https%3A%2F%2Fwww.uv.mx%2Frmipe%2Ffiles%2F2017%2F02%2FGuia-didactica-metodologia-de-la-investigacion.pdf&usg=AOvVaw2_uEPddLyU0HRFHdC-SeIQ

Moreno Granados, D. (2018). *Tipos de Mecanismos para la Protección de los servicios Informáticos y sus Modelos de Seguridad*. http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/4928/51257%20-%20Moreno%20Granados%20Diego.pdf?sequence=1&isAllowed=y

Organismo de Investigación Judicial (OIJ). (2019). *Memoria institucional 2019*. http://d1qqtien6gys07.cloudfront.net/wp-content/uploads/2020/03/Memoria-Institucional-OIJ-2019.pdf

Organización de Estados Americanos. (2019). *Desafíos del riesgo cibernético en el sector financiero para Colombia y América Latina*. https://www.oas.org/es/sms/cicte/docs/Desafios-del-riesgo-cibernetico-en-el-sector-financiero-para-Colombia-y-America-Latina.pdf

Organización para la Cooperación y Desarrollo Económicos (OCDE). (2016)

Políticas de Banda Ancha para América Latina y el Caribe: Un Manual para la Economía digital. https://www.oecd-ilibrary.org/docserver/9789264259027-17-es.pdf?expires=1633384109&id=id&accname=guest&checksum=7A219BC6DEB925BE91D85439AB2381DC

Pino, D. S. (2016). *delitos informáticos: Generalidades*. https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Ramírez, J. (2011). *Cómo diseñar una investigación académica*. Montes de María Editores.

Ramírez, J. *et al.* (2016). *Estudio descriptivo del malware en una dependencia académica de una institución pública de educación superior*. Universidad Veracruzana. https://www.uv.mx/iiesca/files/2016/11/06CA201601.pdf

Scotiabank. (s. f.). *Scotiabank en Costa Rica*. https://www.scotiabankcr.com/acerca/quienes-somos/perfil-corporativo/scotiabank-en-costa-rica.aspx

Telem, D. (2016). *KPMG. The three línes of defense. Making a transition to a mature risk management model*. https://assets.kpmg/content/dam/kpmg/ca/pdf/2017/01/three-lines-of-defense-kpmg.pdf

The Institute of Internal Auditors (IIA). (2013). *Declaración de Posición: Las tres líneas de defensa para una efectiva gestión de riesgos y control*. na.theiia.org/translations/PublicDocuments/PP%20The%20Three%20Lines%20of%20Defense%20in%20Effective%20Risk%20Management%20and%20Control%20Spanish.pdf

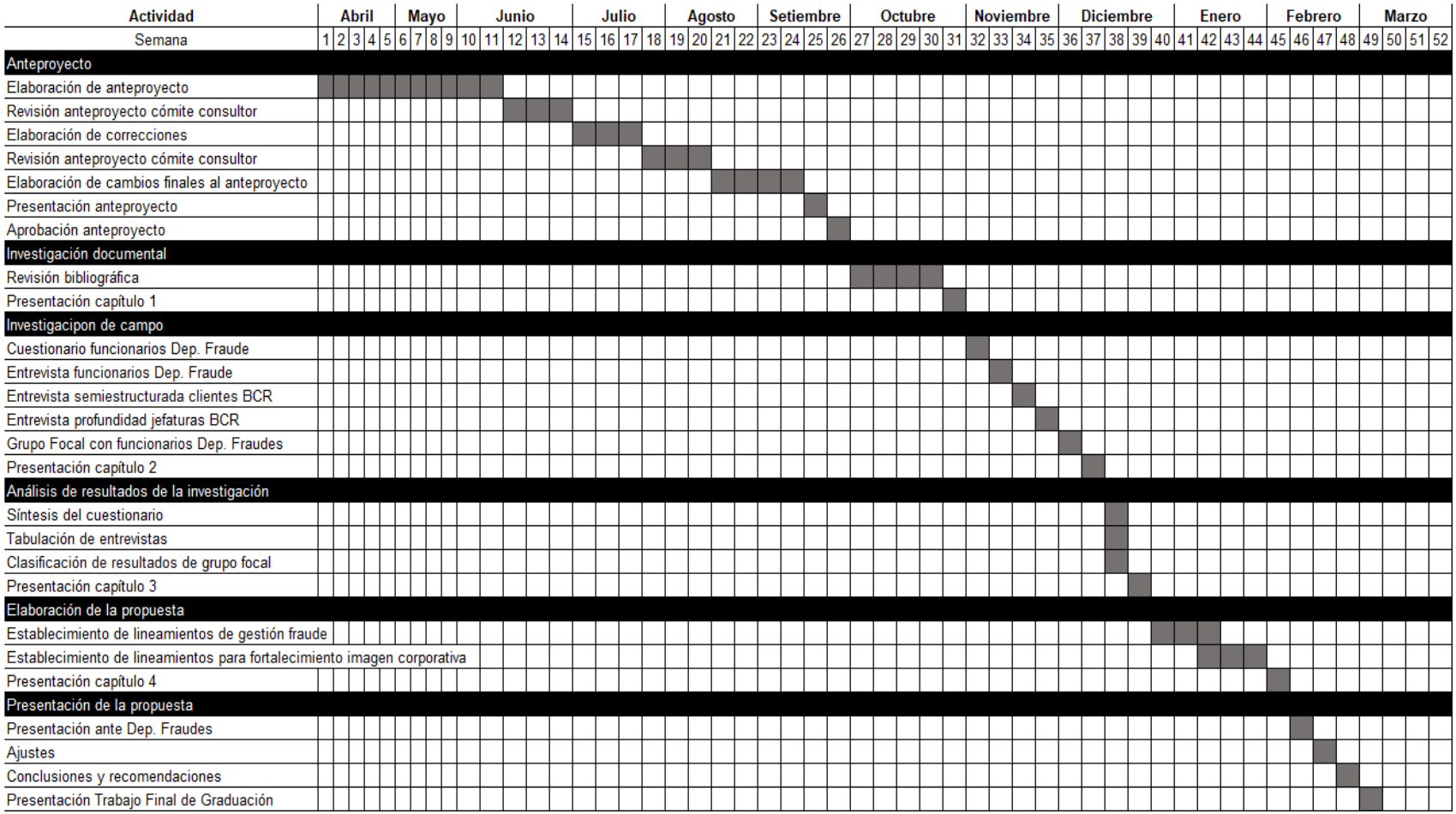
TNI. (2017). *El Banco Popular de Costa Rica: un ejemplo de banco democrático, verde y sostenible*. https://www.tni.org/es/art%C3%ADculo/el-banco-popular-de-costa-rica-un-ejemplo-de-banco-democratico-verde-y-sostenible

Ureña, F. (2015). *Ciberataque, la mayor amenaza actual*.

Vargas, D. (2020). *Al menos seis clientes por día denuncian fraude informático en Banco de Costa Rica*. Ameliarueda.com. https://www.ameliarueda.com/nota/5-6-casos-diario-fraude-informatico-reportan-bcr

Yopo Diaz, N. V. (2010). *Responsabilidad en los casos de fraude por extravío, hurto o robo de la tarjeta de crédito*. Universidad de Chile. http://repositorio.uchile.cl/bitstream/handle/2250/113072/de-yopo_n.pdf?sequence=1

Cronograma de actividades



Anexos

Encuesta Imagen del BCR en medios digitales

Somos estudiantes de la Licenciatura en Dirección de Empresas de la Escuela de Administración de Empresas de la Universidad de Costa Rica. Este cuestionario forma parte de la investigación de imagen corporativa del Banco de Costa Rica (BCR) para analizar y evaluar la gestión del riesgo por fraude a través de medios digitales. El cuestionario ha sido desarrollado por estudiantes con un fin académico y es el único propósito con el cual se desarrolla. La información que usted nos suministre será estrictamente confidencial y utilizada para los fines antes indicados. La aplicación de este cuestionario tiene una duración de 10 minutos aproximadamente. Agradecemos de antemano por su colaboración y su tiempo.

*Obligatorio

1. ¿Es usted cliente del Banco de Costa Rica? *

   Marca solo un óvalo.

   - ◯ Sí *Ir a la pregunta 4*
   - ◯ No *Ir a la pregunta 2*

Sección sin título

2. ¿Fue usted cliente del Banco de Costa Rica en algún momento? *

   Marca solo un óvalo.

   - ◯ Sí *Ir a la pregunta 3*
   - ◯ No

Sección sin título

3. ¿Por qué dejó de ser cliente?(Puede marcar más de una opción) *

Selecciona todas las opciones que correspondan.

- [ ] Mala experiencia del servicio al cliente
- [ ] Fui víctima de fraude o estafa
- [ ] Tengo mala percepción del BCR
- [ ] Encontré una institución bancaria mejor
- [ ] Ya no utilizo bancos
- [ ] No me gustan sus plataformas digitales
- [ ] Otros: _____

4. ¿Utiliza alguna de las plataformas digitales del BCR? *

Marca solo un óvalo.

- ◯ Sí *Ir a la pregunta 7*
- ◯ No *Ir a la pregunta 5*

5. ¿Por qué no utiliza las plataformas digitales del BCR? *

Marca solo un óvalo.

- ◯ Desconfianza
- ◯ No sabe como utilizarla *Ir a la pregunta 16*
- ◯ No sabía que existía *Ir a la pregunta 16*
- ◯ No me gustan *Ir a la pregunta 16*
- ◯ No necesito utilizarlas *Ir a la pregunta 16*
- ◯ Otros: _____

Ir a la pregunta 16

6. ¿Por qué le generan desconfianza las plataformas virtuales del BCR? *

Ir a la pregunta 16

7. ¿Cuál es la frecuencia con la que hace uso de las plataformas virtuales del Banco de Costa Rica? *

Marca solo un óvalo.

- ◯ Una vez cada 2 meses o más
- ◯ Mensual
- ◯ Semanal
- ◯ Diaria
- ◯ Otros: _____

8. ¿Desde cuáles dispositivos ingresa? (Puede marcar más de una opción) *

Selecciona todas las opciones que correspondan.

- ☐ Celular
- ☐ Tableta
- ☐ Computadora
- ☐ Otros: _____

9. Ingresa por medio de la página web ó desde la aplicación *

Marca solo un óvalo.

- ◯ Ingreso desde la página web
- ◯ Uso la aplicación del banco
- ◯ Ambas
- ◯ Otros: _____

1 . *

0 Marque las transacciones que más realiza en la plataforma del BCR (puede marcar más de una opción):

Selecciona todas las opciones que correspondan.

- [ ] SINPE Móvil
- [ ] Transferencias bancarias
- [ ] Pago Servicios
- [ ] Ahorros automáticos
- [ ] Pago de préstamo
- [ ] Tasaciones
- [ ] Pago de tarjetas
- [ ] Inversiones
- [ ] Sobres
- [ ] Otros: _____

11. Con el fin de conocer su opinión sobre el servicio que recibe del Banco de Costa Rica, seleccione las opciones que aplican a su experiencia como cliente (puede marcar más de una opción): *

Selecciona todas las opciones que correspondan.

- [ ] Tiene buen servicio al cliente
- [ ] Tiene acceso a tutoriales del uso de la página
- [ ] Brinda mensajes informativos sobre prevención de fraudes y estafas
- [ ] Usabilidad (Facilidad de uso)
- [ ] Los mecanismos de seguridad le brindan confianza
- [ ] Otros: _____

12. ¿Considera que la percepción que las personas tienen sobre una organización es un factor influyente al momento de adquirir un servicio financiero? *

Marca solo un óvalo.

- ◯ Sí
- ◯ No
- ◯ Otros: _____

3 Cuál es el nivel de confianza que siente con las plataformas digitales del BCR? *

Marca solo un óvalo.

	1	2	3	4	5	
Poco confiable	◯	◯	◯	◯	◯	Muy confiable

Sección sin título

* *

14. ¿Considera que la plataforma digital del BCR es segura para realizar transacciones?

Marca solo un óvalo.

◯ Sí *Ir a la pregunta 15*

◯ No *Ir a la pregunta 19*

Sección sin título

15. ¿Por qué sí? *

Ir a la pregunta 16

Sección sin título

6 Ha recibido información del banco sobre cómo prevenir fraudes? *

Marca solo un óvalo.

◯ Sí *Ir a la pregunta 17*

◯ No *Ir a la pregunta 18*

Sección sin título

9 Por qué no? *

17. ¿Por qué medios ha recibido esta información?(Puede marcar más de una opción)

Selecciona todas las opciones que correspondan.

- [ ] Redes sociales
- [ ] Correo electrónico
- [ ] SMS
- [ ] Whatsapp
- [ ] Televisión
- [ ] Radio
- [ ] Periódico
- [ ] Otros: _____

Sección sin título

18. ¿Considera importante recibir este tipo de información? *

Marca solo un óvalo.

- ◯ Sí
- ◯ No

Ir a la pregunta 20

Sección sin título

_____

_____

_____

_____

Ir a la pregunta 16

Sección sin título

20. ¿Posee cuentas o servicios con otros bancos? *

Marca solo un óvalo.

- ◯ Sí
- ◯ No *Ir a la pregunta 23*

Sección sin título

1 .

1 Cuál es la institución financiera de su preferencia? *

Marca solo un óvalo.

- Banco de Costa Rica
- Banco BCT
- BAC credomatic
- Banco nacional
- DAVIVIENDA
- Scotiabank
- Banco Popular
- Banco Promerica
- Banco LAFISE
- Banco CATHAY
- Banco Improsa
- Otros: _____

22. ¿Por qué razón la prefiere? (Puede marcar más de una opción) *

Selecciona todas las opciones que correspondan.

- [ ] Seguridad
- [ ] Imagen Institucional (identidad ante la comunidad, con relación a su compromiso para asegurar una adecuada protección del patrimonio e información de los clientes)
- [ ] Servicio
- [ ] Ubicación
- [ ] Otros: _____

Sección sin título

3 Entendiendo el concepto de imagen corporativa como la identidad ante la comunidad, clientes, trabajadores y medios, con relación a su compromiso para asegurar una adecuada protección del patrimonio e información de sus clientes ¿Cómo evaluaría la imagen corporativa del BCR? *

Marca solo un óvalo.

- Excelente
- Buena
- Regular
- Mala
- Pésima

24. ¿Como cliente, cuál aspecto considera relevante que se debe rediseñar en el BCR? (Puede marcar más de una opción) *

Selecciona todas las opciones que correspondan.

- [ ] Comunicación visual
- [ ] Publicidad
- [ ] Página Web
- [ ] Aplicaciones móviles
- [ ] Capacitación de empleados
- [ ] Servicio al cliente
- [ ] No cambiaría nada
- [ ] Otros: _____

Demografía

5 ¿Género? *

Marca sol › un óvalo.

- Femenino
- Masculino
- Otros: _____

26. Su edad se encuentra entre: *

Marca solo un óvalo.

- menos de 18 años
- 18 - 20 años
- 20 - 30 años
- 31 - 40 años
- 41 - 50 años
- 51 - 60 años
- 61 - 70 años
- 71 - 80 años
- 81 o más

27. ¿Cuál es su estado civil actual? *

Marca solo un óvalo.

- Soltero
- Casado
- Separado
- Divorciado
- Unión libre
- Prefiero no decirlo
- Otros: _____

8 Para finalizar, ¿Cuál es su lugar de residencia actual? *

Marca solo un óvalo.

- Heredia
- San José
- Cartago
- Alajuela
- Limón
- Puntarenas
- Guanacaste
- Extranjero

Cuestionario Fraudes en Medios Digitales en el BCR

Este cuestionario forma parte de la investigación de imagen corporativa del Banco de Costa Rica que pretende analizar y evaluar la gestión del riesgo por fraude a través de medios digitales, ha sido desarrollado únicamente con un fin académico. La información suministrada es estrictamente confidencial. Muchas gracias por su colaboración y su tiempo.

*Obligatorio

1. ¿Qué metodología de gestión de riesgo utilizan? ¿Por qué? *

2. ¿Qué proyectos de gestión de riesgo están tramitando o valorando? *

3. ¿Cuáles considera que son los puntos fuertes de la gestión de fraude en el BCR? *

4. ¿En la oficina se mantienen registros estadísticos de la cantidad de fraudes y la periodicidad en la que se efectúan?

5. ¿Cuáles son los tipos de fraudes que más afectan a la institución? *

6. ¿Cuál es la plataforma digital más utilizada para realizar fraudes? *

7. ¿Qué plataforma es más segura contra fraudes? (App ó página web? *

8. ¿Cuánto es el presupuesto que destina el BCR a la gestión de riesgo por fraude? *

9. ¿Con qué mecanismo de seguridad cuentan para la detección de fraudes? ¿Creen * que son suficientes? ¿Por qué los eligieron?

10. ¿Existe algún control en tiempo real para prevenir el fraude, por ejemplo, analistas verificando transacciones fraudulentas y llamando al cliente para validar su identidad? *

1 En l a cadena de seguridad del Banco ¿Qué consideran cómo el eslabón más débil?

12. ¿Qué medidas se han tomado para la educación de los clientes sobre fraudes? *

13. ¿Por qué siguen pasando e incrementando las denuncias por fraudes en el país? *

14. ¿Consideran que su departamento cuenta con la cantidad de personas suficientes para atender las necesidades del banco?

5 ¿De qué forma se adaptan a las nuevas modalidades de fraude? * *

16. ¿Cuál es el proceso que se realiza ante una nueva denuncia de fraude?¿Cuánto tarda el banco en investigar cada caso? *

17. ¿En cuáles casos debe el Banco hacerse responsable por las pérdidas? *

18. ¿Cuál es su percepción del BCR sobre el manejo de fraudes? *

9 ¿Cuál es su percepción de la imagen corporativa que tienen los clientes de la institución en el tema de fraudes?