Universidad Latina de Costa Rica

Centro de Estudios de Postgrados

Maestría en Administración de Negocios

Memoria de Graduación

Análisis de riesgos en Ciberseguridad y sus impactos financieros y no financieros en las entidades financieras del Estado costarricense durante el año 2021 y propuesta modelo de mejores prácticas para la administración de riesgos.

Autor

Carlos Portuguez Murillo

Junio 2022

Licencia De Distribución No Exclusiva (carta de la persona autora para uso didáctico)

Universidad Latina de Costa Rica

Yo (Nosotros):	Carlos Portuguez Murillo
De la Carrera / Programa:	Maestría en Administración de Negocios con Énfasis en Finanzas
Modalidad de TFG:	Memoria
Titulado:	Análisis de riesgos en Ciberseguridad y sus impactos financieros y no financieros en las entidades financieras del estado costarricense durante el año 2021 y propuesta modelo de mejores prácticas para la administración de riesgos.

Al firmar y enviar esta licencia, usted, el autor (es) y/o propietario (en adelante el "**AUTOR**"), declara lo siguiente: **PRIMERO**: Ser titular de todos los derechos patrimoniales de autor, o contar con todas las autorizaciones pertinentes de los titulares de los derechos patrimoniales de autor, en su caso, necesarias para la cesión del trabajo original del presente TFG (en adelante la "**OBRA**"). **SEGUNDO**: El **AUTOR** autoriza y cede a favor de la **UNIVERSIDAD U LATINA S.R.L.** con cédula jurídica número 3-102-177510 (en adelante la "**UNIVERSIDAD**"), quien adquiere la totalidad de los derechos patrimoniales de la **OBRA** necesarios para usar y reusar, publicar y republicar y modificar o alterar la **OBRA** con el propósito de divulgar de manera digital, de forma perpetua en la comunidad universitaria. **TERCERO**: El **AUTOR** acepta que la cesión se realiza a título gratuito, por lo que la **UNIVERSIDAD** no deberá abonar al autor retribución económica y/o patrimonial de ninguna especie. **CUARTO**: El **AUTOR** garantiza la originalidad de la **OBRA**, así como el hecho de que goza de la libre disponibilidad de los derechos que cede. En caso de impugnación de los derechos autorales o reclamaciones instadas por terceros relacionadas con el contenido o la autoría de la **OBRA**, la responsabilidad que pudiera derivarse será exclusivamente de cargo del **AUTOR** y este garantiza mantener indemne a la **UNIVERSIDAD** ante cualquier reclamo de algún tercero. **QUINTO**: El **AUTOR** se compromete a guardar confidencialidad sobre los alcances de la presente cesión, incluyendo todos aquellos temas que sean de orden meramente institucional o de organización interna de la **UNIVERSIDAD SEXTO**: La presente autorización y cesión se regirá por las leyes de la República de Costa Rica. Todas las controversias, diferencias, disputas o reclamos que pudieran derivarse de la presente cesión y la materia a la que este se refiere, su ejecución, incumplimiento, liquidación, interpretación o validez, se resolverán por medio de los Tribunales de Justicia de la República de Costa Rica, a cuyas normas se someten el **AUTOR** y la **UNIVERSIDAD**, en forma voluntaria e incondicional. **SÉPTIMO**: El **AUTOR** acepta que la **UNIVERSIDAD**, no se hace responsable del uso, reproducciones, venta y distribuciones de todo tipo de fotografías, audios, imágenes, grabaciones, o cualquier otro tipo de

presentación relacionado con la **OBRA**, y el **AUTOR**, está consciente de que no recibirá ningún tipo de compensación económica por parte de la **UNIVERSIDAD**, por lo que el **AUTOR** haya realizado antes de la firma de la presente autorización y cesión. **OCTAVO**: El **AUTOR** concede a **UNIVERSIDAD.**, el derecho no exclusivo de reproducción, traducción y/o distribuir su envío (incluyendo el resumen) en todo el mundo en formato impreso y electrónico y en cualquier medio, incluyendo, pero no limitado a audio o video. El **AUTOR** acepta que **UNIVERSIDAD.** puede, sin cambiar el contenido, traducir la **OBRA** a cualquier lenguaje, medio o formato con fines de conservación. **NOVENO**: El **AUTOR** acepta que **UNIVERSIDAD** puede conservar más de una copia de este envío de la **OBRA** por fines de seguridad, respaldo y preservación. El **AUTOR** declara que el envío de la **OBRA** es su trabajo original y que tiene el derecho a otorgar los derechos contenidos en esta licencia. **DÉCIMO**: El **AUTOR** manifiesta que la **OBRA** y/o trabajo original no infringe derechos de autor de cualquier persona. Si el envío de la **OBRA** contiene material del que no posee los derechos de autor, el **AUTOR** declara que ha obtenido el permiso irrestricto del propietario de los derechos de autor para otorgar a **UNIVERSIDAD** los derechos requeridos por esta licencia, y que dicho material de propiedad de terceros está claramente identificado y reconocido dentro del texto o contenido de la presentación. Asimismo, el **AUTOR** autoriza a que en caso de que no sea posible, en algunos casos la **UNIVERSIDAD** utiliza la **OBRA** sin incluir algunos o todos los derechos morales de autor de esta. **SI AL ENVÍO DE LA OBRA SE BASA EN UN TRABAJO QUE HA SIDO PATROCINADO O APOYADO POR UNA AGENCIA U ORGANIZACIÓN QUE NO SEA UNIVERSIDAD U LATINA, S.R.L., EL AUTOR DECLARA QUE HA CUMPLIDO CUALQUIER DERECHO DE REVISIÓN U OTRAS OBLIGACIONES REQUERIDAS POR DICHO CONTRATO O ACUERDO. La presente autorización se extiende el día** 1 de Julio **de** 2022 **a las** 10 am

Firma del estudiante(s):

Carta aprobación tutor

UNIVERSIDAD LATINA DE COSTA RICA
POWERED BY Arizona State University

UNIVERSIDAD LATINA CAMPUS HEREDIA
CENTRO INTERNACIONAL DE POSGRADOS

CARTA DE APROBACIÓN POR PARTE DEL TUTOR
DEL TRABAJO FINAL DE GRADUACIÓN

Heredia, 1 de Julio del 2022
Señores
Miembros del Comité de Trabajos Finales de Graduación
SD

Estimados señores:

He revisado y corregido el Trabajo Final de Graduación, denominado: **"Análisis de riesgos en Ciberseguridad y sus impactos financieros y no financieros en las entidades financieras del estado costarricense durante el año 2021 y propuesta modelo de mejores prácticas para la administración de riesgos",** elaborado por el estudiante: **Carlos Portuguez Murillo**, como requisito para que el citado estudiante pueda optar por el grado académico **MÁSTER PROFESIONAL EN ADMINISTRACIÓN DE NEGOCIOS CON ÉNFASIS EN FINANZAS.**

Considero que dicho trabajo cumple con los requisitos formales y de contenido exigidos por la Universidad, y por tanto lo recomiendo para su entrega ante el Comité de Trabajos Finales de Graduación.

Suscribe cordialmente,

MBA. Nelson Carazo Mesen

Carta aprobación del lector

UNIVERSIDAD LATINA DE COSTA RICA
POWERED BY Arizona State University

UNIVERSIDAD LATINA CAMPUS HEREDIA
CENTRO INTERNACIONAL DE POSGRADOS

CARTA DE APROBACIÓN POR PARTE DEL LECTOR
DEL TRABAJO FINAL DE GRADUACIÓN

Heredia, 1 de Julio del 2022
Señores
Miembros del Comité de Trabajos Finales de Graduación
SD

Estimados señores:

He revisado y corregido el Trabajo Final de Graduación, denominado: **"Análisis de riesgos en Ciberseguridad y sus impactos financieros y no financieros en las entidades financieras del estado costarricense durante el año 2021 y propuesta modelo de mejores prácticas para la administración de riesgos",** elaborado por el estudiante: **Carlos Portuguez Murillo**, como requisito para que el citado estudiante pueda optar por el grado académico **MÁSTER PROFESIONAL EN ADMINISTRACIÓN DE NEGOCIOS CON ÉNFASIS EN FINANZAS.**

Considero que dicho trabajo cumple con los requisitos formales y de contenido exigidos por la Universidad, y por tanto lo recomiendo para su entrega ante el Comité de Trabajos Finales de Graduación.

Suscribe cordialmente,

MBA. Mike Osejo Villegas

Carta aprobación del filólogo

UNIVERSIDAD LATINA DE COSTA RICA
POWERED BY Arizona State University

UNIVERSIDAD LATINA CAMPUS HEREDIA
CENTRO INTERNACIONAL DE POSGRADOS

CARTA DE APROBACIÓN POR PARTE DEL FILÓLOGO
DEL TRABAJO FINAL DE GRADUACIÓN

Heredia, 1 de Julio del 2022
Señores
Miembros del Comité de Trabajos Finales de Graduación
SD

Estimados señores:

Leí y corregí el Trabajo Final de Graduación, denominado: "**Análisis de riesgos en Ciberseguridad y sus impactos financieros y no financieros en las entidades financieras del Estado costarricense durante el año 2021 y propuesta modelo de mejores prácticas para la administración de riesgos**", elaborado por el estudiante: **Carlos Portuguez Murillo, con cédula 1-10620646,** para optar por el grado académico MÀSTER **PROFESIONAL EN ADMINISTRACIÓN DE NEGOCIOS CON ÈNFASIS EN FINANZAS.** Corregí el trabajo en aspectos tales como: construcción de párrafos, vicios del lenguaje que se trasladan a lo escrito, ortografía, puntuación y otros relacionados con el campo filológico, y desde ese punto de vista considero que está listo para ser presentado como Trabajo Final de Graduación; por cuanto cumple con los requisitos establecidos por la Universidad.

Se suscribe de ustedes cordialmente,

Jorge Fernández Chaves
Cédula 2-0222-0058
Carné COLYPRO 02545

Carta de declaración jurada

DECLARACIÓN JURADA

El suscrito(a), **Carlos Portuguez Murillo** con cédula de identidad número **1-1062-0646**, declaro bajo fe de juramento, conociendo las consecuencias penales que conlleva el delito de perjurio: Que soy el autor(a) del presente trabajo final de graduación, modalidad memoria; para optar por el título de **MÁSTER PROFESIONAL EN ADMINISTRACIÓN DE NEGOCIOS CON ÉNFASIS EN FINANZAS** de la Universidad Latina, campus Heredia, y que el contenido de dicho trabajo es obra original del (la) suscrito(a).

Heredia, 1 de Julio del 2022.

Carlos Portuguez Murillo

Carta de manifestación de exoneración de responsabilidad de la Universidad

MANIFESTACIÓN EXONERACIÓN DE RESPONSABILIDAD

El suscrito, **Carlos Portuguez Murillo** con cédula de identidad número **1-1062-0646**, exonero de toda responsabilidad a la Universidad Latina, campus Heredia; así como al Tutor y Lector que han revisado el presente trabajo final de graduación, para optar por el título de **MÁSTER PROFESIONAL EN ADMINISTRACIÓN DE NEGOCIOS CON ÉNFASIS EN FINANZAS** de la Universidad Latina, campus Heredia; por las manifestaciones y/o apreciaciones personales incluidas en el mismo. Asimismo, autorizo a la Universidad Latina, campus Heredia, a disponer de dicho trabajo para uso y fines de carácter académico, publicitando el mismo en el sitio web; así como en el CRAI.

Heredia, 1 de Julio del 2022

Carlos Portuguez Murillo

Dedicatoria

Este trabajo final de investigación se lo dedico primeramente a las tres mujeres más importantes en mi vida, una ya no está conmigo, pero sé que aún cuida de mí. La otra, mi madre, que siempre me inculcó el valor de la honestidad, el trabajo duro, el ser agradecido, el estudiar, que con su amor incondicional ha logrado que siga adelante para agradecerlo todo lo que ha hecho por mí.

Mariel, mi pareja de mil batallas, por creer que sí podía hacerlo aun cuando yo no era capaz de hacerlo, su amor me dio las fuerzas y la confianza para seguir adelante. A mis hijos que, si bien estuvieron ahí en silencio sin mostrarse mucho, pero son parte importante de mi vida y a ellos también me debo y son parte importante de las fuerzas que necesito para caminar con la frente en alto, a pesar de las adversidades que nos presenta la vida.

Resumen ejecutivo

Los avances en las tecnologías de información a lo largo de los años han contribuido a que la sociedad avance a pasos agigantados, desde la incursión del Internet da paso al mundo globalizado que hoy se conoce y que cada día se mueve hacia la digitalización de una gran cantidad de sectores, unos con más prisa que otros para no quedarse atrás y perder ventaja competitiva.

Desde luego no todo es tan bueno y con el mundo tan interconectado surge una amenaza que poco a poco evoluciona y desde hace algún tiempo lo hace más rápido que es casi imposible detenerla hasta para las grandes corporaciones con presupuestos enormes lograr mantenerse protegidos contra ellos, y son los ciberdelincuentes.

En los últimos años se han conformado grupos de crimen organizado o de ciberterrorismo, que tiene de cabeza a todos los encargados de gestionar los riesgos, así como a los departamentos de Ciberseguridad, Tecnologías de Información, Altas Gerencias, Juntas Directivas y, desde luego, a todos los seres humanos que utilizan gran cantidad de dispositivos conectados a Internet.

Los enfoques tradicionales de administración de riesgos deben adaptarse a esta nueva realidad y sumar esfuerzos internos y externos para lograr estar un poco más protegidos o, al menos, tener dentro de sus planes de continuidad de negocios y recuperación de operaciones las herramientas necesarias para evitar problemas grandes en caso de ser víctimas de un ciberataque.

Precisamente esta investigación procura realizar un análisis de riesgos en Ciberseguridad junto con sus impactos financieros y no financieros en las entidades financieras costarricenses, y una propuesta de un modelo de mejores prácticas para la administración de riesgos.

En el capítulo uno, se pretende dar un estado actual del tema de investigación, describiendo los antecedentes, además de esto se define la descripción del asunto por tratar y se brindan detalles de información pues existen estudios previos. Además de esto, se documentan las

delimitaciones espacial y temporal, y con aportes del investigador, se definen los objetos y sujetos del estudio. Se hace un planteamiento y sistematización del problema por investigar con sus respectivos planteamientos de hipótesis. Se especifican las justificaciones propias de la investigación y se dejan claros los alcances y limitaciones.

En el capítulo dos se hace la documentación sobre los marcos teóricos y situacionales, con el primero se procura dar la fundamentación teórica de la investigación abarcando los principales conceptos de los distintos temas que se desarrollan para dar un mejor entendimiento de términos propios de cada uno de ellos, porque sobre el marco situacional, lo que se procura es lograr plasmar el análisis de la situación actual que se vive relacionado también con los temas abarcados.

El capítulo tres trata de definir el enfoque metodológico de la investigación, se detalla el tipo de análisis que se utiliza, y los instrumentos requeridos para la recopilación de información primaria y secundaria, por ejemplo, las entrevistas a los expertos y distintas fuentes de información en libros, leyes, sitios *web* oficiales, entre otros más.

Sigue el capítulo cuatro, donde se realizan los análisis e interpretación de los resultados para cada una de las variables definidas, para estas se utiliza la información recabada de las entrevistas a los expertos, así como el análisis documental para lograr dar soporte documental a los principales hallazgos.

Tomando en cuenta la información del punto anterior, para el capítulo cinco se documentan las conclusiones para cada variable de estudio, y constatas contra algo que bien puede ser teoría propia del objeto de estudio, leyes, posiciones de la empresa o del sector. Seguido de esto se dan las recomendaciones de igual forma para cada una de las variables basadas en las conclusiones y análisis e interpretación de los resultados.

Por último, en el capítulo seis, se presenta la propuesta como el objetivo final del trabajo de investigación, la cual lleva dos enfoques: uno estratégico donde se detalla que lo que se procura hacer, es más general, y el otro enfoque es el táctico, donde se definen los pasos que se deben hacer para tener el modelo de mejores prácticas para la administración de riesgos en Ciberseguridad.

Tabla de contenidos

Lista de Figuras

Lista de tablas

Lista de Anexos

Capítulo I

Introducción y propósito

Estado actual de la investigación

Introducción

En el mundo digital en que las empresas se desenvuelven y compiten, está cada día todo está más interconectado. Las tecnologías de información avanzan a pasos agigantados, lo cual desencadena una serie de beneficios y ventajas competitivas para aquellas que con sus inversiones logran estar al tope de las exigencias de sus mercados y clientes, y donde la innovación se vuelve algo intrínseco en productos y servicios, lo cual demanda una búsqueda interminable por tener la mejor tecnología, y donde ya nadie se imagina un escenario sin la tecnología con que cuentan.

Precisamente debido a esta tecno-dependencia desarrollada a lo largo de los años es donde también surgen individuos e incluso organizaciones que dedican sus esfuerzos a planear y lanzar ataques cibernéticos, algunos con la simple razón de buscar fama; sin embargo, existen otros que ven una opción lucrativa donde cada vez son más las personas que están dispuestas a pagar por la información ilegalmente sustraída o las empresas víctimas pagando las exigencias, con tal de recuperar su información.

Las tecnologías de Ciberseguridad procuran crear ambientes más seguros para las empresas, e incluso las regulaciones, leyes nacionales e internacionales les exigen a las compañías contar con las mejores prácticas en tecnologías y procesos para garantizar su continuidad de negocio. Uno de los principales retos que enfrentan las empresas cuyo giro de negocio no es la Ciberseguridad, es precisamente que no existe una cultura adecuada de análisis de riesgos, ya que no se cuenta con personal capacitado y en ocasiones terminan delegando esta tarea a un tercero.

El desarrollo de este trabajo permite la realización de un análisis de riesgos en Ciberseguridad para las entidades financieras, así como listar posibles impactos financieros y no financieros para que, mediante una propuesta de modelo de mejores prácticas para la administración de riesgos, se logren tomar las acciones a tiempo, y evitar que estos se materialicen causando mayores problemas tanto para las entidades como para sus usuarios finales.

Antecedentes

Sin duda alguna, el incremento en el uso de la tecnología, en especial la móvil y los canales digitales provoca que día con día las amenazas a la privacidad de los datos, a la disponibilidad de sistemas, a los fraudes y a muchos otros riesgos de Ciberseguridad aumenten.

La pandemia de COVID-19 incrementa aún más la dependencia de los sistemas digitales y aceleró a la inclusión de la cuarta revolución, donde una gran mayoría de las industrias deben tomar medidas para una digitalización rápida de sus servicios e incluso introducir el trabajo remoto como medida a las constantes restricciones de movilidad impuestas en una gran mayoría de los países.

De la mano con todos estos cambios tan acelerados, las amenazas de Ciberseguridad van en aumento, según el Informe Global de Riesgos del Foro Económico Mundial (2022) para el 2020 los ataques de "*malware*" y "*ransomware*" experimentan aumentos del 358% y 435%.

El reporte de Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe de la OEA (2021) enfatiza en el hecho de que la banca viene con una transformación con pasos acelerados a la digitalización, pues cada vez más son los usuarios que utilizan las bancas electrónicas con el fin de realizar transacciones por internet o dispositivos móviles.

De aquí que de esa gran cantidad de amenazas están más presentes en este sector, principalmente como consecuencia del tipo de información que manejan de sus clientes. En un reporte de investigación sobre filtración de datos realizado por Verizon (2020), muestra que un 63% de los casos analizados los delincuentes procuran monetizar fácilmente los datos robados, seguido de un 18% donde los actores eran internos con motivaciones meramente financieras.

Debido a que cada organización debe enfrentar esta gran variedad de retos y amenazas en Ciberseguridad, en especial las entidades financieras, es importante que los riesgos sean evaluados acorde con su probabilidad de ocurrencia, de aquí que surja la necesidad de realizar una investigación de los principales riesgos que enfrenta este sector junto con un modelo de mejores prácticas para la administración de riesgos que se deben implementar.

Descripción del tema

El ciber espacio en el cual todas las personas y organizaciones se encuentran interconectadas, tiene una alta dependencia de las redes, especialmente la internet. Esto ha dado paso a un sinfín de ventajas y avances tecnológicos, y ha permitido que al alcance de un clic se tenga acceso a realizar transacciones sin necesidad de ir presencialmente a un banco, mantener el contacto con personas a miles de kilómetros de distancia, así como nuevos emprendimientos que se ven fortalecidos por las ventajas que ofrece estar cada vez más conectados.

Si bien los avances tecnológicos junto con la globalización permiten hacer negocios a escala mundial, la penetración de nuevos mercados o expandirse en los actuales, mejorar manejo de recursos y dar la base de importantes innovaciones, todos estos cambios y posibilidades generan nuevos vectores de ataques, que pueden ser explotados (Beissel, 2016). Cada día las organizaciones ven amenazadas y vulneradas sus operaciones por cientos de ciberataques tratando de tomar ventaja de vulnerabilidades encontradas en sus infraestructuras o fallas en su personal.

Para el año 2020, más de 51 millones de ataques de *'hackers'* durante la pandemia en Costa Rica (Pérez, 2020) Sin duda alguna el más recordado del año 2020 el que sufre el Banco de Costa Rica (BCR) por parte del grupo *Maze* con su *Maze Rasonware* donde se publican bases de datos con información de miles de sus clientes (Jenkins, 2020), donde incluso reciben un ultimátum por parte de este grupo de ciberdelincuentes (Castro, 2020).

Este es tan solo uno de los miles de ejemplos y víctimas de este sector y otros no menos importantes como el de Salud; las razones pueden ser muchas, sin embargo, el valor de la información que estas organizaciones manejan y administran es en ocasiones incalculables si se toma en cuenta la reputación y la pérdida de confianza.

El presente trabajo plantea entre otras cosas una interrogante que cada vez toma más importancia, y es poder analizar los principales riesgos para el sector financiero, ya que su materialización tiene implicaciones financieras, así como no financieras, principalmente que es uno de los sectores donde la reputación y credibilidad son pilares en su giro de negocio.

Información existente

Para llevar a cabo este trabajo de investigación se cuenta con artículos en internet de opinión de expertos, así como estudios sobre los retos que enfrentan las organizaciones sobre las inversiones en Ciberseguridad, así como las principales amenazas que son sujetas y que justifican mantenerse actualizados con las últimas tendencias en productos y servicios que los ayuden a mantenerse protegidos y que también resaltan las mejores prácticas para poder hacer frente a estos retos

También se cuentan con libros enfocados en las decisiones de inversión y estrategias económicas en el área de Ciberseguridad, y que permiten tener una visión basadas en estudios sobre los aspectos económicos que se deben considerar, las teorías de inversión e implementación de estrategias, disposiciones de inversión específicas de cada industria, los fundamentos para la toma de decisiones y los ciclos de vida de las inversiones en este campo.

Otra fuente actual y relevante de investigación son las noticias nacionales y extranjeras que permitan entender acontecimientos relacionados con ataques sufridos hacia organizaciones, cuáles son los factores que intervienen, impactos y otros pormenores que ayuden a soportar el enfoque de la presente investigación.

Los estudios de mercado también sirven como una fuente importante para entender cómo se han desarrollado los sectores sujetos de estudio, los hallazgos, factores que repercuten en el comportamiento de estos, así como las recomendaciones, pues si bien no se cuenta con estudios específicos para Costa Rica, los estudios disponibles actualmente sirven de fundamento y punto de comparación, esenciales para el desarrollo del presente trabajo.

Por último, está la Estrategia Nacional de Ciberseguridad del Ministerio de Ciencia y Tecnología (MICIT, 2017) que permite conocer cómo Costa Rica inicia sus primeros pasos en materia de Ciberseguridad junto con los retos que esto conlleva, pues parte de estos esfuerzos es el Decreto 37052 (2012) para la creación del centro de respuesta de incidentes de seguridad informática CSIRT-CR.

Estudios previos

Como punto de partida de esta investigación no se cuenta con estudios previos, por lo que este análisis puede ser un punto de partida para expandir a otros medios e incluso organizaciones dentro del sector objeto de investigación. Sin embargo, se cuenta con algunos estudios realizados por Deloitte sobre la búsqueda de la madurez en Ciberseguridad en las instituciones financieras (Deloitte, 2019), ya que para este sector es de suma importancia reconocer cómo, dónde y cuándo se debe invertir en este campo.

Delimitación del título

Aporte del investigador

El aporte del investigador para este trabajo está dividido en dos partes, el primero es la realización de un análisis de los principales riesgos en Ciberseguridad y sus impactos financieros y no financieros en las entidades financieras que están expuestas a ciberataques y que son reguladas por la Superintendencia General de Entidades Financieras.

El segundo aporte de este estudio es una propuesta de modelo de mejores prácticas para la administración de riesgos que se debe tener implementado para reducir la probabilidad que algún riesgo se materialice.

Objeto de estudio

El objeto de estudio está compuesto de un análisis de los principales riesgos en Ciberseguridad y sus impactos financieros y no financieros en las entidades financieras. El cual tiene especial relevancia en la realidad del sistema financiero debido a que la información que manejan es muy bien cotizada por los ciberdelincuentes. Adicional al análisis también se cuenta con la propuesta modelo de mejores prácticas para la administración de riesgos, a fin de lograr mitigar los principales riesgos a los que estas organizaciones se ven expuestas.

Sujeto de estudio

El sujeto de estudio tiene como enfoque a las entidades financieras del Estado costarricense, al ser de este tipo de sector, y están más expuestos a ser víctimas de ciberataques por lo que el contar con un análisis de sus principales amenazas y asegurarse de que cuentan con un modelo de mejores prácticas para la administración de riesgos implementado, se vuelven aún más importantes.

Delimitación espacial

Para el presente trabajo de investigación, la delimitación espacial consiste en hacer una revisión de políticas en una única entidad financiera.

Delimitación temporal

La delimitación temporal para este trabajo de investigación es durante el año 2021, además la propuesta del modelo de mejores prácticas para la administración de riesgos es efectiva su aplicación a partir del tercer trimestre del 2022.

Una vez establecidas las partes que conforman el presente trabajo de investigación, se tiene que el título es:

Análisis de riesgos en Ciberseguridad y sus impactos financieros y no financieros en las entidades financieras del Estado costarricense durante el año 2021 y propuesta modelo de mejores prácticas para la administración de riesgos.

Planteamiento del problema

El sector financiero es uno si no el sector que es más susceptible a ser blanco de ciberataques en todas sus distintas formas, la razón principal es el tipo de información que guardan de sus clientes impulsando ataques de robo de identidad, y extracción de información para ser vendida en la *Dark Web* (Owaida, 2021).

Los impactos podrían ser incalculables tomando en cuenta que los servicios bancarios se basan en la confianza y al ser sujetos de un ataque o que exista sospecha de uno, puede provocar grandes afectaciones financieras y de imagen. Con los acontecimientos en Ucrania

producto de la guerra con Rusia, el país ucraniano sufrió ataques cibernéticos contra bancos, y otras entidades gubernamentales, donde miles de personas hacían filas en los cajeros para sacar su dinero (El Financiero, 2022), de esta manera el primer problema de estudio es:

¿Cuáles son los principales riesgos de Ciberseguridad y sus impactos financieros y no financieros en las entidades financieras del Estado costarricense durante el año 2021?

Cubierto el primer problema de estudio y para poder dar continuidad al trabajo de investigación, se plantea el segundo problema. Si bien es cierto no existe una solución que dé un 100% de seguridad de no sufrir un ciberataque, existen una serie de mejores prácticas, regulaciones e incluso marcos de referencia aprobados mundialmente, que dictan una serie de guías para reducir la probabilidad de que los riesgos se materialicen, de esa manera se puede establecer el segundo problema del trabajo:

¿Cuál es la propuesta de un modelo de mejores prácticas para la administración de riesgos en las entidades financieras del Estado costarricense durante el año 2021?

Sistematización del problema

En la sistematización del problema, se detallan los subproblemas de investigación que son la base para la definición de los objetivos específicos, para lo cual se establecen los siguientes:

Para la primera pregunta, se pretende obtener los riesgos en Ciberseguridad desde la óptica de los expertos en dos áreas que están directamente interrelacionadas, el encargado de riesgos y el de seguridad de la información de una entidad financiera, lo cual facilita poder obtener una mejor visión sobre cómo se pueden identificar los principales riesgos de Ciberseguridad que afectan a este sector, y se obtuvo como resultado la siguiente pregunta:

- ¿Cuáles son los principales riesgos en Ciberseguridad?

Con respecto a la segunda pregunta, siguiendo la línea de la pregunta anterior lo que se busca es una vez entendido los principales riesgos, es lograr identificar los impactos tanto financieros como no financieros, que de materializarse esos riesgos podrán afectar a las entidades financieras, y de esta manera se formula la siguiente pregunta:

- ¿Cuáles son los impactos financieros y no financieros?

Para la tercera pregunta, se plantea como interrogante lograr obtener el objetivo de poder identificar las principales causas por las que estos riesgos suelen materializarse, teniendo como resultado la siguiente pregunta:

- ¿Cuáles son las principales causes que llevan a la materialización de los riesgos en Ciberseguridad?

Por último, y aclaradas las interrogantes anteriores, se formula la última pregunta del problema, la cual está relacionado con la propuesta del trabajo de investigación, y que para todos los efectos sería esta:

- ¿Cuál es el modelo de mejores prácticas para la administración de riesgos en Ciberseguridad?

Planteamiento de la hipótesis

Con los problemas investigativos planteados anteriormente, se debe hacer el planteamiento de las hipótesis de esta investigación, contemplando las siguientes tres opciones, la principal, la alternativa y la nula.

Con respecto a la hipótesis principal, lo que se busca es probar si el alcance del presente estudio está acorde con lo que el investigador pretende obtener. La segunda corresponde a un punto intermedio en la probatoria de la idea general, mientras que la última es contraria a la hipótesis principal.

- **Hipótesis principal (H_1):** la probabilidad de lograr identificar los riesgos en Ciberseguridad y sus impactos financieros y no financieros es alta, así como el desarrollo de un modelo de mejores prácticas para la administración de riesgos que permita minimizar la materialización de estos.

- **Hipótesis alternativa (H_a):** la probabilidad de lograr identificar los riesgos en Ciberseguridad y sus impactos financieros y no financieros es alta, sin embargo, no

es viable el desarrollo de un modelo de mejores prácticas para la administración de riesgos que permita minimizar la materialización de estos.

- **Hipótesis nula (H_0):** No logra identificar los riesgos en Ciberseguridad y sus impactos financieros y no financieros, así como no hay viabilidad tampoco para el desarrollo de un modelo de mejores prácticas para la administración de riesgos que permita minimizar la materialización de estos.

Con esto se logra dar el contexto necesario para poder entender las posibles viabilidades que se esperan de las tres hipótesis planteadas, las que sirven como guía para el desarrollo del presente trabajo de investigación, donde el objetivo que se persigue es que la hipótesis principal sea la que se pueda alcanzar a probar.

Objetivos

A continuación, se describen los objetivos del trabajo de investigación, pues esto es necesario para lograr establecer el horizonte investigativo por seguir.

Para lo cual se requieren establecer dos objetivos generales, a saber, uno investigativo y el otro propositivo. También se cuenta con cuatro objetivos específicos que son tomados de la sistematización del problema descrito en capítulos anteriores.

Objetivos generales

Como se menciona en la introducción a esta sección, el presente trabajo aborda dos objetivos generales, a saber, el investigativo y el propositivo, por lo tanto, los objetivos generales planteados serían:

1. **Analizar los riesgos en Ciberseguridad y sus impactos financieros y no financieros en las entidades financieras del Estado costarricense durante el año 2021.**

A continuación, se plantea el propositivo:

2. **Proponer un modelo de mejores prácticas para la administración de riesgos en Ciberseguridad en las entidades financieras del Estado costarricense.**

Objetivos específicos

Con incidencia directa después de describir los objetivos generales se deben detallar los objetivos específicos de la investigación. A continuación, la descripción de cada uno:

Lo que se busca con el primer objetivo específico es poder identificar los principales riesgos que constantemente las entidades financieras deben tener presentes, de esta manera el primer objetivo específico sería:

- Identificar los principales riesgos en Ciberseguridad.

Con la definición y aclaración de la identificación de los principales riesgos de Ciberseguridad, el siguiente objetivo específico procura identificar cuáles son los impactos financieros y no financieros que se pueden ver expuestas las entidades financieras si los riesgos son materializados, por lo tanto, el segundo objetivo específico sería:

- Identificar los impactos financieros y no financieros.

Teniendo clara la identificación de los principales riesgos y sus impactos financieros y no financieros, lo que necesariamente sigue es determinar cuáles son las principales causas que llevan a estos riesgos a materializarse. Por lo tanto, el tercer objetivo específico planteado sería:

- Determinar las principales causas que llevan a la materialización de los riesgos.

Como último objetivo específico y para poder dar la base para el desarrollo de la propuesta, se busca la creación de un modelo de mejores prácticas para la administración de riesgos en Ciberseguridad, para lo cual se plantea el siguiente objetivo:

- Sugerir modelo de mejores prácticas para la administración de riesgos.

Justificación

A continuación, es describen las tres justificaciones del presente trabajo de investigación. La práctica es la más importante y desarrolla los pormenores del porqué del análisis. La segunda es la metodológica, que se basa en el campo propiamente de la investigación de campo y finalmente la teórica, donde se sustenta la base teórica propia del estudio.

Justificación práctica

En el informe del 2018 sobre el reporte global de riesgos del Foro Económico Mundial, da evidencia de cómo los riesgos en Ciberseguridad van en aumento y están en el top de los riesgos globales (*World Economic Forum*, 2018), con lo que demuestra una cada vez complicada situación para las organizaciones de mantener sus operaciones en funcionamiento y a salvo de los ciberataques.

Estos ataques en ocasiones tienen consequencias tan severas que incluso llevan a las organizaciones a cerrar sus operaciones por días, incluso después de haber pagado grandes sumas de dinero como producto de todas las acciones de restauración o como medida a cambio de recibir la información que es "secuestrada", muchas otras organizaciones mantienen en el anonimato las consecuencias para no perder credibilidad o competitividad en sus mercados.

En Costa Rica más de 200 millones de intentos de ataques son detectados durante el 2020, con alrededor de $945 mil millones en pérdidas producto de estos ataques y se invierten $145 mil millones en Ciberseguridad (Castro, 2021), lo que se puede evidenciar es la diferencia tan grande del 15% entre inversión y las pérdidas sufridas por las empresas.

Para las entidades financieras, desarrollar un entendimiento innato de cómo y dónde encontrar riesgo cibernético en este ambiente, es de vital importancia (Deloitte, 2019), y es que en la era en que los avances en tecnologías permiten que todos estén más conectados que nunca facilitando a los ciber delincuentes encontrar maneras cada vez más fáciles de poder vulnerar los sistemas de estas organizaciones.

De aquí la importancia para los encargados de la seguridad de la información de las organizaciones que puedan tener un rol protagónico y que puedan contar con la capacidad de transformar el foco de las tecnologías de información a focos de negocios (Putrus, 2019), esto es fundamental, ya que tradicionalmente los intereses de estos no se traducen en los mejores asuntos que buscan las organizaciones.

Con todos los avances en la digitalización bancaria en una gran cantidad de países alrededor del mundo ha dado a pie que día con día cada vez más clientes utilicen medios digitales para realizar transacciones bancarias (OEA, ASOBANCARIA, 2019), y esto sin duda incrementa la cantidad de riesgos a los que se ven expuestos tanto los clientes como las entidades.

Desde luego a partir de aquí las organizaciones pueden realizar una serie de cuestionamientos de manera que les permita lograr responder a todos los riesgos a los que se enfrentan, cuestionamientos como: ¿Qué tan seguros son los controles?, ¿Qué tanto se ha mejorado con respecto al año anterior?, ¿Cómo es la comparación con respecto a los principales competidores?, y la lista podría seguir pero estas interrogantes llevan a cómo se están midiendo las cosas en la organización (Hubbard, Seiersen, 2016).

Para dar soporte a los procesos de administración de riesgos en las organizaciones, así como estas siguen considerando cómo manejar las constantes evoluciones de los riesgos en Ciberseguridad, es importante seguir considerar marcos de referencia de tal manera que den una forma más efectiva y eficiente de como evaluarlos y aún más importante cómo manejarlos (COSO, Deloitte, 2015).

Justificación metodológica

La justificación metodológica del presente trabajo de investigación, parte de una base de revisión documental de libros, artículos y textos con referencia al tema que se plantea en este análisis.

Además de esto, se cuenta con revisión de instrumentos de campo, esta investigación está soportada por la aplicación de una entrevista a los encargados de la seguridad de la información y administración de riesgos de una entidad financiera, para poder contar con criterios más expertos y apegados al objeto de estudio.

Justificación teórica

Este trabajo está compuesto por una base de conceptos finanzas y manejo de riesgos para los negocios, por lo tanto, tiene el sustento de la teoría de administración de James A.F Stoner, adicionalmente tiene el sustento de los principios de administración financiera de Lawrence J Gitman (2007).

Por último, al abarcar temas de Ciberseguridad, se toma como referencia los principios esenciales en Ciberseguridad de Brooks, Grow, Craig y Donald Short (2018) así como estándares de manejo de riesgos como COSO (2012) e ISO 27001 (2013).

Alcances y limitaciones

Alcances

Seguidamente se detallan los alcances del estudio:

- **Entidades financieras costarricenses:** es de los beneficiados más importantes con este trabajo, ya que el análisis y propuesta están enfocados en los requerimientos y factores propios de este sector.
- **Usuarios de las entidades financieras costarricenses:** uno de los beneficiarios indirectos si se quiere ver de esa manera, ya que las plataformas de las entidades financieras podrían contar con mejores controles que salvaguarden la información al tener una metodología enfocada exclusivamente en el manejo de riesgos en Ciberseguridad.
- **Profesionales en administración, finanzas, banca y seguridad de la información:** los profesionales en estas áreas tendrían un recurso más para poder analizar los principales riesgos en Ciberseguridad y lograr identificar los principales impactos de materializarse estos riesgos, y que se logren tomar mejores decisiones sobre los controles por implementar.

- **Estudiantes de administración, finanzas y seguridad de la información:** este trabajo puede convertirse en material de referencia para posteriores estudios e investigaciones.

- **Alcance temporal:** el alcance temporal del presente trabajo va de enero 2021 a diciembre 2021.

Limitaciones

- **Carencia de estudios previos:** ante la falta de estudios sobre inversiones en Ciberseguridad en general y especialmente enfocados en entidades financieras implica una limitación por considerar.

- **Acceso a información:** el hecho de que el realizador de la investigación no es trabajador de ninguna entidad financiera, constituye una limitante si se requiera información adicional de estas organizaciones, está limitación es particularmente importante, ya que no es posible determinar impactos financieros o estimaciones cuantitativas que permitan investigaciones y obtención de resultados más precisos.

- **Versatilidad del tema de estudio:** todo lo relacionado con tecnología avanza a pasos agigantados, lo que hoy aplica para una organización en unos meses ya está desactualizado, por lo que las recomendaciones que se logren dar en este estudio se pueden quedar desactualizadas en unos pocos meses, dependiendo de que tan rápido se estén desarrollando nuevos avances tecnológicos y qué tan versátiles son los ciberdelincuentes para encontrar formas de cometer fraudes que aún no se han explorado.

Capítulo II

Fundación teórica

Marco situacional

Historia de la banca costarricense

Los inicios de la historia de la banca en Costa Rica se remontan a mediados del siglo XIX, cuando el país tiene un gran auge y dependencia del café como principal actividad productiva. Tanto es así que da paso a cambios en patrones de financiamiento tanto socioeconómicos como políticos (Escoto, 2001); sin embargo, el Centro de Información Jurídica en Línea de la Universidad de Costa Rica (2006) comenta que: *"(..) desde tiempos muy remotos veníanse desarrollando diferentes operaciones que, aunque rudimentarias, eran susceptibles de considerarse como bancarias"*, (párr. 2).

Para los años 1847 y 1849, Costa Rica es gobernada por el Dr. José María Castro Madriz y precisamente en estas fechas es cuando la historia registra los primeros intentos sobre la creación de un banco. Para 1851 el entonces presidente presenta al Poder Legislativo lo que es el primer intento formal; sin embargo, el esfuerzo es en vano por la existencia de conflictos políticos y personales contra el Dr. Castro Madriz (Escoto, 2001).

Ya en 1850, Costa Rica se encuentra integrada al mercado internacional gracias a las exportaciones de café, lo que sirve de punta de lanza en la expansión del comercio costarricense, dando paso a la necesidad de contar con un sistema bancario (CIJUL, 2006) y así poder tener un organismo que facilite el comercio y movilización de los recursos económicos que se generen.

Es entonces cuando bajo el gobierno de Juan Rafael Mora en 1857 se firma el contrato Medina-Escalante, donde se establece: *"(...) la creación de un banco emisor exclusivo, con un capital de doscientos cincuenta mil colones, cuyo nombre sería Banco Nacional Costarricense"*, (Escoto, 2001, p. 5).

A partir de aquí se inicia la creación de otros bancos y transformaciones, como el Banco Anglo Costarricense en 1863, el Banco de la Unión en 1877 que luego pasó a llamarse Banco de Costa Rica. El Banco Internacional de Costa Rica que pasa por varios cambios desde su fundación en 1857. El Banco Crédito Agrícola de Cartago en 1918, y el Banco Popular en 1969.

Desde luego se debe hacer referencia a la banca privada que para 1953 mediante la Ley Orgánica 1644 del Sistema Financiero Nacional (1953) y la Ley Orgánica del Banco Central 1552 (1953) se crean para dar órdenes y da paso a la creación de la banca privada (Escoto, 2001), con una serie de limitaciones en cuanto a su funcionamiento, pero al fin y al cabo es el inicio.

Mediante la Ley 9605 (2018) el plenario de la Asamblea Legislativa de la República de Costa Rica aprueba la fusión por absorción del Banco Crédito Agrícola de Cartago y el Banco de Costa Rica, la votación cuenta con cuarenta y ocho votos a favor y cuatro en contra, de acuerdo con el texto: "*La fusión operativa será efectiva dentro de un plazo máximo de sesenta días hábiles posteriores a la entrada en vigencia de la ley, de manera tal que en dicho plazo el Bancrédito deberá efectuar, por medio de quien esté ejerciendo su administración, las tareas administrativas u operativas pertinentes para la consolidación del proceso de fusión y absorción, incluyendo la liquidación del personal remanente de la entidad bancaria."* (Fusión por absorción del Banco Crédito Agrícola de Cartago y el Banco de Costa Rica, 2018, art.1).

En dicha Ley se establecen todas las condiciones para llevar a cabo la fusión, incluido la integración del patrimonio, manejo del personal y directivos, que se deben seguir prestando los servicios mientras dure el proceso de fusión. Es importante resaltar que es el segundo banco estatal que cierra en menos de 30 años.

Marco legal para delitos informáticos en Costa Rica

Desde que inicia la pandemia por el Covid-19, los ciberataques han evolucionado utilizando cada vez mejores técnicas para perpetrar ataques en prácticamente cualquier sector industrial; sin embargo, existen algunos que son más buscados que otros debido a que los ciberdelincuentes han encontrado una verdadera mina en la información sensible que manejan las empresas en sectores como salud, banca y finanzas, así como compañías de terceros que brindan soporte a estas compañías.

Durante el 2020 se tiene el dato que se monitorean más de 150 mil millones de eventos de seguridad por día en más de 130 países (IBM, 2021), de acuerdo con este estudio: "*los ataques cibernéticos a organizaciones de atención médica, fabricación y energía se*

duplicaron con respecto a 2019, siendo manufactura y energía los más atacados en 2020, solo superados por el sector financiero y de seguros", (IBM, 2021, p. 5)

En Costa Rica se estima que más de 200 millones de ciberataques se lanzan durante el 2020 (Castro, 2021), este número de ataques es bastante alto y la preocupación de expertos es que el grado de refinamiento va en aumento, lo que genera más pérdidas a las compañías y si se compara con las inversiones para mejoras en la postura de seguridad el problema incluso puede ser más serio, la firma de seguridad Atlas VPN reafirma está preocupación: "*los delitos cibernéticos costaron al mundo más de $1 mil millones durante 2020; es decir, cerca del 1% del Producto Interno Bruto (PBI) mundial*", (Castro, 2021, párr.7).

Costa Rica está dando algunos pasos para estar mejor preparados, para el 2017 establece su Estrategia Nacional de Ciberseguridad de Costa Rica (MCIT, 2017), como el primer esfuerzo de coordinación entre instituciones para hacerles frente a los retos y problemas en esta área, acompañado a esto están regulaciones y acuerdos con tratados internacionales que mejora los grados de madurez que el país va tomando con respecto a este asunto.

Por último, la Unidad de Informática de Análisis Prospectivo y Política Pública del Ministerio de Planificación Nacional y Política Económica desarrolla un análisis de la Ciberseguridad en el Sistema de Planificación Nacional (2020), con el fin de mostrar el camino por seguir entre las distintas organizaciones gubernamentales para hacer plantear iniciativas estratégicas que les permitan poder atacar estos problemas de manera satisfactoria.

A continuación, se detalla parte del marco jurídico con el que cuenta Costa Rica en materia de ciberdelitos:

Decreto Nº 37052 - Creación CSIRT

Mediante el decreto 37052-MICITT (2012) se crea el Centro de Respuesta de Incidentes de Seguridad Informática de Costa Rica CSIRT-CR, y se detalla:

> *Créase el Centro de Respuesta de Incidentes de Seguridad Informática (CSIRT-CR) con sede en las instalaciones del Ministerio de Ciencia y Tecnología, con facultades suficientes para coordinar con los poderes del Estado, instituciones autónomas, empresas y bancos del Estado todo lo relacionado con la materia de seguridad*

> *informática y cibernética y concretar el equipo de expertos en seguridad de las Tecnologías de la Información que trabajará para prevenir y responder ante los incidentes de seguridad cibernética e informática que afecten a las instituciones gubernamentales.* (37052-MICIT, 2012, art. 1).

Contar con un punto centralizado y responsable de agrupar a otras instituciones del Gobierno costarricense es fundamental, para que exista un hilo conductor de iniciativas y estrategias para dar respuesta a los retos del ciberespacio.

Costa Rica debe seguir avanzando en mejorar las estructuras organizativas y tecnológicas que le permita ser competitivos y que la comunidad internacional la vea como un modelo por seguir soportado por las distintas iniciativas para regular los delitos informáticos.

Reforma Código Penal - Decreto Legislativo Nº 9048

El 10 de julio del 2012, queda publicada la reforma de la Sección VIII, Delitos Informáticos y Conexos, del Título VII del Código Penal N° 9048 (2012), donde quedan reformados los siguientes artículos: 167, 196, 196 bis, 214, 217 bis, 229 bis y 288 de la Ley N.º 4573, Código Penal, de 4 de mayo de 1970, y sus reformas.

A continuación, el detalle de los artículos y aspectos más relevantes sobre la utilización de recursos informáticos u otros, para cometer ciberdelitos y que quedan reformados como parte del decreto anteriormente mencionado:

Artículo 196.- Violación de correspondencia o comunicaciones

"b) Las personas encargadas de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tengan acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos", (Código Penal, 2012, art. 196).

Por mucho tiempo las personas con accesos privilegiados por la información sensitiva que manejan, les hace pensar tener la potestad de que por esto o sus conocimientos en tecnología pueden sustraer información aprovechándose de sus facultades, lo que a partir de esta reforma queda estipula la condena a la que pueden exponerse, incluso incluye aquellos que sin tener

bastos conocimientos en tecnología pero que administran un sistema, hacen mal uso de la información contenida para provecho propio o de terceros.

Artículo 214.- Extorsión

"La pena será de cinco a diez años de prisión cuando la conducta se realice valiéndose de cualquier manipulación informática, telemática, electrónica o tecnológica", (Código Penal, 2012, art. 214).

La extorsión es una de las maneras más comunes que las personas utilizan para sacar provecho de los errores cometidos por quién está siendo extorsionado valiéndose del argumento de que es un castigo justo por lo que la otra persona comete en perjuicio del extorsionador o un tercero. Esto se agrava con el uso de la tecnología, ya que aumenta a tal punto que el mayor temor de quien es extorsionado, es que su situación no se comparta debido a que sabe en cuestión de minutos, millones de personas alrededor del mundo sabrán de lo ocurrido.

Artículo 217 bis.- Estafa informática

> *Se impondrá prisión de tres a seis años a quien, en perjuicio de una persona física o jurídica, manipule o influya en el ingreso, en el procesamiento o en el resultado de los datos de un sistema automatizado de información, ya sea mediante el uso de datos falsos o incompletos (…) que dé como resultado información falsa, incompleta o fraudulenta, con la cual procure u obtenga un beneficio patrimonial o indebido para sí o para otro.* (Código Penal, 2012, art. 217 bis).

Esto es de suma importancia debido a que el auge de la tecnología y los sistemas de información provoca tener acceso a maneras cada vez más fáciles y rápidas de estafar, pero además el mismo artículo hace mención especial sobre si las conductas están hechas en sistemas de información de estado:

> *La pena será de cinco a diez años de prisión, si las conductas son cometidas contra sistemas de información públicos, sistemas de información bancarios y de entidades financieras, o cuando el autor es un empleado encargado de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus*

> *funciones tenga acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos",* (Código Penal, 2012, art. 217 bis).

Existen funcionarios públicos cuyo acceso a información sensible puede representar sacar provecho y utilizarlo para beneficio propio o de terceros, con lo cual la pena puede ser mayor, de comprobarse este tipo de delitos.

Artículo 229 bis.- Daño informático

> *Se impondrá pena de prisión de uno a tres años al que sin autorización del titular o excediendo la que se le hubiera concedido y en perjuicio de un tercero, suprima, modifique o destruya la información contenida en un sistema o red informática o telemática, o en contenedores electrónicos, ópticos o magnéticos*. (Código Penal, 2012, art. 229).

En seguridad de la información existen tres pilares, la confidencialidad, la disponibilidad y la integridad de la información, entendiéndose esta última como la cualidad de que la información se mantenga sin alteraciones no autorizadas por parte de terceros, (Firma-e, 2014).

Artículo 288.- Espionaje

Este artículo establece que: *"La pena será de cinco a diez años de prisión cuando la conducta se realice mediante manipulación informática, programas informáticos maliciosos o por el uso de tecnologías de la información y la comunicación",* (Código Penal, 2012, art. 228).

El espionaje informático en ocasiones se tiende a vincular entre países, pero existe una tendencia mayor a que empresas contraten a ciberdelincuentes para que realicen espionajes sobre la competencia mediante la inclusión de programas de espionaje que se envían principalmente por correo electrónico aprovechándose de la falta de educación de las personas en las empresas en temas de seguridad de la información y donde los hacen más propensos a caer en errores, poniendo en riesgo la integridad de los sistemas que manejan pero más importante aún la información que se encuentra almacenada.

Artículo 230.- Suplantación de identidad

> *Será sancionado con pena de prisión de tres a seis años quien suplante la identidad de una persona en cualquier red social, sitio de Internet, medio electrónico o tecnológico de información. La misma pena se le impondrá a quien, utilizando una identidad falsa o inexistente, cause perjuicio a un tercero*. (Código Penal, 2012, art. 230).

Sin lugar a dudas, la era de las redes sociales trae consigo aspectos muy positivos como la posibilidad de mantenerse en contacto sin importar las fronteras y distancias, ahora se está más conectado que nunca; sin embargo, también trae formas mucho más fáciles de suplantar identidades, solo toma algunos minutos crear un perfil falso en alguna red social con fotos y datos reales de las personas, ya que mucha de esta información se encuentra pública y fácilmente con eso cualquiera se puede hacer pasar por alguien más y, de esta manera, conseguir hacer fraudes o cometer otro tipo de delitos.

Artículo 232.- Instalación o propagación de programas informáticos maliciosos

"Será sancionado con prisión de uno a seis años quien sin autorización, y por cualquier medio, instale programas informáticos maliciosos en un sistema o red informática o telemática, o en los contenedores electrónicos, ópticos o magnéticos", (Código Penal, 2012, art. 232).

Este artículo es bastante extenso en cuanto a los escenarios en los que se puede presentar, por ejemplo inducir a alguien más para que realice la instalación del programa malicioso, y es que los ciberdelincuentes se aprovechan de la falta de cultura en educación en estos temas para inducir a las personas mediante engaños, que van desde promociones atractivas como herencias o premios sorpresas, hasta aprovecharse de acontecimientos relevantes a escala mundial y así pedirles que visiten algún sitio o descarguen el archivo que contiene el correo sin las personas saber qué ocurre por detrás.

Artículo 233.- Suplantación de páginas electrónicas

> *Se impondrá pena de prisión de uno a tres años a quien, en perjuicio de un tercero, suplante sitios legítimos de la red de internet.*

> *La pena será de tres a seis años de prisión cuando, como consecuencia de la suplantación del sitio legítimo de internet y mediante engaño o haciendo incurrir en error, capture información confidencial de una persona física o jurídica para beneficio propio o de un tercero.* (Código Penal, 2012, art. 232).

Similar a la suplantación de identidad, la suplantación de páginas electrónicas es muy efectiva para los ciberdelincuentes, ya que se basa en crear un sitio que luce prácticamente igual al auténtico.

Esto es muy común en sitios bancarios, con los logos y colores propios del banco y solicitan a las personas ingresar sus datos personales, así como usuario y contraseña del sitio para luego desplegar un mensaje, que hace pensar al usuario que la página tiene un error cuando, en realidad, capta la información que el ciberdelincuente requiere para que, posteriormente, pueda transferir el dinero de la persona a otras cuentas propias o de terceros.

Artículo 234.- Facilitación del delito informático

"Se impondrá pena de prisión de uno a cuatro años a quien facilite los medios para la consecución de un delito efectuado mediante un sistema o red informática o telemática, o los contenedores electrónicos, ópticos o magnéticos", (Código Penal, 2012, art. 232).

Este artículo claramente viene a intentar cerrar portillos que, por algún tecnicismo u omisión de algún tipo de situación aún no vivida, pueden quedar fuera de la ley.

Artículo 236.- Difusión de información falsa

> *Será sancionado con pena de tres a seis años de prisión quien, a través de medios electrónicos, informáticos, o mediante un sistema de telecomunicaciones, propague o difunda noticias o hechos falsos capaces de distorsionar o causar perjuicio a la seguridad y estabilidad del sistema financiero o de sus usuarios.* (Código Penal, 2012, art. 236).

Dentro de los poderes que confiere las redes sociales y cualquier tipo de blog en internet es la facultad que les da a las personas de decir lo que sea sin la necesidad de certificar la veracidad de sus palabras, lo cual lleva a la manipulación peligrosa de la opinión pública,

incidir en intensiones de votos para presidente e incluso avivar los ánimos en manifestaciones violentas, pues el poder de las palabras es algunas veces pasado por alto y solo se ve cuando las consecuencias y daños ocasiones son muy caros.

Convenio de Europa sobre Ciberdelincuencia (Budapest, 2001) N° 9452

También conocido como el Convenio de Budapest, se publica en Costa Rica en julio del 2017 la Ley 9452 Convenio de Europa sobre Ciberdelincuencia (Budapest, 2001).

Sus raíces radican en la Unión Europea bajo el Consejo de Europa, sin embargo, este tratado de colaboración internacional no tiene restricciones en cuanto el origen de los países miembros. Actualmente no existe algún otro instrumento internacional sobre delitos informáticos, lo que le lleva a tener muy buena aceptación a escala internacional (Paris, 2017).

El convenio tiene dentro de sus objetivos la tipificación de delitos informáticos en 4 categorías: "*(i) contra la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos; (ii) informáticos; (iii) relacionados con el contenido; y (iv) relacionados con la infracción de propiedad intelectual y derechos afines*", (París, 2017, párr. 1).

La ley en Costa Rica consta de 48 artículos (Convenio de Europa sobre Ciberdelincuencia (Budapest, 2001, N° 9452, 2017) que cumplen con la normativa internacional exigida por la Unión Europea como proceso de adopción y aprobación, y que le permite a Costa Rica ser el país número 56 en adscribirse (Paris, 2017).

Dentro de otras ventajas que permite el convenio es la colaboración de los países miembros en la lucha contra los ciberdelincuentes, especialmente porque estos delitos casi nunca ocurren dentro de los límites del país que está siendo afectado, por lo que este tipo de acuerdos facilitan la ayuda en despliegue técnico, estratégico y de recursos profesionales para poder hacer frente a estos problemas de manera más holística.

Ley Nº 8968 de protección de la persona frente al tratamiento de sus datos personales

Esta ley tiene como objetivo primordial (Asamblea Legislativa, Protección de la Persona frente al tratamiento de sus datos personales, 2011):

> *(…) garantizar a cualquier persona, independientemente de su nacionalidad, residencia o domicilio, el respeto a sus derechos fundamentales, concretamente, su derecho a la autodeterminación informativa en relación con su vida o actividad privada y demás derechos de la personalidad, así como la defensa de su libertad e igualdad con respecto al tratamiento automatizado o manual de los datos correspondientes a su persona o bienes.* (art.1)

Para poder cumplir con este fin, mediante los artículos transitorios II y III de la ley mencionada expresa (Prodhab, 2011):

> *TRANSITORIO II.- A partir de la fecha de entrada en vigencia de esta ley, se iniciará el proceso de conformación e integración de la Prodhab; para ello, se dispondrá de un plazo máximo de seis meses.* (párr.2)
>
> *TRANSITORIO III.- El Poder Ejecutivo emitirá la reglamentación de esta ley en un plazo máximo de seis meses después de la conformación de la Prodhab, recogiendo las recomendaciones técnicas que le proporcione la Agencia.*

Da la conformación a Prodhab (Agencia de Protección de Datos de los Habitantes), adscrita al Ministerio de Justicia y Paz, cuenta con independencia de criterio y administración, así como con una personería jurídica que les permite realizar solicitudes de partidas presupuestarias, suscribir contratos y convenios todo con el fin de que puedan cumplir con las obligaciones y reglamentos asignados por ley (Prodhab, 2011).

Además de su función de cumplir con el objetivo principal de la Ley 8968, esta agencia procura guiar a los ciudadanos costarricenses sobre sus derechos así como a las organizaciones tanto públicas como privadas sobre el correcto manejo de los datos que almacenan de sus clientes para que vayan en concordancia con la ley, buscando que Costa Rica esté al corriente de otras leyes internacionales en la misma materia como GDPR en la

Unión Europea (*General Data Protection Regulation*) por sus siglas en inglés, y más recientemente en Brasil con la LGDP (*Lei Geral de Proteção de Dados Pessoais*) por sus siglas en portugués de Brasil.

Situación de la Ciberseguridad en Costa Rica

El Banco Interamericano de Desarrollo (BID) en conjunto con la Organización de los Estados Americanos (OEA) y con colaboración del Centro Global de Capacitación en Seguridad Cibernética de la Universidad de Oxford, realizan un estudio sobre la Ciberseguridad riesgos, avances y el camino por seguir en América Latina y el Caribe en el año 2020.

En él se detallan las tendencias regionales sobre la preparación en Ciberseguridad, la perspectiva integral de la Unión Europea, amenazas emergentes y las repercusiones para América Latina, los modelos de madurez en cuanto a la capacidad de Ciberseguridad y como dato principal hacer una radiografía de Costa Rica, así como de los demás países Latinoamericanos (Observatorio Ciberseguridad, 2020).

Para el año 2017, Costa Rica tiene poco más del 71% de penetración de internet y alrededor unos 3,5 millones de personas cuentan con acceso a internet (Observatorio Ciberseguridad, 2020). Lo cual es un dato bastante relevante en cuanto a la masificación del uso de la tecnología y el acceso a la red de redes.

El estudio también resalta los esfuerzos de Costa Rica por parte del Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT) en cuanto a la Estratégia Nacional de Ciberseguridad para poder contar con un marco de referencia y guía sobre el uso adecuado de las tecnologías de información, así como la creación del Centro de Respuesta de incidentes de Seguridad Informática de Costa Rica CSIRT-CR en el año 2012 así como otra series de leyes y que procuran mostrar las intenciones del país en tratar de tener una mejor postura para poder enfrentar este mundo tan cambiante como es el de las tecnologías de información y los ciberataques.

Modelo de madurez de la capacidad de Ciberseguridad para las naciones

El informe que elaboran la OEA y el BID en el 2016 es de las primeras en abordar un estudio sobre las capacidades cibernéticas para América Latina, el cual ofrece una evaluación sobre el estado del desarrollo en América Latina y el Caribe (Observatorio Ciberseguridad, 2020).

Para el 2020 se desarrolla el segundo informe lo cual da una perspectiva sobre la evolución en los avances de cada país y cómo están comparativamente con los otros de manera tal que les permita focalizar esfuerzos políticos y presupuestarios de acuerdo con sus objetivos nacionales de seguridad de la información.

Este estudio está basado en un Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones (CMM) por sus siglas en inglés y desarrollado por el Centro Global de Capacidad en Seguridad Cibernética (GCSCC), por sus siglas en inglés de la Universidad de Oxford Caribe (Observatorio Ciberseguridad, 2020).

Abarca cinco dimensiones: "*(i) política y estrategia; (ii) cultura y sociedad; (iii) educación, capacitación y habilidades; (iv) marcos legales y regulatorios, y (v) estándares, organizaciones y tecnologías*", (Observatorio Ciberseguridad, 2020, p. 20) y que pueda brindar un procedimiento más exacto sobre el grado de madurez de los países en cada dimención.

Cada dimensión tiene a su vez cinco etapas (Observatorio Ciberseguridad, 2020):

Inicial

En esta etapa no existe madurez en ciberseguridad o bien se encuentra en un estadio muy embrionario. Puede haber discusiones iniciales sobre el desarrollo de capacidades de ciberseguridad, pero no se han tomado medidas concretas. Falta evidencia observable de la capacidad de seguridad cibernética. (p.42). Básicamente no se cuenta con nada o los esfuerzos de mejorar la ciberseguridad apenas si están iniciando.

Formativa

"Algunos aspectos han comenzado a crecer y formularse, pero pueden ser ad hoc, desorganizados, mal definidos, o simplemente nuevos. Sin embargo, se puede demostrar claramente evidencia de este aspecto", (p 42). Algunos esfuerzos han iniciado; sin embargo, carecen de estructura y organización.

Consolidada

Los indicadores están instalados y funcionando. Sin embargo, no se le ha dado mucha consideración a la asignación de recursos. Se han tomado pocas decisiones acerca de los beneficios con respecto a la inversión relativa en este aspecto. Pero la etapa es funcional y está definida. (p.42). Se cuenta con una estructura que al menos ya tiene indicadores que ayudan a mostrar el estado de los distintos dominios; sin embargo, aún se tienen áreas por mejorar, por ejemplo, asignación de recursos Otro aspecto por resaltar es que no hay una clara definición para la toma de decisiones con respecto a los resultados que se puedan ir obteniendo, se puede considerar como una buena posición en cuanto a nivel de madurez pero aún le falta para consolidarse.

Estratégica

En esta etapa se han tomado decisiones sobre qué indicadores de este aspecto son importantes y cuáles lo son menos para la organización o el Estado en particular. La etapa estratégica refleja el hecho de que estas elecciones se han realizado condicionadas por las circunstancias particulares del Estado o de las organizaciones. (p.42).

Aquí se logra evidenciar una estructura organizacional o de país tomando decisiones estratégicas alineadas a la información obtenida por los indicadores, y se está mejor preparado para seguir al siguiente nivel de madurez.

Dinámica

En esta etapa existen mecanismos claros para alterar la estrategia en función de las circunstancias prevalentes, como la sofisticación tecnológica del entorno de amenaza, el

conflicto global o un cambio significativo en un área de preocupación (por ejemplo, delito informático o privacidad). (Observatorio Ciberseguridad, 2020, p. 42).

Es el estado de mayor madurez de una organización o estado, donde permite reaccionar con mayor prontitud y exactitud a cambios en el entorno.

Este modelo es de suma importancia, ya que permanece en constante revisión de manera tal que sea de relevancia para la realidad mundial, tal es el caso que para el último estudio se adicionan nuevas áreas de estudio tales como:

> *(…) modo de operación de la capacidad de respuesta a incidentes, la "comprensión del usuario de la protección de información personal en línea", los "mecanismos para la presentación de informes", informes de incidentes cibernéticos por "medios y redes sociales", "legislación de protección de datos", "protección infantil en línea", "legislación de protección del consumidor", "legislación de propiedad intelectual", "cooperación formal" y "cooperación informal" sobre asuntos de delitos informáticos, "calidad del software", "controles técnicos de seguridad" y "controles criptográficos".* (Observatorio Ciberseguridad, 2020, p. 21).

Estas modificaciones dan respuesta a la evolución de la Ciberseguridad, de manera tal que este tipo de estudios sigan mostrando información importante, y den valor agregado a los países sobre las principales áreas por corregir y con ello trazar el camino a un país más y mejor preparado.

Como todo modelo de madurez, tiene como idea sentar los parámetros necesarios que los países y sus organizaciones deben trabajar para ir fortaleciendo su posición y solidez en los procesos de seguridad de la información.

A continuación, se detallan las 5 dimensiones:

Dimensión	Subdimensión
Dimensión 1:	D1.1 Estrategia Nacional de Ciberseguridad
Política y estrategia de Ciberseguridad	D1.2 Respuesta a incidentes

Dimensión	Subdimensión
	D1.3 Protección de Infraestructura Crítica (IC) D1.4 Gestión de crisis D1.5 Defensa cibernética D1.6 Redundancia de comunicaciones
Dimensión 2: Cultura cibernética y sociedad	D2.1 Mentalidad de Ciberseguridad D2.2 Confianza y seguridad en internet D2.3 Comprensión del usuario de la protección de información personal en línea D2.4 Mecanismos de presentación de informes D2.5 Medios y redes sociales
Dimensión 3: Educación, capacitación y habilidades en Ciberseguridad	D3.1 Sensibilización D3.2 Marco para la educación D3.3 Marco para la formación profesional
Dimensión 4: Marcos legales y regulatorios	D4.1 Marcos legales D4.2 Sistema de justicia penal D4.3 Marcos de cooperación formal e informal para combatir el delito cibernético
Dimensión 5: Estándares, organizaciones y tecnologías	D5.1 Adhesión a los estándares D5.2 Resiliencia de infraestructura de internet D5.3 Calidad del *software* D5.4 Controles técnicos de seguridad D5.5 Controles criptográficos D5.6 Mercado de Ciberseguridad D5.7 Divulgación responsable

Nota. Observatorio Ciberseguridad (2020, pp.43-44).

De acuerdo con los niveles de madurez y la división de las cindo dimensiones, el estudio arroja los siguientes resultados para Costa Rica al hacer la compación del estudio del 2016 con el 2020:

- **Dimensión 1: Política y estrategia de Ciberseguridad**
    - **D1-1 Estrategia Nacional de Seguridad Cibernética**

Área	2016	2020
Desarrollo de la estrategia	Formativa	Consolidada
Organización	Inicial	Formativa
Contenido	Inicial	Consolidada

Nota. Observatorio Ciberseguridad (2020, p.86).

En esta dimensión, Costa Rica muestra avances importantes comparativamente con el 2016, en las dos primeras áreas avanza un peldaño; sin embargo, el área de contenido pasa de su primera etapa y se posiciona dos peldaños más adelante, lo que significa que en cuatro años pasa de inicial a formativa y por último a consolidada.

    - **D1-2 Respuesta a incidentes**

Área	2016	2020
Identificación de incidentes	Formativa	Formativa
Organización	Formativa	Formativa
Coordinación	Formativa	Formativa
Modo de operación	Incial	Formativa

Nota. Observatorio Ciberseguridad (2020, p.86).

En cuanto al dominio de respuesta a incidentes, los avances no son tan significativos y por el contrario en tres de las cuatro áreas no muestran avances y solo el modo de operación, pasa a un nivel de madurez formativo.

    - **D1-3 Protección de la Infrastructura Crítica (IC)**

Área	2016	2020
Identificación	Incial	Incial
Organización	Incial	Incial
Gestión de riesgos y propuesta	Incial	Incial

Nota. Observatorio Ciberseguridad (2020, p.86).

El dominio de Protección de la Infrastructura Crítica, tiene suma importancia para mantener ambientes seguros y Costa Rica comparativamente 2016 con 2020 no muestra avances en sus niveles de madurez, lo cual representa un área importante de foco de atención por parte del Gobierno y sus organizaciones.

- **D1-4 Manejo de crisis**

Área	2016	2020
Manejo de crisis	Inicial	Inicial

Nota. Observatorio Ciberseguridad (2020, p.86).

Ante situaciones de crisis es importante que se cuenten con todas las herramientas para hacer frente a estos eventos, porque claramente Costa Rica aún tiene cosas por mejorar, ya que ante crisis el tiempo para reestablecer operaciones es crucial, además de que brinda confianza de que las operaciones pueden volver a la normalidad lo más rápido posible.

- **D1-5 Defensa cibernética**

Área	2016	2020
Estrategia	Inicial	Inicial
Organización	Inicial	Inicial
Coordinación	Inicial	Inicial

Nota. Observatorio Ciberseguridad (2020, p.86).

Si bien el CSIRT 37052-MICITT (2012), es un paso que da Costa Rica para tener un punto centralizado de manejo de incidencias cibernéticas, se debe continuar el trabajo y que más organizaciones se unan a este tipo de esfuerzos e iniciativas de manera tal que se logre tener mejores niveles de madurez que brinden más respaldo.

- **D1-6 Redundancia de comunicaciones**

Área	2016	2020
Redundancia de comunicaciones	Formativa	Formativa

Nota. Observatorio Ciberseguridad (2020, p.86).

Principio básico de continuidad de negocio es contar con reduncia, al menos Costa Rica cuenta con algunos esfuerzos; sin embargo se debe seguir mejorando para alcanzar mejores niveles de madurez, ya que en 4 años no se logra alcanzar el siguiente nivel.

- **Dimensión 2: Cultura cibernética y sociedad**
  - **D2-1 Mentalidad de seguridad cibernética**

Área	2016	2020
Gobierno	Formativa	Formativa
Sector privado	Consolidada	Consolidada
Usuarios	Inicial	Formativa

Nota. Observatorio Ciberseguridad (2020, p.86).

Es de esperarse que los sectores privados cuenten con una mejor posición en cuanto a la cultura cibernética, ya que ante un evento de seguridad que afecte su reputación u operaciones tiene mayores impactos; sin embargo, el Gobierno debe mejorar en temas de educación interinstitucional y llevar esto mismo a toda la ciudadanía que en la mayoría de las ocasiones es el primer eslabón en tener afectación.

- **D2-1 Confianza y seguridad en internet**

Área	2016	2020
Confianza y sSeguridad en el internet del usuario	Formativa	Formativa
Confianza del usuario en los servicios de gobierno electrónico	Formativa	Formativa
Confianza del usuario en los servicios de comercio electrónico	Formativa	Formativa

Nota. Observatorio Ciberseguridad (2020, p.86).

Los resultados de este dominio refuerzan los resultados del anterior, pero no hay avance en los niveles de madurez sobre la confianza y seguridad que tienen las personas cuando navegan por internet, así como los servicios que brinda el Gobierno de Costa Rica por distintos medios electrónicos.

- **D2-3 Comprensión del usuario de la protección de la información en línea**

Área	2016	2020
Comprensión del usuario de la protección de información Personal en línea	Inicial	Formativa

Nota. Observatorio Ciberseguridad (2020, p.86).

La educación es importante para que las personas entiendan los daños y repercusiones que existen al navergar por internet. El país muestra ciertos avances; sin embargo, se debe trabajar más especialmente para aquellos que aún son afectados por barreras tecnologícas

- **D2-4 Mecanismos de denuncia**

Área	2016	2020

Mecanismos de denuncia	Incial	Consolidada

Nota. Observatorio Ciberseguridad (2020, p.86).

Parte de la educación es la comunicación de canales para informar posibles incidencias de seguridad, y al menos el país mejora en este dominio comparativamente con el 2016.

- **D2-5 Medios y redes dociales**

Área	2016	2020
Medios y redes sociales	Inicial	Formativa

Nota. Observatorio Ciberseguridad (2020, p.86).

Esto es un área importante para desarrollar, porque cada vez más son las noticias falsas y menos las personas que logran identificarlas. Costa Rica procura seguir con los esfuerzos mediante esfuerzos públicos y privados en hacer conciencia sobre el correcto uso de las redes sociales, máxime con el auge que tiene como medio de comunicación masivo.

- **Dimensión 3: Formación, capacitación y habilidades de seguridad cibernética**
  - **D3-1 Sensibilización**

Área	2016	2020
Programas de sensibilización	Inicial	Formativa
Sensibilización ejecutiva	Formativa	Formativa

Nota. Observatorio Ciberseguridad (2020, p.87).

Continuando con el dominio anterior sobre redes sociales, en este viene a reforzar el esfuerzo al menos en programas de sensibilización incluso desde escuelas, lo que representa el camino correcto por seguir.

- **D3-2 Marco para la formación**

Área	2016	2020
Provisión	Formativa	Consolidada
Administración	Inicial	Formativa

Nota. Observatorio Ciberseguridad (2020, p.87).

Costa Rica sigue mejorando en temas sobre la estructuración en la formación académica en temas de Ciberseguridad, tanto en el provisionamiento de la educación así como en el soporte administrativo que debe acompañar toda la logística detrás de estos esfuerzos.

- **D3-3 Marco para la capacitación profesional**

Área	2016	2020
Provisión	Formativa	Formativa
Apropiación	Formativa	Formativa

Nota. Observatorio Ciberseguridad (2020, p.87).

El domino sobre el marco para la capacitación profesional no muestra avances comparativamente en los estudios del 2016 con respecto al 2020, sin duda se debe mejorar en la produción de más profesionales en Ciberseguridad para satisfacer el mercado laboral cada vez con más demanda y poca oferta.

- **Dimensión 4: Marcos legales y regulatorios**
  - **D4-1 Marcos legales**

Área	2016	2020
Marcos legislativos para la seguridad de las TIC	Formativa	Formativa
Privacidad, libertad de expresión y otros Derechos humanos en línea	Consolidada	Consolidada
Legislación sobre	Inicial	Consolidada

Área	2016	2020
protección de datos		
Protección infantil en línea	Inicial	Consolidada
Legislación de protección al consumidor	Inicial	Consolidada
Legislación de propiedad intelectual	Inicial	Consolidada
Legislación sustantiva contra el delito cibernético	Consolidada	Estratégica
Legislación procesal contra el delito cibernético	Consolidada	Consolidada

Nota. Observatorio Ciberseguridad (2020, p.87).

En términos generales Costa Rica demuestra avances en temas regulatorios y legales, se debe seguir madurando y evaluar reformas necesarias para cumplir con los nuevos retos y desafíos que día a día se representan.

- **D4-2 Sistema de justicia penal**

Área	2016	2020
Fuerzas del orden	Consolidada	Consolidada
Enjuiciamiento	Formativa	Formativa
Tribunales	Formativa	Formativa

Nota. Observatorio Ciberseguridad (2020, p.87).

Si bien no se muestran avances en los niveles de maduración con respecto al sistema de justicia penal, Costa Rica cuenta con un marco jurídico que le permite al menos estar mejor preparados y enfocarse precisamente en las áreas que debe mejorar y madurar en esos procesos.

- **D4-3 Marcos de cooperación formales e informales para combatir el delito cibernético**

Área	2016	2020
Cooperación formal	Inicial	Consolidada
Cooperación informal	Inicial	Consolidada

Nota. Observatorio Ciberseguridad (2020, p.87).

Los cambios en reglamentos y reformas para tipificar los delitos informáticos, le permite a Costa Rica ser parte de organismos internacionales de cooperación en temas de Ciberseguridad como implementar mejores prácticas de países más avanzados en estos asuntos .

- **Dimensión 5: Estándares, organizaciones y tecnologías**
  - **D5-1 Cumplimiento de los estándares**

Área	2016	2020
Estándares de seguridad para las TIC	Inicial	Inicial
Estándares de adquisiciones	Inicial	Inicial
Estándares en el desarrollo de *software*	Inicial	Inicial

Nota. Observatorio Ciberseguridad (2020, p.87).

Costa Ria cuenta con el conocimiento para implementar las mejores prácticas del mercado; sin embargo, en ocasiones las inversiones para llevarlas a cabo son altas, lo que provoca que se requiera de un poco más de tiempo o, en otras oportuniades la inversión no va de la mano con el tamaño y complejidad de las organizaciones, por lo que se decide no implementarlas.

  - **D5-2 Resiliencia de la infraestructura de internet**

Área	2016	2020
Resilencia de la infrastructura de Internet	Inicial	Inicial

Nota. Observatorio Ciberseguridad (2020, p.87).

Una tarea pendiente de Costa Rica es la mejora en la infrastructura de internet, contar con una red de alta velocidad y que sea estable es imprensindible, para que el país sea más competitivo y que permita abrir nuevos mercados.

- **D5-3 Calidad del *software***

Área	2016	2020
Calidad del *software*	Inicial	Inicial

Nota. Observatorio Ciberseguridad (2020, p.87).

El desarrollo del *software* es impresindible que mejore, los principales ciberataques se relacionan con falta de buenas prácticas en el diseño y programación de sistemas.

- **D5-4 Controles técnicos de seguridad**

Área	2016	2020
Controles técnicos de seguridad	Inicial	Inicial

Nota. Observatorio Ciberseguridad (2020, p.87).

Costa Rica debe seguir mejorando los controles de seguridad, y para eso se debe invertir y seguir los estándares internacionales.

- **D5-5 Controles criptográficos**

Área	2016	2020
Controles criptográficos	Inicial	Inicial

Nota. Observatorio Ciberseguridad (2020, p.87).

La criptografía permite garantizar la confidencialidad de la información, por lo que es importante que también existan mejoras en está área, de manera tal que se salvaguarde la información de los ciudadanos.

- **D5-6 Mercado de seguridad cibernética**

Área	2016	2020
Tecnologías de seguridad cibernética	Inicial	Formativa
Seguro cibernético	Inicial	Inicial

Nota. Observatorio Ciberseguridad (2020, p.87).

En el mercado costarricense cada vez más existen opciones para mejorar las posturas de seguridad de las empresas y organizaciones; sin embargo un área de enfoque es el establecimiento de seguros ante ataques informáticos como medida de mitigación de riesgos.

- **D5-7 Divulgación responsable**

Área	2016	2020
Divulgación responsable	Inicial	Inicial

Nota. Observatorio Ciberseguridad (2020, p.87).

Costa Rica debe enfocar esfuerzos, para que exista una estrategia de comunicación responsable en temas de ciberseguridad.

Estrategia Nacional de Ciberseguridad del Ministerio de Ciencia, Tecnología y Telecomunicaciones

La tecnología avanza a pasos agigantados, la innovación representa un reto que resulta dificil por no decir imposible para que las organizaciones y países se mantengan a la vanguardia ya que incluso se dice incluso que cada minuto nuevas tecnologías se lanzan a los mercados cuando la anterior apenas si se está adaptando.

Sin embargo, estos avances deben ser correctamente contextualizados a las realidades y posibilidades, tanto de países como organizaciones, al menos para no perder competitividad y brindar condiciones para los inversionistas existentes y nuevos, ya que las tecnologías de información acompañadas de un buen ambiente político que impulse leyes y regulaciones necesarias, son requeridas para el adecuado desarrollo de mercados lo que ayuda también a mejorar en los aspectos económicos y sociales.

Como se mencionó anteriormente, con los avances también emerge el desarrollo de una tendencia peligrosa y que pone en riesgo la estabilidad de los países y las operaciones de las organizaciones, sin importar su tamaño o complejidad, los ciberdelincuentes.

Ante esta necesidad en el 2017, Costa Rica da un paso adelante en esta lucha con la consecusión de la Estrategia Nacional de Ciberseguridad, con el siguiente planteamiento en mente:

> *La Estrategia Nacional de Ciberseguridad plantea un esfuerzo conjunto y articulado entre todos los sectores del país, para así garantizar que los objetivos que se establezcan sean equilibrados, eficaces y acordes a la realidad nacional, definiendo los principios generales que marcarán la pauta en esta materia* (Estrategia Nacional de Ciberseguridad de Costa Rica, 2017, p. 12)

Esta estrategia requiere de una visión holística y de coordinación con los distintos organizmos gubernamentales bajo el liderazgo del MICITT, para esto su proceso de construcción se basa en:

> *El proceso de construcción fue liderado por el MICITT, que a partir del mes de marzo de 2015 llevó a cabo tres mesas de discusión, orientadas por personal especializado*

de la OEA, cuatro talleres sectoriales y dos consultas en línea. (Estrategia Nacional de Ciberseguridad de Costa Rica, 2017, p.13).

De estas mesas de discusión, se logra extraer las recomendaciones sobre los pareceres de todos los especialistas, consituyendo un borrador que se presenta en la última mesa de discusión para su posterior revisión y aclaración de dudas (Estrategia Nacional de Ciberseguridad de Costa Rica, 2017).

Antes de su publicación el 5 de junio del 2017 en el Diario Oficial La Gaceta N 105 (2017), hay una etapa donde se da espacio a observaciones de fondo y forma, una vez que se completa se hace su publicación.

El documento está constituido de manera tal que hace una descripción del contexto actual, incluyendo el impacto de las TIC en el desarrollo económico del país, con menciones Plan de Desarrollo 2014-2018 "Alberto Cañas Escalante" y Plan Nacional de Desarrollo de las Telecomunicaciones 2015-2021 "Costa Rica sociedad conectada".

Aborda el sector de Telecomunicaciones haciendo mención de los avances en el marco regulatorio y cómo se vincula con la seguridad cibernética, prácticas de seguridad cibernética de los operadores en Costa Rica y la conformación del Centro de Respuesta a Incidentes de Seguridad Informática mediante decreto 37052-MICITT (2012), y el fortalecimiento del marco jurídico en Costa Rica para la atención de los delitos informáticos.

La estrategia está basada en cuatro principios (Estrategia Nacional de Ciberseguridad de Costa Rica, 2017):

- *Las personas son la prioridad*
- *Respeto a los Derechos Humanos y la privacidad.*
- *Coordinación y corresponsabilidad de múltiples partes interesadas.*
- *Cooperación internacional* (p.35)

Las personas son el punto central por donde gira toda la estrategia, debido a su relación con prácticamente toda actividad económica, política y social; por lo tanto, se debe promover el mejoramiento en las condiciones de vida y hacer los cambios requeridos en forma responsable (Estrategia Nacional de Ciberseguridad de Costa Rica, 2017).

Sobre la coordinación y corresponsabilidad de múltiples partes interesadas, se menciona la responsabilidad por igual que tienen las personas que participan en el ecosistema digital y su incursión en la Ciberseguridad (Estrategia Nacional de Ciberseguridad de Costa Rica, 2017).

Un aspecto muy importante de la estrategia es la colaboración internacional debido a que los ciberdelincuentes no conocen de fronteras, tratados limitrofes, etc.. esto ya que un problema en un país no necesariamente concierne solo a este, además de que los ataques no siempre se originan en el país que se desea atacar. Es imperativo unir esfuerzos, que se intercambien conocimiento y buenas prácticas en la lucha contra los ciberataques (Estrategia Nacional de Ciberseguridad de Costa Rica, 2017).

Otro aspecto importante de la estrategia, es el detalle del marco estratégico para la seguridad cibernética, este establece la coordinación y participación de otras organizaciones primordialmente del sector público pero incluye también al privado.

De esta manera el Comité Consultivo está compuesto por (Estrategia Nacional de Ciberseguridad de Costa Rica, 2017):

- *Dos representantes del MICITT*
- *Un representante del Poder Judicial.*
- *Un representante de la SUTEL.*
- *Dos representantes de la sociedad civil.*
- *Dos representantes de la academia.*
- *Dos representantes del sector privado.*(p. 37)

Por último este es la definición del objetivo general de la estrategia:

> *Desarrollar un marco de orientación para las acciones del país en materia de seguridad en el uso de las TIC, fomentando la coordinación y cooperación de las múltiples partes interesadas y promoviendo medidas de educación, prevención y mitigación frente a los riesgos en cuanto al uso de las TIC para lograr un entorno más seguro y confiable para todos los habitantes del país.* (Estrategia Nacional de Ciberseguridad de Costa Rica, 2017, p. 38)

Reforzando la idea de unión, coordinación, cooperación para hacer que el uso de las TIC sea más segura para poder hacer frente a las nuevas tendencias de ciberataques, además estable ocho objetivos específicos enfocados a lograr cumplir ese objetivo general. A continuación la lista de los objetivos (Estrategia Nacional de Ciberseguridad de Costa Rica, 2017):

- *Objetivo específico 1: Coordinación nacional.*
- *Objetivo específico 2: Conciencia pública.*
- *Objetivo específico 3: Desarrollo de la capacidad nacional de seguridad cibernética.*
- *Objetivo específico 4. Fortalecimiento del marco jurídico en Ciberseguridad y TIC.*
- *Objetivo específico 5: Protección de infraestructuras críticas.*
- *Objetivo específico 6: Gestión del riesgo.*
- *Objetivo específico 7: Cooperación y compromiso internacional.*
- *Objetivo específico 8: Implementación, seguimiento y evaluación.* (p. 38)

Con esta estrategia Costa Rica pretende dar un paso adelante en cuanto a la regulación de las TIC, procurar seguir mejores prácticas, ser ejemplo de desarrollo de tecnologías y desde luego garantizar la seguridad de la información de todas las personas, a sabiendas de que los cambios en tecnología vienen acompañados de desafíos cada vez más complejos.

Seguridad tecnológica en el Sistema Nacional de Planificación

Como parte de los esfuerzos que el país trabaja en temas de Ciberseguridad, la Unidad de Informática y la Unidad de Análisis Prospectivo y Política Pública del Ministerio de Planificación Nacional y Política Económica (MIDEPLAN) desarollan el documento Ciberseguridad en el Sistema de Planificación Nacional (Ciberseguridad en el Sistema Nacional de Planificación, 2020).

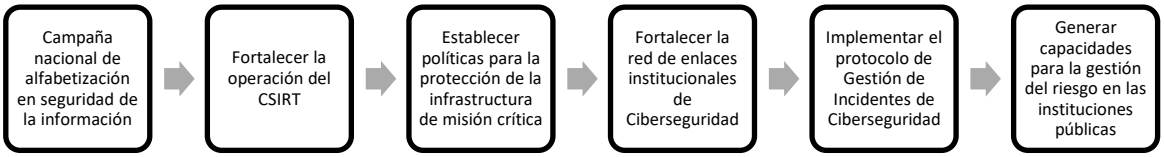
El principal objetivo es pretender sirvir de acompañamiento al Ministerio de Ciencia, Tecnología y Telecomunicaciones en su visión de mejorar el posicionamiento táctico frente a incidentes de Ciberseguridad en conjunto con el Centro de Respuesta de Incidentes de Seguridad Informática.

Con esta alianza se procura que el Gobierno de Costa Rica tenga una posición más más robusta y que les pueda hacer frente a los nuevos retos y desafíos en temas de ciberdelitos y

que le permita al MIDEPLAN tener una idea más precisa sobre el camino por seguir en varias áreas comon la inversión pública, esto una vez que se logre tener el contexto en el que el país se encuentra (Ciberseguridad en el Sistema Nacional de Planificación, 2020).

Entre otros componentes importantes presentes en el documento, es la inclusión de la estrategia de transformación digital, la cual tiene seis ejes sobre los cuales se desarrolla la Estrategia Nacional de Ciberseguridad. A continuación la estrategia:

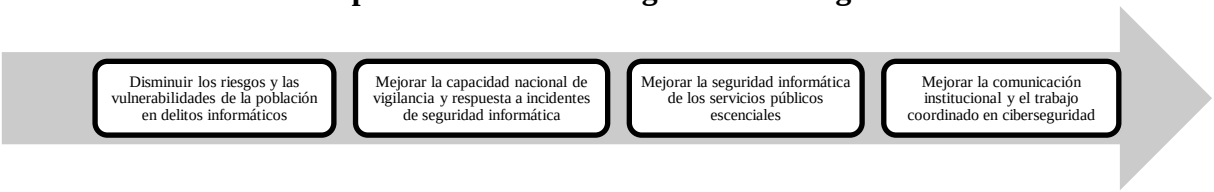
Figura 1
Implementación Estrategia Nacional de Ciberseguridad



Fuente: Ciberseguridad en el Sistema Nacional de Planificación, MIDEPLAN, p.11.

Además define la ruta que se debe:

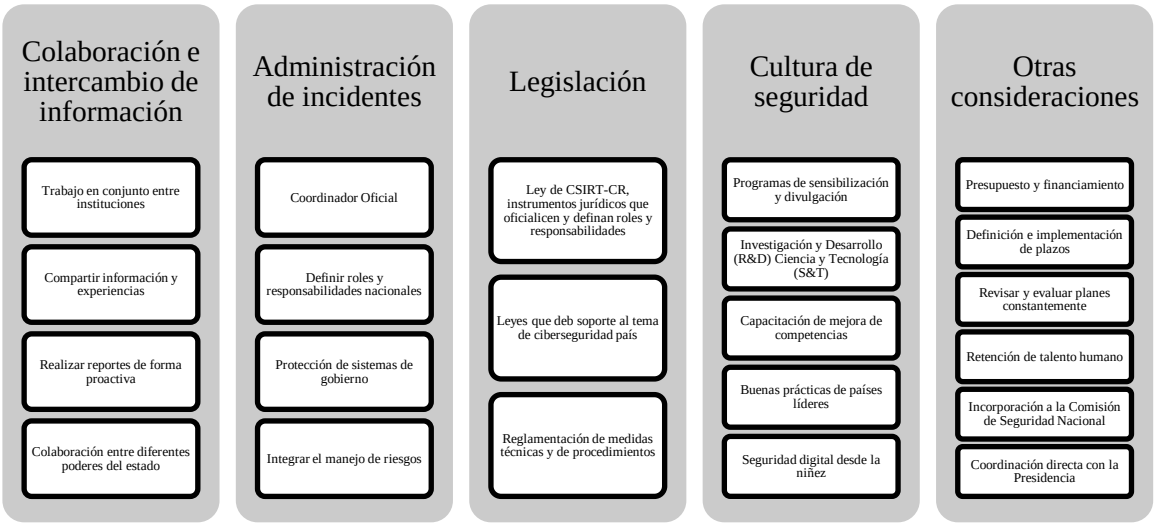
Figura 2
Ruta Implementación Estrategia de Ciberseguridad



Fuente: Ciberseguridad en el Sistema Nacional de Planificación, MIDEPLAN, p.11.

Desde luego esta estrategia viene acompaña de una serie de desafíos, para los cuales es indispensable contar con planes de acción que sean capaces de sacar adelante la hoja de ruta que pretenden establecer.

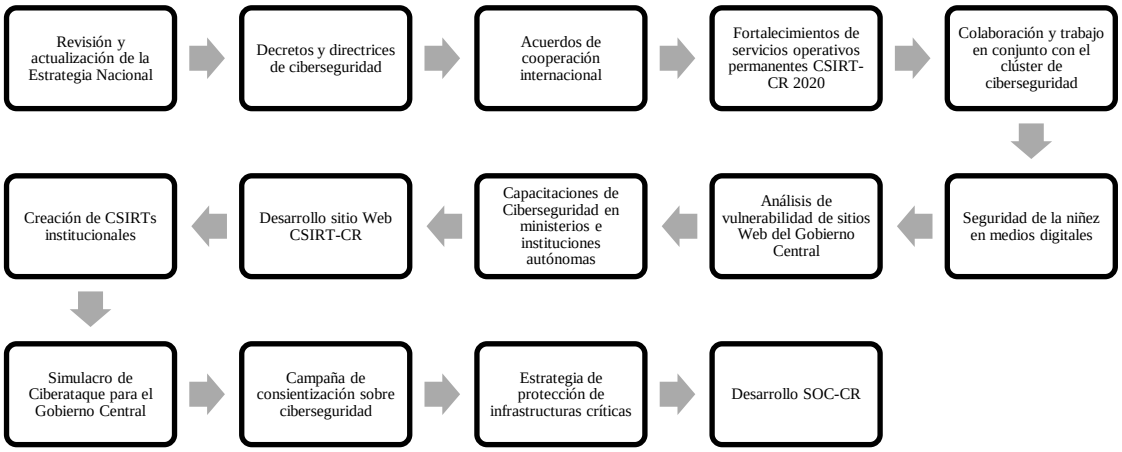
Figura 3
Retos para la Implementación Estrategia de Ciberseguridad



Fuente: Ciberseguridad en el Sistema Nacional de Planificación, MIDEPLAN, p.13.

A continuación, se describe la hoja de ruta del MIDEPLAN, para poder llevar a cabo esta implementación:

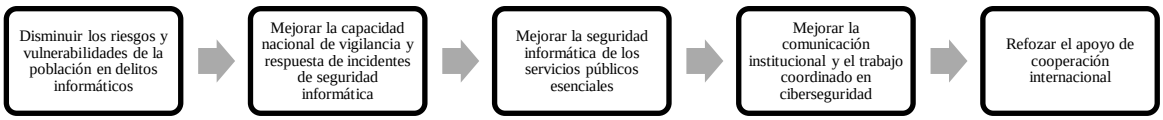
Figura 4
Hoja de Ruta para la Implementación de la Estrategia de Ciberseguridad



Fuente: Ciberseguridad en el Sistema Nacional de Planificación, MIDEPLAN, p.14.

Está hoja de ruta tiene una serie de objetivos por cumplir y de esa manera garantizar que está cumpliendo con la estrategia planteada:

Figura 5
Hoja de Ruta para la Implementación de la Estrategia de Ciberseguridad



Fuente: Ciberseguridad en el Sistema Nacional de Planificación, MIDEPLAN, p.14.

Es importante que todos estos planes incorporen aspectos de Ciberseguridad de manera tal las instituciones del Estado mejoren y colaboren con la estrategia de tener un país mejor preparado y con la ayuda internacional se pueda fortalecer las mejores prácticas en respuesta de incidentes, y mejorar el marco jurídico para que vaya de la mano con las nuevas exigencias y cambios en las formas en que se tipifican los delitos informáticos.

Reglamentación sobre Gestión de Riesgos y Tecnologías de la Información en Entidades Financieras Costarricenses

El Consejo Nacional de Supervisión del Sistema Financiero (CONASSIF), es el órgano colegiado superior, cuyo labor directiva da sobre las principales superintendencias de Costa Rica a saber, Superintendencia General de Entidades Financieras (SUGEF), la Superintendencia General de Valores (SUGEVAL), la Superintendencia General de Seguros (SUGESE) y la Superintendencia de Pensiones (SUPEN).

En la actualidad existe gran cantidad de normas, reglamentos y acuerdos establecidos para la gestión de riesgo en cada una de estas superintendencias; sin emabargo, para efectos de esta investigación existen dos que están enfocadas al objeto de estudio.

El primer acuerdo es el SUGEF 2-10 (2022), Reglamento sobre la Administración Integral de Riesgos. Aquí se establecen los aspectos que deben contenplarse como mínimo para llevar a cabo la implementación así como el mantenimiento de un proceso de administración integral de riesgos.

Mediante el artículo 9 del acta 862-2010 (SUGEF, 2010), el Consejo Nacional de Supervisión del Sistema Financiero aprueba el acuerdo SUGEF 2-10 el cual rige desde el 15 de julio del 2010.

Este acuerdo tiene 8 distintos fundamentos para la justificativa creación y aprobación, dentro los cuales destacan el inciso c) del artículo 131 de la Ley Orgánica del Banco de Costa Rica (1995) para la aprobación de un reglamento para la administración integral de riesgos para todas aquellas entidades que estén bajo la supervisión de la SUGEF y por consiguiente del CONASSIF.

Además existen otras razones como las recomendaciones del Comité de Basilea bajo los Principios Básicos para una Supervisión Efectiva y el Pilar 2 sobre el Acuerdo de Capital (1997), donde se describen los principios sobre la mejora y el fortalecimiento de las prácticas de regulación y supervisión.

Otro aspecto importante es que también incluye los avances en los mercados financieros que desde luego también llevan a desarrollar un nivel de incertidumbre que hace más justificable aún el contar con esta norma.

En términos generales la norma en su cápitulo I establece las disposiciones generales, definiendo el ámbito de aplicación, el proceso de administración integral de riesgos, los lineamientos generales. Como parte del capítulo II, la norma define la reglamentación sobre el Gobierno Corporativo, las políticas para la Administración Integral de Riesgos, las responsabilidades de la junta directiva, de la Administración Superior y define los lineamientos por seguir para contar con un Manual de Administración Integral de Riesgos.

Los cápitulos III y IV son para la reglamentación de la conformación de los comités de Riesgos y de la Unidad de Riesgos así como las funciones para cada uno de ellos. El capítulo V define el Órgano de Control Interno y desde luego los lineamientos de sus funciones.

El capítulo VI establece los lineamientos claros para la Auditoría del Proceso de Administración Integral de Riesgos y sus requisitos que debe cumplir el experto independiente. El último capítulo es sobre el Informe Anual de Riesgos, donde se indica que con corte al 31 de diciembre de cada año las entidades deben preparar y divulgar en su respectivo sitio *web* y en caso de no contar con uno lo debe hacer en algún otro medio, un informe anual y establece los requerimientos mínimos que tiene que cumplir ese informe.

El otro reglamento que es de suma importancia mencionar es el Reglamento General de Gestión de la Tecnología de Información (SUGEF 14-17,2020). Mediante este acuerdo del Consejo Nacional de Supervisión del Sistema Financiero en los artículos 9 y 11 de las actas 1318-2017 y 1319-2017 se da por aprobado este reglamento el día 17 de abril del 2017 y que entra a regir 10 días hábiles después de su publicación en el diario oficial La Gaceta.

Ese reglamento cuenta con 17 considerandos que se toman en cuenta para hacer la resolución de la necesidad de contar con una disposición para la gestión de las tecnologías de información en las entidades financieras bajo la supervisión de la SUGEF y el CONASSIF.

Entre algunas se destacan acuerdos de la SUGEF como la 14-09 (2009), la Ley Reguladora del Mercado de Valores (1997), Régimen Privado de Pensiones Complementarias (1995), además detalla que la gestión de TI es de suma importancia para lograr tener una adecuada governanza y tomar decisiones dentro de las organizaciones, entre otras.

Dentro de las capítulos que desarrolla la norma están, el I, que establece las disposiciones generales, por ejemplo, el alcance y los lineamientos generales. En el II se define la organización de las tecnologías de información, a saber, la Unidad de TI, el Gobierno de TI y la Gestión de TI.

En el capítulo III, define la supervisión y auditoría externa de TI, detallando el perfil tecnológico y tipo de gestión de TI. Sobre la auditoría externa de TI, da las guías sobre el alcance y plazos de la auditoría, y aclara cuáles son los entregables y la manera de presentar los resultados. Dentro de mismo capítulo, está la sección III para establecer el reporte de supervisión y plan de acción. En la sección IV las prorrogas y calificación de riesgos de TI y la última sección es sobre bases de datos.

De esta maner,a la Superintendencia General de Entidades Financieras, procura establecer el marco de referencia para dar guía a las entidades financieras bajo su supervisión sobre una adecuada gestión de riesgos y de gobernanza sobre las tecnologías de información.

Marco teórico

Principios de Administración

Administración y su gestión

Los principios fundamentales de la administración se remontan a la necesidad que siempre ha tenido el ser humano de trabajar, ya que les permite poder coordinar tareas, y también determinar los esfuerzos que requieren para lograr conseguir sus objetivos, (Münch, 2018).

Puede no existir una única definición sobre administración, sin embargo, Benavides (2014, p.3), proporciona tres:

- Proceso para alcanzar metas organizacionales, trabajando con y por medio de personas y empleando otros recursos organizacionales.
- Sistema de funciones coordinadas, que contiene las decisiones adoptadas, para lograr con máxima eficiencia los objetivos de un organismo social.
- Proceso de tomar decisiones bajo condiciones de incertidumbre y riesgo con recursos escasos y limitados para alcanzar determinados objetivos y obtener resultados.

Dentro de todas estas características, es importante notar que existen conceptos claves que ayudan a desglosar la administración, consecución de objetivos, coordinación y toma de decisiones que son las que cuentan con más peso dentro de esta definción.

Aquí se comienzan a detallar los elementos básicos de la administración, para Münch (2018), se cuentan con seis. El primero tiene que ver con los objetivos y lo que busca es enfocar todos los esfuerzos para que se logren conseguir los resultados. El segundo es la eficiencia que procura alcanzar los objetivos planteados a tiempo sin descuidar la calidad. La competitividad es la tercera y tiene un componente importante y es el valor agregado que generen estas organizaciones y que se refleje en los costos, características, calidad y precio.

Como cuarto elemento, la calidad debe estar alineada con lo que esperan los clientes, de lo contrario se pierde competitividad, además de que se debe contar con una adecuada coordinación de recursos y que estos se optimizen. Como último elemento se tiene la

productividad, que procura lograr los mejores y máximos resultados, pero utilizando los mínimos recursos.

La administración dentro de los entornos organizacionales, se debe enfocar en la coordinación de los recursos principalmente internos y que estos tengan un propósito, de aquí que una buena administración interna es clave para alcanzar con éxito los objetivos estratégicos así como una dependencia de uan adecuada gestión a nivel ejecutivo (Hernández y Palafox, 2012).

Misión y visión

Toda organización debe definir de manera precisa y exacta su misión y visión, de manera tal que le brinda la guía sobre el norte que debe seguir para lograr la consecución de los objetivos estratégicos, la idea es poder en alguna medida asegurarse el éxito que busca o al menos ser más competitivos. La gran mayoría de las empresas publican sus respectivas misiones y visiones en sus estados de resultados y más comunmente en los sitios *web* u otros medios publicitarios.

Misión

Procura establecer el propósito de la organización, da un sentido y dirección, establecer cual es el giro de negocio, para David (2017), la declaración de misión *"es la expresión perdurable del propósito que distingue a una organización de otras similares; es la declaración de la "razón de ser" de una organización y es la respuesta a la pregunta fundamental "¿Cuál es nuestro negocio?"*. (p.42).

Se debe procurar que sea muy breve y concisa, procurando ser guía para establecer prioridades e incluso para hacer evaluaciones de desempeño (Benavides, 2014).

Visión

La visión trata de definir hacia dónde se dirige una organización, de acuerdo con Münch (2018), la visión *"es el enunciado del estado deseado en el futuro para la organización, provee dirección y estimula acciones concretas."* (p.108). Se debe tomar en cuenta los distintos puntos de vista así como las conclusiones que la administración tenga con respecto

a la dirección a largo plazo (Thompson, Strickland III, Janes, Sutton, Peteraf y Gamble, 2018).

Por último, una correcta definición de la visión es de suma importancia si se tiene en cuenta que ahí se puede encontrar el ADN de los planes estratégicos, dicta la guía en la consecución de estos (Hernández y Palafox, 2012).

Administración estratégica

La administración estretegica se basa en cómo conseguir y mantener una ventaja competitiva, para esto David (2017) la define como *"arte y la ciencia de formular, implementar y evaluar decisiones multidisciplinarias que permiten a una empresa alcanzar sus objetivos",* (p.5). Se aplica en los altos niveles de la directiva que pretende alcanzar una productivad tal que sea eficiente, eficaz de calidad y que permita a la organización ser competitiva Münch, (2018).

Un aspecto importante dentro de la administración estrategica es la planeación, y para Benavides (2014) es :

> *Es el conjunto de acciones que hace una institución en el presente con objeto de lograr resultados a futuro que le permitirán tomar decisiones con la mayor certidumbre posible, además de una organización eficaz y eficiente que coordine esfuerzos para ejecutar las decisiones, dándoles el seguimiento correspondiente.* (p.62).

La planeación estratégica no procura predecir lo que va pasar, si no más bien les permite a las organizaciones poder estar mejor preparadas ante distintas circunstancias como enfrentar problemas futuros, corregir erorres, y tomar decisiones más adecuadas (Luna, 2014).

Para terminar, se define las etapas que consitutiyen la administración estratégica, David (2017) establece tres etapas:

- **La formulación de estrategias:** aquí se desarrolla una gran etapa estratégica, y conlleva establecer misión, visión, realizar análisis FODA (Fortalezas, Oportunidades, Debilidades y Amenazas), y los objetivos a largo plazo.

- **La implementación de la estrategia:** para que sea exitosa se debe establecer objetivos en todos los niveles jerárquicos, crear la cultura necesaria para que acompañe la estrategia, pues de otra manera la resistencia al cambio podría ser un factor en contra de una implementación exitosa.
- **La evaluación de la estrategia:** la tarea no concluye con la implementación, se debe dar seguimiento en todos los niveles, asegurarse de que las personas están adaptando la estrategia y que se sienten identificados. Se deben evaluar constantemente puntos de mejora y establecer planes de acción que ayuden a corregirlos.

Principios de la administración financiera

Finanzas administrativas

Sin duda alguna el objetivo de toda empresa es generar riqueza, o sea buscar cómo hacer que estas tengan más valor en el mercado, para Gitman y Zutter (2016) las finanzas se pueden definir como: *"el arte y la ciencia de administrar el dinero"* (p. 4), si se analiza esta definición con cuidado lleva a un punto importante, la administración del dinero, ya que todas las personas y organizaciones de una u otra manera procuran ganar dinero y este a su vez sea gastado en bienes, servicios o incluso en inversiones.

Es lógico pensar que cuando se habla de administrar algo viene consigo la toma de decisiones, en el caso de las finanzas puede ser, ahorrar, invertir o simplemente no hacer nada con el dinero, al final son decisiones que se toman después de hacer un análisis responsable sobre qué es lo mejor o más conveniente por hacer, todo de acuerdo con el ambiente en que se estén desarrollando las cosas.

No es lo mismo hacer una inversión importante de dinero es momentos de crisis financiera que en tiempos de bonanza; sin embargo, puede ser que esa inversión en momentos de crisis sea la decisión responsable que salve la compañía, pues al final se sustentan del análisis sobre qué es lo mejor y más adecuado por hacer.

En las finanzas existen tres funciones básicas que ayudan a detallar y comprender mejor la actividad financiera de las empresas (Baena, 2014):

- **Preparación y análisis de la información financiera: la preparación** tiene dos pasos :

  (…) procesos al cual le corresponde la recopilación de los estados financieros básicos y la información cualitativa relevante a nivel interno y externo de la empresa", y el análisis *"se deriva de la interpretación de los datos obtenidos en razones o indicadores financieros.* (p.3).

Este primer paso le permite a la empresa poder tomar decisiones con conocimiento de causa y de igual forma poder hacer proyecciones.

- **Determinación de la estructura de inversión (activos):** está compuesta: *"(…) por todos aquellos bienes y derechos adquiridos para la realización de su actividad operacional"*, (p.3).

Esta permite delinear la estructura compuesta de los activos corrientes y los no corrientes.

- **Estructura financiera:** es la última de las funciones básicas, y lo que pretende es *"Al definir las proporciones de inversión en los activos fijos, la empresa podrá recurrir a sus necesidad de financiación (…)"*, (p.4).

La función financiera

Es claro que cualquier organización procura cómo ser más competitivo y lograr sobrevivir en sectores donde la competencia puede ser alta, por lo que deben enfocar esfuerzos en la mejora contínua, desde luego tratar de crecer dentro de sus mercados o mediante la expansión en nuevos, y tener un control de riesgo tal que le permita seguir dentro de la competencia.

De aquí que se debe tener una correcta gestión financiera, bajo este contexto Pérez (2015) establece una serie de misiones que son indispensables denro de la función financiera:

- Apoyar el crecimiento rentable, este tiene que ir de la mano con los objetivos estratégicos planteados por la empresa.

- Hacer evaluaciones sobre las inversiones, tomando en cuenta la rentabilidad que van a obtener y los riesgos que esta conlleva, ambas deben estar alineadas a qué tanto está dispuesta la empresa a arriesgar.
- La manera en que las actividades y el crecimiento organizacional se financian planeando cuidadosamente la captación de recursos requeridos.
- Tener un adecuado manejo de los riesgos, de tal manera que se protejan los intereses de la organización.
- Generar liquidez y solvencia, importante para que la organización pueda hacer frente a las obligaciones financieras.
- Tener una adecuada gestión de todos los procesos administrativos.
- Transparencia en la preparación y presentación de los resultados económicos y financieros para que ayuden a la planificación y toma de decisiones bien informadas.

Al final de lo que se trata es asegurar que la organización tenga un manejo responsable sobre el capital, que se le dé un uso eficaz y eficiente, procurando siempre la optimización de los recursos al máximo, pero que a la vez se puedan hacer las inversiones necesarias para mejorar la competitividad con su correspondiente planeación y análisis de riesgos.

Análisis financiero

Mediante los análisis financieros es posible comunicar la situación financiera de las empresas por lo que es de suma importancia tener un entendimiento tal que permita a los tomadores de decisiones tener clara la posición de la organización y así tomar mejores decisiones (Ross, Westerfield, Jaffe y Jordan, 2018).

Para Baena (2014), el análisis financiero *"es un proceso de recopilación, interpretación y comparación de datos cualitativos y cuantitativos, y de hechos históricos y actuales de una empresa."* (p.11), y esto permite ver todos los resultados de la empresa, para luego realizar un diagnóstico integral sobre cuál es el desempeño financiero y que se puedan encontrar las causas por no lograr los rendimientos esperados y establecer las acciones que se requieran para corregir el rumbo, (Lavalle, 2016).

De aquí ya se empieza a esclarecer dos preguntas que Beana (2010) plantea sobre los análisis financieros, y la primera es ¿Para qué sirve el análisis financiero?, tal y como se menciona anteriormente su utilidad es mostrar la situación de la empresa en un tiempo determinado y a la vez permita hacer proyecciones sobre el crecimiento e inversiones, así como llevar los resultados que espera la compañía hacia la consecución de los objetivos financieros trazados.

La segunda interrogante tiene que ver con ¿Para quién sirve el análisis financiero? Con la información ya lista, se debe determinar quién debe ver esta información. Directores y administradores sin duda deben tener esta información, porque es su herramienta de análisis. Los inversionistas ya que el capital que aportan podría estar en riesgo. Entidades financieras y el Estado, para que logren tener la información pertinente sobre niveles de endeudamiento, entre otros.

Principales estados financieros

Existen cuatro estados financieros claves (Gitman y Zutter, 2016):

- Estado de pérdidas y ganancias, también se conoce como estado de resultados y su objetivo es mostrar el estado financiero durante un periodo determinado, normalmente un año (Ross *et ál*, 2018).
- El siguiente es el estado del patrimonio de los accionistas, para Gitman y Zutter (2016), *"Muestra todas las transacciones de las cuentas patrimoniales que ocurren durante un año específico"*, (p.66).
- Balance general o también se conoce como estado de situación financiera, tiene como objetivo mostrar el estado financiero en una fecha determinada. Mostrando la relación contable que los activos es igual a los pasivos más el capital año (Ross *et ál*, 2018).
- Por último, se tiene el estado de flujos de efectivo, donde se logra tener un resumen de los flujos de efectivo que ocurren en un lapso determinado. Ofrece los efectivos operativos, de inversión y financieros (Gitman y Zutter, 2016).

Principios de Ciberseguridad

Conceptualización de la Ciberseguridad

La Ciberseguridad desde un punto de vista empresarial, es asociado con aspectos sobre descubrimiento de amenazas en la red, vulnerabilidades en los sistemas de información de las empresas, los ciberdelincuentes procuran vulnerar los sistemas y cómo las organizaciones se pueden proteger y no ver afectadas sus operaciones.

De igual manera para las personas los fundamentos son muy similares y las diferencias radican principalmente en lo atractivo que es uno frente al otro, sin olvidar que las personas son un vector que es utilizado por los ciberdelincuentes para vulnerar los sistemas empresariales.

Los conceptos de amenaza y vulnerabilidad son usados como sinónimos o hacen referencia a uno cuando en realidad se están refiriendo al otro, para conceptualizarlos correctamente, la amenaza es cualquier situación potencial ya sea con mala intención o no y que esta vaya a tener una repercusión no deseada en la organización (PROSIC, 2010). La vulnerabilidad por su lado está necesariamente relacionada con una amenaza, donde el sistema debe tener una falla o carencia (intencional o no) que facilita que la amenaza ocurra (PROSIC, 2010). Para cerrar este ciclo se tiene el ataque, el cual incluye a un atacante (ciberdelincuente) que explota una vulnerabilidad para ejecutar una amenaza (PROSIC, 2010).

Para ejemplificar cómo estos tres conceptos interactúan: un banco tiene la amenaza de que le roben la información de las cuentas de sus clientes, su sistema tiene un problema que permite hacer consultas sin tener un usuario válido registrado (vulnerabilidad). Un ciberdelincuente sabe de esta vulnerabilidad, accede al sistema y roba toda la información concerniente a los usuarios del banco.

Existen varios tipos de amenazas cada una de ellas tiene un impacto mayor, dependiendo de la empresa que se ve vulnerada, por ejemplo. un tipo de amenaza es la revelación de información, otro es la afectación de los servicios o también llamado denegación de servicio y la corrupción de la integridad de los recursos.

Estos tres están alineados a los pilares de la seguridad de la información, confidencialidad, integridad y disponibilidad.

La confidencialidad de la información está estrictamente relacionada con el principio de que los datos deben ser vistos únicamente por las personas que tienen la autorización para hacerlo.

La integridad se refiere a que los datos no pueden ser modificados por nadie que no sea la persona dueña de ellos o por algún tercero que previamente tiene el consentimiento del titular para hacerlo.

Por último, la disponibilidad, que este principio está relacionado con que la información debe estar disponible siempre y en todo momento.

Tipos de ataques más comunes y su modo de protección

Actualmente existe una gran cantidad de ciberataques, los cuales varían en su complejidad, la que está ligada a los objetivos que pretenden alcanzar los ciberdelincuentes. Hay algunos que son muy rápidos y simplemente requieren del envío de un correo electrónico con el programa que contiene la forma del ataque, por ejemplo, un virus.

También hay otros más complejos que para penetrar las redes de datos de una empresa, se pueden llevar días y hasta meses antes de lograr su cometido, pues una vez adentro se tiene otra gama de posibles ataques, (Ramiro, 2018).

Fuerza bruta

Tiene como finalidad adivinar las contraseñas, llaves de inscripción y otros, a base de prueba y error (Kaspersky, 2021) con el fin de que se logre ingresar a los sistemas, para esto utilizan un *software* que contiene un algoritmo que va probando cientos de miles de combinaciones hasta lograr adivinar la contraseña correcta.

Sin embargo, también existe la posibilidad de que logren adivinar la contraseña basados en un estudio de la persona, sus gustos, preferencias, fecha de nacimiento, nombre de familiares en fin algo que sea muy representativo de ella, ya que existe una alta probabilidad de que sus contraseñas estén basadas en ellos.

Ataque por diccionario

Es similar al anterior en cuanto a la utilización de un *software*, en este caso tiene una base de datos con una gran lista de posibles combinaciones de palabras hasta que logra averiguar la contraseña correcta.

Existen varios controles y recomendaciones que se pueden implementar para evitar ser víctima de este tipo de ataques, y el mejor, es el uso de contraseñas seguras basadas en frases que combinen caracteres especiales, números, minúsculas y mayúsculas. Además, es oportuno el uso de autenticación múltiple donde sea posible (OSI, 2020), y esto consiste en después de haber ingresado el usuario y contraseña, el sistema solicita un código adicional el cual puede ser enviado por mensaje SMS, al correo electrónico o incluso mediante el uso de Tokens físicos o lógicos instalados en una computadora o dispositivo móvil.

Ataque de ingeniería social

Se le conoce como el arte del engaño y está dirigido a los usuarios con el fin de que revelen información personal o incluso den acceso a físicos y lógicos a los ciber delincuentes y así poder tener acceso a sitios restringidos. Las intenciones pueden ser muchas, desde el robo de información, espionaje, sabotaje, hasta insertar *software* malicioso para perpetrar futuros ataques (OSI, 2020).

De acuerdo con la Oficina de Seguridad del Internauta (2020), de aquí se pueden dividen tres tipos:

- ***Phishing*: "***Suele emplearse el correo electrónico, redes sociales o aplicaciones de mensajería instantánea"*, (p. 8)
- ***Vishing:* "***Se lleva a cabo mediante llamadas de teléfono"*, (p. 8)
- ***Smishing:* "***El canal utilizado son los SMS"*, (p. 8)

Ataques a las conexiones

Son ataques dirigidos a las redes de telecomunicaciones, con el propósito de robar información como usuarios, contraseñas o incluso causar interrupciones en las comunicaciones, lo que provoca que los sistemas no se encuentren disponibles.

Redes trampa

Se basa en la creación de redes inalámbrica (*Wifi*) falsas, donde los ciberdelincuentes configuran redes gemelas con el fin de verlas como legítimas y que los usuarios se conecten a ella, para que, a partir de ahí, ellos puedan robar datos e información de los equipos (OSI, 2020).

La principal recomendación es aprender a identificar este tipo de redes, por ejemplo, no pueden existir dos redes con el mismo nombre, desconfiar si la red inalámbrica no tiene ningún tipo de autenticación o permite ingresar cualquier contraseña, pues lo mejor es configurar los equipos móviles para que no se conecten automáticamente a las redes que son descubiertas.

Ataque DDoS

Conocido como ataque de denegación de servicio (*Distributed Denied of Service DDoS*) por sus siglas en inglés. Se basa en el ataque a un servicio, por ejemplo, un sitio *web* bancario desde varios puntos o equipos donde todos al mismo tiempo envían solicitudes de conexión con el fin de causar una inhabilitación del servicio por tantas solicitudes que el servidor no es capaz de manejar, (Ramiro, 2018). Para esto regularmente se utilizan *bots o botnets* que son equipos o redes "zombis" que previamente son secuestradas por los ciberdelincuentes empleando otro tipo de ataque, una vez que son controladas.

Man in the middle

Consiste en que el ciberdelincuente coloca un servidor en medio del usuario y el sitio donde se desea realizar la conexión, con el objetivo de poder interceptarla y tener acceso a los datos e información que se está intercambiando, (OSI, 2020).

Este tipo de ataques se aprovecha cuando los usuarios utilizan redes públicas que no cuentan con ningún tipo de seguridad, por lo que se debe evitar el uso de estas. Mantener el equipo actualizado y procurar utilizar VPNs autorizados por ejemplo el de la empresa para la cual trabajan y no acceder a sitios http, ya que la transferencia de información se realiza sin ningún tipo de cifrado o lo que también se conoce como texto plano.

Ataques por *Malwares*

También llamados *software* malicioso, este tipo de ataques están basados en la utilización de *software* malicioso o "*malware"*, tienen la finalidad de causar daño a los equipos infectados, como robo de información o afectación del desempeño, (Ramiro, 2018).

Dentro del "*malware"* se tienen varias categorías, y entre las principales están:

- Virus.
- *Adware.*
- *Spyware.*
- Troyanos.
- *Backdoors.*
- *Keyloggers.*
- *Ransomware*.
- Gusanos.
- *Botnets.*

El "*ransomware*" es uno de los más letales ataques y su finalidad es tomar secuestrar el equipo informático mediante la encriptación de los archivos del sistema y donde los ciberdelincuentes solicitan un pago por la llave para desencriptarlos (IBM 2021).

Como medidas de protección se tienen:

- Utilizar antivirus.
- Mantener los equipos actualizados.
- Utilizar contraseñas seguras.
- Desconfiar de cualquier archivo adjunto en correos o mensajes.
- Hacer descargas solo de sitios oficiales o con reconocida reputación.
- Evitar conectarse a redes públicas o desconocidas.
- No compartir información personal.
- Hacer copias de seguridad.

Proceso de administración de riesgos

El concepto de riesgo está directamente ligado a la incertidumbre que, precisamente, es la que lleva a no saber los eventos que impactaran a la empresa, y los resultados que traen consigo efectos negativos para las organizaciones y sus objetivos estratégicos (ACCID, 2019).

Control interno

El marco de referencia denominado Control Interno – Marco Integrado (COSO, 2017), desarrollado por *The Committee of Sponsoring Organizations of the Treadway Commission (COSO)* por sus siglas en inglés, establece una serie de técnicas para que las organizaciones logren implementar y evaluar el control interno.

La definición dada por COSO en su resumen ejecutivo (2017) define Control Interno:

> *Los controles internos son un proceso, llevado a cabo por la junta directiva, la gerencia y otro personal de una entidad, diseñado para proporcionar una seguridad razonable con respecto al logro de los objetivos relacionados con las operaciones, la presentación de informes y el cumplimiento.*

Ciertamente el control interno contribuye a las organizaciones a lograr sus objetivos estratégicos, que está constituido de una serie de tareas y actividades y que tiene una relación con el recurso humano que no está limitado a las políticas y procedimientos que se tengan en la organización.

El objetivo de este marco de referencia está basado en tres categorías (COSO, 2017):

- **Objetivos operativos:** que se relacionan con la efectividad y eficiencia de las operaciones, tanto las metas financieras como las operativas, asegurándose que los activos de la organización estén a salvo de pérdidas o robo.
- **Reporte de objetivos:** implica los reportes internos y externos tanto de información financiera como la que no lo es, incluyendo la fiabilidad, transparencia o cualquier término incluido por entes reguladores.

- **Objetivos de cumplimiento:** aquí se refieren a todo lo concerniente a leyes, y regulaciones a las que la organización está sujeta.

Componentes del control interno

Está integrado por cinco componentes:

- **Control del ambiente:** provee un conjunto de estándares y estructuras que dan las bases para echar a andar controles internos dentro de la organización.
- **Evaluación del riesgo:** las evaluaciones de riesgo envuelven procesos dinámicos e interactivos para la identificación y evaluación de los riesgos.
- **Actividades de control:** aquí es donde se establecen las acciones que están basadas en las políticas y procedimientos, los cuales le van a ayudar a la organización a lograr mitigar los riesgos en procura de alcanzar sus objetivos.
- **Información y comunicación:** la información es de suma importancia para poder llevar a cabo las distintas etapas del control interno, en tanto la comunicación es el proceso mediante el cual se logra obtener, compartir y dar la información necesaria.
- **Monitoreo de actividades:** todo proceso para poder mejorarlo se debe controlar y medir ya sea con evaluaciones periódicas, por separado, pero lo importante es que cada uno de los cinco componentes sea monitoreado y evaluado.

A partir de estos cinco componentes, se desprenden diez y siete principios asociados a cada uno de los componentes.

Existen otros modelos de control interno, aquí un cuadro comparativo con los más importantes (Estupiñan, 2015):

Tabla 1
Modelos de control

Atributo	COBIT	SAC	COSO	COCO
Audiencia primaria	Dirección, usuarios Auditores internos	Auditores internos	Dirección	Dirección
Control visto como	Conjunto de procesos incluyendo prácticas procedimientos, políticas y estructuras organizacionales.	Conjunto de procesos Subsistemas y gente	Conjunto de procesos	Conjunto de procesos

Atributo	COBIT	SAC	COSO	COCO
Objetivos organizacionales de control interno	Operaciones efectivas y eficientes confiabilidad e integridad disponibilidad de información. Informes financieros confiables. Cumplimiento de las leyes y regulaciones,	Operaciones efectivas y eficientes. Informes financieros confiables. Cumplimiento de leyes y regulaciones.	Operaciones efectivas y eficientes. Informes financieros confiables. Cumplimiento de leyes y regulaciones.	Operaciones efectivas y eficientes. Informes financieros confiables. Cumplimiento de leyes y regulaciones.
Componentes o dominios	Dominios: Planteamiento, organización. Adquisición e implantación. Entrega, soporte y monitoreo.	Componentes: Ambiente de control manual y automatización. Procedimiento de control de sistemas.	Componentes: Ambiente de control manual. Gestión de riesgos. Actividades de control. Información. Monitoreo.	Criterios: Propósito. Compromiso. Capacidad. Vigilancia. Aprendizaje.
Foco	Tecnología informática.	Tecnología informática.	Toda la organización	Toda la organización
Efectividad del control	Por un período.	Por un período.	Un momento dado.	Un momento dado.
Responsabilidad por los sistemas de control interno	Dirección.	Dirección.	Dirección.	Dirección.

Clasificación de los riesgos

Recordando que el riesgo es cuando tenemos una probabilidad de que algo suceda, normalmente tiene consecuencias negativas, pero también existen las positivas. La oportunidad está para las organizaciones de poder encontrarlos oportunamente de manera tal que se logren establecer los controles adecuados para minimizar su impacto.

Bajo la premisa de que los riesgos se derivan de las amenazas externas y de las debilidades internas, donde se pueden encontrar algunas que se puede lograr cuantificar, así como otras no.

De aquí surge la importancia de hacer una clasificación de los riesgos, para Estupiñán (2015), existen:

- **Riesgos estratégicos:** algunos de los principales que se encuentran en esta categoría son, el político y de país, macroeconómicos, guerrillas, inflación, riesgos de crédito, como altas tasas de interés, regulaciones, riesgo de operación y de liquidez, de intervención estatal, entre otros.

- **Riesgos financieros:** que se clasifican en riesgos de interés, como la volatilidad de las tasas, y el cambiario.
- **Riesgos generales o de apoyo:** riesgo de la organización, como estructura organizacional, ausencia de planificación, mal clima laboral, riesgos de auditoría y los tecnológicos, de operaciones ilícitas y seguridad física y humanas.

Proceso de evaluación de riesgos

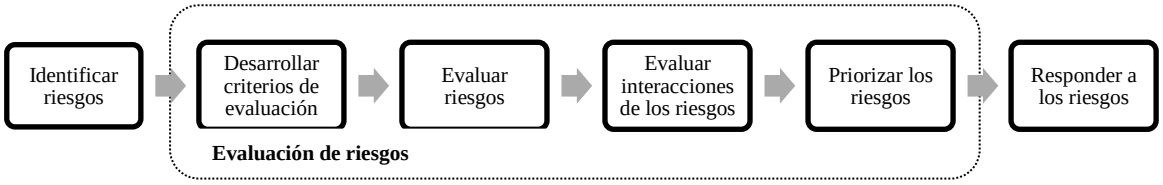
Una adecuada gestión de riesgos, sin duda alguna, implica que todos los riesgos a las que una organización se ve expuesta estén integrados, esto alineamiento con la Junta Directiva y la estrategia de la organización (ACCID, 2019).

Dentro del marco de referencia dado por COSO (2012), el propósito del proceso de evaluación de riesgos es lograr evaluar cómo son los riesgos más significativos, tanto individuales como grupales de la organización.

La idea es permitir a la administración enfocar los esfuerzos en aquellas amenazas que son más importantes, y poder establecer los controles adecuados que den respuesta oportuna.

A continuación, el proceso establecido por COSO (2012):

Figura 6
Modelo de evaluación de riesgos



- **Identificar riesgos:** se trata de producir la lista de riesgos e incluso de oportunidades. Debe estar organizada según la categoría de riesgo, y abarcar a cada uno de los departamentos de la organización.
- **Desarrollar criterios de evaluación:** para poder evaluar a los riesgos se deben establecer los criterios que se van a utilizar, para esto es recomendable que los riesgos y de incluirse las oportunidades sean evaluados conforme su impacto y probabilidad de ocurrencias.

- **Evaluar los riesgos:** una vez que se tenga la lista de riesgos y oportunidades más los criterios de evaluación, lo que se debe hacer es asignar precisamente la evaluación a cada riesgo tomando en cuenta los criterios que se establecieron, y se puede realizar en dos etapas, utilizando técnicas cualitativas para luego hacer un análisis más cuantitativo.
- **Evaluar las interacciones de los riesgos:** si bien los riesgos se pueden clasificar en distintas áreas, lo cierto es que no están ahí de forma aislada unos de los otros, todo lo contrario, los riesgos que podrían ser de menor importancia o de impacto, y podrían tener relación con otros que al materializarse uno siguen los demás causando daños mayores a los evaluados, de aquí lo importante de hacer ese mapeo de las interacciones entre los riesgos.
- **Priorizar los riesgos:** una vez completados los pasos anteriores, las organizaciones muy probablemente obtengan una lista extensa de riesgos los cuales muy probablemente no puedan atenderlos a todos. A partir de aquí es que es importante hacer una adecuada priorización de los riesgos, para esto se debe hacer una comparación de los niveles de cada riesgo con los objetivos predeterminados, así como los umbrales de tolerancia. Además, existen otros criterios subjetivos por ejemplo salud, para hacer esta priorización más allá de los impactos y probabilidades más medibles.
- **Responder a los riesgos:** en esta última etapa es donde se define la respuesta a cada riesgo, por lo tanto tomando en cuenta los resultados de la evaluación realizada a cada riesgo priorizado, se determina si se va aceptar, reducir, compartir o evitar, basado en un análisis costo-beneficio, normalmente las organizaciones acuden a estrategias como adquirir pólizas para dar respuesta a una posible materialización de un riesgo que el costo beneficio es muy alto, pero el impacto negativo es tal que se debe acudir a este tipo de soluciones.

Banca comercial

¿Qué es un banco?

Según la RAE (Real Academia Española) (2020) se tiene la siguiente definición: *"Empresa dedicada a realizar operaciones financieras con el dinero procedente de sus accionistas y de los depósitos de sus clientes",* (párr. 5), por lo que se sobreentiende que abarca aquellas instituciones que tengan como giro de negocio dedicarse a recibir dinero en depósitos y otras captaciones y ese dinero también ponerlo a disposición de sus clientes a manera de préstamos, principalmente.

¿Por qué se estudia la banca?

Esta interrogante es importante, ya que plantea la relación de la banca, el dinero y desde luego la economía en general, ante esto Ramírez (2001) plantea las siguientes razones:

- *Proveen un canal para vincular a quienes desean ahorrar con aquellos que quieren invertir.*
- *Desempeñan un importante papel en la determinación de la cantidad de dinero en la economía.*
- *Han sido fuente de rápida innovación financiera que continuamente expande las vías por las que el público puede invertir sus ahorros.* (p. 9).

Esto sirve de guía para poder delinear los objetivos que persigue la banca, por ejemplo, como su naturaleza de intermediación financiera busca poder asesorar a los clientes en sus proyectos de inversión personales y empresariales de gran alcance tanto de fondos económicos como de impacto social, político e incluso ambiental.

Para Cuartas (2013), además de proveer esa guía que es más con un punto de vista de inversiones, debe también enfocarse en *"(…) ser la guía financiera de procesos como: restructuración de deudas, privatizaciones, colocación de acciones y obligaciones negociales, actúan como los principales intermediarios del mercado",* (p. 39).

En general los alcances y funciones de los bancos son bastante amplios y han evolucionado (y seguirán bajo esa misma línea) para lograr satisfacer los cambios en los comportamientos

de consumo y avances en la tecnología. Por ejemplo, ya existen bancos en el mundo que son 100% virtuales sin presencia de sucursales físicas.

A esto se le tiene que agregar que los bancos se deben ver desde dos perspectivas, como empresas y como intermediarios (Cuartas, 2013). Como empresa, está ligada a la finalidad financiera y que es creada por capital accionario y aportado, procura administrar recursos monetarios, financieros y busca como colocarlos, en resumen, como dar soporte financiero a personas y empresas.

Desde el punto de vista de intermediación, su trabajo es mover dinero de un lugar a otro, este puede ser en efectivo o como documentos, títulos, entre otros (Cuartas, 2013), siempre y cuando estos bienes tengan valor monetario y económicos.

Intermediación financiera

Para ampliar un poco más el concepto de intermediación de la banca, para Escoto (2001), lo entiende por *"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).

Por ejemplo, si alguien procura hacer un préstamo a una gran corporación por ejemplo una cervecería, la persona se presenta directamente al presidente de la compañía a ofrecerlo. Lo que sucede en la mayoría de los casos es que los préstamos se hacen mediante la intervención de instituciones financieras, quienes "piden prestado" del dinero que sus otros clientes les han depositado para prestárselo a alguien más.

Otro ejemplo es cuando una persona busca un préstamo para la compra de casa, carro o por alguna razón donde requiere de liquidez para cumplir con otras obligaciones.

Se puede resumir que la intermediación financiera en los bancos es definitivamente una actividad importante para cualquier economía debido a que logra utilizar recursos que en otras circunstancias no se les da un uso más productivo, lo que consigue dinamizar la economía de una manera más eficiente, (Ramírez, 2001).

El dinero

El dinero es definitivamente el medio actual más utilizado para el intercambio de bienes y servicios, y como tal tiene mucha inherencia en las actividades económicas de todas las economías, por ejemplo, en la fijación de precios y en la inflación, las tasas de interés por nombrar algunos. Para Escoto (2001) el dinero se define como: *"La suma de monedas y billetes en poder del público más los depósitos en cuenta corriente y exigibles a la vista en los bancos",* (p. 34).

Cuando en una economía existe inflación, se habla que el valor del dinero es menor, y la relación con esto está directamente ligada a que con la misma cantidad de dinero con una inflación muy alta se puede comprar menos bienes o servicios, de aquí el fundamento que el dinero pierde su valor y caso contrario con la deflación donde el dinero tiene un valor mayor por lo tanto los consumidores pueden adquirir más o sea el poder adquisitivo es mayor. Estos préstamos se depositan a la vista y que, a su vez, van a tener una nueva reserva legal, donde se tiene la posibilidad de prestar el residuo. Este proceso se puede repetir las veces que sean necesarias lo cual aumenta el tamaño de la oferta monetaria del mercado (Escoto, 2001).

Características de la banca

Se manejan dos tipos de banca comercial, por objetividad/actividad y por la propiedad del patrimonio. Los bancos con características de objetividad/ actividad, están ligadas a la razón del banco, o sea qué objetivo persiguen.

A nivel general y según Escoto (2001) entre estos se encuentran:

- **Banca comercial:** básicamente está ligada al mercado monetario, sin embargo, no es solo al dinero también servicios.
- **Banco de desarrollo:** tiene su razón en buscar el desarrollo de empresas mediante créditos con condiciones más favorables.
- **Banca de inversión:** estas las pueden realizar tanto bancos como casas de banca de inversión, permitiéndoles nuevas inversiones y desde luego ayudar a las empresas a obtener financiamiento.

- **Banca múltiple:** se puede resumir como una combinación de las anteriores, por lo que tiene un alcance más amplio de desarrollo.

Bajo la misma línea se tiene la banca por la propiedad, la cual está relacionada con quienes son los propietarios de esta, para Escoto (2001) su cuentan con las siguientes bancas:

- **Bancos multilaterales o internacionales:** su propiedad puede ser de varios estados y además de que se crean por un convenio internacional.
- **Bancos estatales:** como su nombre lo expresa, son bancos que le pertenecen al Estado, por lo tanto, su capital social también.
- **Bancos públicos no estatales:** estos colaboran con el Gobierno, sin embargo, están segregados de la administración pública, por ejemplo, el Banco Popular que tiene capital del gobierno y del sector privado.
- **Bancos privados:** claramente son aquellos bancos cuyo capital es total y absolutamente privado.

Capítulo III

Marco metodológico

Definición del enfoque

Es importante que se defina el enfoque sobre el cual se guía la investigación científica del presente trabajo. Los métodos que se utilizan están basados en un paradigma, con supuestos, percepciones de la realidad, así como juicios de valor que al final apoyan a la investigación sobre qué investigar, los datos por recolectar y cómo hacerlo, sin olvidar su posterior análisis e interpretación, (Pimienta y Hoz, 2017).

El presente trabajo tiene como base el enfoque cualitativo, con el fin de que se pueda recolectar, analizar e interpretar información captada por medio de actividades de campo como la entrevista. Este enfoque se selecciona cuando se desea captar de qué manera el objeto de estudio reacciona al interactuar con el ambiente que lo rodea, dando énfasis a los puntos de vista, interpretaciones, así como los significados (Hernández, Fernández y Baptista, 2014).

Diseño de la investigación

El diseño de la investigación detalla el plan o estrategia por seguir para lograr tener la información que se requiere, de manera tal que el objeto de estudio sea abordado correctamente y se logren alcanzar los objetivos planteados, (Bisquerra, 2009).

No experimental

El diseño no experimental es aquel donde las variables no son manipuladas, dicho de otra manera:

> *Podría definirse como la investigación que se realiza sin manipular deliberadamente variables. Es decir, se trata de estudios en los que no haces variar en forma intencional las variables independientes para ver su efecto sobre otras variables. Lo que efectúas en la investigación no experimental es observar o medir fenómenos y variables tal como se dan en su contexto natural, para analizarlas*, (Hernández, Mendoza, 2018, p.174).

Este diseño se aplica a la presente investigación, debido a que presenta el análisis de los riesgos en Ciberseguridad y sus impactos financieros y no financieros, sin que medie

manipulación alguna, y se centra en analizar las variables para posteriormente se puedan interpretar y se identifiquen causas y consecuencias, (Pimienta y Hoz, 2017).

Seccional

Para efectos de la presente investigación, se debe tener claro que la recolección, análisis e interpretación de la información se dan en un momento único, o sea *"describir variables y analizar su incidencia e interrelación en un momento dado"*, (Hernández *et ál*, 2014, p.154).

Por lo tanto, este diseño se aplica al trabajo de investigación, ya que este se comprende de las fechas de mayo del 2022 para finalizar en el mes de junio del mismo año, de igual manera la recolección de los datos y los estudios de campo necesarios para la interpretación y análisis correspondientes del objeto de estudio y se realizan durante este mismo tiempo.

Transversal

El diseño transversal se utiliza en esta investigación de manera tal manera que se logre estudiar las alteraciones de una o más variables del objeto de estudio en un lapso determinado, estas variaciones se realizan mediante una sola medición durante el tiempo del estudio, (Hurtado y Toro, 2007).

Por lo tanto, la aplicación de las entrevistas que se plantean como instrumentos de recolección de información, son aplicados una vez a los sujetos de estudios.

Método de investigación

A continuación, se describen los métodos de investigación sobre los cuales se basa este análisis y cómo aplican cada uno de ellos para los efectos del objeto de estudio.

Analítico

Tiene su base en el análisis, en el cual se procura descomponer todas las partes del estudio para que puedan ser analizadas por separado (Bernal, 2016). De aquí que también se parta de un proceso cognitivo que según Pimienta y Hoz (2017):

> *Se centra en el descubrimiento de leyes o teorías acerca del fenómeno estudiado, por tanto, es un proceso cognitivo que busca —al fragmentar o separar las partes de un todo, sea cuerpo, elemento u objeto— estudiar su composición de manera individual*, (p.47).

Con la aplicación de los instrumentos de recolección de información, se trata de que mediante la aplicación de este método se pueda interpretar y analizar las variables de manera tal que permita observar los comportamientos que se procura dar.

Inductivo

Mediante la aplicación de este método, es posible pasar de hechos particulares o individuales a los generales. Para Hurtado y Toro (2007) *"Consiste en partir de la observación de múltiples hechos o fenómenos para luego clasificarlos y llegar a establecer las relaciones o puntos de conexión entre ellos (...)*", (p.64).

Para efectos de aplicación al presente trabajo se aplica el instrumento cualitativo de la entrevista para conocer el criterio experto de los gerentes de Seguridad de Información y de Gestión de Riesgos de una entidad financiera costarricense, para posteriormente analizar e interpretar los resultados y así poder obtener conclusiones sobre ellos.

Deductivo

Este método se puede ver cómo *"(...) un proceso mental o de razonamiento que va de lo universal o general a lo particular "*, (Hurtado y Toro, 2007, p.62).

La deducción además permite mediante un razonamiento lógico poder inferir o llegar a conclusiones sobre premisas que se creen verdaderas.

La aplicación de la deducción al trabajo de investigación se sustenta en que primero se realizan estudios generales sobre los conceptos por evaluar y mediante la recolección de la información utilizando los instrumentos se logra analizar e interpretar los datos para posteriormente identificar conclusiones, recomendaciones y la propuesta de un modelo de retorno de la inversión para inversiones en Ciberseguridad.

De campo

Según Pimienta y Hoz (2017), esta modalidad de investigación consiste en *"Recabar la información obtenida del análisis directo del entorno y de la realidad circundante"*, (p.9). Se debe tener claro que la obtención de la información utilizando este método requiere que el investigador esté presente en el espacio y contexto desde donde se está obteniendo la información.

Para fines de la presente investigación, este método es utilizado al aplicarse los instrumentos de obtención de información primaria. Las entrevistas se realizan a los gerentes tanto del área de Seguridad de la Información cómo al del Gerente del Área de Gestión de Riesgo aplicado a una entidad financiera costarricense, ya que ellos son los expertos en el área que se está evaluando y su a vez, son tomadores de decisiones o consultores en cuanto al manejo de riesgos dentro de la organización.

Documental

Mediante la aplicación de este método, es posible colectar, seleccionar y analizar información a partir de diversos tipos de documentos, tales como libros, noticias, artículos, periódicos, leyes, reglamentos por mencionar algunos. Permite tener fuentes muy importantes de información, para que puedan facilitar y extender la comprensión y contexto del fenómeno que se está estudiando (Hernández *et ál*, 2014).

Con respecto a la aplicación de este método a la presente investigación, se basa en la revisión de libros de las distintas áreas del objeto de estudio, utilizando principalmente libros, leyes, decretos, marcos de referencias, reglamentos y artículos de expertos.

Tipo de investigación

Descriptiva

La investigación descriptiva se entiende por *"(…) una forma de estudio para saber quién, dónde, cuándo, cómo, y por qué del sujeto de estudio"*, (Namakforoosh, 2005, p. 91). Basados en un método analítico se puede identificar y describir características de objetos de

estudio, y con este conocimiento se logra también realizar investigaciones más detalladas, (Pimienta y Hoz, 2017).

La aplicación de este tipo de análisis al trabajo de investigación se hace necesario, debido a que se debe abarcar las distintas áreas de estudio, sus contenidos y particularidades. Es preciso entender los fundamentos de finanzas y de las entidades financieras costarricenses y cómo estos afectan el manejo de riesgos en Ciberseguridad, que a su vez se trata de un tema de toma de decisiones para la administración de riesgos y entendiendo el entorno del objeto de estudio.

Exploratorio

Este tipo de investigación es útil cuando el objeto de estudio es poco conocido o estudiado, y Hernández y Mendoza (2018) lo aclaran de la siguiente manera *"(…) cuando la revisión de la literatura reveló que tan solo hay guías no investigadas e ideas vagamente relacionadas con el problema de estudio, o bien, si deseamos indagar sobre temas y áreas desde nuevas perspectivas",* (p.106).

Con respecto a esta investigación es precisamente uno de los objetos de estudio el identificar por qué es complicado el manejo de riesgos de Ciberseguridad y que cada vez son más frecuentes los ataques que logran su cometido.

Explicativa

La investigación explicativa trata de ir más allá de una descripción de un fenómeno, sus relaciones y más bien procura identificar las causas que provocan el cómo se comporta frente a distintos entornos (Hernández *et ál*, 2014). Para Bernal (2016) *"Son investigaciones en las que el investigador se plantea como objetivos estudiar el porqué de las cosas, los hechos, los fenómenos o las situaciones",* (p.148).

Su aplicabilidad para esta investigación radica precisamente en la propuesta del trabajo de un modelo de mejores prácticas para la administración de riesgos en Ciberseguridad, de manera tal que se pueda tener mejor conocimiento de las áreas donde las entidades financieras pueden ser más vulnerables y establecer controles necesarios para mitigar la probabilidad de ocurrencia y, por lo tanto, su impacto financiero y no financiero.

Correlacional

Para Hernández y Mendoza (2018), *"Este tipo de estudios tiene como finalidad conocer la relación o grado de asociación que existe entre dos o más conceptos, categorías o variables en un contexto en particular"*, (p.109).

Esta investigación plantea variables que puede influir una en la otra, identificar los riesgos de Ciberseguridad que más están expuestas las entidades financieras, ver la influencia de estos con los impactos financieros y no financieros y, desde luego, la relación con las principales causas que llevan a la materialización de los riesgos.

Hermenéutica

Para Grondin (2008), existen tres grandes acepciones de la hermenéutica, sin embargo, para efectos de la aplicabilidad del trabajo de investigación, la más relacionada es la tercera la cual se ve desde el punto de vista metodológico *"La interpretación se muestra entonces cada vez más como una característica esencial de nuestra presencia en el mundo"*, (p.4).

Para este trabajo de investigación es de vital importancia utilizar documentación en distintos textos de igual diversificación de fuentes, basados en finanzas, administración, el sistema financiero, análisis de riesgos y Ciberseguridad, de manera tal que logren sustentar la consecución del objeto de estudio y la elaboración de la propuesta.

Nomotética

La investigación nomotética hace referencia al análisis que crea o propone algo, y Bisquerra (2000) da un enfoque a este estudio sobre el establecimiento de leyes generales, propuestas.

Como parte del desarrollo de este trabajo, la investigación nomotética se aplica ya que, como parte de los objetivos del trabajo, es la propuesta de crear un modelo de mejores prácticas para la administración de riesgos de Ciberseguridad en las entidades financieras costarricenses.

Sujetos y fuentes de información

Sujetos de información

El sujeto no es más que el objeto de estudio, para esto Pimienta y Hoz (2017) lo definen como: *"El sujeto cognoscitivo es la persona que conoce, es decir, aquella que por medio de sus sentidos y razonamiento capta e interpreta aspectos de la realidad que lo circunda"*, (p.22). Este concepto es muy importante en una investigación científica por la relevancia en la identificación del problema que se procura estudiar, como son recolectados los datos, así como que grado de validez de los resultados, todo esto acorde con el entorno en que las variables estén interactuando, (Bisquerra, 2009).

Con respecto al presente trabajo de investigación, se consideran los siguientes sujetos:

- **Gerentes de Seguridad de la Información y de Gestión de Riesgos:** La información cualitativa que se trata de obtener mediante la aplicación de una entrevista está dirigida a los encargados de la Seguridad de la Información y de Gestión de Riesgos de una entidad financiera costarricense y ellos a su vez tienen injerencia directa sobre el proceso de análisis de riesgos y todas sus distintas etapas, de manera tal que la información que se obtiene es más exacta.

Fuentes primarias

En cualquier investigación existen dos fuentes, las primarias son aquellas donde la información se obtiene directamente y de primera mano (Hernández *et ál*, 2014). Para Bernal (2016) las fuentes primarias son: *"(…) todas aquellas de las cuales se obtiene información directa, es decir, de donde se origina la información"*, (p. 258).

Para la presente investigación, se cuenta con una fuente primaria:

- **Información de los gerentes de Seguridad de la Información y de Gestión de Riesgos:** Con esto se procura obtener la información cuantitativa de la investigación, mediante la aplicación de una entrevista a los gerentes de Seguridad de la Información y de Gestión de Riesgos de una entidad financiera costarricense y así lograr captar

sus criterios profesionales que den un sustento más exacto sobre el problema del objeto de estudio.

Fuentes secundarias

La segunda fuente de información son las secundarias, según Pimienta y Hoz (2007) están compuestas *"(...) por libros, revistas, enciclopedias, artículos que interpretan otros trabajos o investigaciones"*, (p. 49) y que con el tiempo y gracias a su aporte continuo a otras investigaciones, llegan a demostrar que tienen una utilidad importante.

Para la presente investigación, se cuenta con las siguientes fuentes secundarias:

- **Libros de texto:** Fundamentos de finanzas administrativas, administración, principios de la banca, procesos de manejo de riesgos, así como de Ciberseguridad es la literatura sobre la cual se basan los libros de texto que se utilizan en esta investigación.

- **Leyes y decretos y reglamentos:** En Costa Rica se cuenta con leyes que regulan el marco de los delitos informáticos, así como el decreto 37052-MICITT (2012) para la creación del Centro de Respuesta de Incidentes de Seguridad Informática de Costa Rica (CSIRT-CR) son objeto de fuente de información para el desarrollo de esta investigación así como el reglamento 2-10 sobre Administración Integral de Riesgos (2022) y el 14-7 Reglamento de Gestión de la Tecnología de Información (2017) de la Superintendencia General de Entidades Financieras.

- **Internet:** La última fuente secundaria de información es el internet, especialmente sitios de los bancos, así como otras páginas de organismos e instituciones nacionales y de organismos internacionales de marcos de referencia de Seguridad de la Información y de Gestión de Riesgos. Además, otros de sitios internacionales de especialistas y expertos en los distintos temas por analizar y de otros que por su relación con los temas desarrollados, sustentan de mejor manera la investigación.

Población y muestra

Población

Bernal (2016) se refiere a población como: *"el conjunto de todos los elementos a los cuales se refiere la investigación. Se puede definir también como el conjunto de todas las unidades de muestreo"*, (p.210). Este conjunto de elementos debe poseer las siguientes características: homogeneidad, tiempo, espacio y cantidad.

Para efectos del presente trabajo no se utiliza la encuesta como fuente de información primaria, por lo tanto, no se requiere de definir una muestra a quién aplicárselo. En su lugar se utiliza la entrevista a los encargados de Seguridad de la Información y de Gestión de Riesgos en una entidad del sistema financiero costarricense.

La razón de esto radica principalmente porque el tema objeto de estudio requiere de dos características muy específicas pero que, a la vez, son muy necesarias y dan un nivel de confianza de lograr obtener la información que se requiere. La primera de ellas es contar con un nivel amplio de conocimiento del tema. La segunda es la experiencia en estas áreas para lograr la consecución del objetivo final de la propuesta del modelo de mejores prácticas para la administración de riesgos de Ciberseguridad.

Es importante complementar que ambos encargados de las áreas de Ciberseguridad y gestión de riesgos aparte de sus atestados, trabajan para uno de los dos bancos más importantes del país, el cual cuenta con más del 15% que representan poco más de treinta mil millones de colones del total de los activos del sistema bancario costarricense (SUGEF, 2022) y los más importante es que está entidad sufre uno de los ciberataques más importantes en la historia de la banca de Costa Rica en el 2020, donde ambos encargados de las áreas mencionadas anteriormente tienen la responsabilidad junto con un equipo interdisciplinario de trabajar en la investigación y acciones correctivas.

Muestra de gerentes de Seguridad de la Información y de Gestión de Riesgos

Existen dos tipos de muestras, la probabilística que básicamente toda la población definida tiene la misma probabilidad de ser elegida y la no probabilística. Según Hernández y Mendoza (2018) en las muestras no probabilísticas *"la elección de las unidades no depende de la probabilidad, sino de razones relacionadas con las características y contexto de la investigación",* (p.200).

Por lo tanto, la muestra se basa en dos gerentes, uno el de la Seguridad de la Información y el otro el de Gestión de Riesgos de una entidad financiera, ya que cuentan con los elementos de juicios requeridos al estar relacionados con las dos áreas principales que son objetivo de estudio, la Ciberseguridad y la gestión de riesgos.

Muestreo

A criterio

Se dice que este método está basado en la selección de la población basado mucho en juicios subjetivos y conocimiento del investigador, y donde priva su criterio profesional, (Requena, 2014).

Por lo tanto, para efectos de esta investigación, es requerido para poder seleccionar a los gerentes de Seguridad de la Información y de Gestión de Riesgos de una entidad financiera costarricense, debido a que ellos son los que precisamente tienen el conocimiento del área y están relacionados con el proceso de manejo de riesgos de Ciberseguridad.

Instrumentos

Entrevista

La entrevista permite mediante una conversación obtener información más personalizada sobre acontecimientos vividos, opiniones y aspectos subjetivos del entrevistado con respecto a un tema en estudio, (Bisquerra, 2009).

Las entrevistas se dividen en estructuradas, no estructuradas o también conocidas como abiertas, para Hernández *et ál* (2018):

> *En las primeras, el entrevistador realiza su labor siguiendo una guía de preguntas específicas y se sujeta exclusivamente a esta (el instrumento prescribe qué cuestiones se preguntarán y en qué orden). Las entrevistas semiestructuradas se basan en una guía de asuntos o preguntas y el entrevistador tiene la libertad de introducir preguntas adicionales para precisar conceptos u obtener mayor información. Las entrevistas abiertas se fundamentan en una guía general de contenido y el entrevistador posee toda la flexibilidad para manejarla,* (p.403).

Con respecto al trabajo de investigación, se utiliza la entrevista estructurada a los gerentes del área de Seguridad de la Información y de Gestión de Riesgos de una entidad financiera costarricense, permitiendo seguir un orden de las preguntas que por su naturaleza son abiertas y obtener un enfoque cualitativo de las opiniones y experiencias con respecto al tema objeto de estudio, además se aplica de manera personal mediante la constatación de una cita previa. A continuación, se detalla los asuntos de la entrevista, definiendo los ítems, reactivos y el indicador respectivo:

Tabla 2
Desglose del cuestionario aplicado a la muestra del Gerente de Seguridad de la Información y al Gerente de Gestión de Riesgos

Ítem	Naturaleza	Reactivo	Indicador
1	Abierta	Principales amenazas en Ciberseguridad.	De razón
2	Abierta	Impactos financieros y no financieros más significativos.	De razón
3	Abierta	Importancia del compromiso y valores éticos.	De razón
4	Abierta	Regularidad en la actualización de políticas y procedimientos de seguridad.	De razón
5	Abierta	Manejo del talento humano.	De razón
6	Abierta	Entendimiento de roles y responsabilidades.	De razón
7	Abierta	Mantener actualizado perfil de riesgo.	De razón
8	Abierta	Mecanismos de comunicación de noticias de riesgos de Ciberseguridad.	De razón

9	Abierta	Principales razones de materialización de los riesgos.	De razón
10	Abierta	Comunicación de los riesgos.	De razón
11	Abierta	Administración de controles de seguridad.	De razón
12	Abierta	Perfil educación de riesgos de Ciberseguridad de clientes.	De razón
13	Abierta	Desafíos para manejo de los perfiles de los clientes.	De razón
14	Abierta	Acciones o recomendaciones para atacar los desafíos de los perfiles de los clientes.	De razón

Fuente: Elaboración propia para tesis

Revisión documental

Según Bernal (2016), *"La investigación documental consiste en el análisis de la información escrita sobre un determinado tema, con el propósito de establecer relaciones, diferencias, etapas, posturas o estado actual del conocimiento respecto al tema objeto de estudio"*, (p. 146). Con la revisión de documentos es posible poder hacer varias cosas, complementar lo dicho, y constatar o reafirmar criterios emitidos personalmente o por terceros.

Para esta investigación se realiza la revisión de material documental para hacer el análisis de las leyes costarricenses en temas de delitos informáticos y decretos, así como el analizar aspectos de finanzas administrativas, el entorno de la banca costarricense y desde luego normas de administración de riesgos y de gestión de la tecnología de información, con el fin de poder determinar las variables requeridas para la conformación de un modelo de mejores prácticas para la administración de riesgos de Ciberseguridad.

Confiabilidad y validez

Confiabilidad

La confiabilidad se debe utilizar para todos los instrumentos que se utilicen en la investigación científica, para Hurtado y Toro (2007) es un requisito fundamental cuando se realizan investigaciones cuantitativas y se basa en que los instrumentos de medición cumplan con su propósito y que la información que se extrae se pueda considerar como válida.

Para este trabajo de investigación, la confiabilidad se alcanza mediante la comprobación de la experiencia de los gerentes responsables de la Seguridad de la Información y de Gestión de Riesgos de manera tal, que ellos transmiten su conocimiento y experiencia adquirida gracias a la aplicación de las leyes, políticas, procedimientos, y normas que regulan al sistema financiero costarricense.

Validez

Sin duda alguna la validez es un aspecto fundamental en la investigación científica, ya que ayuda a determinar si los resultados que se obtienen son válidos o no. Para Villasís, Márquez, Zurita, Miranda y Escamilla (2018), *"El concepto de validez en investigación se refiere a lo que es verdadero o se acerca a la verdad. Se considera que los resultados de una investigación son válidos cuando el estudio está libre de errores"*, (p.415).

Su aplicación en esta investigación está basada en tres aspectos, el primero es por su validez de contenido, para Hurtado y Toro (2007) *"Se refiere a que los instrumentos de medición estén construidos de tal modo que realmente midan los aspectos que se quiere medir"*, (p.100), en otras palabras, procura mediante la aplicación del instrumento comprobar un dominio específico de lo que se está midiendo, además de que las preguntas de los instrumentos se formulan con base en los objetivos establecidos.

El otro es la validez constructo que según Hernández *et ál* (2018) *"Debe explicar cómo las mediciones del concepto o variable se vinculan de manera congruente con las mediciones de otros conceptos correlacionados teóricamente"*, (p.203), o sea permite verificar que el instrumento esté bien hecho y que cumpla con el resultado esperado.

Por último, los instrumentos que se utilizan en esta investigación son revisados y aprobados por el tutor antes de que sean aplicados.

Proceso de análisis

El proceso de análisis según Bisquerra (2009) es: *"El proceso de análisis se puede entender como el flujo y conexión interactiva de tres tipos de operaciones básicas: la reducción de la información, la exposición de los datos y la extracción o verificación de conclusiones (...)"*,

(p.355) o sea es la descripción de las etapas para el procesamiento de la información y definición que se hace con ella.

Para efectos del trabajo de investigación, se requiere recopilar la información primaria y secundaria. Para la primera se utiliza la entrevista como el instrumento, y se realiza a los gerentes de Seguridad de la Información y de Gestión de Riesgos de una entidad financiera costarricenses, y cuando se obtiene, se debe organizar las respuestas en tablas y así proceder al análisis, y una vez que se concluya se deben presentar los principales hallazgos.

Por último, también se cuenta con las fuentes secundarias, aquí se utiliza la información documental, para efectos de la presente investigación, se requiere analizar los datos contenidos en libros de texto relacionados con el objeto de estudio, leyes, normas y decretos, así como la información en internet, todo esto debe ser sistematizado y ordenado de manera tal que permita analizar los informes que apoyen a los resultados finales de la investigación.

Operacionalización de variables

Primera variable: riesgos en Ciberseguridad

Definición conceptual

En un contexto administración de riesgos de la información, un proceso de administración de riesgos contribuye a las organizaciones para que puedan realizar evaluaciones y manejos de incidentes que puedan causar daños importantes a sus datos sensibles. Este proceso también incluye la identificación de vulnerabilidades que los cibercriminales puedan explotar o hacer que las personas caigan en errores sin darse ellos cuenta.

Las organizaciones constantemente consideran cómo poder manejar los riesgos que día a día evolucionan especialmente en Ciberseguridad, la organización de especialidad en manejo de control interno COSO (2015) adapta su marco de referencia (2012) para brindar una opción a las organizaciones para implementar un proceso de manejo de riesgos que cubra las vulnerabilidades a las que están expuestas por los ciberdelincuentes.

Definición instrumental

Esta variable es evaluada y estudiada a detalle por la entrevista que se aplica a los gerentes de Seguridad de la Información y al de Gestión de Riesgos, además, busca la relación con los reactivos enfocados en la identificación de impactos financieros y no financieros, así como con las principales razones de la materialización de los riesgos.

Los ítems de la entrevista utilizados para evaluar esta variable son:

- **Ítem 1:** naturaleza abierta, reactivo de principales amenazas en Ciberseguridad.
- **Ítem 4:** naturaleza abierta, reactivo de regularidad en la actualización de políticas y procedimientos de seguridad.
- **Ítem 7:** naturaleza abierta, reactivo de mantener actualizado perfil de riesgo.
- **Ítem 10:** naturaleza abierta, reactivo de comunicación de los riesgos.
- **Ítem 11:** naturaleza abierta, reactivo de administración de controles de seguridad.
- **Ítem 12:** naturaleza abierta, reactivo de perfil educación de riesgos de Ciberseguridad de clientes.

Además de la utilización de este instrumento, se utiliza la revisión documental de normas, regulaciones y leyes que dictan el marco de referencia en Ciberseguridad y manejo de riesgos.

Definición operacional

La naturaleza de esta variable es cuantitativa, ya que busca el criterio de los expertos sobre el manejo de riesgos en Ciberseguridad a las que se enfrentan las entidades financieras costarricenses.

El objetivo principal que busca esta variable es poder identificar los principales riesgos en Ciberseguridad que se ven expuestas las entidades financieras, poder discernir cómo es el proceso de manejo de riesgos y administración de los controles que se deben implementar y el perfil de riesgo de los clientes de estas entidades.

A continuación, los indicadores utilizados en la entrevista para esta variable:

- **Ítem 1:** indicador de razón.

- **Ítem 4:** indicador de razón.
- **Ítem 7:** indicador de razón.
- **Ítem 10:** indicador de razón.
- **Ítem 11:** indicador de razón.
- **Ítem 12:** indicador de razón.

Segunda variable: impactos financieros y no financieros

Definición conceptual

Un análisis de riesgos no está completo si no incluye a qué se ve expuesta una organización, además de saber identificar cuáles son las consecuencias de materializarse un riesgo es sumamente importante, ya que puede determinar incluso el cierre o cese del servicio que presta, lo cual implica en la mayoría de los casos cuestiones económicas, pero sin duda alguna la reputación que no tiene precio es de las principales razones por las cuales se debe hacer este tipo de ejercicios.

Para la firma Deloitte en su estudio "Bajo la superficie de un ciberataque Una mirada más profunda a los impactos comerciales", (2022), "*Hay muchas maneras que un ciberataque pueda afectar a una organización y los impactos podría variar dependiendo de la naturaleza y severidad del ataque*", por lo que es sumamente importante que los impactos sean alineados al sector en el que se está para así tener la idea clara de las implicaciones si se sufre un ciberataque.

Definición instrumental

Esta variable es evaluada y estudiada a detalle por la entrevista que se aplica a los gerentes de Seguridad de la Información y al de Gestión de Riesgos, además, busca la relación con los reactivos enfocados al análisis de riesgos, así como con las principales razones de la materialización de los riesgos.

Los ítems de la entrevista utilizados para evaluar esta variable son:

- **Ítem 2:** naturaleza abierta, reactivo de impactos financieros y no financieros más significativos.

- **Ítem 3:** naturaleza abierta, reactivo de importancia del compromiso y valores éticos.
- **Ítem 5:** naturaleza abierta, reactivo de manejo del talento humano.
- **Ítem 6:** naturaleza abierta, reactivo de entendimiento de roles y responsabilidades.

Definición operacional

La naturaleza de esta variable es cuantitativa, ya que busca el criterio de los expertos sobre los impactos financieros y no financieros a las que se enfrentan las entidades financieras costarricenses.

El objetivo principal que busca esta variable es poder identificar los principales impactos financieros y no financieros que se ven expuestas las entidades financieras, este es un paso muy importante ya que en esos organismos uno de sus puntos más críticos es la confianza, y aquí esto es casi todo, con la más mínima duda o inseguridad que sientan los clientes, socios comerciales puede significar el cierre de operaciones.

A continuación, los indicadores utilizados en la entrevista para esta variable:

- **Ítem 2:** indicador de razón.
- **Ítem 3:** indicador de razón.
- **Ítem 5:** indicador de razón.
- **Ítem 6:** indicador de razón.

Tercera variable: Causas que llevan a la materialización de los riesgos

Definición conceptual

Sin duda alguna si las organizaciones lograran anticipar cuándo van a ser víctimas de un ciberataque, serían muy afortunadas y van a tener presencia en el mercado por mucho tiempo, incluso no habría razón por la cual no deban seguir siendo, pero la verdad es que por más que exista un proceso de análisis de riesgo, es complicado lograr determinar siempre las causas por las cuales estos se materializan, esto debido a que en ambientes digitalizados donde la tecnología es el pilar fundamental, cambian constantemente y con estos cambios los ciberdelincuentes se vuelven cada vez más listos en buscan nuevas formas de vulnerar a las organizaciones.

Según el estudio realizado por Verizon (2020) sobre "Investigaciones de Filtraciones de Datos": "*Los ataques en este sector son perpetuados por actores externos quienes están motivados por razones financieras con un 63%*", esto simplemente es una de las razones principales a las que este sector se ve expuesto, precisamente por el tipo de información que manejan.

Definición instrumental

Esta variable es evaluada y estudiada a detalle por la entrevista que se aplica a los gerentes de Seguridad de la Información y al de Gestión de Riesgos, además, busca la relación con los reactivos enfocados al análisis de riesgos, así como los principales impactos a los que se puede ver expuesta una entidad financiera.

Los ítems de la entrevista utilizados para evaluar esta variable son:

- **Ítem 3:** naturaleza abierta, reactivo de importancia del compromiso y valores éticos.
- **Ítem 4:** naturaleza abierta, reactivo de regularidad en la actualización de políticas y procedimientos de seguridad.
- **Ítem 8:** naturaleza abierta, reactivo de mecanismos de comunicación de noticias
- **Ítem 9:** naturaleza abierta, reactivo de principales razones de materialización de los riesgos.
- **Ítem 11:** naturaleza abierta, reactivo de administración de controles de seguridad.
- **Ítem 12:** naturaleza abierta, reactivo de perfil educación de riesgos de Ciberseguridad de clientes.
- **Ítem 13:** naturaleza abierta, reactivo de desafíos para manejo de los perfiles de los clientes.
- **Ítem 14:** naturaleza abierta, reactivo de acciones o recomendaciones para atacar los desafíos de los perfiles de los clientes.

Definición operacional

La naturaleza de esta variable es cuantitativa, ya que busca el criterio de los expertos sobre las principales causas que llevan a la materialización de los riesgos en Ciberseguridad para las entidades financieras costarricenses.

El objetivo principal que busca esta variable es poder identificar cuáles son las principales causas que provocan que los riesgos en Ciberseguridad se materialicen en las entidades financieras. Si bien la tecnología avanza a pasos agigantados, lo que hoy parece ser actual dentro de unos meses ya deja de serlo, sin duda alguna, el hecho de que las organizaciones se mantengan en constante revisión sus procesos de administración de riesgos y principalmente su apetito, puede lograr reducir las posibilidades de que esos riesgos al final se logren materializar.

A continuación, los indicadores utilizados en la entrevista para esta variable:

- **Ítem 3:** indicador de razón.
- **Ítem 4:** indicador de razón.
- **Ítem 8:** indicador de razón.
- **Ítem 9:** indicador de razón.
- **Ítem 11:** indicador de razón.
- **Ítem 12:** indicador de razón.
- **Ítem 13:** indicador de razón.
- **Ítem 14:** indicador de razón.

Cuarta variable: modelos mejores prácticas para la administración de riesgos.

Definición conceptual

Un modelo de mejores prácticas se debe al cambio, el ambiente de las tecnologías de información es tan cambiante que lo que hoy se considera un avance importante dentro de unos meses deja de serlo, porque ya hay alguna manera más eficiente y segura de hacerlo, el problema es que mientras eso pasa los ciberdelincuentes van un paso adelante y toman ventaja de que siempre la solución va a venir después del problema, es realmente imposible llegar a tener una seguridad 100% infalible, al menos con la tecnología actual no lo es, eso más saber que el eslabón más débil siguen siendo las personas que utilizan esa tecnología, lo que provoca que las entidades financieras deban buscar nuevas formas de garantizar que la seguridad de sus sistemas y de la información de sus clientes está a salvo.

En la actualidad uno de los estándares más adaptados para control interno es el de COSO (2013), este marco de referencia ha logrado ganar gran aceptación a nivel mundial y es utilizado en muchas partes del mundo, precisamente porque su marco de referencia ha servido de referencia para el diseño, implementación y conducir controles internos, así como evaluar la eficacia de los controles internos.

Definición instrumental

Esta variable es evaluada y estudiada a detalle por la entrevista que se aplica a los gerentes de Seguridad de la Información y al de Gestión de Riesgos, además, procura proponer un modelo de mejores prácticas para la administración de riesgos de Ciberseguridad, y sus relaciones con el análisis de riesgo, así como los principales impactos a los que se puede ver expuesta una entidad financiera y, desde luego, las causas principales por las cuales los riesgos en esta área son materializados.

Definición operacional

La naturaleza de esta variable es mixta, ya que busca el criterio de los expertos sobre las principales recomendaciones sobre las mejores prácticas en manejos de riegos en Ciberseguridad, pero a la vez también existe un juicio experto del investigador basando en los marcos de referencia internacionalmente aceptados, y que son fundamento del objeto de estudio.

El objetivo principal que busca está variable, es poder plantear una propuesta de un modelo de mejores prácticas para la administración de riesgos en Ciberseguridad para las entidades del sistema financiero utilizando como referencias marcos internacionalmente aceptados y para lograr este objetivo, se procede a utilizar las variables anteriores para hacer su fundamentación.

Capítulo IV

Análisis e interpretación de resultados

Análisis e interpretación de resultados

A continuación, se desarrolla la etapa donde se presentan el análisis e interpretación de los resultados obtenidos de la aplicación de la entrevista para la recolección de la información primaria de acuerdo con las variables definidas.

Es importante mencionar que la información obtenida es resultado del trabajo de campo realizado con la aplicación de la entrevista para la recolección de información primaria aplicada a los gerentes de Seguridad de la Información y al de Gestión de Riesgos de una entidad financiera costarricense.

El enfoque para cada variable está fundamentado en el objeto de estudio de esta investigación, de manera tal que permita captar las consideraciones que conlleva hacer un análisis de riesgos en Ciberseguridad, sin dejar de lado las consecuencias que pueden exponerse las organizaciones y donde el criterio de los expertos es fundamental para dimensionar correctamente estas implicaciones, y por último, se procura constatar las principales razones por lo que los riesgos se materialicen recordando todas las leyes y regulaciones a las que están sujetas las entidades financieras.

Por último, cada variable es verificada mediante un análisis documental, de manera tal que se constate los resultados versus la teoría que se encuentra en la bibliografía que incluye normas, reglamentos, leyes que regulan el sector financiero costarricense y marcos de referencia internacionalmente aceptados para el análisis de riesgos.

Análisis e interpretación de resultados de la primera variable: riesgos en Ciberseguridad

Esta primera variable corresponde específicamente a los resultados obtenidos sobre las opiniones de los gerentes de Seguridad de la Información y al de Gestión de Riesgos sobre los principales riesgos que afectan al sector financiero costarricense.

Resultados de la entrevista

A continuación, se describen y analizan los resultados obtenidos para la primera variable basados en la entrevista aplicada a los expertos:

Tabla 3
Resultados de la primera variable de estudio derivados de la entrevista aplicada a los expertos

Ítem	Reactivo	Sujeto 1: Alejandro Salazar Sanabria
1	**Principales amenazas en Ciberseguridad.**	El "*ransomware*" es de las principales amenazas, sin embargo, lo que más está afectado a las entidades financieras es la ingeniería social, ya que ataca al eslabón más débil que son los clientes.
4	**Regularidad en la actualización de políticas y procedimientos de seguridad.**	La documentación debe ser revisada y aprobada por la Junta Directiva al menos una vez al año, pero también se debe contemplar hacerlo bajo demanda, especialmente después de un incidente grave de seguridad.
10	**Comunicación de los riesgos.**	Es complejo, internamente existe la regulación y normativa de lo que se le debe entregar a SUGEF u otros organismos reguladores y se salvaguarda la confidencialidad de la información, hacia afuera, se debe manejar con cuidado no solo para no crear una idea errónea de que el banco está mal ya que las personas podrían interpretarlo, se debe manejar con profesionales en comunicación.
11	**Administración de controles de seguridad.**	En Costa Rica e incluso a nivel de Latinoamérica existe en algunas instituciones problemas de madurez y en ocasiones se encuentran departamentos que implementan, revisan y reportan sus propios controles, debe existir una adecuada segregación de funciones basados en líneas de defensas independientes una de la otra.

Fuente: Entrevista de elaboración propia para tesis

Tabla 4
Resultados de la primera variable de estudio derivados de la entrevista aplicada a los expertos

Ítem	Reactivo	Sujeto 2: Luis Carlos Hernández
1	**Principales amenazas en Ciberseguridad.**	La extorsión y cibercrimen, el hacktivismo ahora lo usan para sacar beneficio económico para financiar sus ataques. El conflicto Rusia con Ucrania ha convertido esto en una gran amenaza.
4	**Regularidad en la actualización de políticas y procedimientos de seguridad.**	Norma ISO 27001 es clara en pedir políticas de alto nivel que deben complementarse con procedimientos y disposiciones más específicas donde se puede usar estándares como la NIST. Políticas al no cambiar con mucha frecuencia puede revisarse 1 vez cada dos años y los procedimientos y disposiciones al menos 1 vez al año.
10	**Comunicación de los riesgos.**	En Costa Rica apenas se está creando una directriz para que todo incidente sea comunicado, aún no se sabe si al MICIT, tener cláusulas en los contratos sobre comunicación de incidentes de seguridad, echar mano del comité de Ciberseguridad que es multidisciplinario para analizar todas las áreas incluso manejo de proveedores.
11	**Administración de controles de seguridad.**	La palabra clave es gobierno, que cada control tenga su gobernanza. Tener personas que definan los controles, otros los ejecutan, tener esa definición clara de recursos tanto humanos como tecnológicos, definición de indicadores y sus respectivas pruebas.

Fuente: Entrevista de elaboración propia para tesis

De acuerdo con las respuestas brindadas durante las entrevistas por parte de los expertos, se aprecian ideas muy enfocadas al área de experiencia de cada quién sin llegar a un punto en común en algunas de las preguntas, a continuación, se detalla las principales apreciaciones dadas.

De primera entrada se aprecia como ambos coinciden en como los ciberataques son una clara amenaza para las entidades financieras; sin embargo, el enfoque dado por uno y el otro es un tanto distinto, el gerente de Riesgos describe que la principal amenaza es el ataque de

ingeniería social, el cual está enfocado al eslabón más débil como son las personas, pero principalmente a los clientes de las entidades bancarias.

Para el encargado de Seguridad de la Información, su perspectiva va más hacia los ataques más desarrollados que se relacionan con la extorsión e incluso la conformación de grupos criminales en procura de obtener beneficios económicos y tomando partido en el conflicto entre Rusia y Ucrania.

Algunas opiniones en común se logran identificar sobre la regularidad con que las políticas y procedimientos de seguridad se deben actualizar; no obstante, también hay algunas diferencias. Para el Gerente de Gestión de Riesgos si bien debe existir plazos definidos que a su consideración tiene que ser al menos una vez al año, sin embargo, debido al ambiente tan cambiante que son las tecnologías de información y especialmente el de Ciberseguridad, cada vez que se enfrente alguna situación o incidente grave se deberían estar revisando los documentos.

Por su parte el Gerente de Seguridad de la Información basa su opinión en normas y estándares internacionales, los cuales que una mejor práctica es al menos revisar documentos que casi no presentan cambios como políticas con periodos más extendidos y la documentación que define el cómo se hacen las cosas y que se deben revisar al menos una vez al año.

Con respecto al enfoque sobre la comunicación de los riesgos al exterior, existen posiciones diferentes, por un lado el pensamiento es más pensando hacia el impacto de la imagen que puede sufrir una entidad financiera si algo sale al exterior y no se contextualiza correctamente, los clientes pueden sentir que no pueden confiar en la entidad donde tienen su dinero y desde luego el papel que juega la prensa, donde el mensaje no se comunique de la manera en que se tiene pensado, a la vez hace hincapié en que ya existe regulación sobre comunicación de los perfiles de riesgos ante la SUGEF donde se mantiene la confidencialidad de la información.

Por otro lado más bien se apoya sobre una directriz que al parecer es reciente y que intenta definir claramente cómo se debe manejar la comunicación de incidentes y riesgos de seguridad, además toca un punto muy importante como lo es el manejo de riesgos con

proveedores y sobre las cláusulas que deben existir en los contratos para las empresas que deseen ser proveedores de entidades financieras, esto porque se tiene conocimiento que muchos no cumplen con requerimientos mínimos, lo que pone a ambas partes en riesgo.

Sobre la administración de controles, ambos expertos coinciden en que tener un adecuado modelo de gobernanza es esencial e imprescindible, y esto se fundamenta en el grado de madurez que tienen en general las empresas independientemente del sector en que trabajan, el cual no es el suficiente y carecen de mecanismos que les garanticen que un control está cumpliendo su objetivo porque fue puesto como resultado de un análisis de riesgos que fundamente su inversión, función y que se tenga la manera correcta de medir si está cumpliendo su función.

Análisis documental

A continuación, se presenta el análisis documental para la primera variable. La administración del riesgo es un proceso mediante el cual toda organización debe utilizar para efectos de lograr identificar, medir, evaluar y reportar las distintas amenazas, así como oportunidades que pueda afectarla en la consecución de sus objetivos estratégicos (Estupiñán, 2015).

Los avances en la digitalización de las entidades financieras y en general del mundo empresarial, sin duda alguna ha generado una gran cantidad de ventajas e incluso se considera como un factor diferenciador en mercados competitivos, pero por otro lado los ataques a este sector se han incrementado, según Verizon (2020) la frecuencia en que estos incidentes ocurren es de 1,509 veces y en 448 casos se confirma la divulgación de información confidencial.

Para lograr establecer un adecuado proceso de evaluación de riesgos, se debe establecer los objetivos o requerimientos mínimos de manera tal que se logre maximizar las posibilidades de identificar y evaluar los riesgos de la organización y vaya acorde con los objetivos o requerimientos planteados (COSO, 2012).

En Costa Rica las entidades financieras están sujetas a las disposiciones dadas por las distintas superintendencias, dentro del marco de esta investigación la Super Intendencia de

Entidades Financieras es la que se está haciendo referencia, pues tiene el reglamento 2-10 (2022) para la gestión integral de riesgos.

Debido a las variables que se deben considerar que hacen vulnerable al sector financiero, es de esperar que se cuente con un reglamento que dé guía sobre las consideraciones importantes y que justifican la elaboración de este tipo de procesos.

La gestión de riesgos debe ser integral a escala organizativa, debe necesariamente incluir todos los demás riesgos dentro de una organización, ya que una vulnerabilidad en uno de los sectores de la organización podría repercutir en otros, además de que gestionar riesgos por separado implica mayores esfuerzos e incluso duplicidad y desperdicio de recursos. Al final las políticas y prácticas adecuadas de manejo de riesgo pueden aumentar la confianza entre los distintos actores del sector financiero e incluso generar ventajas competitivas (ACCID, 2019).

Análisis e interpretación de resultados de la segunda variable: impactos financieros y no financieros

Esta segunda variable tiene como finalidad mostrar los resultados obtenidos sobre las opiniones de los gerentes de Seguridad de la Información y al de Gestión de Riesgos sobre los principales impactos financieros y no financieros que se ven expuestos en el sector financiero costarricense.

Resultados de la entrevista

A continuación, se describen y analizan los resultados obtenidos para la segunda variable basados en la entrevista aplicada a los expertos:

Tabla 5
Resultados de la segunda variable de estudio derivados de la entrevista aplicada a los expertos

Ítem	Reactivo	Sujeto 1: Alejandro Salazar Sanabria
2	**Impactos financieros y no financieros más significativos.**	El negocio de los bancos es de confianza, por lo que si las personas no confían en quién está administrando su dinero se lo van a querer llevar a otro lado, además hay un impacto en la imagen muy grande.
5	**Manejo del talento humano.**	Se hacen ejercicios de simulación de ataques como tipo phishing, hay empleados que caen, esos casos son llevados a alta gerencia y comité de TI, el banco tiene la percepción de que un funcionario bancario debería tener una alta integridad y profesionalismo por los datos que maneja.

Ítem	Reactivo	Sujeto 1: Alejandro Salazar Sanabria
6	**Entendimiento de roles y responsabilidades.**	Va de la mano con modelos de gobernanza, las líneas de defensa internas y externas, ejercicios para garantizar que cada quien desempeñe su rol de acuerdo con las expectativas dadas.
14	**Acciones o recomendaciones para atacar los desafíos de los perfiles de los clientes.**	Cuidar información sensible, no dar información a terceras personas, para las entidades implementar segundos o hasta terceros factores de autenticación.

Fuente: Entrevista de elaboración propia para tesis

Tabla 6
Resultados de la segunda variable de estudio derivados de la entrevista aplicada a los expertos

Ítem	Reactivo	Sujeto 2: Luis Carlos Hernández
2	**Impactos financieros y no financieros más significativos.**	Las entidades financieras siempre están propensas a fraudes, por lo tanto, tienen pólizas por ejemplo para ciberincidentes o tarjetas, pero el impacto más importante es la imagen, al estar en competencia si una entidad está fallando o hay una inseguridad por parte de los clientes, podría provocar que ellos busquen moverse a otras entidades. La seguridad se vuelve algo inherente en los servicios.
5	**Manejo del talento humano.**	Según la ISO 27001 hay un aspecto básico que es la segregación de funciones, exista un ejecutor y un aprobador. Existe algo llamado conociendo al cliente y otro conociendo a los empleados, este último perfila a el empleado sin violentar su privacidad de manera tal que permita darse una idea de si esa persona vive realmente acorde con sus ingresos, pero también permite a las entidades financieras verificar que no exista ningún tipo de financiamiento al ciberterrorismo.
6	**Entendimiento de roles y responsabilidades.**	Tener una unidad de control interno donde se defina claramente los perfiles y se analicen, que no exista concentración ni técnica ni comercial, que haya una adecuada segregación de roles y responsabilidades. Es importante tener pruebas de que los empleados entienden sus funciones si reciben capacitación hacer pruebas que garanticen que la persona entendió y que se puedan tener sanciones en caso de fallas, hay normas que son de acatamiento obligatorio.
14	**Acciones o recomendaciones para atacar los desafíos de los perfiles de los clientes.**	Adaptar nuevas tecnologías, neuro análisis, inteligencia artificial que permite automáticamente diseñas y asignar perfiles a los usuarios de acuerdo con el perfil que tienen o que van desarrollando acorde con las transacciones que realiza, ir lo más rápido posible conforme se vaya moviendo las necesidades y desafíos tecnológicos y poder dar opciones a los usuarios.

Fuente: Entrevista de elaboración propia para tesis

Para la segunda tabla, se muestra el detalle de las respuestas dadas por los expertos en función de la segunda variable sobre los impactos financieros y no financieros, que puedan afectar más a las entidades financieras.

Ambos expertos están de acuerdo en que más allá de cualquier impacto financiero que puedan sufrir las entidades financieras, el que peores consecuencias tiene es sobre la imagen, esto porque en este sector la confianza lo es todo, por lo tanto, si los clientes personas o empresas no sienten que su dinero está siendo bien administrado es muy probable que muchos de ellos busquen la competencia donde sí les briden ese respaldo y confianza que necesitan, y esto puede ser incalculable para una empresa.

Para el gerente de Gestión de Riesgos, la Alta Gerencia e incluso la Junta Directiva tienen la idea sobre los empleados que trabajan en esta industria y es simple, dan por un hecho que ellos se deben comportar con alta integridad y profesionalismo, y sin duda esto es cierto, pero a la vez se deben asegurar de realizar ejercicios para garantizar que esto se esté dando.

Para el gerente de Seguridad de la Información, existe una nota sobre lo que establecen estándares internacionales con respecto a la segregación de funciones, además de un programa llamado Conozca a su Empleado, de manera tal que, sin violentar la privacidad de los ellos, se logre establecer un perfil de quién es esa persona que trabaja en una entidad financiera, si es apto, o por lo contrario está ligado a grupos organizados en general o con el ciberterrorismo.

Sobre la misma línea de entender los roles, ambos expertos coinciden en que se debe tener un adecuado modelo de gobernanza o Unidad de Control Interno, de manera tal que se tengan claras cada una de las responsabilidades que cada puesto de trabajo debe desempeñar, que no exista concentración ni técnica ni comercial, donde se puedan realizar pruebas o ejercicios que prueben que cada persona está desempeñando su trabajo acorde con las expectativas definidas para ese puesto.

Algo importante sobre los impactos financieros y no financieros es precisamente conocer el perfil de los clientes y las recomendaciones que los expertos puedan dar, los enfoques dados son un poco diferentes; sin embargo, ambos atacan distintas necesidades que este sector debe enfocarse, por un lado está el cuidar la información sensible que viene de la mano de los ataques de ingeniería social y la excesiva confianza que los costarricenses tienen; por otro lado, uno de los expertos busca la modernización donde se utilicen herramientas como inteligencia artificial y neuro análisis, de manera tal que se creen perfiles que estén alineados a las necesidades de cada cliente, que sean específicas y que se agreguen o quiten funciones automáticamente conforme al uso que cada cliente les dé a los servicios ofrecidos por la entidad financiera.

Análisis documental

Los ciberataques pueden afectar a las organizaciones de distintas maneras y van a variar de acuerdo con la naturaleza y severidad de este, algunos tendrán una manera bien conocida de

medir su impacto financiero, pero otros están más asociados a costos intangibles que son más complejos de cuantificar y que en ocasiones no se hacen de conocimiento público, (Deloitte, 2022).

El impacto financiero a causa de una falla materializada en alguno de los controles proviene o está dado por el valor del riesgo del activo que es vulnerado (Hubbard, *et ál*, 2016), sin embargo, la Organización de Estados Americanos en conjunto con la AsoBancaria de Colombia desarrollaron un estudio el estudio Desafíos del Riesgo Cibernético en el Sector Financiero para Colombia y América Latina (2019), y "*El 37% de las organizaciones aún no han estimado el impacto financiero de un ataque cibernético*".

La normativa 2-10 v20 (2022) de la SUGEF con respecto a la gestión de riesgos, procura dejar claro que la identificación de posibles impactos es una tarea esencial para las entidades financieras costarricenses, especificando dentro de las funciones del Comité de Riesgos, donde aparte de realizar un monitoreo sobre la exposición de tal situación y las acciones necesarias para mantenerlos dentro del apetito de riesgo, es que debe dar cuentas a la Junta Directiva sobre los impactos que puedan ocurrir sobre la estabilidad y solvencia de la entidad.

Otro modo de medir el impacto para dar respuesta y recuperación ante un incidente de Ciberseguridad es medirlo ante su EBITDA (OEA, 2018). De acuerdo con el estudio realizado a distintos bancos en Latinoamérica, para un banco grande promedio el costo equivale al 1,86% con respecto al año anterior, para los bancos medianos es del 1,38% y de un 1,36% para un banco pequeño. Los números sobre los costos totales tanto para dar respuesta a los incidentes como para implementar todas las acciones de recuperación para los bancos grandes, representa alrededor de $5,253,000 USD al año, para los bancos medianos el monto aproximado es $605,000 USD y de $161,000 para los bancos pequeños, desde luego no son cifras menores tomando en cuenta que el giro de negocio de las entidades financieras no es la Ciberseguridad, por lo tanto este tipo de gastos impactan los objetivos estratégicos planteados, principalmente los de la rentabilidad.

Por último, Deloitte da un detalle de 14 factores de impacto para los ciberataques utilizando la analogía del iceberg, donde en la parte de arriba están los costos de los incidentes que son

mejor conocidos o que salen a la luz pública, en contra de la parte de abajo se encuentran los costos invisibles o que tienen menos visibilidad, (Deloitte, 2022).

Tabla 7
14 Factores de impacto de los ciberataques

Por encima de la superficie	Investigaciones técnicas
	Notificación a clientes por incidentes
	Protección a los clientes después del incidente
	Regulaciones y cumplimiento
	Relaciones Públicas
	Honorarios de abogados y procesos legales
	Mejoras en la Ciberseguridad
Por debajo de la superficie	Subida en primas de los seguros
	Incremento costos por solicitud de créditos
	Impacto operacional (disrupción o destrucción)
	Pérdida de relación con clientes
	Pérdida de ganancias por ruptura de contratos
	Desvalorización de la imagen
	Pérdida de propiedad intelectual

Fuente: Elaboración propia con datos estudio Deloitte

En realidad, pueden existir una gran variedad más de costos intangibles y tangibles que están presentes por los impactos ante ciberataques, especialmente si son incidentes graves lo que hace realmente importante tener conciencia de estos.

Análisis e interpretación de resultados de la tercera variable: Principales causas que llevan a la materialización de los riesgos

Esta tercera variable tiene como objetivo detallar los resultados obtenidos sobre las opiniones de los gerentes de Seguridad de la Información y al de Gestión de Riesgos sobre cuáles son

las principales causas por las cuales los riesgos se llegan a materializar en el sector financiero costarricense.

Resultados de la entrevista

A continuación, se describen y analizan los resultados obtenidos para la tercera variable basados en la entrevista aplicada a los expertos:

Tabla 8
Resultados de la tercera variable de estudio derivados de la entrevista aplicada a los expertos

Ítem	Reactivo	Sujeto 1: Alejandro Salazar Sanabria
3	**Importancia del compromiso y valores éticos.**	Es sumamente importante, se debe crear cultura en riesgos y concientización esto es pilar en los bancos, sin embargo, el eslabón más débil sigue siendo las personas, especialmente los clientes.
7	**Mantener actualizado perfil de riesgo.**	Entidades financieras están reguladas por SUGEF y tienen normas que exigen tener el apetito de riesgo claramente identificado y actualizado, el cual es revisado en diferentes comités, alta gerencia y Junta Directiva.
8	**Mecanismos de comunicación de noticias de riesgos de Ciberseguridad.**	Campañas de comunicación para los distintos niveles de detalle de la información y que vaya progresando, se debe tomar en cuenta la transformación digital que se está atravesando, cambio cultural y generacional, tomar en cuenta perfil de los clientes.
9	**Principales razones de materialización de los riesgos.**	No hay seguridad 100% sin embargo, los bancos van muchos pasos adelante a otras instituciones y aun así lo que más afecta al banco son los ataques de ingeniería social, es difícil para un cliente darse cuenta de que un mínimo detalle es suficiente para engañarlo, además antes seguridad se veía más como un gasto y no inversión, pero la pandemia vino acelerar muchas cosas que venían trabajándose hace años.
12	**Perfil educación de riesgos de ciberseguridad de clientes.**	Es complejo, ya que las entidades financieras en su gran mayoría atienden personas de distintas edades, escolaridad, etc., lo que en sí se puede coincidir es que unos están más educados en temas de riesgos y ciberseguridad que otros.
13	**Desafíos para manejo de los perfiles de los clientes.**	Precisamente por la variedad de clientes se deben desarrollar estrategias que vayan enfocadas a cada grupo, que sean constantes y unirse las distintas entidades del sector financiero y de tecnología del gobierno costarricense.

Fuente: Entrevista de elaboración propia para tesis

Tabla 9
Resultados de la tercera variable de estudio derivados de la entrevista aplicada a los expertos

Ítem	Reactivo	Sujeto 2: Luis Carlos Hernández
3	**Importancia del compromiso y valores éticos.**	La extorsión ha estado enfocada en atacar a usuarios del sistema financiero para facilitar ataques informáticos, también hay dos frentes en la superficie de riesgos, los proveedores y los empleados, los proveedores es más crítico el tema de manejo de riesgo porque no se tiene tanto control, con los empleados sí.
7	**Mantener actualizado perfil de riesgo.**	La organización debe definir y comunicar su apetito de riesgo. Gestión de Riesgos y Ciberseguridad deben trabajar muy de la mano que una sea el insumo de la otra, no tiene sentido implementar un control si no está basado en un análisis de riesgo.

Ítem	Reactivo	Sujeto 2: Luis Carlos Hernández
8	**Mecanismos de comunicación de noticias de riesgos de Ciberseguridad.**	Existe varios foros a nivel de la Cámara de Bancos, también la ABC, se dan capacitaciones, se comparten mejores prácticas, consejos, productos, intenta generar sinergia entre el sector, aún hay mucho que trabajar, hay desafíos en cuanto a recursos tanto humanos como financieros.
9	**Principales razones de materialización de los riesgos.**	Los ciberatacantes son más sofisticados, hay grupos con mucha tecnología y recursos, las organizaciones deben ir un paso adelante, pero muchas veces el tiempo no da, los ciber criminales suelen ser más ágiles, más rápidos. Aprender de errores del pasado, por ejemplo, hacer análisis a los proveedores ya que en los últimos años muchos incidentes fueron porque estos no tenían medidas de seguridad acorde para ser proveedor de una entidad financiera.
12	**Perfil educación de riesgos de ciberseguridad de clientes.**	El usuario que utiliza el banco es el eslabón más débil, pero esto implica para las entidades financieras contemplar esto al momento de lanzar nuevos módulos o aplicativos, tener en consideración esas necesidades sin dejar de lado la seguridad y la usabilidad ya que competencia podría tener mejor aplicación de acuerdo con las necesidades de esa entidad.
13	**Desafíos para manejo de los perfiles de los clientes.**	Hay un desafío grande entre la usabilidad de las aplicaciones y la seguridad, puede afectar la experiencia de usuario y perder presencia de mercado.

Fuente: Entrevista de elaboración propia para tesis

Con respecto a la variable para determinar las principales causas que llevan a la materialización de los riesgos, se busca precisamente desde la óptica de los expertos cuáles pueden ser esas causas, tomando en cuenta que las entidades financieras son las que en muchos mercados y Costa Rica no es la excepción, pues están un paso adelante debido al tipo de información que manejan.

Lo primero es poder aclarar la importancia que tienen el compromiso y valores éticos con que las entidades financieras deben predicar, para el Gerente de Gestión de Riesgos, es de suma importancia que las entidades financieras establezcan una cultura de riesgos, pero también es claro que al ser los clientes el eslabón más débil, los esfuerzos también deben enfocarse en esta área.

Sin embargo, el Gerente de Seguridad de la Información detalla un punto interesante y que del poco se habla, la extorsión que puedan verse envueltos los empleados de entidades financieras de manera tal que faciliten información u herramientas para perpetrar ciberataques, sin dejar de lado que aparte de los empleados en los cuales se pueden establecer cierto tipo de controles, también hay otro frente como los proveedores, donde es más complicado el tema de controles, pero de igual manera debe existir un análisis de riesgos para saber en nivel de compromiso y valores que ellos tengan, y que estén alineados a los de la entidad financiera al menos en la medida que no representen un conflicto para ellas.

Haciendo referencia al perfil de riesgo, existen criterios de convergencia y otros donde difieren un poco, por ejemplo, para el Gerente de Gestión de Riesgos, las entidades financieras al estar reguladas por SUGEF y otras superintendencias, deben cumplir con las normas establecidas con respecto a la identificación del apetito de riesgo, que esté debidamente identificado y actualizado. El Gerente de Seguridad de la Información también considera que las organizaciones deben definir su apetito de riesgo, para esto, tienen que trabajar en conjunto con el comité de Gestión de Riesgos y Ciberseguridad que ambos sean insumos uno del otro, estableciendo controles que estén acorde con los resultados de un análisis de riesgo.

Sin duda alguna es importante mantener al personal informado sobre los principales riesgos que pueden estar afectando a una entidad financiera y la manera de prevenirlos, con respecto a esto, el Gerente de Gestión de Riesgos comenta que las campañas deben ir dirigidas por niveles y que se vaya progresando tomando en cuenta la transformación digital que están viviendo las entidades financieras, así como los cambios culturales de la sociedad costarricense, especialmente con las nuevas generaciones que son más tecnológicas.

Por su parte, el Gerente de Seguridad de Información, profundiza más en foros con que las entidades financieras cuentan y que son colaborativos entre entidades del mismo sector, donde se comparten mejores prácticas, consejos, y se logra generar una sinergia ya que el problema de una entidad bien puede ser el de la otra.

Es seguridad de la información hay una premisa y es que nada es 100% seguro, sobre lo cual el Gerente de Gestión de Riesgos hace énfasis en este punto pero a la vez asegura que las entidades financieras deben estar un paso adelante y lo están con respecto a otras entidades principalmente del Gobierno, pero el mayor problema sigue siendo el cliente, el eslabón más débil, aquella persona que fácilmente es engañada o que no distingue que el sitio *web* no es realmente el de la entidad financiera sino más bien uno falso y las diferencias pueden ser mínimas. La pandemia del COVID-19 aceleró la adopción de tecnologías que se venían trabajando por años lo cual cambia el enfoque de inversión en seguridad y deja de verse como un gasto.

Según el Gerente de Seguridad de la Información, los ciberataques son más elaborados, pues hay grupos organizados con mucha tecnología y recursos, lo que debe provocar que las organizaciones procuren estar un paso adelante, pero aquí el factor tiempo es determinante y gana la batalla en muchas ocasiones, ya que los cibercriminales en eso suelen actuar más rápido.

Tanto se menciona el tema del eslabón más débil que son los clientes del banco que es importante conocer las opiniones de los expertos sobre el perfil de educación en temas de riesgos en Ciberseguridad, para el Gerente de Gestión de Riesgos establecerlo es un poco complejo debido a la diversidad de clientes que atienden, pero sí es cierto que unos están más educados que otros.

Con la misma referencia al eslabón más débil, el Gerente de Seguridad de la Información hace énfasis en que las entidades financieras deben contemplar las diferencias entre los grupos de clientes al momento de lanzar nuevos módulos o aplicativos, se debe considerar las necesidades de todos los grupos sin dejar de lado la seguridad y la usabilidad, ya que si no hay un equilibrio y la competencia tiene mejores funcionalidades, esto puede provocar incluso que los clientes prefieran utilizar más una entidad que otra.

Por último, en cuanto a los desafíos de los perfiles de clientes, debido a la diversidad que manejan las estrategias deben enfocarse en contemplar cada uno de esos grupos, y tienen que considerarse estrategias que sean constantes y lo importante que se unan distintas organizaciones en un frente común, sin dejar de lado la usabilidad de las aplicaciones y la seguridad; por lo tanto, las mejores deben ir de la mano con la experiencia de usuario de manera tal las aplicaciones sean de valor agregado y no algo imposible pero seguro de usar.

Análisis documental

El sector financiero continúa siendo uno de los objetivos más buscados por cibercriminales, y las razones principales son la cantidad y tipo de información que manejan de los clientes.

Según Verizon (2020), esta industria sigue como una de las preferidas por las motivaciones financieras de los grupos de crimen organizado. El mismo estudio muestra cómo es realmente preocupante que la cantidad de errores de los empleados es casi igual a las razones de causas

de los ataques por razones externas, que son las que normalmente están atacando a las entidades financieras.

Según el estudio de la OEA sobre el estado de la Ciberseguridad en el sector bancario en América Latina y el Caribe, como resultado de los planes de gestión de riesgos en seguridad de la información, 41% de las entidades bancarias realizó evaluaciones de madurez que les permiten tener los insumos para las acciones que deben tomar sobre las áreas de mejora.

Sin embargo, el estudio detalla que las entidades que no logran hacer este tipo de evaluaciones dan razones como insuficiencia de personal y falta de presupuesto, que son motivos muy importantes por las cuales también los riesgos siguen materializando si no se invierten recursos humanos especializados y en mejoras tecnológicas.

Para IBM en su estudio anual de *X-Force Threat Intelligence Index* (2022) para el tercer trimestre del 2021, los ataques de *phishing* y de ingeniería social continúan teniendo gran éxito con el 43% de los ataques.

En Costa Rica, la SUGEF mediante el reglamento 14-17 (2020), dentro del marco de Gestión de TI, establece en su punto 4.3 Gestionar Problemas, que se deben "*Identificar y clasificar problemas y sus causas raíz y proporcionar resolución en tiempo para prevenir incidentes recurrentes. Proporcionar recomendaciones de mejora*", (p. 32) de manera que les permitan a las entidades financieras contar con un procedimiento para tener visibilidad de este tipo de desviaciones, llevar el control con respecto a los umbrales del apetito de riesgo establecido e informar a la gerente y al comité de riesgos oportunamente (SUGEF 2-10, 2022).

Análisis e interpretación de resultados de la cuarta variable: modelo de mejores prácticas para la administración de riesgos

La cuarta variable tiene como objetivo detallar los resultados obtenidos de la aplicación de la entrevista.

Resultados de la entrevista

A continuación, se describen y analizan los resultados obtenidos para la última variable, es importante que para esta no se presentan ítems específicos, sino más bien en toda la información brindada por los expertos y que sirvieron de análisis para las anteriores variables.

- Los expertos identifican que pese a que las entidades financieras son sujetas a un gran número de ciberataques, el eslabón más débil sigue siendo las personas, ya que los controles tecnológicos pueden hacerse cargo de cierto tipo de riesgos, pero ante el ser humano es más complicado e incluso obliga a pensar en capaz de autenticación para lograr solventar el problema, pero sin duda ante las decisiones que tomen los clientes de dar su información ante engaños es poco el campo de acción.
- También existe una necesidad más allá de las regulaciones a las que se ven sujetas las entidades financieras de mantener actualizadas sus políticas, procedimientos, reglamentos y otros documentos importantes, pero lo que va variar es el tipo de documentos, ya que se tienen algunos que no deben ser sujetos a mayores cambios porque no es su naturaleza, por ejemplo políticas; sin embargo, se deben revisar cada vez que exista un incidente grave de seguridad independientemente si el afectado directo es la misma entidad, ya que en el sector financiero pueden ser muchas las similitudes entre sí.
- Ambos expertos coinciden en que la eficacia del modelo de gobernanza que tenga una entidad financiera va de la mano con su grado de madurez, ya que este le permite ir avanzado en el grado de refinamiento de los controles que implementen en todos los niveles.
- Los impactos sobre la imagen y reputación de las entidades financieras son las principales preocupaciones para los expertos. El negocio de las entidades financieras está basado principalmente en la confianza y si no existe, los clientes pueden optar por mover su dinero a donde sí se les brinden la tranquilidad de que está bien administrado.
- Los expertos son bastante enfáticos en resaltar la necesidad de establecer controles adecuados para contrarrestar las vulnerabilidades que el eslabón más débil representa; sin embargo, uno apunta más por incorporar nuevas tecnologías y automatización y

el otro sigue abogando por mejorar la concientización de estos temas y sensibilizar a los clientes de lo importante de no compartir la información sensible de sus cuentas.

- En cuanto a las razones de la materialización de los riesgos, los puntos de vista que se comparten, están alineados con la realidad que se enfrenta este tipo de sector, pues la seguridad 100% efectiva no existe, no hay de momento ningún control, tecnología en fin nada que logre garantizar que ningún riesgo se va a materializar, por lo que obliga a todas las organizaciones a procurar estar un paso adelante, echar mano de nuevas tecnologías que permitan establecer controles más eficientes y proactivos que bien no puedan estar en la misma línea de los ciberatacantes donde se pueda prever el siguiente ataque, pero sí al menos hacer que las cosas sean más difíciles o mejor que logren desincentivar a los ciberatacantes.

Análisis documental

Para la última variable, el análisis documental no se detalla en esta sección del trabajo de investigación, esto se debe a que el modelo de mejores prácticas para la administración de riesgos supone la base para desarrollar el capítulo seis; en este, se desarrolla la propuesta propia de esta investigación.

Cabe resaltar que el modelo de mejores prácticas se basa en los marcos de referencia internacionales como COSO (2012), ISO 27001 (2013), ISO 31010 (2019) y desde luego la reglamentación existente por parte de la SUGEF (2-10, 2022) y (14-17, 2020).

Como parte de la reglamentación establecida en Costa Rica, es necesario que las entidades financieras reguladas por la SUGEF cuenten con procesos adecuados para la identificación y tratamiento de los riesgos de acuerdo con el tamaño, complejidad y realidad de cada entidad y que permitan establecer los requerimientos mínimos que permitan la implementación y mantenimiento de un proceso de esta índole.

Capítulo V

Conclusiones y recomendaciones

Conclusiones

Una vez que se concluye las etapas de recolección de datos, análisis de la información documental, así como la recolectada durante las entrevistas, se requiere documentar las conclusiones alcanzadas durante esta investigación sobre el análisis de los riesgos en Ciberseguridad y sus impactos financieros y no financieros en las entidades financieras costarricenses.

Las conclusiones se presentan por orden de las variables definidas en esta investigación, por lo que siguen el mismo orden con el que se desarrollaron en el capítulo anterior; por lo tanto, las conclusiones correspondientes a la primera variable sobre identificar los riesgos de Ciberseguridad son las primeras en desarrollarse, posteriormente, las conclusiones referentes a identificar los impactos financieros y no financieros que corresponden a la segunda variable. Por último, aparecen las conclusiones sobre los hallazgos obtenidos de la tercera variable sobre determinar las principales causas que llevan a la materialización de los riesgos.

Cerrando esta parte, se documentan las conclusiones generales, tomando en cuenta los resultados finales que se logran obtener durante toda la investigación de acuerdo con las variables y objetivos definidos al inicio, por lo que es importante tener presentes las entrevistas y el análisis documental.

Conclusiones de la primera variable: riesgos en Ciberseguridad

A continuación, se documentan las conclusiones relacionadas con la primera variable de esta investigación y que se trata sobre el análisis de riesgos en Ciberseguridad.

- Sin lugar a duda, los ciberataques en general son una gran amenaza en una era donde la digitalización de muchos sectores da paso a grandes avances, pero también implica grandes retos. Dentro de todos los posibles ataques existen algunos que tienen más probabilidades de ser más satisfactorios, por lo tanto, se concluye que para el sector financiero la principal amenaza es el ataque de ingeniería social.
- Por otra parte, los marcos de referencia internacionales sobre manejo de riesgos (COSO, 2012), Gestión de Riesgos (ISO 31010, 2019) o de seguridad (ISO 27001, 2013), dan guías sobre los manejos de la documentación que se requiere para una

adecuada gobernanza. La administración de riesgo es un proceso esencial para identificar, medir, evaluar y reportar las amenazas que cualquier organización se ve expuesta (Estupiñán, 2015). Con base en las respuestas dadas por los expertos, se logra determinar que las entidades financieras al menos cumplen con las prácticas que estos marcos sugieren.

- Con temas de comunicación de riesgos que están presentes en las entidades financieras, se infiere que no existe un proceso que esté alineado a las necesidades de estas entidades, ya que ambos expertos tienen opiniones muy diferentes y esto es particularmente importante, ya que hay reglamentación y regulaciones que se deben cumplir.
- Establecer controles es una de las acciones más importantes dentro de cualquier sistema, por lo tanto, el proceso para su administración es esencial, a partir de lo recabado en esta investigación se logra concluir que se debe contar con una adecuada gobernanza en el proceso de administración de controles para que se logre garantizar su correcta funcionalidad, reporteo y análisis de resultados.

Conclusiones de la segunda variable: impactos financieros y no financieros

- Hay sectores dentro de las economías de todos los países que a nivel de riesgos pueden ser muy similares y su impacto y probabilidades si bien pueden ser diferentes, su impacto real va a estar marcado por su giro de negocio. Hay otras que ni tan siquiera han estimado el impacto financiero de un ciberataque (AsoBancaria, 2019). Para un sector como el financiero el impacto que todos pueden pensar es el económico que pueden sufrir si son víctimas de un ciberataque, si bien esto es cierto, existe otro que es más relevante, ya que su materialización desencadena en otros impactos indirectos de gran proporción; por lo tanto, se concluye que el impacto a nivel de imagen en un negocio donde la confianza significa todo, pues es el principal impacto al que se ven expuestas las entidades financieras.
- Se viene mencionando sobre el eslabón más débil que son las personas, tanto clientes como colaboradores de las entidades financieras, es sobre el segundo donde se puede tener un poco más de control; no obstante, se logra identificar una discrepancia y es que hay una posición riesgosa por parte de la gerencia de suponer que sus empleados

por defecto se deben comportar con integridad y profesionalismo, lo cual es cierto de acuerdo con el alcance de la información que tienen, pero por otro lado, al contar con el programa "Conozca a su Empleado" le permite tener cierta garantía sobre el personal contratado que ayude a identificar si el candidato es o no apto para el rol que estará desempeñando.

- Por otro lado, para que las personas entiendan cuáles son los alcances de sus funciones y así evitar lo más posible los errores humanos por falta de capacitación y que puedan desencadenar en impactos importantes para las entidades, se concluye que mantener una gobernanza o Unidad de Control Interno es requerido de manera tal que se tengan claras las responsabilidades de cada uno de los puestos dentro de las entidades financieras y que se logren detectar y corregir concentración de puestos, conflictos de intereses y que las personas se estén desempeñando conforme las expectativas del puesto.
- Un aspecto importante dentro de toda organización, independiente del sector en que se desarrollen es el talento humano, contar con una adecuada estrategia que permita seguir buscando talento humano, con nuevas capacidades, que permita dar una idea de cómo está el mercado y seleccionar las personas que ingresan a la compañía, cómo se desarrollan y se logran retener de manera tal que no cause un impacto en alguna área donde el perfil se desarrolla de tal forma que pueda crear una dependencia en una u otra persona, con base en la información que se brinda por parte de los expertos, no se logra concluir de manera precisa si cuentan con este tipo de estrategias y cómo están implementadas.
- Para poder tener un mejor entendimiento de los impactos a los que se ven expuestas las entidades financieras, se debe conocer el perfil de clientes que tienen dentro de sus carteras, por lo tanto, se concluye que el no hacerlo puede provocar no tener claridad sobre los controles y perfiles más adecuados que se deben otorgar de manera tal que el acceso o funciones son estrictamente relacionadas y limitadas a las necesidades individuales de cada cliente.
- Por último, el lograr cuantificar los impactos financieros se puede tornar una tarea difícil, puesto que se debe evaluar el área afectada, esto dada la versatilidad de servicios que brindan las instituciones financieras; sin embargo, se logra concluir que

los principales impactos financieros a los que se ven expuestas este tipo de entidades están relacionados con principalmente el dinero que pueden dejar de percibir como resultado de un ciberataque, ya sea por cuenta de las comisiones que se dejan de cobrar, ya que un cliente decida ir a otro banco a realizar el trámite que no logra hacer en la entidad afectada, los costos de oportunidad por negocios que no se consiguen cerrar. Firmas de créditos o incluso el no poder cobrar intereses por tener su plataforma fuera de servicio.

Conclusiones de la tercera variable: causas que llevan a la materialización de los riesgos

- El negocio de las entidades financieras gira entorno a la confianza, si esta se rompe van a estar expuestas a una serie de malas y graves consecuencias y la confianza empieza desde adentro; por lo tanto, se determina que el compromiso y valores éticos de sus empleados es sumamente importante para salvaguardar ese pilar por el cual gira un elemento vital para la consecución de objetivos estratégicos y sostenibilidad de las entidades financieras.
- Para lograr determinar qué nivel de riesgo están expuestas las entidades financieras y en general cualquier organización, pero se debe tener claro contra qué se está midiendo. Para esto se debe definir el perfil de riesgo o apetito de riesgo, las entidades financieras en Costa Rica se rigen bajo las regulaciones de ley y reglamentos establecidos por las distintas superintendencias, y debido a esto, se logra concluir que existen los mecanismos correctos para definir ese perfil y mantener actualizado ese perfil y que es una labor en conjunto de Gestión de Riesgos y Ciberseguridad.
- El cómo se reciben la información sobre los principales riesgos a los cuales están expuestas las organizaciones, genera cultura y entendimiento de lo importante que es el trabajo que cada persona realiza, el mensaje debe ser claro y principalmente aplicable para la función que se es responsable, de aquí que se logra inferir que las comunicaciones sobre riesgos en Ciberseguridad deben adaptarse a cada área dentro de las organizaciones y, además, es de suma importancia y da un valor agregado el hecho que las organizaciones del mismo sector se intenten unir en frentes comunes para atacar problemas que son del interés de ellos.

- En seguridad de la información existe una premisa y es que no hay nada 100% seguro; sin embargo esto no limita el hecho de que las organizaciones deban estar preparadas y establecer controles necesarios de acuerdo con sus necesidades y apetito de riesgo, y con base en esta premisa, se concluye que los controles no siempre alcanzan cuando se está frente al eslabón más débil como son las personas, y el campo de acción se limita a las decisiones que estos toman, por otro lado también se logra inferir que uno de los factores que más logra influir en la conclusión de ataques son los avances en tecnología de los grupos organizados, los cuales logran actuar con mayor prontitud en sus ataques en comparación con la velocidad que lo hacen las organizaciones en su afán por defenderse.
- Para las entidades financieras existe un desafío complejo en cuanto a la determinación de qué tan educada está su cartera de clientes en temas de Ciberseguridad y de riesgos en general; por lo tanto, se logra identificar que debido a lo heterogéneo de sus carteras se hace difícil la tarea de establecer ese nivel, lo que impacta en tener más insumos para lograr determinar las causas por las cuales los riesgos se siguen materializando por consecuencia de sus clientes.
- Complementando el punto anterior, se logra concluir que las estrategias deben estar enfocadas dependiendo al grupo en el cual se consiguen categorizar teniendo un balance entre usabilidad de las aplicaciones y la seguridad, con el fin de no perder ventaja competitiva con respecto a los otros competidores.

Conclusiones de la cuarta variable: modelos mejores prácticas para la administración de riesgos

Para esta sección, al tratarse de la última variable la cual está directamente relacionado con la propuesta de esta investigación y, por lo tanto, recopila toda la información que se concluye de las anteriores variables, y siendo así se procede a detallar las conclusiones generales que dan sustento a la investigación.

Conclusiones generales

- Pese a la gran cantidad de ciberataques que una entidad financiera pueda verse expuesta y los controles tecnológicos e inversiones que se realicen, lo cierto es que el

problema principal sigue siendo las personas, tanto clientes como personal, donde el campo de acción se limita a las acciones que estos tomen y que pueda estar influenciada por el nivel de educación y conciencia de las consecuencias de las acciones que estén por tomar.

- La documentación requerida por regulación o por estar en cumplimiento con algún marco de referencia internacional es de suma importancia; por lo tanto, se deben tener procesos claros sobre la regularidad en que estos documentos se actualicen tomando en cuenta el nivel de este y que existan mecanismos de revisión de documentos para cuando se es víctima de un ciberataque.
- Sin importar los controles que se establezcan o incluso por qué se implementaron, es claro y determinante que sin un modelo de gobernanza adecuado no se logra cumplir el fin último, que es garantizar que estén en el lugar correcto, que se midan y sus resultados tengan la visibilidad que se requiere de manera tal que se puedan tomar decisiones prontas.
- La confianza pueda que sea fácil de ganársela y en muchas ocasiones se da por sentada; sin embargo, para las entidades financieras este aspecto es muy complicado ya que su negocio se basa en este principio, y una falla va a desencadenar en consecuencias que pueden ser incalculables.
- Ante el mundo de las tecnologías de información y principalmente con la digitalización de sectores como el financiero, se vuelve complejo y difícil para las entidades financieras lograr mantener sus líneas de defensa, de tal manera que se vaya de la mano con estos grandes avances, limitaciones de presupuestos, expertos y hasta de recursos hacen que la materialización de riesgos sea una constante en algunos riesgos.

Recomendaciones

Una vez elaboradas las conclusiones en el capítulo anterior para cada una de las variables definidas, así como las conclusiones generales, es el turno de desarrollar las recomendaciones correspondientes a la presente investigación basada en el análisis de riesgos en Ciberseguridad y sus impactos financieros y no financieros en las entidades financieras costarricenses.

El orden de desarrollo de las recomendaciones está en completo apego al mismo que se define en las conclusiones, por lo tanto las recomendaciones para la variable sobre la identificación de riesgos de Ciberseguridad se desarrollan de primero, seguido de las conclusiones relacionadas con la segunda variable sobre identificar los impactos financieros y no financieros, y después están las recomendaciones para la tercera variable relacionadas con las causas que llevan a la materialización de los riesgos.

Por último, se documentan las recomendaciones generales basadas en todos los elementos estudiados y analizados en los distintos capítulos, todas estas sirven de guía para la elaboración de la propuesta que se documenta en el capítulo seis, planteando un modelo de mejores prácticas para la administración de riesgos en Ciberseguridad.

Recomendaciones de la primera variable: riesgos en ciberseguridad

- En relación con la actualización de las políticas y procedimientos de seguridad, se recomienda a la gerencia y a las Juntas Directivas de las entidades financieras, definir el estándar de un año para todas las políticas de seguridad y de al menos dos veces al año para todos los procedimientos de seguridad para los distintos departamentos, donde se establezca un control de versiones con su respectiva fecha de próxima revisión, y que el tema de revisión de documentos esté incluido dentro de la agenda del Comité de Riesgos.
- Adicionalmente a la recomendación anterior, se insta al Comité de Riesgos solicitar a todos los departamentos de manera proactiva, la revisión de estos documentos cada vez que exista un incidente grave de seguridad, ya sea interno o que acontezca en alguna otra entidad del sector, por medio de una solicitud formal dirigida al área responsable de la actualización de los documentos que requieren ser actualizados.
- En tiempos de crisis normalmente lo que se deja más de lado es el qué y cómo comunicar lo que acontece, ocurre tanto a lo interno como hacia todo ente externo de las organizaciones y uno de los grandes desafíos es no generar especulación en general de manera que los distintos interesados como clientes, empleados, proveedores, inversionistas y otros, no tomen decisiones por falta de información. Por lo tanto, se sugiere a la gerencia y a las Juntas Directivas de las entidades financieras en conjunto con los departamentos de comunicaciones, definir un protocolo de

comunicación para incidentes de seguridad conformado por las áreas antes mencionadas, así como las de Ciberseguridad, Gestión de Riesgos, Tecnología de la Información, donde se define qué se va a comunicar, a nombre de quién se hace el comunicado, a quiénes, y los medios donde se publican y la periodicidad de estos.

- Dentro de los modelos de gobernanza es importante que se mida el nivel de madurez de la organización, así como de los distintos departamentos, con el objetivo de que se planteen las acciones necesarias sobre los controles de seguridad, por lo tanto, se recomienda a la gerencia aplicar modelos para medir y determinar el nivel deseado de madurez para cada uno de los procesos críticos del negocio y así lograr conseguir una adecuada gobernanza sobre los controles de seguridad existentes o que se requieran instalar.
- La búsqueda de talento humano no debe limitarse únicamente cuando se tiene alguna necesidad por llenar una vacante, es una búsqueda constante que permita al equipo de reclutamiento valorar las nuevas capacidades y conocimientos que la oferta laboral está mostrando, por lo que se recomienda al equipo de reclutamiento hacer búsquedas constantes de perfiles en plataformas como LinkedIn en las distintas áreas de Ciberseguridad y en conjunto con el área respectiva valorar cuáles de esas habilidades pueden ser valiosas para la organización.

Recomendaciones de la segunda variable: impactos financieros y no financieros

- Es importante contar con toda la información disponible para realizar análisis cuantitativos sobre los impactos financieros producto de ciberataques; por lo tanto, se recomienda al equipo de Gestión de Riesgos, realizar análisis cuantitativos sobre los impactos financieros tomando como base la estimación de pérdidas económicas por interrupción de los servicios críticos del banco los cuales deben ir alineados con el tiempo objetivo de recuperación y del objetivo de punto para recuperarlos se pasa a los documentados en el plan de recuperación y de continuidad de negocios, esto también se puede aplicar por unidad de negocio en caso de que se deba evaluar por unidad de negocio en lugar de toda la organización.

- Existen amenazas que desafortunadamente vienen desde adentro de las organizaciones, y sin importar el sector donde se desempeñe deben existir mecanismos para tener un control adecuado sobre los accesos y trabajos que realizan los empleados; por esta razón, se plantea a la gerencia y a las Juntas Directivas de las entidades financieras, reforzar el programa "Conozca a su Empleado".
- Si bien es cierto es de suma importancia contar con el perfil de las personas como parte de este programa, se debe tener la documentación sobre cómo se están evaluando, que logre identificar si las áreas de desempeño están acordes con el rol, y que se incluya los ejercicios de prueba relacionados con Ciberseguridad, y que se sepa cuáles son los resultados esperados y constatarlos con los obtenidos e incluir sesiones de realimentación. Estas evaluaciones se deben hacer al menos dos veces al año.
- El desarrollo del talento humano es un aspecto fundamental en todas organización, la falta de una estrategia de selección, desarrollo y retención de personal pensado desde el punto de vista de seguridad es importante para asegurarse que no se esté seleccionando a la persona equivocada o que no se sea capaz de darle las herramientas de conocimiento necesarias o crear dependencias o concentración de conocimiento en unos pocos que genere un riesgo si esa persona decide irse de la compañía, por lo que se recomienda a la gerencia y a la Junta Directiva complementar con una estrategia de administración del talento humano contemplando aspectos de seguridad dentro de los perfiles o manual de puestos, y que se realicen revisiones al menos una vez cada seis meses, con el fin de establecer si existe algún riesgo con el personal activo.
- Existen otras amenazas que vienen desde afuera, y uno de los más comunes y que se menciona como el eslabón más débil o sea los clientes, requiere una atención especial por parte de las entidades financieras, por lo que se recomienda a los departamentos de Tecnologías de Información y Ciberseguridad implementar controles de asignación de roles dentro de las aplicaciones mediante la utilización de herramientas de inteligencia artificial, análisis de datos y de "*machine learning*", de manera tal que los accesos a las aplicaciones o módulos de las entidades financieras estén dados de manera automática y acorde con el perfil de cada usuario y sus comportamientos dentro de los sistemas de estas y utilizando fuentes alternas de información

estructurada y no estructurada, para tener un perfil de riesgo más acertado; esto se debe balancear con la usabilidad y experiencia de usuario para que no provoque un efecto adverso y que el uso de la aplicación es muy segura pero poco usable.

Recomendaciones de la tercera variable: causas que llevan a la materialización de los riesgos

- Para las entidades financieras saber que su negocio se basa en la confianza representa un desafío importante, por lo que el compromiso y valores éticos con que trabajen ayuda de cierta manera a asegurarse que sea menos probable algún desliz de sus colaboradores, de esta manera se insta a la gerencia y a las Juntas Directivas de las entidades financieras reforzar su compromiso de crear cultura ante los riesgos en general, pero en especial en Ciberseguridad, mediante ejercicios periódicos de pruebas como reconocimiento de correos tipo phishing, campañas de concientización por ejemplo crear un mes dedicado a detección temprana de fraudes y mejoramiento de aspectos de Ciberseguridad en general para todos los empleados, y establecer mecanismos internos y confidenciales para reporte de anomalías relacionadas con posibles conductas fraudulentas.
- La recomendación anterior se enfoca principalmente en los empleados; sin embargo, también se identifica otra necesidad casi igual de importante y tiene que ver con manejo de proveedores y los controles que se tienen para el manejo de estos, por lo tanto, se sugiere a la administración y Junta Directiva junto con el Comité de Riesgos, establecer un marco de referencia interno de administración de proveedores, donde se establezcan los puntos de control que cualquier proveedor debe cumplir y que estos tienen que proveer la información que respalde dichos controles para verificar si realmente los tienen o no, y que esta revisión sea un requisito obligatorio antes de establecer alguna relación comercial, por ejemplo adjudicar una licitación.
- La capacitación es, sin duda, una arma que las entidades poco utilizan y se suele subestimar y en ambientes tan cambiantes como las tecnologías de información es indispensable que los distintos departamentos de Tecnologías de Información y especialmente Ciberseguridad se encuentren capacitándose constantemente en las mejores prácticas para la identificación, contención y resolución de ciberataques, por

lo que se recomienda a la gerencia, desarrollar un plan de capacitación constante mediante alianzas con las universidades que actualmente están más a la vanguardia en capacitaciones en Ciberseguridad como Lead University y Cenfotec que ya cuentan con programas y técnicos en Ciberseguridad.

- Se tiene claro que toda organización, incluso las del sector financiero, deben tener su apetito o perfil de riesgo claramente definido, las entidades financieras en Costa Rica al estar reguladas por SUGEF así como otras superintendencias, deben cumplir con reglamentos y leyes que solicitan tener esto correctamente documentado y aprobado; por lo tanto, se sugiere al Comité de Riesgos continuar con el fortalecimiento de las revisiones de los riesgos definidos actualmente, asegurándose de tener dentro de la agenda la revisión de estos al menos una vez cada tres meses o, ante un incidente severo de seguridad, tanto interno como que aquellos donde otras entidades del sector sean los afectados donde se pueda establecer si el nivel de riesgo es el mismo o se establecieron controles adicionales que reduzcan el perfil respectivo.
- Las comunicaciones y como se comparte la información sobre riesgos en Ciberseguridad si bien ayudan a generar cultura y conciencia sobre lo importante que es el trabajo que hacen cada una de las personas en una entidad financiera, también debido a la multiplicidad de funciones, hacen que todos los puestos tengan sus diferencias y particularidades así como sus necesidades sobre qué tipo de información recibir; por lo tanto se plantea la recomendación al Comité de Riesgos que se implemente una estrategia de comunicación que esté dirigida a cada departamento de acuerdo con sus necesidades e intereses en cuanto al alcance de sus funciones, mediante el envío de comunicados, reuniones mensuales o trimestrales, boletines y los fondos de pantalla de los equipos con consejos de cómo mejorar la seguridad en sus funciones.
- Asimismo, se recomienda al equipo de Ciberseguridad y Gestión de Riesgos la conformación de un Comité de Ciberseguridad, para que sirvan de puente con otras entidades financieras a fin de reforzar los canales de comunicación interinstitucionales, de manera tal que les permita recibir e intercambiar información y que sirva de insumo para estrategias de comunicación interna.

- Sin duda alguna parte de los resultados de esta investigación muestran cómo la vulnerabilidad más fuerte que tienen las entidades financieras está del lado de los clientes y los controles tecnológicos y de factores de autenticación múltiple no son suficientes cuando se depende de las decisiones que toma un cliente en dar su información sensible como consecuencia de un engaño, por lo que ante este panorama se insta a la gerencia y a las Juntas Directivas a continuar desarrollando campañas de concientización para sus clientes, pero que estén enfocadas al perfil de cada uno, pues debe ser entendible para todos los niveles y tipos de clientes que manejan las entidades financieras, enviando comunicados a los correos electrónicos, mediante publicaciones en las redes sociales oficiales, en las entradas de las oficinas virtuales y físicas donde personas les hagan compartan información breve y con infografía.
- En cuanto a los controles tecnológicos se sabe que los ciberdelincuentes van un paso adelante e incluso cuentan con mejores herramientas para burlar los controles que se establezcan tanto en la red perimetral como en los equipos locales, si bien las entidades financieras están a un paso adelante en protección, no hay seguridad 100% infalible y se recomienda evaluar la implementación de herramientas de nueva generación para antivirus, *Firewalls*, soluciones XDR (detección avanzada y respuestas extendidas), SIEM con inteligencias artificial y *machine learning* para agilizar la detección de amenazas, y que todas estas dependen menos de firmas y trabajan más con base en comportamientos.

Recomendaciones de la cuarta variable: modelos mejores prácticas para la administración de riesgos

Para esta sección, al tratarse de la última variable la cual está directamente relacionado con la propuesta de esta investigación y por lo tanto recopila todas las recomendaciones anteriores, y siendo así se procede a detallar las recomendaciones generales de la investigación.

Recomendaciones generales

- Se recomienda a la gerencia, Juntas Directivas y Comités de Riesgos trabajar en la implementación de un plan que les permita identificar tipos de clientes, sus

necesidades en cuanto al tiempo de transacciones y usabilidad de las herramientas con el fin de que se logren establecer mecanismos de control que garanticen que los accesos se dan de acuerdo con los niveles de comprensión y seguridad que se requieren para realizar cierto tipo de transacciones que son consideradas críticas o más propensas a ser utilizadas de forma irregular o ilícita y que sean bloqueadas si no cumplen los criterios de usabilidad.

- Los avances en el refinamiento de los ataques hacen que las organizaciones deban estar un paso adelante, por lo que se sugiere al Departamento de Ciberseguridad adoptar medidas de última generación para detección y control de ciberataques basadas en comportamientos y no en firmas así como la especialización del personal en área claves como *hackeo* ético, identificación de vulnerabilidades, planes de remediación y contención de ataques mediante las certificaciones de entidades con reconocimiento internacional, de igual manera se recomienda estipular en los contratos con proveedores cláusulas que les permitan contar con actualizaciones constantes y flexibles que les permitan realizar cambios en aplicaciones o infraestructura de manera rápida y expedita.
- Cuando existen situaciones de incertidumbre sin duda la falta de comunicación hace que las cosas tiendan a empeorar, por lo que el sector financiero al estar tan expuesto a ciberataques, de manera tal que la gerencia y las Juntas Directivas deban contemplar dentro de sus planes de continuidad de negocios, el plan de respuesta a incidentes o plan de recuperación junto con la conformación de un comité una estrategia de comunicación ante este tipo de situaciones, donde se establezca claramente qué, cómo, quién y a quiénes se comunica lo que está aconteciendo para intentar devolver cierto nivel de tranquilidad a los distintos interesados, entendiendo, a estos como los clientes, proveedores, y socios comerciales entre otros.
- Por último, la gerencia y las Juntas Directivas deben continuar reforzando los valores éticos y gran integridad con la que todas las personas que trabajan en ellas se deben desempeñar, que entiendan lo importante que es el trabajo que realizan, y crear un sentido de pertenencia e identificación con la marca, mediante campañas de comunicación, eventos y canales confidenciales para reporte de anomalías.

Capítulo VI

Propuesta

Introducción

La incursión de nuevas tecnologías, sin duda, ayuda a que cada día se realicen tareas más eficientes y eficaces, incluso existen las que no ya no requieren intervención alguna de un ser humano, la transformación digital por las que atraviesan varios sectores de las principales industrias a escala mundial, así como muchos otros avances de la tecnología a lo largo de la historia moderna representan grandes avances con múltiples ventajas, pero lo cierto es que también tienen importantes desafíos.

Desde finales del 2019, el mundo se enfrenta a un hecho sin presentes que si bien tiene una contribución importante en la aceleración de la revolución industrial 4.1, también enfrenta a las distintas organizaciones a adaptar sus procesos, políticas y procedimientos de manera que se adaptan a la nueva realidad que se vive.

Esos procesos de adaptación también se ven en las áreas de tecnologías y seguridad de la información, donde cada día hay nuevas variantes de ciberataques, más refinadas y complicadas y expeditas, y que dan como resultado que los ciberdelincuentes se encuentren un paso adelante y que el reto y gran desventaja es que cualquier solución que hoy se lance al mercado, pues en unos meses puede que ya esté desactualizado.

Uno de los sectores más vulnerables son las entidades financieras, pero desde luego no es la única; sin embargo, por lo relevante y lo bien cotizado que es la información que estas entidades administran, las hacen el blanco perfecto para poner todos los esfuerzos para intentar vulnerar las distintas capaz de seguridad que se puedan tener dentro de ellas.

Aquí es donde se vuelve sumamente importante la adopción e implementación de mejores prácticas de seguridad dictadas por estándares internacionales, así como leyes y regulaciones locales y acuerdos internacionales, pero de igual manera debe existir la capacitación continua a todo el personal orientado específicamente al puesto que desempeña, donde se brinden las herramientas necesarias para que desempeñen sus funciones acorde con las expectativas y que existan mecanismos de control para garantizar que eso está pasando, sin olvidar los

planes de continuidad y de recuperación de desastres que necesitan estar actualizados y probados en caso de que se sea afectado por un incidente grave de seguridad.

Otra de las áreas importantes es el proceso de administración de riesgos, sin duda alguna, es la que define la posición de vulnerabilidad (apetito de riesgo o perfil de riesgo) de las organizaciones, si no se cuenta con una adecuada gestión de riesgos, no se es capaz de identificar donde están las necesidades de implementación y monitoreo de controles, donde se deben estar destinando más recursos o si los objetivos estratégicos están en peligro de no alcanzarse, la pérdida de reputación, perder ventaja frente a competidores, sanciones por no cumplir con las regulaciones establecidas, en fin, la lista de posibles consecuencias es amplia y de igual manera los impactos en caso de materializarse los principales riesgos a las que están expuestas las entidades financieras.

Objetivo general

Desarrollar un modelo basado en las mejores prácticas del mercado para una adecuada administración de los riesgos en Ciberseguridad para las entidades financieras costarricenses, de manera tal que los impactos financieros y no financieros se logren minimizar y que sus causas que llevan a la materialización de los principales riesgos estén cada vez más bajo control.

Objetivos específicos

Las entidades financieras en Costa Rica se consideran están y deben estar un paso adelante en avances tecnológicos fundamentados en las leyes y reglamentaciones a las que están sujetas, así como a la sensibilidad de la información a la que tienen accesos. Los avances en la tecnología y lo avanzados y refinados que son cada día más los ciberataques, provoca que se deba estar en una constante revisión de las políticas, procesos y procedimientos, que se realicen evaluaciones y mediciones continuas e implementando las mejores prácticas para intentar estar un paso más cerca de lo que están los ciberdelincuentes, por lo tanto, el primer objetivo específico de esta propuesta es:

- Plantear un modelo de mejores prácticas para una adecuada administración de riesgos en Ciberseguridad para las entidades financieras costarricenses.

Existen impactos tangibles e intangibles, por lo que es importante entender que no siempre se puede llegar a tener un número que represente el valor de la pérdida económica que pueda sufrir una organización, si un riesgo se llega a materializar. Existen impactos intangibles cuyos valores son muy difíciles de determinar por ejemplo la afectación de imagen, ¿cuánto cuesta una imagen?, ¿cuánto es el valor de una marca?, es complicado y algunas veces hasta incalculable. Por esta razón el segundo objetivo específico es:

- Lograr que las causas que llevan a la materialización de los principales riesgos en ciberseguridad estén cada vez más bajo control.

Las razones por la cuales entidades de todos los sectores siguen siendo afectadas son variables, incluso aquellas que cuentan con controles, políticas y procedimientos bien definidos, sin duda alguna, la versatilidad del ciberespacio genera avances y desafíos que provocan que los amenazas por parte de los ciberdelincuentes sean cada vez más complejas y que requieran despliegues de recursos para intentar estar un poco más protegidos. De esta manera, el tercer objetivo específico es:

- Lograr minimizar los impactos financieros y no financieros causados por la materialización de los principales riesgos en Ciberseguridad.

Público meta

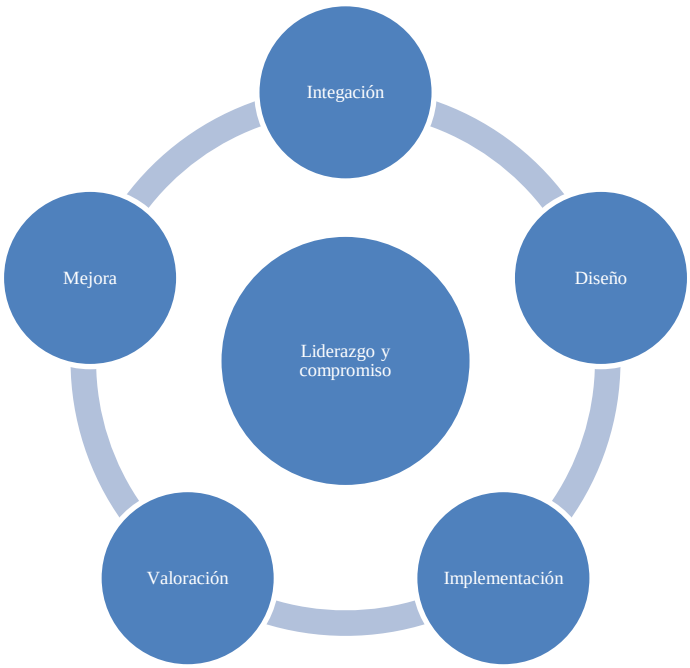
El desarrollo de esta propuesta tiene su enfoque en dar una guía sobre un modelo que contemple las mejores prácticas en administración de riesgos, con el objetivo que se pueda dirigir a las principales amenazas en Ciberseguridad que están expuestas las entidades financieras.

De esta manera los encargados de Gestión de Riesgos, los de Ciberseguridad, así como los Comités de Riesgos, desde luego a la gerencia y a las Juntas Directivas de las entidades financieras, puedan contar con una guía que sirva para mejorar el proceso con el que puedan contar actualmente y funcione como complemento sobre lo que esté establecido por temas de regulación a las que están sujetas las entidades financieras y, desde luego, que sirva de insumo para la consecución de los planes estratégicos trazados por ellos.

Propuesta estratégica

Con el fin de lograr conseguir una implementación satisfactoria de la propuesta, se requiere que las entidades financieras tomen en cuenta los siguientes puntos que están basados en la guía ISO 31000:2018 (2018), específicamente basado en su marco de referencia.

Figura 7
Marco referencia ISO 31000:2018



Fuente: ISO 31000:2018 Gestión de Riesgo - Directrices

Liderazgo y compromiso

Una parte elemental de cualquier proceso dentro de las organizaciones es contar con el respaldo y compromiso de la gerencia e incluso de la junta directiva. Por lo tanto, se debe impulsar la idea de que la gestión de riesgo tiene que ser parte de todas las actividades que realizan, donde se demuestre liderazgo y compromiso.

A partir de aquí, se requiere la adaptación e implementación de las mejores prácticas contenidas en esta propuesta, y desde luego que los recursos son una parte importante de esta implementación por lo que es importante que existan los necesarios requisitos para la

adecuada gestión de los riesgos, otro aspecto vital en esta implementación es que existan los niveles de autoridad, responsabilidad y dueños de dar las actualizaciones, y dar cuentas de lo que está aconteciendo en los niveles donde se están implementado estas mejores prácticas.

Esto puede traer beneficios a las entidades financieras, por ejemplo, que exista un adecuado alineamiento con los objetivos estratégicos y la cultura de riesgos, que se tengan mejores parámetros para definir de maneras más exacta las severidades y las decisiones sobre las acciones de los riesgos y que exista una adecuada comunicación de estos, para poder dar seguimiento a la evolución de los riesgos así como contar con un proceso de monitoreo para garantizar que el apetito de riesgo se encuentre actualizado.

Integración

Para que un proceso de gestión de riesgos sea satisfactorio, los distintos niveles de las organizaciones deben integrarse en un objetivo común, desde luego se tiene que considerar que cada nivel mantiene su estructura con objetivos propios; sin embargo, los riesgos se deben administrar en todos esos niveles y cada persona tiene una responsabilidad que cumplir.

Tener una gobernanza bien establecida ayuda a establecer el curso que se debe seguir, definiendo las dependencias internas y externas, procesos entre otros. La integración de la administración de riesgos debe lograr adaptarse a las necesidades propias de la organización de manera dinámica y tan transparente como sea posible, y no puede estar alejada de los objetivos estratégicos de la organización.

Diseño

Existen cinco puntos que se consideran dentro de la fase del diseño:

Comprensión de la organización y de su contexto

Se debe tener en cuenta los contextos externos e internos cuando se diseñan modelos de administración de riesgos, por ejemplo, para la parte externa hay que tener en consideración aspectos como factores sociales, culturales, financieros, tecnológicos, económicos, internacionales, nacionales. Para la parte interna, se pueden considerar asuntos como visón,

misión y valores de la organización, modelos de gobernanza, objetivos estratégicos, la cultura de la entidad, normas, políticas, procedimientos, sistemas de información, entre otras más.

Articulación del compromiso con la gestión del riesgo

Para lograr dar mayor respaldo a la implementación de un modelo de mejores prácticas para la administración de riesgos, la gerencia y también las juntas directivas, deben mostrar su compromiso con el modelo que se procura implementar, y puede ser mediante declaratorias, comunicados oficiales entre otros, pero lo importante es que el compromiso no se limite solamente a aspectos como el propósito de la entidad para la administración de riesgos y cómo se relacionan estos con los objetivos estratégicos y políticas establecidas, cómo se vincula con la cultura de la organización, recursos necesarios, y de qué manera se informa sobre el desempeño en general de la gestión de riesgos.

Asignación de roles, autoridades, responsabilidades y obligación de rendir cuentas en la organización

Se deben definir correctamente las responsabilidades, obligaciones, rendición de cuentas dentro de la organización, de manera tal que se logre dar énfasis especial y es que la administración de riesgos es una responsabilidad de todos y que se logren identificar los respectivos dueños de los riesgos declarados dentro de la organización.

Asignación de recursos

Es necesario reforzar que la administración y las juntas directivas de las organizaciones en general, muestren su apoyo a la asignación de recursos necesarios para una adecuada gestión de riesgos, dentro de lo que se puede incluir recursos como, personas específicamente sus habilidades, experiencias y competencias, lo mismo que los procesos con sus métodos y herramientas.

Establecimiento de la comunicación y la consulta

Debe existir una adecuada estrategia de comunicación de los riesgos, esta sin lugar a duda tiene que incluir la información que se pueda compartir al público al cual va dirigida la comunicación. Se debe permitir la realimentación de manera tal que permita mejorar para

futuras comunicaciones y que, además, proporcionen comunicaciones y consultas oportunas y consistentes.

Implementación

Es importante para esta etapa dentro del modelo de mejores prácticas para la administración de riesgos que se tomen en cuenta aspectos como desarrollo del plan de implementación, así como establecer la manera en que las decisiones se toman, y si se debe modificar algún proceso requerido para la toma de decisiones, sin olvidar que las indicaciones dadas por la organización son entendidas y puestas en marcha.

Como aspecto adicional, se debe manejar adecuadamente la incertidumbre que pueda prevalecer durante la implementación del modelo, como cualquier proceso nuevo y que se logren atacar oportunamente atrasos o problemas que aparezcan, pero esto requiere compromiso y tomar las decisiones que sean más acertadas de todas las partes que estén comprometidas durante las distintas etapas.

Valoración

Toda la implementación y puesta en marcha puede marchar bien, sin embargo, se debe contar con mecanismos para asegurarse que el desempeño del modelo esté funcionando de acuerdo con los objetivos establecidos, para lo cual es imprescindible que se establezcan métodos de medición de desempeño como indicadores y lograr comparar si los resultados están o no acordes con las expectativas planteadas.

Mejora

Como último aspecto, se deben considerar las acciones que hay que tomar como parte de los resultados del monitoreo de los indicadores de desempeño, considerando los cambios que se detecten en los ambientes externos e internos, así se pueda garantizar que la propuesta siga agregando valor a la organización. Por lo tanto, estos insumos deben servir para el establecimiento de procesos de mejora continua que contribuyan a que el proceso de administración de riesgos se vea robustecido.

Propuesta táctica

Una vez aclarado lo que se requiere para llevar a cabo la propuesta, se pasa a desarrollar la propuesta táctica que se trata de ir detallando las distintas etapas que se deben cumplir para la implementación del modelo de mejores prácticas. Es importante que este modelo esté basado en algunos de los principios de COSO (2013) que son los que más se amoldan a la gestión de riesgos en Ciberseguridad o también conocido como ciberriesgos.

Se debe tener claro que los ciberriesgos no aplican igual para todas las organizaciones y cada una perfectamente varía en cuanto a las fuentes internas y externas de los ciberataques que forman parte de esos riesgos. Los ciberriesgos son evaluados con referencia a la probabilidad de ocurrencia y el impacto que van a tener contra los objetivos de la organización, ante esto lo ciberdelincuentes que buscan en la mayoría de los casos, obtener un beneficio económico, las motivaciones para hacerlo pueden variar desde tener grupos de crímenes organizados, ciberterrorismo hasta el personal interno buscando algún tipo de venganza.

Tener un proceso adecuado de riesgos puede lograr grandes beneficios, si se toma en cuenta que los resultados que se obtienen permiten a las organizaciones tomar decisiones sobre qué tipo de controles se requieren para detectar, manejar estos riesgos, y todo esto va de la mano con mejores decisiones de inversiones en mejorar la posición de Ciberseguridad.

Aplicación del componente de evaluación de riesgos

Principio 6

La Organización especifica los objetivos con suficiente claridad, lo que permite la identificación y evaluación de los riesgos relacionados.

Con la aplicación de este principio se procura dar a las entidades financieras como evaluar los objetivos de manera tal que logre tener una influencia sobre el proceso de administración de riesgos en Ciberseguridad, pero para esto se debe:

1. Establecer los objetivos de las áreas operativas por evaluar, estos deben estar alineados a los objetivos estratégicos establecidos por la entidad financiera.
2. Asignar los niveles de tolerancia al riesgo para cada uno de los objetivos establecidos.

3. Definir los indicadores de desempeño para los objetivos planteados.
4. Evaluar si pasos 1 al 3 cumplen con las regulaciones establecidas para la gobernanza de las entidades financieras, así como de sus normas internas.

Principios 7 y 8

El primero describe que: 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 determinar cómo se deben gestionar.

El segundo describe que: La organización considera la probabilidad de fraude al evaluar los riesgos para la consecución de los objetivos.

Los resultados obtenidos del principio 6, les permite a las entidades financieras tener un mejor entendimiento de qué tan críticos son los sistemas de información para lograr la consecución de sus objetivos, por lo que mediante la aplicación de las acciones basadas en los principios 7 y 8, se puede lograr un nivel más profundo en la evaluación de riesgos y que permita asignar la severidad, así como la probabilidad de los impactos por los riesgos de ciberseguridad, pero para lograr esto se debe:

1. Establecer los mecanismos para identificar riesgos potenciales que afecten los objetivos de la entidad financiera. Riesgos tales como:
    a. Operativos, económicos, leyes, normas y otras regulaciones, productos o servicios, procesos de negocio, tecnología de la información e infraestructura, transacciones.
2. Incluir qué incentiva a una persona a cometer un fraude: presiones que reciba, actitudes sospechosas, oportunidades que tenga y posibles justificaciones.
3. Llevar a cabo revisiones periódicas, que permitan entre otras cosas, identificar y anticipar eventos que puedan afectar la consecución de los objetivos operativos y financieros.
4. Identificar relaciones de los procesos críticos de negocio con otras áreas y sus dependencias.
5. Resultados de las evaluaciones de riesgo son revisadas por la gerencia.

6. Desarrollar planes de remediación para las áreas identificadas en las evaluaciones de riesgo.

Principio 9

La organización identifica y evalúa los cambios que podrían afectar significativamente al sistema de control interno.

Las entidades financieras están en constante evolución, adoptando nuevas formas de dar sus servicios, desarrollar nuevos productos, mejorando procesos; en fin, están en un constante cambio, por lo que deben anticipar los impactos que estos tengan para las evaluaciones de ciber riesgos, ya que dentro del ciber espacio también se encuentran nuevos ciberataques y técnicas para explotar vulnerabilidades.

Normalmente, las evaluaciones de los ciberriesgos reflejan el estado actual de las entidades financieras; sin embargo, el proceso tiene que ser dinámico, pues considerando lo siguiente, se debe:

1. Establecer las situaciones que sirvan como desencadenantes para hacer una reevaluación de los riesgos y que puedan impactar los objetivos establecidos.
    a. Cambios en el entorno externo.
    b. Cambios en procesos internos.
    c. Cambios de la gerencia y Junta Directiva.
2. Realizar las actualizaciones resultantes de la evaluación de los cambios del punto anterior.
3. Ajustar cambios en presupuestos y proyecciones que estén afectadas por los cambios.
4. Comunicar los cambios a la gerencia y a la Junta Directiva.

Aplicación del componente de actividades de control

Principio 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.

Principio 11

La organización define y desarrolla actividades de control a nivel de organización sobre la tecnología para apoyar la consecución de los objetivos.

Principio 12

La organización despliega las actividades de control mediante políticas, que establecen las líneas generales del control interno y procedimientos que llevan dichas políticas a la práctica.

Las actividades de control son aquellas acciones que se llevan a cabo por personas dentro de las entidades financieras, con el objetivo de asegurar que las direcciones dadas por las jefaturas competentes se sigan para lograr mitigar los riesgos y que esté conforme a los objetivos que se establecen. Todas estas actividades de control deben ser documentadas en forma de políticas para asegurarse que se cumplan en todos los niveles de la organización, y para lograr esto, se requiere:

1. Definir el diseño de las actividades de control según los niveles de la organización, tomando como referencia algunos de los siguientes métodos:
    a. Revisión de desempeños en los niveles altos de la organización.
    b. Revisiones gerenciales a las distintas áreas funcionales dentro de la organización.
    c. Manejo del capital humano.
    d. Controles sobre procesamiento de información o transacciones financieras.
    e. Controles físicos de acceso a activos críticos.
    f. Revisión de medidas e indicadores de desempeño.
    g. Documentación de procedimientos y control interno.
2. Incluir análisis de segregación de funciones en el diseño de las actividades de control, en caso de que no sea posible hacer segregación de funciones, se debe implementar controles adicionales.
3. Con respecto a los controles sobre las Tecnologías de Información (TI):
    a. Planes estratégicos y procesos de manejo de riesgos para dar soporte a procesos de negocios:

i. Conformar un comité responsable de revisar y aprobar los planes de TI y sus prioridades.
ii. Hacer evaluaciones periódicas sobre los riesgos de TI y cualquier riesgo identificado, definir planes de remediación según su severidad a impacto.
iii. Establecer un proceso de revisión de proveedores externos que utiliza la organización con el propósito de determinar si existen riesgos y si están aptos para proveer servicios a la organización.

b. Los sistemas de información son estables e incluyen procesos de respaldo de datos y de recuperación ante fallas:
    i. Establecer políticas de retención de datos.
    ii. Definir frecuencias de los respaldos.
    iii. Definir los requerimientos físicos y de seguridad sobre el sitio donde se guardan las cintas u otros medios de respaldo que se utilizan para los respaldos.
    iv. Respaldar las aplicaciones, servidores de archivos para reducir riesgos de pérdida o corrupción de los datos.
    v. Documentar procedimientos de recuperación de sistemas críticos incluyendo sus datos y hacer pruebas al menos una vez al año.
    vi. Asegurarse de contar con controles ambientales para garantizar seguridad y confiabilidad de los equipos, por ejemplo: detectores de humo o fuego, controles de temperatura, fuentes de poder alternas.
    vii. Documentar procesos de respuesta a incidentes, problemas o errores reportados por usuarios de manera que se logren resolver en el menor tiempo posible.
    viii. Establecer controles de acceso físico y a la información en los sistemas de manera que se evite accesos no autorizados, divulgar, modificar, alterar o perder datos.
    ix. Establecer proceso de revisión de accesos de área físicas y sistemas críticos.

x. Documentar la política de seguridad donde se definan los objetivos de seguridad de la organización, esta debe ser complementada con estándares y procedimientos.

xi. Documentar proceso de suspensión o salida de personal, por renuncia o despido de manera tal que los accesos sean removidos o deshabilitados de manera oportuna (no mayor a 24 horas) o en casos de emergencia que sea inmediato.

xii. Documentar proceso de provisionamiento de accesos para los distintos sistemas, redes, aplicaciones, bases de datos) con base al principio de necesita-saber, necesita-hacer o menor-privilegio.

xiii. Crear política de manejo de contraseñas, con base en estándares internacionales y mejores prácticas, incluir política de contraseña compleja, historial de contraseñas, expiración y bloqueo de cuentas por fallas de ingreso o autenticación.

xiv. Establecer controles para garantizar que todos los usuarios con acceso a redes, sistemas, aplicaciones, bases de datos, se logren identificar de manera única (no uso de cuentas compartidas).

xv. Establecer controles de seguridad perimetral de la red interna y a la corporativa, por ejemplo, *Firewalls*, seguridad en la red *Wireless*, sistemas de detección de intrusos, escáneres para detectar vulnerabilidades, entre otros.

xvi. Restringir acceso a códigos fuentes, compiladores, documentación de la programación de los sistemas.

c. Cambios en los programas, sistemas desarrollados o comprados sean manejados apropiadamente:

   i. Establecer proceso y políticas de manejo de cambios, incluir manejos de cambios de emergencia, de manera que:

      1. Cambios o puesta en producción de aplicaciones, bases de datos, sistemas operativos, equipos de red se aprueben apropiadamente y que estos estén registrados en un repositorio central con sus debidas pruebas de aceptación de los usuarios.

2. Se tengan controles que solo personal autorizado realice migraciones de aplicaciones y sistemas a producción.

Aplicación del componente de información y comunicación

Principio 13

La organización obtiene o genera y utiliza información relevante y de calidad para apoyar el funcionamiento del control interno.

Dentro de este principio la organización debe identificar los requerimientos de información, esto es crítico para el control interno y análisis de ciber riesgos. Por otro lado, procesar datos relevantes en información es importante, ya que las organizaciones manejan cantidades enormes de datos, por lo que se debe transformar todo esto en información de valor, con significado y que sirva para poder tomar acciones.

Utilizar información interna y externa, ya que, si bien la información que puede ser más relevante para un análisis de riesgo pueda venir a lo interno de la organización, lo cierto es que se debe considerar la información externa pertinente al sector.

Por último, se debe mantener la calidad en todo este proceso, para que se logre no solo obtener la información requerida si no que las actividades de control se lleven a cabo correctamente. De tal manera hay que:

1. Definir los requerimientos de información que se desea captar.
2. Definir proceso de evaluación de fuentes de datos internos y externos de manera que se logre identificar su confiabilidad. Datos pueden ser operacionales, financieros, cumplimiento, información de competidores, entre otras.
3. Datos se deben obtener de manera pronta de manera que sean válidos y efectivos para la realidad que se está analizando.
4. Documentar formalmente los procedimientos operacionales y financieros de manera tal que los responsables de su ejecución lo hagan conforme lo documentado (se garantice la calidad del proceso) y que se logre obtener información importante de ellos.

Principio 14

La organización comunica información internamente, incluidos los objetivos y responsabilidades que son necesarios para apoyar el funcionamiento del sistema de control interno.

Con respecto a la comunicación de información sobre control interno, se debe considerar hacia el personal de la organización, esto es importante, porque el estar seguros, mantenerse vigilantes y resilientes es una responsabilidad organizacional, cada persona tiene un papel preponderante en cuanto a la protección de la información.

Por otro lado, están aquellos que son responsables de manejar y monitorear controles de los ciberriesgos, por lo que se deben contar con los canales para que la información se comparta y que se puedan tomar decisiones más acertadas.

Por último, está la comunicación hacia la Junta Directiva, sin duda alguna en la realidad actual es esencial que los miembros de las juntas directivas entiendan las tendencias con respectos a los ciberriesgos y cómo pueden impactar la consecución de sus objetivos estratégicos.

Para cumplir con estos puntos se debe:

1. Establecer canales de comunicación de manera tal que el personal se reúna con sus respectivas jefaturas para revisar y discutir resultados operativos y financieros según aplique y de acuerdo con las funciones realizadas.
2. Establecer mecanismos para que la información se colecte a tiempo para que pueda ser monitoreada efectivamente.
3. Definir tiempos dentro los cuales la información deba ser revisada.
4. Crear mecanismos de comunicación que estén orientados a los distintos niveles de la organización y que estén conforme a la responsabilidad individuales de saber del personal.
5. Implementar proceso de reporte de situaciones anómalas que afecten el control interno, de tal manera que se establezcan las acciones por tomar con cada incidencia.

Principio 15

El segundo principio describe: La organización se comunica con las partes interesadas externas sobre los aspectos clave que afectan al funcionamiento del control interno.

La aplicación de políticas y estándares son importantes para el manejo y control de las comunicaciones que se deban hacer a las entidades externas. Estas comunicaciones pueden ser relevantes para clientes, aliados de negocios, proveedores, entidades del Gobierno entre otros. Para tales efectos, el hilo conductor para las comunicaciones externas está dado si se permite la comunicación hacia adentro que influencie las evaluaciones de los ciberriesgos, así como los controles y que se facilite la comunicación hacia afuera para informar a esas entidades externas sobre eventos de Ciberseguridad u otro tipo de situaciones que afectar la comunicación con ellos. Por lo tanto, se debe:

1. Establecer los mecanismos de comunicación sobre el funcionamiento del control interno de las distintas áreas operativas y financieras.
2. Cualquier reporte de posibles anomalías debe ser investigado con prontitud y que se establezcan las acciones para resolverlas.
3. Considerar los siguientes factores para la elaboración de los mecanismos de comunicación:
    a. Público meta que va a recibir la comunicación.
    b. Naturaleza de la información, el propósito y tipo de información que se comparte.
    c. Requerimientos de disponibilidad de la información, que esté disponible cuando el público meta la requiera.
    d. Costos y recursos involucrados para comunicar la información.
    e. Requerimientos legales, regulatorios, normas que puedan impactar lo que se comunica y el cómo.

Aplicación del componente de actividades de monitoreo

Principios 16 y 17

El primer principio describe: La organización selecciona, desarrolla y realiza evaluaciones continuas o independientes para determinar si los componentes del sistema de control interno están presentes y en funcionamiento.

El segundo describe: La organización evalúa y comunica las deficiencias de control interno de forma oportuna a las partes responsables de aplicar medidas correctivas, incluyendo la dirección y el consejo, según corresponda.

La evaluación oportuna de los controles es vital para estar vigilantes del desempeño de los otros componentes. El que se puedan realizar evaluaciones recurrentes dentro de los procesos de negocio en los distintos niveles organizativos puede dar información importante y a tiempo, y esto desde luego puede variar dependiendo del alcance y frecuencia de las evaluaciones de los ciberriesgos, la efectividad con que se ejecutan, así como otras consideraciones que especifique la organización. Las evaluaciones se realizan ya sea basadas en criterios como regulaciones, estándares internacionales, la gerencia o la Junta Directiva, además es importante que las fallas o deficiencias que se encuentran se comuniquen apropiadamente. De esta manera, se requiere:

1. Establecer la base entre el diseño del control interno y el estado actual, de manera que se puedan realizar cambios para reducir las diferencias entre el criterio que se define y la condición actual.
2. Realizar actividades de monitoreo periódicas para evaluar la efectividad del sistema de control interno.
3. Ejecutar evaluaciones continuas de los resultados de los monitoreos para mejorar el sistema de control interno.
4. Evaluar las fallas o errores que se detectan como resultado de las evaluaciones para conocer deficiencias en el diseño o efectividad operativa del control interno.
5. Implementar las acciones correctivas lo más pronto posible por parte de los dueños de los controles que se evalúan, para esto se requiere tener control donde se lleve el registro de cada una de las acciones, y donde se indique quién o quiénes son las personas responsables, cuánto es el tiempo estimado para la resolución del problema identificado y la fecha en que se inician y concluyen las acciones necesarias; además debe indicar si existen situaciones que pongan en riesgo la consecución de las tareas en los tiempos establecidos.
6. Este control de seguimiento debe además contar con revisiones periódicas, donde cada responsable dé el estado de las acciones ejecutadas, si existe algún problema o

retraso importante o alguna ayuda que se necesite, de manera tal que se pueda dar visibilidad a la gerencia sobre los retos y avances alcanzados.

Bibliografía

ACCID. (2019). *Prevención y gestión de riesgos*. España: ACCID. Revista de Contabilidad y Dirección, número 28.

Agencia de Protección de Datos de los Habitantes. (2021). *Normativa de protección de datos personales vigente en Costa Rica*. Tomado el 8 de mayo de 2021 desde: http://www.prodhab.go.cr/reformas/

Archivo Nacional. (2021). *Fondo Junta Fundadora de la Segunda* República. Tomado el 7 de mayo de 2021 desde: https://www.archivonacional.go.cr/web/fondos/isadg_junta_fundadora_seg_rep%20.docx

Asamblea Legislativa. (2012). Reforma de la Sección VIII, Delitos Informáticos y Conexos, del Título VII del Código Penal N° 9048.

Asamblea Legislativa. (2011). Protección de la persona frente al tratamiento de sus datos personales.

Asamblea Legislativa. (1995). Ley Orgánica del Banco de Costa Rica.

Asociación Bancaria Costarricense. (2010). *Acceso a Servicios Financieros en Costa Rica*. Tomado el 23 de mayo de 2021 desde: https://www.abc.fi.cr/wp-content/uploads/2019/03/acceso-a-servicios-financieros-en-costa-rica.pdf

Baena, T. (2014). *Análisis financiero Enfoque y proyecciones*. (2da ed.). Colombia: Ecoe.

Banco de Costa Rica. (2021). *Historia*. Tomado el 7 de mayo de 2021 desde: https://www.bancobcr.com/wps/portal/bcr/bancobcr/acerca-del-bcr/informacion_corporativa/historia/

Banco Interamericano de Desarrollo., y Organización de los Estados Americanos. (2020). *Ciberseguridad Riesgos, Avances y el Camino a seguir en América Latina y el Caribe*.

Tomado el 4 de mayo de 2021 desde: 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). *Conózcanos*. Tomado el 7 de mayo de 2021 desde: https://www.bncr.fi.cr/conozcanos

Beissel, S. (2016). *Cybersecurity Investments*. Suiza: Springer.

Benavides, R. (2014). *Administración*. (2da ed.). México: McGrawn Hill.

Bernal, C. (2016). *Metodología de la investigación. Administración, economía, humanidades y ciencias sociales*. (4ta ed.). Colombia: Pearson.

Bisquerra, R. (2009). *Metodología de la investigación educativa*. (2da ed.). Madrid: La Muralla.

Brangetto, P., y Kert-Saint M. (2015). *Economic Aspects of national cyber security strategies*. Tomado el 1 de mayo de 2021 desde: https://ccdcoe.org/uploads/2018/10/Economics-of-cybersecurity.pdf

Brooks, C., Greo, C., Craig, P., y Short, D. (2018). *Cybersecurity Essentials*. Indianapolis: Sybex.

Calle, A, Quizhpe, K. (2017). *Evaluación integral del sistema de control interno en la unidad particular Rosa de Jesús Cordero – Catalinas, periodos 2017 – 2018*. Universidad de Cuenca.

Cipriano, A. (2014). *Administración estratégica*. México: Editorial Patria.

Cordero, C. (2022). *Ucrania es víctima de ciberataques contra bancos, ministerios y otras entidades*. Tomado el 10 de mayo de 2022 desde: https://www.elfinancierocr.com/tecnologia/ucrania-es-victima-de-ciberataques-contra-bancos/R4JN7JNZIVDBLODDCAN6ICOVC4/story/

Cordero, C. (2020). *Más de 51 millones de ataques de 'hackers' durante la pandemia en Costa Rica: empresas siguen basando su estrategia de seguridad en la educación*. Tomado el 2 de mayo de 2021 desde: https://www.elfinancierocr.com/tecnologia/mas-de-51-millones-de-ataques-de-hackers-durante/AXLI7EOQQZD7RA6X5O5DJPFNAA/story/

COSO. (2013). *Internal Control Integrated Framework. Executive Summary*. Tomado el 7 mayo de 2022 desde: https://www.coso.org/Shared%20Documents/Framework-Executive-Summary.pdf

COSO. (2015). *COSO in the Cyber Age*. Tomado el 7 mayo de 2022 desde: https://www.coso.org/Shared%20Documents/COSO-in-the-Cyber-Age.pdf

Cuartas, F. (2013). *Banca comercial y de inversión*. Bogotá: Ediciones de la U.

David, F., y David, F. (2017). *Conceptos de administración estratégica*. (15ta ed.). México: Person.

Deloitte. (2022). *Beneath the surface of a cyberattack A deeper look at business impacts*. Tomado el 14 de mayo de 2022 desde: https://www2.deloitte.com/content/dam/Deloitte/es/Documents/governance-risk-compliance/Deloitte-ES-GRC-Los-riesgos-ocultos-de-un-ciberataque.pdf

Deloitte. (2019). *En búsqueda de la madurez en Ciberseguridad en las instituciones financieras*. Tomado el 2 de mayo de 2021 desde: https://www2.deloitte.com/co/es/pages/risk/articles/el-futuro-del-riesgo-en-los-servicios-financieros1.html

Denman, C., y Armando, J. (2000). *Antología de métodos cualitativos en la investigación social*. México: El Colegio de Sonora.

Escoto, R. (2001). *Banca Comercial*. San José: Universidad Estatal a Distancia.

Estupiñan, R. (2015). *Administración de riesgos E.R.M y la auditoría interna*. Colombia: Ecoe Ediciones.

Firma-e. (2014). *Pilares de la Seguridad de la Información: confidencialidad, integridad y disponibilidad*. Tomado el 8 de mayo de 2021 desde: https://www.firma-e.com/blog/pilares-de-la-seguridad-de-la-informacion-confidencialidad-integridad-y-disponibilidad/

FISA. (2021). *Ciberseguridad Retos para el sector bancario este 2021*. Tomado el 7 mayo desde: https://www.fisagrp.com/blogs/ciberseguridad-reto-sector-bancario-2021.html

Gitman, L., y Zutter, C. (2016). *Principios de administración financiera*. (11era ed.). México: Pearson.

Grondin, J. (2008). *¿Qué es la hermenéutica?* Barcelona: Herder Editorial.

Hernández, R., y Mendoza, C. (2018). *Metodología de la investigación. Las rutas cuantitativa, cualitativa y mixta*. México: McGrawn Hill.

Hernández, R., Fernández, C., y Baptista, P. (2014). *Metodología de la investigación*. (6ta ed.). México: McGraw Hill.

Hernández, S., y Palafox, G. (2012). *Administración. Teoría, Proceso, Áreas Funcionales y Estratégicas para la Competitividad*. (3era ed.). México: McGraw Hill.

Hubbard, D, Seiersen, R. (2016). *How to Measure Anything in Cibersecurity Risk*. Estados Unidos: John Wiley & Sons, Inc

Hurtado, I., Toro, G. (2007). *Paradigmas y métodos de investigacion en tiempos de cambios*. Caracas: CEC.

IBM. (2021). *IBM X-Force Threat Intelligence Index*. Tomado el 8 de mayo de 2021 desde: https://www.ibm.com/security/data-breach/threat-intelligence

IBM. (2022). *IBM X-Force Threat Intelligence Index*. Tomado el 22 de mayo de 2022 desde: https://www.ibm.com/downloads/cas/ADLMYLAZ

IBM. (2022). *What is a cyberattack?*. Tomado el 22 de mayo de 2022 desde: https://www.ibm.com/topics/cyber-attack

Idoate, M. (2017). *El mercado de la ciberseguridad en México*. Tomado el 2 de mayo de 2021 desde: https://www.camarabilbao.com/ccb/contenidos.downloadatt.action?id=8572999

ISO (2018). *ISO 31000:2018 Gestión del riesgo – Directrices*. Tomado el 28 de mayo de 2022 desde: https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es:sec:5.4.1

ISO (2019). *Risk management – Ris assessment techniques (31010)*. https://www.iso.org/standard/72140.html

ISO (2013). *Information Security Management (27001)*. https://www.iso.org/isoiec-27001-information-security.html

Jenkins, C. (2020). *BCR denuncia "extorsión" de grupo cibercriminal que amenaza con publicar datos de tarjetas de créditos cada semana*. Tomado el 2 de mayo de 2021 desde: https://observador.cr/noticia/el-bcr-denuncia-extorsion-de-grupo-cibercriminal-que-amenaza-con-publicar-datos-de-tarjetas-de-creditos-cada-semana/

Juárez, M., Gaitán, L., Urosa, B., y Cabrera, P. (1993). *Trabajo social e investigación: temas y perspectivas*. Madrid: Universidad Pontificia Comillas.

Kaspersky. (2021). *Brute Force Attack: Definition and Examples*. Tomado el 14 junio de 2021 desde: https://www.kaspersky.com/resource-center/definitions/brute-force-attack

Lavalle, A. (2016). *Análisis financiero*. México: Digital UNID.

Martínez, A., Muñoz, J., y Pascual A. (2004). *Tamaño de muestra y precisión estadística*. Almería: Universidad de Almería.

Martinez, M. (2014). *Ciberamenazas en el sector bancario español*. Tomado el 10 de mayo 2022 desde: https://www.tendencias.kpmg.es/2014/06/ciberamenazas-en-el-sector-bancario-espanol/

Ministerio de Ciencia, Tecnología y Telecomunicaciones. (2021). *Estrategia Nacional de Ciberseguridad*. Tomado el 2 de mayo de 2021 desde: https://www.micit.go.cr/gobierno-digital/ciberseguridad

Ministerio de Ciencia, Tecnología y Telecomunicaciones. (2012). *Decreto (37052) Creación Centro de Respuesta de incidentes de Seguridad Informática CSIRT-CR*. Costa Rica: Ministerio de Ciencia, Tecnología y Telecomunicaciones.

Ministerio de Planificación Nacional y Política Económica. (2020). *Ciberseguridad en el Sistema de Planificación Nacional*. Tomado el 4 de mayo de 2021 desde: https://www.hacienda.go.cr/Sidovih/uploads/Archivos/Articulo/Ciberseguridad%20en%20el%20Sistema%20Nacional%20de%20Planificaci%C3%B3n-MIDEPLAN.pdf

Münch, L. (2018). *Administración Gestión organizacional, enfoques y proceso administrativo*. (3era ed.). México: Pearson.

Naghi, M. (2005). *Metodología de la investigación*. (2da ed.). México: Limusa Noriega.

Organización de los Estados Americanos, Asobancaria. (2019). *Desafíos del riesgo cibernético en el sector financieros para Colombia y América Latina*. Tomado el 7 de mayo de 2022 desde: https://www.oas.org/es/sms/cicte/docs/Desafios-del-riesgo-cibernetico-en-el-sector-financiero-para-Colombia-y-America-Latina.pdf

Organización de los Estados Americanos. (2018). *Estado de la Ciberseguridad en el sector bancario en América Latina y el Caribe*. Tomado el 7 de mayo de 2022 desde: https://www.oas.org/es/sms/cicte/sectorbancariospa.pdf

Oficina de Seguridad del Internauta. (2020). *Guía de Ciberataques*. Tomado el 9 de mayo de 2021 desde: https://www.osi.es/sites/default/files/docs/guia-ciberataques/osi-guia-ciberataques.pdf

Owaida, A. (2021). *Ciberseguridad en la industria financiera: riesgos y desafíos*. Tomado el 7 de mayo de 2022 desde: https://www.welivesecurity.com/la-es/2021/03/24/ciberseguridad-industria-financiera-riesgos-desafios/

Paris, M. (2017). *Convenio de Budapest sobre Ciberdelincuencia ya es Ley en Costa Rica*. Tomado el 8 de mayo de 2021 desde: http://bonafide.cr/convenio-de-budapest/

Pérez, J. (2015). *La gestión financiera de la empresa*. Madrid: ESIC Editorial.

Pimienta, J., y Hoz, A. (2017). *Metodología de la Investigación*. (3era ed.). México: Pearson.

Putrus, R. (2019). *The Role of the CISO and the Digital Security Landscape*. Tomado el 1 de mayo de 2021 desde: https://www.isaca.org/resources/isaca-journal/issues/2019/volume-2/the-role-of-the-ciso-and-the-digital-security-landscape

Raghu, R. (2018). *World Economic Forum Report Reinforces Rising Prominence of Cybersecurity*. Tomado el 1 mayo de 2021 desde: https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2018/world-economic-forum-report-reinforces-rising-prominence-of-cybersecurity

Ramirez, E. (2001). *Moneda, banca y mercados financieros*. México: Pearson.

Ramiro, R. (2018). *25 Tipos de ataques informáticos y cómo prevenirlos*. Tomado el 4 de junio de 2021 desde: https://ciberseguridad.blog/25-tipos-de-ataques-informaticos-y-como-prevenirlos/

Robbins. S., y Coulter, M. (2018). *Administración*. (13era ed.). México: Pearson.

Ross, S., Westerfield, R., Jaffe, J., y Jordan, B. (2018). *Finanzas corporativas*. (11era ed.). México: McGrawn Hill.

Superintendencia General de Entidades Financieras. (2020). *Acuerdo SUGEF 14-17. Reglamento General de Gestión de la Tecnología de Información.* Tomado el 11 de mayo 2022 desde: https://www.sugef.fi.cr/normativa/normativa_vigente/SUGEF%2014-17%20(v%204_%2016%20de%20setiembre%20de%202020).pdf

Superintendencia General de Entidades Financieras. (2022). *Acuerdo SUGEF 2-10. Reglamento sobre Administración Integral de Riesgos.* Tomado el 11 de mayo 2022

desde: https://www.sugef.fi.cr/normativa/normativa_vigente/SUGEF%202-10%20(v20%2031%20marzo%202022).pdf

Thompson, A., Strickland III, A., Janes, A., Sutton, C., Peteraf, J., y Gamble, J. (2018). *Administración estratégica teoría y casos*. México: McGrawn Hill.

U.S Securities and Exchange Commission. (2022). *Cybersecurity and Resiliency Observations*. Tomado el 7 de mayo de 2022 desde: https://www.sec.gov/files/OCIE%20Cybersecurity%20and%20Resiliency%20Observations.pdf?mod=article_inline

Verizon. (2020). *2020 Data Breach Investigation Report*. Tomado el 7 mayo de 2022 desde: https://www.verizon.com/business/resources/reports/2020-data-breach-investigations-report.pdf

Vila, G. (2020). *SEC Insta a mejores prácticas de Ciberseguridad en empresas financieras*. Tomado el 7 de mayo de 2022 desde: https://www.delitosfinancieros.org/sec-insta-a-mejores-practicas-de-ciberseguridad-en-empresas-financieras/

Villasís-Keever, M., Márquez, H., Zurita, J., Miranda, G., y Escamilla, A. (2018). *El protocolo de investigación VII. Validez y confiabilidad de las mediciones*. México: Revista Alergia México, 65(4). pp 415.

World Economic Forum. (2021). *The Global Risks Report 2021*. Tomado el 3 de mayo de 2021 desde: https://www.weforum.org/reports/the-global-risks-report-2021

World Economic Forum. (2022). *The Global Risks Report 2022*. Tomado el 9 de mayo de 2022 desde: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf

Anexos

Anexo 1
Entrevista a expertos

1. ¿Cuáles considera usted son las principales amenazas en Ciberseguridad a las que se puede ver expuesta una entidad financiera?

2. ¿Cuáles considera usted son los principales impactos financieros y no financieros más significativos para una entidad financiera, si fuera víctima de un ciberataque?

3. ¿Qué tan importante es para una entidad financiera mostrar su compromiso de integridad y valores éticos?

4. ¿Cada cuánto considera usted se deben actualizar las políticas y procedimientos de seguridad en las entidades financieras?

5. ¿Cómo considera usted que una entidad financiera se pueda asegurar de contratar al personal adecuado, desarrollarlo, medirlo, capacitarlo y retenerlo?

6. ¿De qué manera se asegura una entidad financiera que las personas entiendan sus roles y responsabilidades para los puestos que desempeñan?

7. ¿Cuál es su opinión sobre la cultura de identificación, reporte de riesgos y posibles fraudes en todos los niveles de una entidad financiera de manera tal que le permita mantener actualizado su perfil de riesgo?

8. ¿Cuáles foros o espacios deben contar en las entidades financieras para mantener el personal actualizado de las principales noticias sobre los riesgos de Ciberseguridad?

9. ¿Cuáles considera usted son las razones principales por las cuales los riesgos se materializan en las entidades financieras?

10. ¿De qué manera se deben comunicar los riesgos a entidades externas (proveedores, aliados comerciales, clientes) en una entidad financiera?

11. ¿De qué manera los controles deben ser seleccionados, desarrollados y evaluados de modo que cumplan con los objetivos de identificar, responder y alertar posibles incidentes o riesgos de seguridad en una entidad financiera?

12. ¿Cuál es el perfil de educación en riesgos de Ciberseguridad que tienen los usuarios de entidades financieras en Costa Rica?

13. ¿Cuáles considera usted son los principales desafíos que enfrentan las entidades financieras sobre este perfil de cliente?

14. ¿Cuáles acciones o recomendaciones deben hacer o están haciendo las entidades financieras para poder abordar este problema? (Administrativas, tecnológicas, etc.)