PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

ESCUELA DE POSGRADO

IMPLEMENTACIÓN DE PROGRAMAS DE CUMPLIMIENTO EN CIBERSEGURIDAD COMO UNA PRÁCTICA DE BUEN GOBIERNO CORPORATIVO EN LAS ENTIDADES QUE FORMAN PARTE DEL SISTEMA FINANCIERO PERUANO

TRABAJO DE INVESTIGACIÓN PARA OPTAR EL GRADO ACADÉMICO DE MAGÍSTER EN DERECHO DE LA EMPRESA

AUTOR

MANSILLA PIZARRO, DANIELA

ASESOR

DEBENEDETTI LUJAN, BRUNO EDOARDO

LIMA, PERÚ

AGOSTO, 2020

Dedicatoria

A mi madre, por impulsarme a cumplir mis sueños,
por darme la fortalece de continuar
y por darme su apoyo incondicional.

Daniela Mansilla Pizarro

RESUMEN EJECUTIVO

En los últimos años, el uso y el avance de las tecnologías de la información y de la comunicación (TICs), han cobrado un rol importante en el desarrollo de la economía digital, pues es gracias al uso de la tecnología que diversas actividades tradicionales como la venta de productos, o el desarrollo de transacciones bancarias han podido ser simplificadas. Sin embargo, pese a que el uso de la tecnología ofrece una gran gama de oportunidades y que facilitan el desarrollo de actividades, sectores como el retail, consumo y financiero se han visto afectados de forma directa por su uso, a raíz de la mayor incidencia de ciberataques; es en tal sentido que por medio del presente trabajo, se busca poner de relieve la necesidad de contar con un programa de cumplimiento de ciberseguridad como una práctica de buen gobierno corporativo en las entidades que forman parte del sistema financiero peruano, considerando que dicho sector es uno de los más afectados por este tipo de incidentes y que tiene un papel importante dentro de la economía de nuestro país.

Por tal motivo, con el propósito de entender la situación problemática planteada, se ha plasmado dentro del presente trabajo, los conceptos clave para lograr un mejor entendimiento del problema de la investigación, además de desarrollar la experiencia en otros países, hecho que además de mostrar la gravedad y el perjuicio ocasionado por un ciberataque, nos permite tener una idea más clara de los aspectos esenciales que pueden ser implementados en nuestro país.

Finalmente, considerando que existe la necesidad de implementar un programa de cumplimiento en ciberseguridad en las entidades que forman parte del sistema financiera peruano y que a la fecha no existe ningún tipo de regulación nacional sobre el tema, se pone en consideración los aspectos mínimos que deberán ser implementados en las empresas que forman parte del sistema financiero como parte de la implementación de prácticas de buen gobierno corporativo.

ÍNDICE

LISTA DE TABLAS

LISTA DE FIGURAS

INTRODUCCIÓN

En pleno siglo XXI, es gracias al uso del internet que se nos han abierto las puertas a un mundo más dinámico y ágil, hoy en día podemos realizar un sinfín de actividades sin tener que salir de la comodidad de nuestros hogares. Si una persona desea buscar información sobre un tema en particular, ya no necesita ir en busca de una biblioteca, simplemente haciendo uso de las distintas plataformas de búsqueda obtendrá la información deseada; si una persona quiere hacer compras para su hogar, podrá entrar a los portales web de los distintos supermercados y ordenar los productos que desee, y lo mismo sucede con la forma de prestación de servicios financieros; en cualquier momento, si una persona desea realizar una transferencia o pago de servicios solo necesita entrar al portal web de su banco para poder realizar la operación.

Entonces, el cambio en la forma de prestación de servicios tradicionales a través de su digitalización, ha dado pase al desarrollo de la economía digital, la misma que se caracteriza por ser fuente de mayor productividad, por lograr el crecimiento económico de forma más ágil y por asegurar el desarrollo sostenible de los distintos sectores económicos.

No obstante ello, es importante mencionar que no todos los sectores se han desarrollado de la misma forma, los únicos sectores que han logrado un mayor desarrollo en esta época de digitalización son el sector educación, servicios alimentarios y sector financiero, siendo este último, uno de los sectores más determinantes o clave dentro del desarrollo económico de una sociedad, en consideración de que las actividades que realiza como son la recaudación de dinero, otorgamiento de créditos, proveer de liquidez entre otros, son esenciales para el desempeño económico y productivo (Asobancaria).

Es en ese sentido que las distintas empresas que forman parte del sector financiero, con el propósito de seguir fidelizando su cartera de clientes y poder mantenerse vigentes en el mercado, han apostado por la implementación de softwares, sistemas y aplicaciones que sean compatibles con los servicios que ofrecen, logrando mayor dinamización de las transacciones financieras, dejando atrás el obstáculo que representaban las distancias geográficas; y que ha propiciado mayor inversión en estos sistemas, desarrollo de nuevos proceso de adecuación a estas nuevas tecnologías, así como la modificación de sus estructuras orgánicas para garantizar la eficacia y eficiencia de esta nueva forma de prestar sus servicios.

Sin embargo; pese a los denodados esfuerzos por brindar mayores beneficios a sus clientes, estos no han sido los suficientes, considerando que la digitalización de los servicios financieros, ha abierto una gran brecha de riesgos para dicho sector, convirtiéndose en uno de los sectores más contingentes, pues a medida que se han desarrollado los sistemas, se han detectado amenazas que buscan obstruir los activos de la información, que ha generado la exposición latente de sufrir ciberataques, es decir que personas ajenas a una empresa puedan explotar de forma deliberada, los sistemas informáticos causando la alteración de datos, perdida de dinero, pérdida de confianza, en consecuencia, disminución de clientes, afectación a la reputación de la empresa entre otras consecuencias.

Según estudios presentados por el Fondo Monetario Internacional, señala que este tipo de eventos pueden comprometer desde el 9% al 62% de los ingresos netos de estas entidades, encendiendo las alarmas de precaución. Según refiere IBM, *uno de cada cinco ciberataques a la confidencialidad, integridad y disponibilidad de la información se da en contra del sector financiero.* (El Economista), en esa misma línea de ideas según lo expuesto por el Foro Económico Mundial, los ciberataques forman parte de los principales riesgos mundiales. (OEA).

Y así es preciso mencionar, que Latinoamérica, no ha sido ajena a estos sucesos que en los últimos años ha ido aumentando su nivel de incidencia. En mayo del 2018, el Banco de Chile, fue víctima de unos de los más grandes ciberataques internacionales que genero una perdida aproximada de 10 millones de dólares al banco (Solís, 2018), otro ejemplo, lo encontramos en los bancos de México, así lo confirmó el gobernador del Banco de México, al afirmar que el sistema de transferencias electrónicas de diversos bancos fueron hackeados, llegando a procesarse miles de transferencias de dinero por varios días generando perdidas valorizadas entre 21 y 42 millones de dólares.

En ese sentido, si bien es cierto, que nuestro país no ha sido objeto de un ciberataque de tal magnitud, experiencias como las suscitadas en Chile y en México, han puesto en evidencia el nivel de vulnerabilidad de las empresas pertenecientes al sector financiero, demostrando la carencia de leyes, bajo nivel de protección en ciberseguridad y por ende la necesidad de tener que garantizar el desarrollo de políticas y medidas de protección en este ámbito.

En merito a ello, la SBS ha determinado que es obligación de las entidades de dicho sector, la adecuada gestión de riesgos a los cuales se encuentran expuestos, es así como, por medio del

Reglamento de Gobierno Corporativo y Gestión Integral del Riesgo, se ha establecido que las empresas que se encuentran bajo el ámbito de aplicación de la referida norma, deban de identificar los posibles riesgos que pudieran afectar el normal desempeño de labores y en consecuencia adoptar los planes de acción, que acorde a su naturaleza y tamaño, otorguen seguridad razonable para la consecución de sus objetivos. (Resolución N°272-2017).

Entonces, teniendo en cuenta el rol trascendental del sector financiero dentro del desarrollo económico, considerando que las medidas otorgadas por la SBS no son suficientes para hacer frente a aquellos incidentes de seguridad de la información, resulta determinante tener que adoptar medidas necesarias de protección y prevención de riegos a los cuales se encuentran expuestas las entidades que forman parte del sistema financiero peruano.

En tal sentido, el problema de investigación está orientado a determinar la necesidad e importancia de implementación de un programa de cumplimiento en ciberseguridad como una práctica de buen gobierno corporativo en las entidades que forman parte del sistema financiero peruano, teniendo en cuenta los siguientes aspectos:

Primero, la implementación de las prácticas de buen gobierno corporativo coadyuva en gran magnitud a generar valor, solidez y eficiencia, trayendo consigo una mejor administración de los riesgos a los cuales están expuestas las empresas. (SMV).

Segundo, el desarrollo de la economía digital, necesita de forma urgente que se tomen las medidas de protección adecuadas para prevenir riesgos como los ciberataques.

Tercero, la actual regulación propuesta por la SBS sobre gestión de riesgos, resulta insuficiente, frente a todas las medidas que se deben tomar respecto a ciberseguridad, considerando la magnitud y el nivel de incidencia de este tipo de sucesos.

Cuarto, además de un desarrollo normativo nacional se requiere que las empresas que forman parte del sistema financiero, consideren dentro de sus estructuras orgánicas, políticas, directrices, lineamientos más complejos y sofisticados para la defensa de cualquier ciberataque.

Así mismo se debe tener en cuenta que la implementación del programa de cumplimiento, como parte de los principios de buen gobierno corporativo, según lo detalla Artaza Varela, permitirá

controlar dentro de los límites exigibles los peligros de infracción al ordenamiento jurídico, derivados por la misma actividad de la empresa. (2014)

Hipótesis

Considerando que además de ser una exigencia normativa que las empresas del sector financiero tengan que gestionar el riesgo que les es inherente de acuerdo con su tamaño y naturaleza, teniendo en cuenta que en los últimos años la economía digital ha alcanzado un desarrollo a gran escala y que el uso de las tecnologías de la información y de la comunicación han abierto una gran brecha de riesgos para el sector financiero, como los casos suscitados en Chile y México, es pertinente determinar que las entidades que forman parte del sistema financiero peruano no están exentas de ser objeto de un ciberataque. En tal sentido, existe la necesidad de que nuestro país tome medidas de precaución respecto a la gestión de riesgos digitales, considerando la implementación de un programa de cumplimiento de ciberseguridad como la medida de prevención más idónea dentro de la implementación de buenas prácticas de buen gobierno corporativo.

Así mismo, es importante tener en consideración, que a la fecha no existe ninguna ley y/o reglamento emitido por el ente supervisor del sector financiero, que hable o regule de forma específica algo referente a ciberseguridad, como se podrá apreciar posteriormente, nuestro país tan solo ha previsto de forma básica la gestión de riesgos operacionales y gestión de seguridad de la información; por ello, hasta que no exista un pronunciamiento y en aras de prevenir sucesos como los ocurridos en Chile o en México, con el propósito de implementar prácticas de buen gobierno corporativo y asegurar que las empresas están asumiendo la gestión de riesgo según su naturaleza, tamaño y actividades que realizan, es importante que las empresas del sector financiero delimiten los aspectos básicos que se deben de seguir para asegurar que estén protegidas frente a ciberataques y en ese sentido, se delimiten los aspectos esenciales que deberá contener un programa de cumplimiento de ciberseguridad.

Es oportuno mencionar que también será necesario tomar en consideración las medidas que han adoptado otros países y otras entidades del sector financiero como es el caso HSBC (The Hong Kong and Shanghai Banking Corporation) quienes a través de su experiencia mejoraron su sistema de gestión de riesgos.

Objetivos

El presente trabajo de investigación busca determinar la necesidad de implementar un programa de cumplimiento de ciberseguridad como una práctica de buen gobierno corporativo en las entidades que forman parte del sistema financiero peruano, teniendo en consideración que nuestro país no está alejado de ser víctima de un ciberataque y que el desarrollo económico digital, prácticamente obliga a que tanto gobiernos centrales, como las empresas del rubro financiero adopten medidas específicas en ciberseguridad, que contemplen la implementación de políticas, directivas, delegación de funciones, entre otras acciones.

Enfoque Metodológico

Por medio del problema de investigación planteado, se busca determinar la necesidad de tomar medidas de salvaguarda que permitan afrontar o evitar ciberataques en las entidades que forman parte del sistema financiero peruano, por medio de la implementación de programas de cumplimiento en ciberseguridad como una buena práctica de gobierno corporativo; debido a que el constante desarrollo de la tecnología y de la economía digital ha abierto una gran brecha de riesgos para las entidades del sector financiero, tal es el caso del Banco de Chile y entidades del sector financiero de México, que al ser víctimas de diversos ciberataques durante el año 2018, sufrieron pérdidas de millones de dólares.

En tal sentido, nuestro país y de forma especial las entidades del sector financiero están en la obligación de adoptar medidas de prevención, como la implementación de programas de cumplimiento como una buena práctica de gobierno corporativo. Por tal motivo, para el desarrollo del presente trabajo, se propone la aplicación de los siguientes enfoques:

Enfoque comparativo: Teniendo como precedente que países como Chile y México han sufrido ciberataques y en base a ello han desarrollado e implementado su sistema de ciberseguridad, el desarrollo de dicho enfoque permitirá determinar alternativas y/o medidas que podrán ser adoptadas en nuestro país. Asimismo, se tomará en cuenta la experiencia del HSBC en lo referido a gestión de riesgos.

Enfoque de riesgos legales: Teniendo como precedente que el presente trabajo de investigación busca la implementación de un programa de cumplimiento en ciberseguridad y considerando que el programa se traduce en un plan o estrategia que debe ser implementado, corresponde el enfoque de riesgos legales.

CAPÍTULO I: ESTADO DEL ARTE

Como se precisó anteriormente, en los últimos años es gracias al avance tecnológico que se ha logrado un avance a gran escala de la economía digital, la misma que ha demostrado que las fronteras geográficas ya no representan un limitante para la realización de diversas transacciones económicas.

Si bien es cierto que dicha circunstancia representa un logro frente a la optimización de tiempo, resulta innegable que ha creado la necesidad y obligación de las entidades pertenecientes al sector financiero de adoptar las medidas de protección necesarias en el marco de ciberseguridad, con el propósito de evitar situaciones similares a las acontecidas en Chile y México, países que fueron víctimas de ciberataques que provocaron la pérdida de más de 10 millones de dólares respectivamente, por el hecho de no contar con las medidas necesarias de protección.

Es en merito a ello, que el presente trabajo de investigación busca determinar la necesidad de implementar un programa de cumplimiento en ciberseguridad como una buena práctica de gobierno corporativo en las entidades que forman parte del sistema financiero peruano, a fin de evitar o al menos aminorar el nivel de incidencia de ataques digitales como los ya mencionados.

En tal sentido, para poder lograr el objetivo de la investigación y finalmente poder comprobar la hipótesis planteada inicialmente, se requiere desarrollar conceptualmente los siguientes términos:

- Sistema Financiero Peruano
- Estructura del Sistema Financiero
- Economía digital
- Seguridad de la información
- Riesgos
- Tipos de riesgos
- Gestión de Riesgo
- Modelos de Gestión de Riesgo
- Ciberseguridad
- Compliance

- Programa de Cumplimiento
- Gobierno Corporativo.
- Pilares de Gobierno Corporativo

1.1 Sistema Financiero Peruano

Según Hartmann el sistema financiero es definido como aquel conjunto de instituciones, tanto como mercados, que permiten canalizar los ahorros percibidos hacia aquellas unidades que necesitan fondeo para cubrir su déficit. (2003), en esa línea de ideas, el instituto Peruano de Economía ha indicado que gracias a las instituciones que forman parte del sistema financiero se puede canalizar el ahorro hacia la deuda o hacia las inversiones, siendo necesaria la presencia de intermediarios financieros tales como los bancos o a través del uso de instrumentos financieros.

Autores como Samuelson (2005) y Joseph Stiglitz (2006) indican que el sistema financiero constituye una parte muy importante dentro de nuestra sociedad, debido a que, a través del desarrollo de actividades financieras como la transferencia de recursos, hacen posible el uso de dinero de una forma más efectiva y donde se pueda obtener mayor rentabilidad. Samuelson (2005) agrega que el sistema financiero dentro de un país constituye una de las herramientas más importantes para poder controlar los ciclos económicos, hecho que permite adoptar las políticas o medidas necesarias para estabilizar la economía. Stiglitz (2006) precisa que, así como el sistema financiero coadyuva en la creación de riqueza, su colapso también podría generar crisis en un país.

En consecuencia, se puede concluir que gracias a la presencia del Sistema Financiero es posible canalizar los recursos hacia sectores que necesitan fondeo, además de hacer posible la inversión del dinero en actividades económicas como la construcción, industria, entre otras, que promueven el desarrollo económico de un país.

1.1.1 Estructura del Sistema Financiero Peruano

El sistema financiero peruano se encuentra conformado por todo el conjunto de entidades bancarias, financieras y demás entidades que se encuentran bajo el ámbito de supervisión de la SBS.

Las empresas que forman parte del sistema financiero tienen entre sus funciones realizar el flujo monetario y canalizar el dinero hacia aquellas personas que tengan el deseo de invertir, básicamente está conformado por:

- Bancos
- Financieras
- Cajas Municipales de Ahorro y Crédito.
- EDPYME
- Cooperativas
- Cajas Rurales, etc

1.2 Economía Digital

Es definida como aquel entorno caracterizado por el predominio del uso de tecnología de la información por medio del cual se pueden realizar transacciones con la participación de los distintos agentes económicos, fomentando la creación de nuevas costumbres y patrones de consumo, teniendo en cuenta que las barreras geográficas ya no representan una limitación para poder concretar negocios, propiciando un mercado más transparente y eficiente gracias a que con el uso de las tecnologías de las información, los clientes pueden obtener mayor y mejor información sobre los productos y servicios que el mercado ofrece. (Duarte, 2010)

Según CEPAL[1] (2013) la economía digital también ha sido definida como un facilitador del desarrollo de actividades económicas a través de una infraestructura constituida por las telecomunicaciones, software, hardware, computación en la nube, redes sociales, así como las móviles, que está constituida principalmente de tres componentes que se encargan de determinar su grado de madurez; dependiendo el nivel de desarrollo en cada país, los componentes son:

- Infraestructura de redes de banda ancha: Constituido por la conectividad a nivel nacional e internacional, redes de acceso, así como los puntos de acceso

[1] CEPAL: Es una de las cinco comisiones regionales de las Naciones Unidas, se fundó con el propósito de contribuir al desarrollo económico de América Latina.

- Industria de aplicaciones: Este componente toma en consideración la industria de software y hardware, infraestructura de redes, así como la industria de negocios (incluye servicios financieros, contables) y procesos de conocimiento (se refiere a servicios analíticos, de diseño, investigación y desarrollo tecnológico)
- Usuarios finales: Grupo en el que se encuentran los individuos, distintas empresas del mercado y finalmente el gobierno.

Sin embargo, según un informe emitido por el Departamento de Comercio ha identificado como componentes de la economía digital:

- Industrias de las Tecnologías de la Información y la Comunicación.
- Comercio electrónico entre empresas
- Distribución de bienes y servicios en un entorno digital
- Sistemas y servicios que necesitan de internet

Otros autores han definido a la economía digital como un nuevo sistema socio – político y económico, cuya característica principal es que se encuentra compuesto por un entorno inteligente que se encuentra constituido por instrumentos de acceso, información, así como el procesamiento de dicha información, además de considerarlo como un fenómeno emergente íntimamente relacionado con la microeconomía, macroeconomía y teoría de la Organización y de la Administración.

Autores como Margherio y Kling y Lamb citados por del Águila, realzan la importancia de la economía digital al precisar que esta se encargara de explicar el crecimiento económico en las siguientes décadas. (2001)

Entidades financieras como BBVA, sostienen que la economía digital a través del desarrollo de nuevos sectores de las tecnologías de la información y de la comunicación, así como la promoción del desarrollo de nuevas empresas, contribuyen directamente al desarrollo de la economía, gracias al mayor grado de eficiencia y productividad que se ha alcanzado con el uso de la tecnología.

Este hecho ha generado la transformación de las empresas, gobierno y cultura, incidiendo directamente en el estilo de vida de sus usuarios, transformando, por ejemplo, la forma de prestación de los servicios financieros.

Si bien es cierto que ha traído innumerables beneficios para sus usuarios, este hecho ha abierto una gran brecha de amenazas y riesgos que necesitan la intervención inmediata del gobierno con el fin de garantizar la seguridad de las transacciones realizadas, así como el desarrollo normativo, para seguir fomentando en el crecimiento económico. (BBVA, 2015)

Es preciso indicar que, según informes sobre economía digital, se ha logrado determinar que esta tiene un volumen que oscila entre el 4.5% y 15.5% del PIB mundial, siendo los servicios informáticos los que tiene un mayor desarrollo a nivel mundial y los principales generadores de empleo, pero que necesita de forma inmediata el establecimiento de las reglas a seguir, considerando la adaptación de las normas ya existentes y la creación de nuevas políticas y normas que regulen los aspectos necesarios que abarca la transformación digital, que además de necesitar de políticas nacionales requiere llegar a un consenso global, creando políticas internacionales. (Naciones Unidas, 2019)

Básicamente, la importancia de la economía digital consiste en entender que el uso de las tecnologías de la información han facilitado el rol de la economía a nivel mundial, promoviendo de forma directa su desarrollo, gracias a que el uso de la tecnología ha permitido mayor eficiencia en el desarrollo de diversas actividades, como es el caso del sistema financiero, que gracias al uso de la tecnología permite que sectores que no eran atendidos puedan tener acceso a los servicios que ofrecen además de brindarnos la posibilidad de realizar diversas transacciones a través de plataformas virtuales, teniendo en cuenta ello, es importante que cada una de las empresas que forman parte de este sector, adopten las medidas de seguridad más idóneas y convenientes, de acuerdo a su naturaleza y tamaño para evitar, prevenir y reaccionar frente a un ciberataque; en tal sentido, resulta conveniente desarrollar que es seguridad de la información.

1.3 Seguridad de la Información

Según la circular SBS N°G-140-2009, se entiende como seguridad de la información a la adecuada combinación de políticas, procedimientos, estructura organizacional y herramientas informáticas especializadas, con el propósito de que dicha información cumpla con los siguientes criterios:

- Confidencialidad: Indica que la información solo estará disponible para aquellas personas que estén debidamente autorizadas para su acceso.
- Integridad: La información deberá estar completa, exacta y valida.
- Disponibilidad: Implica que la información debe estar disponible y de forma organizada, para aquellas personas que tenga autorización para su acceso cuando lo requieran.

Según lo regulado en la ISO N°27001 se entiende por seguridad de la información, a aquella actividad que tiene como objetivo principal asegurar que los activos de información de una empresa, sean utilizados de forma adecuada, lo cual implica que se respeten los accesos de información que se hayan establecido.

Considerando que el objetivo del presente trabajo de investigación es prevenir aquellos eventos o contingencias que pretendan afectar activos de información, es importante definir que es riesgo, cuáles son los tipos de riesgo y cuáles son los modelos de gestión de riesgo.

1.4 Riesgos

Dentro del problema de investigación que se ha planteado, se necesita tener una noción de riesgo, para comprender con mayor amplitud los problemas que ha traído consigo el uso de las tecnologías de la información y así entender la necesidad de fomentar la implementación de programas de cumplimiento en ciberseguridad como buena práctica de buen gobierno corporativo.

Según lo ha definido el Banco Interamericano de Desarrollo (Garcia Zavallos, 2017), riesgo es aquella posibilidad que se tiene de sufrir un daño, el mismo que es consistente en la pérdida de valor económico. Por otro lado, Murillo desarrolla una definición distinta de riesgo, indicando que se trataría de la posibilidad de obtener una ganancia.

Etchichury en concordancia con las dos posiciones desarrolladas previamente, indica que se pueden distinguir dos tipos de riesgo: negativos y positivos. Los primeros hacen referencia a aquellas circunstancias que obstaculizan el normal funcionamiento del mercado, impidiendo que se desarrollen actividades de comercio en un ambiente seguro; mientras que los riesgos positivos son aquellos que vienen a formar parte de la organización social y económica que las mismas entidades financieras generan, un ejemplo de ello son las acciones que se toman con el fin de

obtener un mayor margen de eficiencia frente a otras entidades y así generar una mayor fidelización de sus clientes. (2016)

Según lo referido por el ISO 31000 – Gestión Integral de Riesgo, indica que la palabra riesgo hace referencia a un estado de incertidumbre respecto a los objetivos planteados por una organización, pudiendo ser positivos o negativos que crean o ayudan a destacar oportunidades y amenazas. Asimismo, se ha precisado que el término riesgo va de la mano de los términos: gestión del riesgo, fuente del riesgo, evento, consecuencia.

Según lo desarrollado en el Reglamento de Gobierno Corporativo y de la Gestión Integral de Riesgo, se trata de la posibilidad de ocurrencia de eventos que pudieran impactar de forma negativa en los objetivos que ha adoptado la empresa o incidir de forma negativa en la situación financiera de una empresa, ante estos hechos generadores de resultados negativos para una empresa, se ha regulado de forma expresa, el deber de las empresas de realizar la gestión integral de riesgos, que consiste en determinar de manera clara los potenciales eventos que pudieran afectar el logro de los objetivos. (Resolución SBS N°272-2017)

Entonces según lo desarrollado previamente, se puede definir *riesgo*, como aquel daño o perjuicio que puede entorpecer la normal consecución de objetivos de una empresa; así, desde el año 2017 a través de la publicación del Reglamento de Gobierno Corporativo y de la Gestión Integral de Riesgos, se ha implementado como parte de las prácticas de buen gobierno corporativo, la obligación y/o el deber de las empresas de gestionar el riesgo que le es inherente a una empresa, requiriendo que, desde los directores, gerentes y demás colaboradores, tengan la facultad de identificar los potenciales riesgos que puedan afectar sus labores y gestionarlos de acuerdo a su apetito por el riesgo. En tal sentido, es obligación de todas las empresas diseñar y aplicar la gestión integral de riesgos de acuerdo a su naturaleza, tamaño y complejidad de las operaciones que realizan.

1.4.1 Tipos de Riesgo

Según lo desarrollado por el Reglamento de Gobierno Corporativo y Gestión Integral de Riesgos, emitido por la SBS, se distinguen los siguientes tipos:

- Riesgo de Crédito: Asociado con la omisión de las obligaciones contractuales (por ejemplo: la falta de voluntad de pago).
- Riesgo de Lavado de Activos: Que se utilice a la empresa con el fin de realizar el lavado de activos y financiamiento del terrorismo.
- Riesgo de Liquidez: Hace referencia a la pérdida de activos.
- Riesgo de Mercado: Hace referencia a la posibilidad de sufrir pérdidas debido a las fluctuaciones de las tasas de interés., tipo de cambio.
- Riesgo Reputacional: Cuando el nombre de la empresa se ve dañado, además de generar la pérdida de confianza de clientes.
- Riesgo Estratégico: Relacionado con la creación de ventajas competitivas.
- Riesgo Operacional: Posibilidad de sufrir pérdidas debido a prácticas inadecuadas, ***uso de tecnología,*** o eventos externos, incluyendo la gestión de riesgo legal.

Como se puede apreciar, en el caso de riesgo operacional se ha incluido dos tipos más de riesgo, y son:

- Riesgo Tecnológico o Digital: Según la definición desarrollada por Ganguly (2017), se entiende por riesgo digital a aquel término que engloba a todos aquellos riesgos que son producto del uso de las tecnologías de la información (software, sistemas, inteligencia artificial, fuentes de datos. Explica además que riesgo digital implica la adecuación de las tecnologías de la información dentro de la estructura organizacional y cultural de una empresa, para su mejor gestión.
- Riesgo Legal: Conforme a lo desarrollado en el Reglamento para la Gestión de Riesgo Operacional, se entiende por riesgo legal a aquella posibilidad de que ocurran pérdidas financieras, a causa de fallas en la ejecución de contratos o acuerdos, incumplimiento de las normas, así como la existencia de factores externos, por ejemplo, cambios regulatorios, etc.

La importancia de determinar los tipos de riesgos que existen, nos permite entender que cada uno de estos tipos tiene o engloba un ámbito de acción distinto, por ejemplo mientras que el riesgo de crédito hace referencia a la omisión de pago de una obligación contractual, el riesgo reputacional hace referencia a la posibilidad que el nombre de una empresa se vea afectado, en tal sentido, las medidas, políticas, acciones, planes a implementar serán distintos; es así que resulta

conveniente tener conocimiento sobre como los riesgos que se han identificado deben de ser tratados o gestionados.

1.4.2 Gestión de Riesgo

Según el ISO 31000 se indica que para una adecuada gestión de riesgo (actividades realizadas con el propósito de dirigir y controlar la organización con relación a los riesgos identificados de una sociedad) se deberán cumplir ciertos principios, siendo los siguientes:

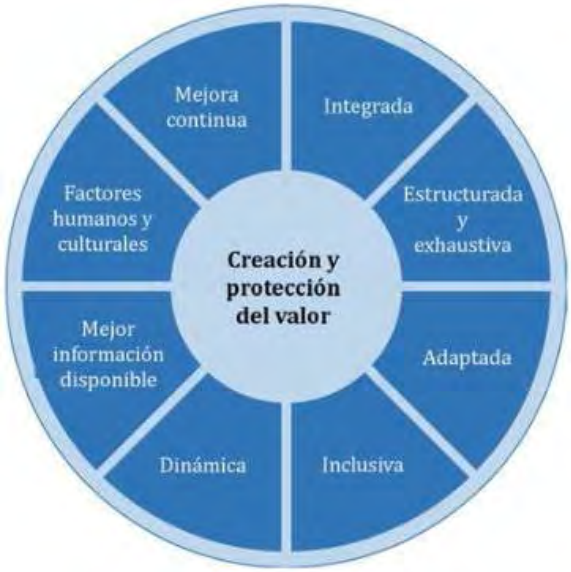

Figura 1. Principios gestión de riesgo (ISO 31000)

- Integrada: Indicando que la gestión del riesgo es parte integral de las actividades de una organización.
- Estructurada y exhaustiva: Haciendo referencia a que se necesita un enfoque estructurado y exhaustivo contribuyendo a obtener resultados coherentes y comparables.
- Adaptada: La gestión del riesgo deberá ser adaptada y proporcional a los contextos externos e internos ligados con los objetivos de la empresa.
- Inclusiva: Deberá considerar a todas las áreas que forman parte de la organización.

- Dinámica: La gestión del riesgo deberá responder tanto a los cambios internos como a los cambios externos de la organización.
- Mejor información disponible: Indicando que la gestión del riesgo se basa en información histórica y actualizada, además de tomar en consideración expectativas futuras, para lo cual se requiere que la información tenga que ser clara además de disponible para las partes interesadas.
- Factores humanos y culturales: indicando que el comportamiento humano y cultura cobran un papel importante.
- Mejora continua: Precisando que a través del aprendizaje y experiencia se tendrá una mejor continua de la gestión de riesgo.

En tanto para que todos los principios descritos anteriormente puedan ser cumplidos, se necesita el trabajo conjunto de los miembros de la alta dirección así como de los órganos de supervisión, para ello es necesario establecer una cultura de cumplimiento, plan o línea de acción, asegurar los recursos necesarios; elementos que propiciaran que la organización gestione el riesgo conforme a los objetivos, estrategia y cultura, establecer la forma en la cual se gestionara el riesgo, promover el seguimiento de riesgos y finalmente asegurar que los riesgos están siendo gestionados de manera adecuada. (2018)

Diversos autores han definido gestión de riesgo como aquel proceso por medio del cual se identifican, analizan y cuantifican todas las probabilidades de perdida y efectos secundarios que se desprenden por la ocurrencia de algún incidente; asimismo, precisan que la gestión de riesgo comprende las acciones preventivas que deben adoptarse para evitar la incidencia de riesgos que pudieran generar daños o perdidas.

Según lo definido por la Federación Europea de Administración del Riesgo (FERMA) la gestión de riesgos constituye parte medular de la gestión estratégica de una empresa, explicando que por medio de este proceso las empresas obtienen un beneficio, aumentando sus probabilidades de tener éxito y al mismo tiempo reduce las probabilidades de sufrir un impacto negativo, precisando que es necesario que la gestión de riesgos este articulada con la cultura de la empresa a través de la implementación de una política y un programa que deberá contar con la participación activa de la alta dirección. (2002)

Según lo regulado en el artículo 22° del Reglamento de Gobierno Corporativo y de la Gestión Integral de Riesgos emitido por la SBS, se refiere a aquel proceso que es desarrollado por los miembros del directorio, gerentes y trabajadores de toda la empresa para la definición, identificación de potenciales eventos, para determinar la forma de gestionarlos de acuerdo al nivel de apetito por el riesgo de la empresa.

Mientras que el mismo reglamento, ha definido apetito por el riesgo, como el nivel de riesgo que una empresa puede asumir para lograr los objetivos que se hayan planteado.

Según lo desarrollado previamente, se puede concluir que la gestión de riesgos está referida a aquellas acciones, procesos, por medio de los cuales se identifican, analizan los riesgos que le son inherentes a una empresa, y de esa forma se adoptan las medidas de mitigación o prevención necesarias para controlar los riesgos identificados. Para ello, en la actualidad existen una serie de modelos de gestión de riesgo que desarrollan de forma detallada las consideraciones que se deben de tener en cuenta para realizar una adecuada gestión de riesgos.

1.4.3 Modelos de Gestión de Riesgo

Como se precisó previamente, en la actualidad existen diversos modelos de gestión de riesgo que dan la pauta sobre los procesos que se deben de seguir para una óptima gestión de riesgos; en ese sentido, para el desarrollo del presente trabajo se han tomado en consideración los siguientes modelos de gestión de riesgo:

1.4.3.1 Modelo ISO 31000

Según lo desarrollado por la ISO 31000, el proceso para la correcta gestión de riesgos, implica la implementación de políticas, procedimientos, además del establecimiento de evaluaciones, tratamiento, revisión y registro de riesgos, conforme se puede apreciar en el siguiente esquema:

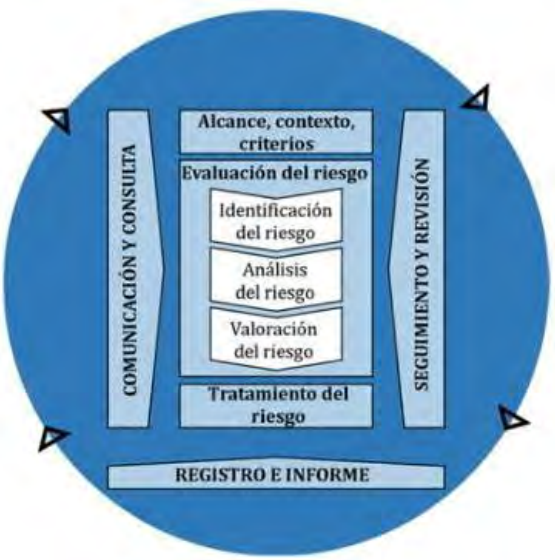

Figura 2. Modelo de Gestión ISO 31000

Se ha precisado que el proceso de gestión de riesgo forma parte importante de la gestión y toma de decisiones, siendo necesaria su integración dentro de los procesos y en general dentro de la estructura de toda organización.

- **Comunicación y consulta:** Proceso por medio del cual se brinda soporte a las partes interesadas para que puedan comprender el riesgo, aspectos preliminares para la toma de decisiones. Por medio de la comunicación se busca sembrar conciencia respecto a la importancia del riesgo, mientras que por medio de la consulta se busca dar retroalimentación para ayudar en la toma de decisiones.
- **Alcance, contexto y criterios:** Con el propósito de realizar una evaluación de riesgo eficaz y darle un tratamiento adecuado, es importante tener que definir el alcance, el contexto y criterios a usar durante la gestión de riesgos.

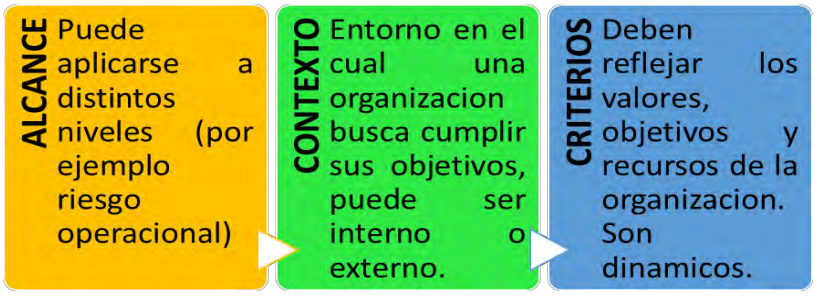

Figura 3. Alcance, contexto, criterios (Adaptado de: ISO 31000)

- **Evaluación del riesgo:** Esta parte del proceso incluye la identificación del riesgo, análisis del riesgo y valorización del riesgo. Este proceso puede ser entendido con el siguiente esquema:

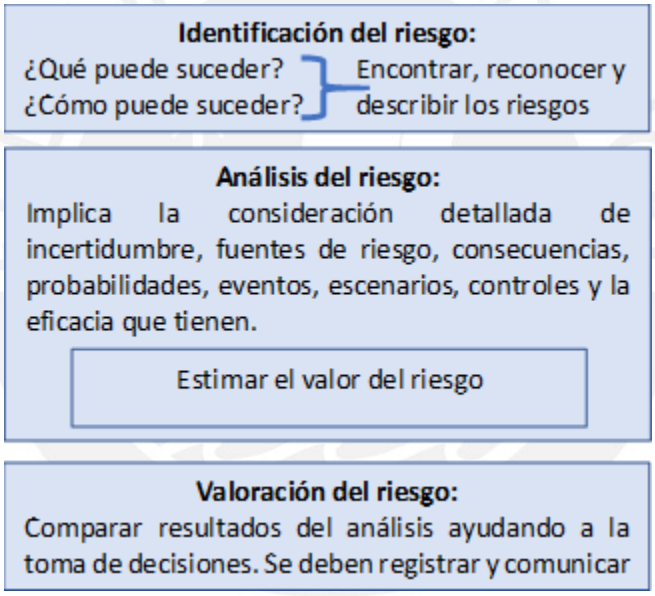

Figura 4. Evaluación del riesgo (Adaptado de: ISO 31000)

- **Tratamiento del riesgo:** Consiste en establecer opciones para la gestión del riesgo. Este proceso implica la formulación y selección de opciones para el tratamiento, así como la planificación y evaluación del tratamiento y en base a los resultados obtenidos, tomar acciones adicionales en caso el nivel de riesgo no sea aceptable. Dentro de las opciones de tratamiento están:
  a. Aceptar o aumentar el riesgo.
  b. Eliminar la fuente de riesgo.

c. Evitar el riesgo.
d. Retener el riesgo.
e. Modificar su probabilidad.
f. Compartir el riesgo.
g. Modificar sus consecuencias.

- **Seguimiento y revisión:** A través de este paso se puede verificar y tener aseguramiento respecto de la calidad y eficacia del diseño del proceso de gestión de riesgo. Esta etapa incluye la planificación, recopilación y análisis de información.

- **Registro e informe:** La importancia del registro incide en la posibilidad de brindar información para la correcta adopción de decisiones, mejorar aquellos procesos en los cuales se hayan encontrado deficiencias.

1.4.3.2 Modelo AIRM, IRM

El referido modelo ha sido desarrollado con la participación del Institute of Risk Management (IRM), Association of Insurance and Risk Managers (AIRMIC) y ALARM, principales organizaciones de riesgos en Reino Unido.

El equipo encargo del desarrollo del modelo, preciso que para la correcta gestión de riesgos, es necesario tener que definir reglas con el propósito de determinar cuál será el proceso por medio del cual se podrán gestionar los riesgos, la estructura orgánica de la empresa y cuáles son los objetivos a seguir.

Según este modelo, la gestión de riesgos seguirá el siguiente esquema:

Figura 5. Modelo de gestión AIRM (Federation of European Risk Management Associations)

Se ha precisado que por medio de este proceso se da soporte para la consecución de objetivos a través de:

- Estructura orgánica que hace posible que las actividades desarrolladas dentro de la empresa sean realizadas de manera estable y controlada.
- Visión integrada del negocio, lo cual permite tener conocimiento de las oportunidades y amenazas de la empresa, además de servir para la toma de decisiones.
- Contribuye a la asignación eficiente de los recursos de la empresa.
- Ayuda a proteger la imagen y nombre de la empresa.
- Ayuda a la formación de cultura.

1.4.3.3 COSO ERM

El modelo fue desarrollado por el Committee of Sponsoring Organizations of the Treadway Commission (COSO) cuyo propósito principal, es el de brindar marcos integrales así como orientación para la gestión de riesgos empresariales, control interno y la disuasión de fraude.

Según este modelo, existe una relación estrecha entre los objetivos y la gestión de riesgos empresariales, los mismos que han sido reflejados a través de una matriz tridimensional en forma de cubo, de la siguiente manera:

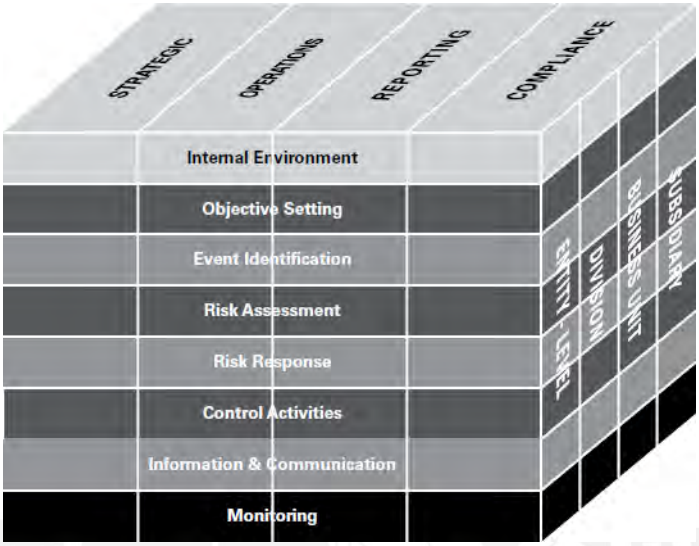

Figura 6. Modelo de gestión COSO (Approaches to risk management)

El cubo COSO ERM constituye un marco de gestión influyente y se encuentra conformado por ocho componentes interrelacionados y son:

- Entorno interno: establece la base sobre cómo debe ser abordado el riesgo.
- Establecimiento de objetivos: indica que se deben de establecer objetivos antes de que la gerencia identifique algunos eventos que pudieran evitar la consecución de objetivos.
- Identificación de eventos: Implica que se deberán de reconocer aquellos eventos internos o externos que perturban la consecución de objetivos; es preciso que se realice la distinción de riesgos y de oportunidades de mejora.
- Evaluación de riesgos: Indica que los riesgos deberán ser analizados, tomando en consideración la probabilidad y el impacto para determinar cómo deben ser gestionados.
- Respuesta al riesgo: En este punto se deberá determinar si se evita, se acepta o se reduce el riesgo.

- Actividades de control: En esta etapa deberán de establecerse e implementar políticas y procedimientos que puedan garantizar que la respuesta a los riesgos que han sido identificados de forma previa, sean gestionados de manera efectiva.
- Información y comunicación: La información obtenida deberá ser puesta de conocimiento, para que las personas puedan cumplir con sus responsabilidades.
- Monitoreo: En esta etapa se debe de monitorear todos los pasos efectuados de forma previa a fin de ver como se gestión los riesgos identificados y realizar modificaciones en caso sean necesarias.

Es preciso mencionar que todos los modelos desarrollados previamente brindan un enfoque general para la correcta gestión de riesgos, detallando que estos modelos son una combinación de los procesos que deben de seguirse para la gestión riesgos y el marco recomendado.

En merito a lo expuesto, considerando que la gestión de riesgos permite a las empresas obtener un valor añadido, que logra proteger los activos de la empresa y que permite la optimización de recursos, es importante conocer lo referido a ciberseguridad, teniendo en cuenta que en los últimos años este tema ha cobrado mayor relevancia en el sector financiero a raíz de los distintos ciberataques que han afectado a este sector.

1.5 Ciberseguridad

Según lo desarrollado por la Unión Internacional de Telecomunicaciones[2], se trata del conjunto de herramientas, políticas, conceptos de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden ser utilizados con el fin de proteger los activos digitales de la organización si como la información de los usuarios en el ciber entorno. (2008)

[2] Unión Internacional de Telecomunicaciones: Es el organismo especializado en tecnologías de la información y comunicación de las Naciones Unidas, está encargado de regular los TIC a nivel mundial.

Por su parte ISACA (Systems Audit and Control Association)[3] define ciberseguridad como la protección de los activos de información a través del tratamiento de las diversas amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados.

En esa misma línea de ideas Kshetri define ciberseguridad como aquella que involucra tecnología, conceptos, políticas, procesos y prácticas que buscan proteger y salvaguardar los accesos a computadoras, infraestructura, aplicaciones, servicios, sistema de telecomunicaciones e información de ataques, daños y accesos no autorizados. (2016)

Otros autores refieren que ciberseguridad y seguridad de la información son términos equivalentes; en tal sentido, según lo expuesto en la ISO 27001 – Sistemas de Gestión de Seguridad de la Información, el termino seguridad de la información hace referencia al conjunto de medidas con carácter preventivo y reactivo que adoptar las organizaciones con el propósito de mantener la confidencialidad, disponibilidad e integridad de la información:

- Por confidencialidad se entiende que la información no es ni será puesta a disposición de individuos que no cuenten con una autorización.
- Por integridad se entiende como el propósito u objetivo de mantener de forma "completa" la información y procesos de la organización.
- Por disponibilidad se entiende a la posibilidad de poder acceder a la información y sistemas cada vez que sea requerido.

Además de ello se tiene que el Sistema de Gestión de Seguridad de la Información (SGSI) es un concepto central del referido ISO, el cual busca garantizar la protección total de los activos digitales a tras del cumplimiento de la normativa, protección de información.

Se ha precisado que el SGSI deberá contener al menos:

- Manual de Seguridad: el mismo que deberá determinar los alcances, objetivos a seguir, responsabilidades de las partes integrantes, políticas.
- Procedimientos: que tienen la calidad de operativos, que buscan asegurar la planificación, operación y control de procesos de seguridad de la información.

[3] ISACA (Systems Audit and Control Association): Es una asociación independiente global, que tiene como objetivo el desarrollo de actividades relacionadas con la práctica de la auditoria, el control y la seguridad de los sistemas de información.

- Instrucciones / checklists / Formularios: son aquellos documentos que describen la forma de realización de tareas y demás actividades.
- Registros: estos documentos son evidencia del cumplimiento del SGSI.

Entonces, según lo desarrollado de forma preliminar, se deduce que el termino ciberseguridad está referido a aquellas medidas (procedimientos, directrices, políticas, etc) adoptadas con el propósito de salvaguardar los activos de información de una empresa, es así que, para el desarrollo del presente trabajo de investigación, resultante bastante conveniente desarrollar la noción de compliance.

1.6 Compliance

Para entender que es un programa de cumplimiento, es necesario tener en cuenta que es compliance y cuáles son sus implicancias.

Garat, ha definido compliance como aquellos actos que están destinados a dar cumplimiento a las normas que regulan determinadas empresas, indicando que comúnmente este término es asociado al sector financiero, aunque en realidad el compliance abarque más áreas como el derecho ambiental, penal, entre otros. (2018)

La empresa auditora Deloitte, considerada una de las *big four,* precisa que compliance o cumplimiento normativo en español, hace referencia al establecimiento de políticas así como de procedimientos que sean lo suficientemente adecuados para asegurar que determinada empresa, pueda desarrollar sus actividades conforme a la normativa vigente que le es aplicable, políticas y procedimientos internos establecidos por la empresa, promoviendo entre todos los que conforman la empresa (alta dirección, colaboradores) una cultura de cumplimiento. Dicha empresa, ha precisado también que dentro de los retos que debe afrontar el cumplimiento normativo se encuentran los siguientes:

a. Reto Humano: Que consiste en la especialización de los profesionales en este campo de cumplimiento normativo, teniendo la responsabilidad de adquirir los conocimientos necesarios.
b. Reto de Procesos: Se deben delimitar procesos sólidos, que minimicen los riesgos de incumplimiento normativo. Contar con metodologías de reporte y de seguimiento.

c. Reto Tecnológico: Para lo cual se debe de tener presente el desarrollo de las tecnologías de la información y de la comunicación, logando determinar los riesgos a los cuales están expuestas las empresas. (Deloitte)

En esa misma línea de ideas, según lo desarrollado en el Libro Blanco, por medio del compliance se *asume las tareas de prevención, detección y gestión de riesgos,* lo cual contribuye a promover y desarrollar una cultura de cumplimiento en el seno de la organización. (2017)

Por su parte Soler, ha precisado que en consideración al gran desarrollo que ha alcanzado la tecnología en los últimos años, y que ello ha propiciado una brecha de riesgos digitales, es obligación de las empresas tener que asegurar la protección de sus datos, por ello, a través de compliance se deben de delimitar controles de seguridad.

Como se puede discernir de los conceptos desarrollados, a través del compliance se adoptan una serie de medidas y políticas que buscan cumplir con lo establecido con la normativa externa e interna de la empresa, hecho que coadyuva a desarrollar la cultura de cumplimiento dentro de la empresa y que podrá ser esquematizada de mejor forma a través del programa de cumplimiento.

1.7 Programa de Cumplimiento

Dentro del trabajo de investigación, se propone la implementación de programas de cumplimiento como una alternativa de solución frente a los riesgos y eventos de perdida que se han generado en las entidades financieras, como consecuencia del desarrollo de la economía digital, es decir el mayor uso de las tecnologías de la información y de la comunicación para realizar transacciones comerciales.

Según lo desarrolla Artaza Varela, cuando se habla de programa de cumplimiento, se habla de aquellas medidas adoptadas por determinada sociedad, con el propósito de controlar, dentro de los límites exigibles, los peligros de infracción al ordenamiento jurídico, derivados por la misma actividad de la empresa. (2014)

En esa misma línea de ideas, Clavijo indica que el programa de cumplimiento es aquel dispositivo que adecuan las empresas con el fin de dar cumplimiento a la normativa, que además

se encarga de prevenir y detectar las infracciones legales en las que podrían incurrir las empresas a consecuencia de las actividades que están realizan. (2014)

Conforme establece la US Federal Sentencing Guidelines for Corporations (citado por Astudillo, 2015), un programa de cumplimiento deberá tener mínimamente los siguientes elementos:

- Tener un oficial de cumplimiento.
- Establecer procedimientos para prevenir y detectar la conducta criminal.
- Presencia de un órgano que se encargue de la revisión y mejora del programa de cumplimiento.

En esa línea de ideas, Gómez (citado por Astudillo) indica que un programa de cumplimiento deberá tener mínimamente:

- Personal encargado de la supervisión del programa de cumplimiento.
- Reforzamiento del programa a través de controles y auditorias.
- Aplicación de sanciones disciplinarias.
- Capacitación a todos los miembros de la empresa.

Es importante precisar que los programas de cumplimiento y gobierno corporativo son términos que deben ir de la mano para la correcta administración de una empresa, ya que su implementación de forma conjunta, permitirá dar un valor agregado. Ambos conceptos implican la participación de forma activa de la alta dirección.

1.8 Gobierno Corporativo

Según define el Código de la Organización para la Cooperación y el Desarrollo Económico (OCDE), el gobierno corporativo es aquel sistema por medio del cual se dirigen y controlan las sociedades. Dicho sistema realiza la distribución de derechos y responsabilidades entre todos los agentes que forman parte de la sociedad (accionistas, directorio, gerentes y demás agentes económicos).

La Superintendencia de Mercado y Valores (SMV) por su parte indica que la adopción de prácticas de buen gobierno corporativo además de generar un clima de respeto dentro de la

empresa, coadyuvan en gran magnitud a generar valor, solidez y eficiencia, trayendo consigo una mejor administración de los riesgos a los cuales están expuestas las empresas.

Por su parte Hundskopf citado por Alfaro, indica que cuando se habla de gobierno corporativo se hace referencia a aquellas políticas que adoptan las empresas con el fin de *obtener mayor transparencia credibilidad y valor ante posibles inversionistas.* (2008)

Gregory, indica que gobierno corporativo es aquella combinación de normas, regulaciones, normativa interna de las empresas privadas que permiten generar mayores beneficios dentro de una empresa. (2005)

Según lo definido por la Superintendencia de Banca, Seguros y AFP gobierno corporativo es el conjunto de procesos, políticas, normas y prácticas que determinaran la forma en la que una empresa es dirigida, gestionada y controlada. En tal sentido por medio del artículo 3 de la Resolución SBS 272-2017 se indica que las empresas del sector financiero están en la obligación de determinar los principios y lineamientos que adoptaran para la implementación de prácticas de gobierno corporativo.

1.8.1 Pilares de Gobierno Corporativo

Según lo regulado dentro del Código de Buen Gobierno Corporativo para las Sociedades Peruanas, emitido por la SMV, existen cinco pilares que guían su correcta implementación, siendo los siguientes:

- Derechos de los accionistas: hace mención a la participación de los accionistas dentro de la empresa
- Junta general de accionistas: hace referencia a la forma en la que los accionistas podrán ejercer sus derechos.
- Directorio y Alta Gerencia: hace mención a la forma en la que deberá estar conformada, imponiendo el deber, de ser los pioneros en cumplir con las prácticas de buen gobierno corporativo.
- Riesgo de Cumplimiento: implica que la empresa este alineada con la normativa que le es aplicable, además de ayudar a determinar los riesgos a los cuales estaría expuesta una empresa al no cumplir la implementación de determinada norma.

- Transparencia de la información: La misma que constituye el factor principal para poder generar confianza.

Luego del desarrollo conceptual de los términos descritos previamente, es oportuno indicar que se comprueba la conexión estrecha que tienen, considerando que el presente trabajo está orientado a que las entidades del sistema financiero puedan adoptar medidas de protección frente a los riesgos digitales a los cuales están expuestos.

En tal sentido, ha sido importante conocer la noción de sistema financiero y cuál es su estructura, para entender que su presencia tiene un rol protagónico en el desarrollo económico del país, según lo expuesto por Samuelson (2005) y Stiglitz (2006) gracias al desarrollo de las actividades financieras, además de obtenerse mayor rentabilidad, se hace uso del dinero de forma más efectiva, llegando a sectores menos beneficiados y promoviendo la inversión en los distintos sectores económicos de nuestro país.

Seguidamente, como parte fundamental del presente trabajo, ha sido imprescindible denotar la importancia del uso de las tecnologías de la información y de la comunicación para el desarrollo de la economía digital, circunstancia que ha permitido mayor dinamización de los distintos sectores económicos, siendo el sector financiero uno de los sectores que ha tenido mayor desarrollo gracias al uso de la tecnología, que si bien es cierto ha traído consigo grandes ventajas para sus clientes, también ha significado la apertura de una gran brecha de riesgos para este sector, estas brechas son traducidas en el incremento de incidentes que afectan los activos de la información de las empresas, causando la perdida de cuantiosas sumas de dinero además de generar daños reputacionales, entre otros.

Es así que, en consideración del nivel de vulnerabilidad de los activos de información y el riesgo latente de sufrir ciberataques, ha sido oportuno desarrollar lo referido a riesgos y el proceso que se sigue para su adecuada gestión. Este tema nos conecta de forma directa con las nociones de programa de cumplimiento, compliance y gobierno corporativo, términos que cobran gran relevancia al vislumbrar que gracias a su implementación se logra que las empresas tengan un valor añadido, que va siempre alineado a los objetivos de la empresa y en la protección de todos sus activos.

CAPÍTULO II: PROBLEMA DE INVESTIGACIÓN

Como punto de partida, es importante destacar que gracias al avance de las Tecnologías de la Información y de la Comunicación (TIC) que en la actualidad existe mayor dinamicidad en nuestra vida diaria; acceder a la información es más sencillo, comunicarnos con otras personas resulta totalmente fácil, las cartas o telegramas pasaron a la historia con la aparición de las redes sociales; y diversas actividades han sido simplificadas, como por ejemplo realizar compras desde casa.

Dicha circunstancia ha dado pie a la digitalización de la economía o al desarrollo de la *economía digital,* la misma que ha sido definida o es entendida por el uso extendido de las TIC, a través de la promoción y desarrollo de las empresas, y la innovación en la forma de llevar a cabo negocios tradicionales, como por ejemplo la transformación de los servicios financieros. (Carmen Cuesta, 2015).

Numerosos estudios, tanto del Banco Mundial, del Foro Económico Mundial como del BID han demostrado que en América Latina ha crecido a pasos agigantados, identificándose entre los servicios con mayor desarrollo el comercio, educación, servicios alimentarios y servicios financieros. (García Zavallos, 2017)

Sin embargo, pese a los nuevos beneficios que aportan tanto a sus usuarios como a las mismas empresas, también ha significado la creación de riesgos y amenazas potenciales, dirigidos principalmente a atentar en contra de los activos de información de las empresas.

Es importante resaltar que, según datos brindados por el Foro Económico Mundial, al año 2018, el robo de datos, afectación de activos de la información o ciberataques, forman parte del top cinco de los principales riesgos mundiales por su nivel de probabilidad; en esa línea de ideas, según una encuesta realizada por la consultora Price Waterhouse Cooper sobre *Delitos Económicos* durante

el año 2016, se pudo determinar que a nivel mundial los ciberataques tienen un nivel de incidencia alarmante, como se puede corroborar en el siguiente cuadro:

Figura 7. Fuente: Delitos económicos durante el 2017 (Aroni Cordova, Nancy, Barrios Elias, Rita)

En el caso específico de nuestro país, estas cifras son igual de alarmantes, según el informe sobre índice de Exposición Nacional, elaborado por la empresa Rapid7, empresa estadounidense especialista en la protección de activos digitales, al 2018 nuestro país formaba parte del top 50 de países con mayor exposición de sufrir ciberataques. Y al 2019, según un estudio desarrollado por la empresa ESET en América Latina, nuestro país es el tercer país que presento mayores niveles de ciberataques. Según reporte del diario Gestión, al año 2018 los ciberataques aumentaron en un 600%, siendo las empresas más vulnerables las pertenecientes al sector financiero, retail y consumo masivo.

Los ciberataques en nuestro país, dirigidos a afectar el sector bancario y financiero han crecido de forma potencial, y así lo afirma la empresa Kaspersky concluyendo que el sector financiero es el más afectado, y que el nivel de incidencia de estos eventos alcanzan el 28.63%.

Dicho problema además de poner en peligro los sistemas de seguridad de la información de las empresas del sector financiero, ha significado la perdida de millones de soles a nivel mundial. Al año 2018, el número de ciberataques reportados a nivel mundial causaron pérdidas de más de

US$45 millones, en nuestro país el número de ciberataques aumento, generando perdidas de alrededor de 4 millones de dólares. (El Comercio, 2016).

En tal sentido, los datos brindados de forma precedente, ponen de relieve como la digitalización de actividades del sector financiero, ha abierto una brecha de riesgos que además de generar la perdida de cuantiosas sumas de dinero, ponen a flote la importancia y necesidad de tener que desarrollar mecanismos, investigaciones que hagan frente a este problema.

En merito a ello, considerando la gran magnitud de incidencia que tienen los ciberataques dentro de la economía mundial y de forma especial, la repercusión que tienen dentro del sector financiero, el presente trabajo está orientado a determinar la necesidad de implementar un programa de cumplimiento de ciberseguridad como una práctica de buen gobierno corporativo en las entidades que forman parte del sistema financiero peruano, para ello será importante considerar la siguiente información:

- La experiencia en otros bancos, como es el caso de HSBC, da un gran ejemplo para la mejor gestión de riesgos operacionales a través de la adopción de su modelo de las tres líneas de defensa y posterior gestión de riesgos recurriendo al uso del regtech.
- Experiencias en otros países: Según reportes e informes, el año 2018, Chile y México fueron víctimas de los más grandes ciberataques perpetrados en los últimos años, hecho que les ha permitido identificar las debilidades de sus sistemas de ciberseguridad y potenciarlos para hacer frente a futuros ciberataques.
- Conocer cuáles son las medidas que ha adoptado nuestro país.
- Conocer la importancia de implementar prácticas de buen gobierno corporativo.
- Determinar la importancia de contar con un sistema de cumplimiento en ciberseguridad como una buena práctica de gobierno corporativo.

2.1 Experiencias es otros países

Como se ha detallado de forma preliminar, el reporte de ciberataques ha crecido de forma vertiginosa y a pesar de las medidas adoptadas por entidades del sector financiero, estos ataques son cada vez más sofisticados, lo cual hace necesario e imprescindible el desarrollo de medidas de

seguridad que van desde los más altos directivos de la empresa. Siendo así, es importante tomar en consideración la experiencia de otros países y entidades del sector financiero.

2.1.1 Caso HSBC

El origen del banco se remonta al año 1865, fundado como Hongkong y Sanghai Banking Corporation Limited, teniendo como objetivo financiar el comercio internacional. Es a partir del año 1991 que es conocido como HSBC holdings; y es desde la década de los noventas, que el banco inicia una campaña publicitaria promocionándose como el *banco local del mundo,* logrando un crecimiento de 25 millones de clientes en el año 1998 a 110 millones de clientes en el año 2003.

Al año 2019, HSBC es posicionado como uno de los siete bancos más grandes a nivel mundial, con activos equivalentes a 2.6 trillones de dólares.

Sin embargo, pese a su reconocido posicionamiento en el sistema financiero y pese al gran tamaño del banco, esta institución se ha visto involucrada en diversos escándalos a nivel mundial. (2019)

A inicios de la década del 2000, las entidades reguladoras descubrieron una serie de deficiencias dentro de HSBC, se pudo corroborar que el banco estuvo involucrado en el *delito de lavado de activos del narco mexicano y de otros focos del lavado de dinero mundial.* (BBC, 2012), además de estar involucrado en el fraude de Bernie Madoff en Estados Unidos y la realización de acciones que cooperaban a la evasión de impuestos de sus clientes. (2019)

Estas son algunas de las actividades irregulares que llevo a cabo el HSBC:

- Se pudo verificar que existió el transporte físico de México a EEUU, de al menos U$S7,000 millones, indicando que dicha cantidad de dinero tuvo su origen en la venta de drogas en EEUU que luego fueron depositados en la filial mexicana del banco.
- Se confirmo que el banco mantenía relación con bancos en Arabia Saudita y Bangladesh, bancos que mantenían vínculos con organizaciones terroristas.

- Se corroboro el ingreso de U$S19,400 millones al sistema financiero, dinero que estuvo vinculado a organizaciones terroristas, para ello, el banco debió de realizar una serie de ardides para burlar controles de la OFAC (2012)

Todos estos datos sobre las acciones irregulares dentro del HSBC, han podido ser corroborados a través de las revelaciones obtenidas de Hervé Falciani, ex trabajador del banco – experto informático, quien durante los años 2005-2007, almacenó información del banco, conteniendo datos de al menos 100 mil clientes alrededor de todo el mundo que evadieron impuestos. (Management Society, 2015) Este suceso *ha sido calificado como la mayor filtración de datos en toda la historia bancaria.* (RFI, 2018)

Según las investigaciones realizadas, de acuerdo a la normativa vigente en Europa al año 2005, el banco debió de actuar recaudando impuestos de aquellas cuentas que no estaban declaradas, para después pasar el dinero recaudado al fisco; sin embargo, se comprobó que el banco tuvo trato directo con sus clientes, ofreciéndoles la forma para eludir estos tributos. (Management Society, 2015)

Es en merito a todas las circunstancias descritas previamente, que se realizaron una serie de acciones contra el banco, de forma particular, el Departamento del Tesoro de Estados Unidos, califico como *ineficaz* el programa de cumplimiento del banco, de tal forma que por medio de una orden de cese y desistimiento (Deferred Prosecution Agreement: DPA) se solicita al banco, la presentación de un plan para mejorar la gestión de riesgo de cumplimiento.

Tras estas revelaciones, en EEUU el banco fue sancionado con una multa igual a los 1.8 billones de dólares, igual suerte tuvo en Argentina y Reino Unido, al recibir multas de 5 millones y 2.3 millones de dólares respectivamente. (Decisio)

Asimismo, además de las sanciones pecuniarias, el banco sufrió un gran impacto reputacional. Tras el escándalo, al año 2012 el banco sufrió la disminución de ganancias en un 17% en relación con el año 2011, además que el banco se vio en la obligación de cerrar o vender más de 47 negocios y despedir a más de 30 mil colaboradores. Otro aspecto que se vio afectado fue la cantidad de depósitos realizados en el banco, concluyendo que la variación interanual fue igual al 16.29% respecto al año 2011.

El impacto del banco, puede ser graficado de la siguiente forma:

Figura 8. Impacto HSBC (Decisio)

2.1.1.1 Cambios en el HSBC

Es en base a las situaciones descritas previamente y la crisis financiera de 2008 que conllevo a los reguladores a exigir la adopción de medidas para la correcta gestión de riesgos, que el HSBC se vio obligado a reestructurar su sistema de cumplimiento, adoptando además una serie de medidas para la mejor gestión de los riesgos operativos que le eran inherentes.

Durante los años 2009 – 2011 el banco invirtió fuertes cantidades de dinero a fin de reforzar su función de cumplimiento, además de quintuplicar la cantidad de recursos destinados a combatir el lavado de activos. (Dey Aiyesha, 2019)

El acuerdo del banco con el Departamento del Tesoro de Estados Unidos también requería que el banco realice la designación de un monitor de cumplimiento por el plazo de 05 años, además de requerir la modernización de su sistema contra el lavado de activos y cambios estructurales dentro de la organización de dicha empresa. (Dey Aiyesha, 2019)

Considerando la importancia que tiene el rol de cumplimiento dentro de una empresa y que este juega un rol competitivo, el banco emprendió la búsqueda de mejores controles que sean más efectivos, además de la gestión de riesgos operacionales, el banco se planteó como propósito la gestión de riesgos operacionales no financieros, como son las infracciones a la norma, fraude, riesgos reputacionales, fallas del sistema y riesgo de conducta. Bajo ese contexto, el modelo para gestión de riesgos adoptado por el banco, fue el modelo 3LoD o modelo de las tres líneas de defensa, que puede ser explicado con el siguiente esquema:

Figura 9. Modelo de las 3 líneas de defensa (Universidad del Norte – Colombia)

- Según el modelo adoptado, la primera línea de defensa es dueña del riesgo, en tal sentido, es la responsable de identificar, registrar, informar y gestionar los riesgos; garantizando la existencia de controles y evaluaciones que sean necesarias para mitigar estos riesgos.
- La segunda línea de defensa esta encargada del establecimiento de políticas y lineamientos para la correcta gestión del riesgo operativo. Es importante aclarar que quienes forman parte de esta segunda línea no son dueños del riesgo ni los responsables de la implementación de controles.
- Finalmente, la tercera línea de defensa comprende el área de auditoria, que es la encargada de verificar que se cumpla con la gestión de riesgo de forma efectiva.

Según algunos comentarios, a través de este modelo se puede lograr la eliminación de ineficiencias, lagunas o debilidades que se puedan presentar durante la gestión de riesgo además de promover una cultura de gestión de riesgo mucho más sólida. (Dey Aiyesha, 2019)

No obstante, el banco indico que el modelo no funcionaba de la forma esperada, razón por la cual, el banco lanzo un programa de transformación de gestión de riesgo operativo basado en actividades, creando dos *áreas* que brinden apoyo en las dos primeras líneas de defensa, siguiendo el siguiente esquema:

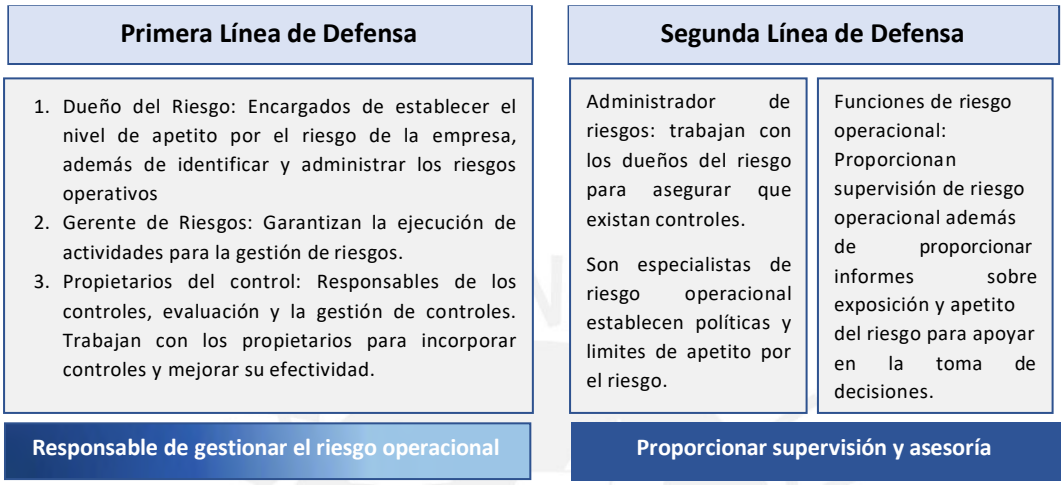

Figura 10. Cambios modelo HSBC

Para la correcta aplicación de este modelo, el banco realizó una serie de capacitaciones y reuniones con todos sus colaboradores, en especial con aquellas personas que tenían roles centrales, de forma especial, el banco realzo la importancia de la cultura de riesgo.

A pesar de la adopción del modelo de las tres líneas de defensa, HSBC en aras de asegurar su efectividad, optó por la implementación de una nueva tecnología conocida como *Regtech.*

Regtech es definida como aquella tecnología emergente que a través del uso del big data, inteligencia artificial y aprendizaje automático, coadyuva en la reducción de riesgos y ayuda a cumplir con los requerimientos normativos.

2.1.2 Caso Banco de Chile

Según el reporte anual del Banco del Chile del año 2017, su origen se remonta al año de 1893 con la fusión de los bancos de Valparaíso, Agrícola y Nacional de Chile; al día de hoy, dicha

institución financiera se ha convertido en uno de los bancos más sólidos dentro de Latinoamérica, hecho que le ha permitido recibir importantes reconocimientos internacionales por tener una de las mejores bancas digitales y móviles de su país; además de reportar al año 2019, más de 2 millones de clientes en calidad de activos y 353 sucursales.

Dicha entidad se ha caracterizado por tener un sólido marco de cumplimiento de gobierno corporativo, así como de control interno, asegurando el cumplimiento de la normativa, cumplimiento permanente de sus valores corporativos y la creación de valor para sus accionistas, clientes, trabajadores, mercado y comunidad en general, al año 2017, el esquema de control interno del banco estuvo conformado de la siguiente manera:

Figura 11. Modelo de Control Interno Banco de Chile (2017)

Al año 2017, el Banco de Chile ha calificado su gestión de riesgos como superior e integral, indicando que el banco ha previsto la existencia y aprobación por los máximos órganos del gobierno, de políticas, directrices y demás lineamientos que permitan una adecuada y eficiente administración de los riesgos a los cuales se encuentra expuesta dicha entidad, resaltando que la administración de riesgos forma parte de los pilares básicos de la estrategia del banco y abarca la administración de riesgos de crédito, de mercado y operacional.

Se ha especificado que la gestión de riesgo operacional del banco es inherente a todas las actividades que son realizadas por el banco, considerando que la materialización de un evento de

perdida podría derivar de forma directa en pérdidas financieras, así como en daños reputacionales de la empresa. (Banco de Chile)

En materia de riesgo operacional, la estructura de gobierno del banco, toma en consideración al Directorio además de la existencia de un Comité Superior de Riesgo Operacional y un Comité Ejecutivo de Riesgo Operacional; de forma adicional, el banco ha previsto la existencia de una División de Control Global de Riesgos que está conformada por la Gerencia de Riesgo Operacional y la Gerencia de Riesgo Tecnológico (Banco de Chile), para la gestión de esta última área el banco ha considerado:

- La existencia de políticas y procedimientos en seguridad de la información y continuidad del negocio.
- Procesos para llevar adelante la evaluación continua de los activos de información considerados como críticos además de las posibles amenazas que podría afectar al banco.
- Definición, actualización y desarrollo permanente de pruebas de los planes de continuidad.

2.1.2.1 Ciberataque en el Banco de Chile

Tal como ha sido referido por la alta dirección del banco, el día 24 de mayo de 2018, el banco fue víctima de un ciberataque internacional, calificado como sofisticado e inédito dentro de los 125 años de existencia del banco, su gerente general preciso que ante dicho evento se activaron todos los protocolos de seguridad, afirmando que dicho suceso es la muestra de la existencia de una amenaza de carácter global para todas las entidades del sector financiero. (Banco de Chile, 2018)

La Superintendencia de Bancos e Instituciones Financieras de Chile (SBIF) preciso que dicho incidente fue a raíz de una acción cibernética que actuó de forma consecutiva por días, afectando servidores y terminales del personal, afectando de forma directa el normal desarrollo de funciones, impactando en la prestación de servicios. Como consecuencia de este suceso, se activaron los planes de contingencia del banco, determinando la desconexión de equipos.

Medios locales informaron que, mientras el banco hacia sus mayores esfuerzos por lograr la recuperación de más de 9 mil computadoras y más de 500 servidores que tenían problemas para re

iniciar el sistema operativo, en paralelo, criminales robaron aproximadamente US$10 millones de una red interna *SWIFT*.[4]

Ese mismo día, además de fallas en el sistema, los clientes reportaron recibir correos que solicitaban información y brindaban un link falso del banco[5]. Por su parte el banco emitió un comunicado oficial, reportando haber sufrido falla en el sistema, generando la activación del protocolo de continuidad del negocio[6].

Finalmente se informe que el referido incidente, fue solucionado entre el día 27 y 28 de mayo.

La SBIF indico que, al cierre del mes de mayo, el banco realizo la constitución de una provisión, por el valor de US$8,672 millones, aclarando que US$6,800 fueron por el incidente suscitado el día 24 de mayo y US$1,800 millones correspondían a los gastos generados por la contratación de asesorías y servicios tecnológicos.

Además de la constitución de provisiones, la SBIF reporto haber recibido cinco reclamos en contra del Banco de Chile entre el 24 de mayo y 18 de junio, mientras que el banco reporto un total de 48 reclamos entre en 24 de mayo y el 14 de junio.

2.1.2.2 Cambios en el Banco de Chile

Directivos del Banco informaron que después de ocurrido dicho suceso, de forma inmediata se realizaron una serie de cambios dentro de la estructura orgánica del banco, siendo las principales las siguientes:

[4] SWIFT (The Society for Work Interbank Financial Telecommunication), es un sistema de origen belga, que ha sido creado con el objetivo de ser empleado como una herramienta que permite la transmisión de mensajes seguros sobre transacciones financieras internacionales, dicho sistema permite el intercambio de transacciones interbancarias
[5] Revisar Anexo 01
[6] Revisar Anexo 02

- Se remplaza la Gerencia de Seguridad Tecnológica, con la creación de una nueva división de Ciberseguridad en el mes de junio del año 2018, con el propósito de contar con una estructura más sólida preparada para responder de forma eficaz a este tipo de sucesos, el trabajo de esta división incide de forma directa en la mitigación de amenazas cibernéticas y está conformada por dos gerencias y de un área de apoyo, según el siguiente esquema:

Figura 12. División de Ciberseguridad Banco de Chile

- Según su nuevo modelo de control interno, la gestión de ciberseguridad, forma parte de la primera línea de defensa del banco, tal como se puede apreciar en el siguiente grafico

Figura 13. Modelo de Control Interno Banco de Chile (2018)

Esta primera línea de defensa tiene entre sus principales responsabilidades las siguientes:

a. Identificación y evaluación de riesgos.
b. Control y mitigación de riesgos.
c. Implementación de acciones de mitigación requeridas.
d. Asegurar la eficacia y eficiencia en el desarrollo de operaciones.
e. Asegurar la confiabilidad de la información.
f. Salvaguarda de activos.
g. Ejecución de controles sobre los riesgos.
h. El diseño e implementación de procedimientos destinados a supervisar la ejecución de controles.

Otros de las medidas adoptadas son:

- Fortalecimiento de las actividades de monitoreo y perimetrales.
- Se realizaron cambios dentro del sistema del banco.
- Se realizaron diversas capacitaciones tanto para los colaboradores como para los clientes en ciberseguridad.

- Se planeo la construcción de un centro de ciberseguridad del Banco de Chile, dejando de contratar proveedores externos.
- El año 2019, uno de los hitos más importantes sobre ciberseguridad estuvo marcado por la actualización de su código de ética, que además de contemplar nuevas prácticas, incluye dentro de los principios rectores de la empresa el principio fundamental de riesgos de ciberseguridad, el cual precisa que es responsabilidad de todos quienes forman parte del banco, revisar constantemente los riesgos inherentes al trabajo internos como externos. (Banco de Chile, 2019).

2.1.3 Experiencia Sistema Financiero de México

A diferencia de lo ocurrido en Chile, en México, se reportaron ciberataques en varias entidades del sector financiero, entre ellas, se encuentran: Banco de México (Banxico), Kuspit Casa de Bolsa, Banjercito, Banorte, Inbursa y una caja de ahorro, de la cual no revelaron su nombre.

Medios locales reportaron que los ciberataques iniciaron desde el día 17 de abril, cuando Banxico confirmo que un participante del SPEI[7] reporto un ciberataque.

Al 27 de abril, Banorte reconoció tener problemas de interconexión con el SPEI, volviendo el sistema más lento, mientras que Citibanamex reporto tener problemas para pagar a la nómina de empleados de las empresas que le contrataron el servicio. No obstante, a las fallas presentadas, Banxico emitió un comunicado indicando que tres instituciones financieras tuvieron incidentes operativos, pero que el funcionamiento del SPEI no se vio afectado y que por el contrario venía trabajando de forma normal y *segura,* pero que las entidades que mantendrían el uso del SPEI debían hacerlo bajo la activación de sistemas de contingencia.

Al día 30 de abril, se reportaron retrasos en la realización de transferencias y que el dinero no llegaba a su destino, en merito a ella Banxico reporto que las empresas afiliadas al SPEI venían haciendo uso de un sistema alternativo.

[7] SPEI o Sistema de Pagos Electrónicos Interbancarios: Es la infraestructura de pagos del Banco de México que permite a sus participantes, (bancos, casas de bolsa, sofipos y otras entidades financieras reguladas) enviar y recibir pagos entre sí y ellos a su vez, brindan a sus clientes finales el servicio de transferencias electrónicas en tiempo real.

El día 09 de mayo, Banorte admitió haber sido afectado por los incidentes ocurridos dentro del SPEI, haciendo la aclaración de que el dinero de los clientes estaba completamente seguro.

Al 11 de mayo se siguen reportando demoras en el tiempo de las transacciones, y al término del día, Banxico informa que cinco entidades del sector financiero registraron transferencias no autorizadas vía SPEI desde el día 27 de abril.

El 14 de mayo, el gobernador de Banxico se pronuncia sobre los hechos ocurridos anteriormente, confirmando que si hubo un ciberataque en contra del software que se utiliza para hacer uso del SPEI, informando que el daño ascendía a la suma de 400 millones de pesos mexicanos o 14 millones de dólares aproximadamente.

El Banco de México informo que el ciberataque fue realizado a través de la vulneración de la infraestructura tecnológica de las entidades financieras, introduciendo transacción ilegitimas de envío de dinero haciendo uso de cuentas fantasma.

El banco reportó que gracias a la implementación de las señales de alerta de operaciones sospechosas que pudieron detectar el ataque a estas entidades.

2.1.3.1 Cambios en Banco de México (Banxico)

Luego de ocurridos los sucesos narrados previamente, Banxico precisó que, pese a que el SPEI no fue afectado con el ciberataque, se implementaron una serie de medidas para prevenir y garantizar la seguridad de las entidades financieras en futuros ataques.

- En primer lugar, se realizó el cambio de plataforma de las principales entidades afectadas.
- Se implementaron señales de alerta para detectar anomalías, además de la implementación de controles adicionales.
- Se implemento una estrategia de comunicación entre las empresas que hacen uso del SPEI, además de emitir regulación para que las entidades puedan adoptar medidas de control, ante la detección de movimientos irregulares.
- El banco fortaleció su labor de supervisión, por medio de la implementación de visitas de inspección a las empresas que hacen uso del SPEI.

Además de ello, el banco ha recalcado la existencia de un protocolo de reacción ante aquellas amenazas que pudieran poner en peligro a las empresas que utilizan el SPEI, el referido protocolo conlleva a la desconexión de la entidad que presenta problemas y de forma inmediata se inició al uso de un sistema de contingencia. Este protocolo también toma en consideración canales de comunicación, tanto para las empresas como para los clientes además de ofrecer un sistema alterno que permite seguir desarrollando transacciones, este sistema reduce los riesgos de la operación al tener una infraestructura distinta a la que se pretendía afectar. Adicionalmente, se analiza si otras entidades pudieran tener elementos comunes de riesgo para poder activar el protocolo de reacción.

Otras de las medidas adoptadas, fue la implementación de un semáforo de alertas operativas, para que las empresas tomen conocimiento de las medidas que deben de adoptar de forma inmediata de acuerdo al nivel de alerta.

A través de lo ocurrido en el HSBC, se pone de relieve la importancia de contar con un adecuado sistema de gestión de riesgos, necesitando para ello la participación activa y constante de la alta dirección.

El poder conocer más a fondo lo ocurrido tanto en Chile como México, pone de relieve y de forma clara la gran incidencia de ciberataques dentro del sector financiero y la magnitud de los daños; evidenciando los desafíos que se tienen en cuanto a seguridad de la información y medidas de ciberseguridad.

En ambos casos se ha evidenciado, que pese a tener áreas encargadas de la gestión de ciberataques, estas no estuvieron suficientemente implementadas para hacer frente al ataque, lo que denota cuales son algunos de los desafíos en los cuales se debe trabajar para lograr la correcta gestión de riesgos digitales, y son los siguientes:

- El nivel de prioridad: Muchas empresas, no le dan la debida importancia al tema, simplemente se han limitado a cumplir lo que de forma escasa el ente regulador del sistema financiero ha propuesto.
- La capacidad de cambio: La digitalización de los servicios requiere estar en constante cambio, a medida que pasa el tiempo, los sistemas son más sofisticados y los hackers también.

- Nivel de complejidad: Es necesario entender que la correcta gestión de riesgos requiere la presencia de personas especialistas además de la interacción y la implementación de nuevos enfoques.
- Los datos recolectados: La tarea no es recolectar todos los datos, la idea es diferenciar cuales son de relevancia para la empresa o cuales dan una señal de alerta para la implementación de sistemas de contingencia.

Otro punto importante a resaltar de ambas experiencias, es la rapidez en la toma de decisiones y de los cambios efectuados, que van desde el gobierno central, altos directivos, colaboradores en general e involucramiento de los clientes.

A raíz de estos sucesos, ambos países reforzaron su sistema de ciberseguridad. En el caso específico de Chile se aprobó la creación del Centro Nacional de Ciberseguridad Policial, que tiene como objetivo principal la detección de amenazas digitales que pudieran afectar al país: además de la formación del Comité Interministerial de Ciberseguridad.

Por su parte el banco de Chile, repotenció el área de ciberseguridad a través de la creación de la división de ciberseguridad, unidad orgánica que cuenta con dos gerencias y un área de apoyo, asimismo a la fecha ha emprendido diversas campañas que buscan concientizar sobre la importancia de la ciberseguridad en las empresas, teniendo como uno de sus objetivos lograr convertirse en un banco ciber-resiliente.

En el caso de México, la Comisión Nacional Bancaria y de Valores (CNBV) siete meses después de ocurrido el ataque a cinco entidades del sector financiero, lanzo un nuevo protocolo de ciberseguridad que busca inmediatez en el reporte de incidentes. Asimismo, la CNBV indico que a través de la regulación en ciberseguridad de busca el fortalecimiento de los sistemas de control interno de las instituciones que forman parte del sistema financiero. No obstante a las medidas adoptadas, los esfuerzos realizados en México aún no han sido lo suficientemente eficaces considerando que al 2019, según la revista Forbes, México sigue siendo uno de los países con mayor incidencia de ciberataques a nivel global.

2.2 Situación actual en Perú

En el caso específico de nuestro país, el año 2017 la Superintendencia de Banca y Seguros y Administradoras Privadas de Fondos de Pensiones (SBS) por medio de la Resolución SBS N°272-2017 aprobó el Reglamento de Gobierno Corporativo y de la Gestión Integral de Riegos, con el propósito de establecer que las empresas que están bajo el ámbito de supervisión de la SBS, es decir las empresas comprendidas en los artículos 16° y 17° de la Ley General de Sistema Financiero y del Sistema de Seguros, cuenten con una adecuada gestión integral de riesgos de acuerdo a su naturaleza, tamaño y a la complejidad de sus operaciones y servicios.

Dentro del referido reglamento, la SBS ha establecido aspectos generales para la implementación de las prácticas de gobierno corporativo, estructura de los órganos de gobierno de la empresa, gestión del sistema de remuneraciones y gestión integral de riesgos.

Dentro de los aspectos para la Gestión Integral de Riesgos se ha considerado que este es un proceso que necesita la participación del directorio, gerencias y en general todo el personal que forma parte de la empresa, para la definición de estrategia, identificación de potenciales eventos que pudieran afectar a la empresa y gestionarlos de acuerdo a su apetito por el riesgo a fin de garantizar el logro de objetivos, todo ello en consideración de la naturaleza de la empresa, tamaño, nivel de complejidad de las operaciones que realizan.

Asimismo, para que las empresas del sector financiero, puedan llevar adelante la gestión de riesgos, la SBS ha previsto que su marco de gestión debe tomar en consideración los siguientes elementos:

- Contar con un ambiente interno, indicando que dentro de la estructura orgánica de la empresa se deberá tomar en cuenta la delegación de facultades y asignación de responsabilidades para hacer frente a los riesgos a los cuales está expuesta la empresa.
- Establecer cuáles son los objetivos que deberá alcanzar el área encargada de la gestión de riesgos.
- Identificar cuáles son los riesgos a los cuales se encuentra expuesta la empresa, se deben de considerar riesgos internos como externos.

- Evaluación de los riesgos a los cuales se encuentra expuesta la empresa, haciendo uso de técnicas cualitativas o cuantitativas.
- Respuesta al riesgo a través de la adopción de medidas que disminuyan la probabilidad de incidencia, disminución de impacto de acuerdo al nivel de apetito y límites de riesgo que han sido fijados por la empresa.
- Establecer controles que permitan asegurar que las medidas adoptadas, han sido las más adecuadas.
- Establecer un proceso de comunicación e información que involucre a los directores, gerencia, comité de riesgos.
- Realizar monitoreo constante, para verificar que las medidas adoptadas sean cumplidas de manera adecuada.

En tal sentido, por medio del referido reglamento, la SBS ha establecido la obligatoriedad de que todas las empresas que se encuentran bajo su ámbito de aplicación, tengan que asegurar dentro de su estructura interna, un adecuado marco de gestión de riesgos, para lo cual se necesita el involucramiento del Directorio, miembros de la Gerencia, y colaboradores en general.

Se ha precisado que para una adecuada gestión de riesgos, las empresas deberán asegurar la implementación de la cultura de riesgos en toda la empresa dependiendo de su nivel de apetito por el riesgo; asimismo, las empresas deberán garantizar la presencia de un área encargada de la gestión de riesgo, a quienes deberán delimitar de forma precisa su estructura y responsabilidades; y a su vez, este área deberá estar encargada de la implementación y adopción de medidas para gestionar de forma adecuada los riesgos a los cuales está expuesta la empresa, además de monitorear de forma permanente, si las medidas adoptadas funcionan de forma correcta.

Adicional a ello, por medio del referido reglamento la SBS ha enumerado una lista no limitativa de riesgos a los cuales se encuentran expuestas las empresas. En el caso de aquellos riesgos relacionados con los TIC, de acuerdo a lo desarrollado en el reglamento se sobreentiende que estos han sido considerados dentro de la gestión de riesgo operacional.

Conforme a lo regulado en el reglamento, el riesgo operacional ha sido definido como toda aquella posibilidad de sufrir pérdidas que tiene la empresa, debido a la ocurrencia de procesos inadecuados, fallas del personal, *problemas con las tecnologías de la información*, así como la

ocurrencia de eventos externos. Haciendo la aclaración que dicha definición incluye el riesgo legal, pero excluye el riego estratégico y riesgo reputacional. (Resolución SBS N°272-2017, 2017)

Según la resolución SBS N°2116-2009 que aprueba el Reglamento para la Gestión del Riesgo Operacional, determina en su artículo 4° que las empresas están en la obligación de gestionar aquellos riesgos que están asociados a la tecnología de la información, que están relacionados con fallas en la seguridad y continuidad a nivel operativo de los sistemas informáticos, gestión de aquellos errores detectados durante el desarrollo e implementación de sistemas y de su integración, además de la gestión de problemas relacionados con la calidad de información, inadecuada inversión en tecnología, entre otros aspectos, indicando que su gestión deberá seguir los lineamientos establecidos en las normas específicas.

Es así que los lineamientos específicos para la gestión de seguridad de la información, los encontramos en la Circular N°G-140-2009, documento que establece de forma preliminar que seguridad de la información es aquella característica de la información que se obtiene a través de la combinación de políticas, procedimientos, estructura organizacional y el uso de herramientas informáticas especializadas a fin de que la información cumpla con criterios de confidencialidad, integridad y disponibilidad.

El referido documento, ha determinado que, con el propósito de asegurar la adecuada gestión de la seguridad de la información, las empresas están en la obligación de establecer, mantener y documentar un sistema en seguridad de la información y que por lo mínimo deberán:

- Tener una política de seguridad de la información.
- Definir una metodología de gestión de riesgo.
- Mantener un registro del cumplimiento de normas, políticas y procedimientos de la empresa.

Como se ha podido apreciar, nuestra normativa nacional no ha previsto la regulación de medidas preventivas o de mitigación frente a la presencia de riesgos digitales, hecho que es bastante necesario si se toma en consideración que, según un estudio de Fortinet a mayo de 2020, en nuestro país se han registrado más de 433 millones de intentos de ciberataques, hechos que hacen una suma total de 9,7 billones en todo América Latina. (Andina, 2020). Asimismo, según un estudio realizado por la empresa Kaspersky, a febrero del 2020 el sector financiero es uno de los sectores más afectados por la incidencia de ciberataques, según Fabio Assolini – Analista senior de la

empresa Kaspersky, el uso de aplicaciones para la realización de transacciones financieras, influye el aumento de ciberataques.

Según un reporte realizado por Fabiola Seminario, a raíz del COVID-19 ha incrementado la necesidad de que las empresas que forman parte del sector financiero, fortalezcan su cultura digital. (2020)

2.3 Importancia de implementar prácticas de buen gobierno corporativo.

Tal como ha sido definido por Fuertes, la importancia sobre la implementación de prácticas de buen gobierno corporativo, radica en la contribución del proceso de creación y preservación del valor monetario y social que tiene una empresa. (2016)

Por otra parte, el BIS (Bank for International Settlements) ha determinado que la importancia del gobierno corporativo para las empresas del sector financiero, radica en la posibilidad de garantizar la seguridad y estabilidad de la entidad. Recalcando la importancia de la labor que cumplen sus órganos de gobierno (Junta General de Accionistas, Directorio, Gerencia Central) pues a través de ellos es posible la aplicación y cumplimiento de todas aquellas normas que les sean exigibles a la empresa, garantizando la protección de los depositantes y por otro lado la confianza de los entes supervisores.

Es oportuno indicar que para garantizar el cumplimiento de la normativa interna como externa, es imprescindible que los órganos de gobierno den lineamientos estratégicos para garantizar la consecución de los objetivos de la empresa, asegurando una adecuada gestión de riesgos dependiendo del tamaño y naturaleza de la empresa, identificación de riesgos, cuidando que todos los recursos destinados a esta gestión sean utilizados de manera responsable.

Entonces considerando que el sector financiero tiene gran probabilidad de incidencia de ciberataques o amenazas que atenten contra de los sistemas de información de las empresas, la implementación de prácticas de buen gobierno corporativo garantizará:

- Cumplimiento de la normativa externa aplicable
- Involucramiento de los órganos de gobierno en la gestión e identificación de los riesgos.

- Delimitación de medidas de acción frente a ciberataques o eventos similares.
- Correcta distribución de recursos.
- Obtención de valor agregado.

Y de forma general, las prácticas de buen gobierno corporativo coadyuvarán en la generación de un ambiente de confianza, de eficacia frente a las medidas adoptadas y de transparencia e las operaciones realizadas.

Entonces, habiendo determinado de forma preliminar que el continuo desarrollo de las TIC ha abierto una gran brecha de riesgos para la economía digital, que actualmente los ciberataques constituyen a nivel global cinco de los principales riesgos globales, que uno de los sectores más afectados es el sistema financiero, que con el avance de la tecnología estos ataques son más frecuentes y sofisticados, y que dichos incidentes son generadores de la perdida de millones de dólares a nivel mundial, corresponde determinar la necesidad que nuestro país tome medidas de precaución respecto a la gestión de riesgos digitales, proponiendo como medida de solución, la implementación de un programa de cumplimiento de ciberseguridad como una buena práctica de buen gobierno corporativo en las entidades que forman parte del sistema financiero peruano.

Para ello, ha sido importante conocer la experiencia de otros países, hecho que ha demostrado que existe debilidad en la regulación en ciberseguridad en varios países, la falta de recursos para fortalecer las unidades encargadas de gestión de riesgos, además de la falta de atención en el tema, hecho que ha generado que varias entidades del sector financiero, como es el caso del Banco de Chile y Banco de México, se vean en la obligación de fortalecer la gestión de riesgos digitales.

No obstante, el resultado no ha sido el mismo; desde el incidente suscitado en Chile, se pudo apreciar la adopción de nuevas medidas que refuerzan el sistema de gestión de riesgos digitales que van desde el estado. Dentro de las medidas que se adoptaron están el perfeccionamiento de la normativa aplicable, asumiendo la gestión de riesgos digitales y la gestión de ciberseguridad como un componente critico dentro de la infraestructura nacional; se inició un proceso de actualización normativa de riesgo operacional y ciberseguridad, se detectaron once entidades con mayor nivel de transaccionalidad y posteriormente se les solicito información respecto a las medidas adoptadas para fortalecer los niveles de seguridad.

Por su parte el Banco de Chile, fortaleció su área de gestión de riesgos digitales, se ha demostrado el compromiso en la gestión de riesgos desde el directorio, gerentes, colaboradores, hasta la inclusión de clientes en charlas de concientización sobre la importancia de adoptar medidas de ciberseguridad y demás medidas que han potenciado la gestión de riesgos.

En este caso, es innegable que los cambios han generado un impacto positivo, y que el nivel de incidencia de ciberataques es menor.

En el caso de México, pese a la adopción de medidas que buscaban reforzar los sistemas de seguridad de las entidades, no se han conseguido cambios sustanciales, ni tampoco se le ha dado la debida importancia al tema de ciberseguridad, una prueba de ello son los numerosos informes que demuestran que México sigue siendo uno de los principales países con mayor incidencia de ciberataques.

El caso de HSBC ha sido esencial para comprender la importancia de gestionar los riesgos, que no solo comprende su identificación y su correcta gestión, pues también realza la importancia de contar con prácticas de buen gobierno corporativo, logrando la participación activa de los miembros de la alta gerencia para la correcta gestión de riesgos, lo cual permite lograr mayor sostenibilidad de la empresa, mayor aseguramiento respecto al funcionamiento de los sistemas de control, obtener información para la mejor toma de decisiones así como un mayor aseguramiento respecto a la seguridad y protección de los activos de la empresa.

Por otro lado, el conocer la situación actual en nuestro país, nos hace caer en cuenta que nuestro país no tiene los mecanismos mínimos y necesarios de protección frente a un ciberataque que tenga el mismo nivel de magnitud de los ocurridos en Chile y México respectivamente, y que existe una necesidad latente de desarrollar medidas de prevención, más aún si se ha demostrado que este tipo de incidentes han aumentado a gran escala.

Según se puede disgregar de la normativa vigente, el ente regulador peruano (SBS), tan solo ha considerado dentro del ámbito de gestión de riesgos, la gestión de seguridad de la información; sin embargo, como se ha recalcado a lo largo del trabajo, la constante transformación y evolución de los TIC y el uso de estos en la prestación de servicios financieros además de ofrecer una gama ventajas y oportunidades ha significado el aumento de riesgos que deben ser gestionados por las

empresas, hecho que hace necesaria la adopción de nuevas medidas que se adapten a las condiciones actuales.

Por lo que, a estas alturas, ya no resulta concebible que la gestión de riesgos digitales sea llevada de forma tan superflua. Se debe considerar también que la inadecuada gestión de riesgos operacionales incide en requerimientos patrimoniales por parte de SBS, genera desconfianza entre los clientes, afecta la reputación de la empresa y además de que la sofisticación y frecuencia de ciberataques cada año va en aumento, amenazando el normal desarrollo del sector financiero.

CAPÍTULO III: DISCUSIÓN

Para el desarrollo del presente trabajo de investigación se ha determinado, de forma preliminar, que existe la necesidad de que nuestro país adopte medidas de prevención y precaución respecto a la gestión de riesgos digitales; en tal sentido, se ha considerado como una medida idónea, la implementación de un programa de cumplimiento de ciberseguridad como parte de la aplicación de las prácticas de buen gobierno corporativo en las entidades que forman parte del Sistema Financiero Peruano.

En ese sentido, ha sido importante entender y evidenciar que conforme los TIC han evolucionado, también ha surgido una modernización o digitalización de los modelos de negocio, la prestación de servicios tradicionales ahora es realizado a través del uso de canales digitales, brindándonos una serie de ventajas, como la simplificación de nuestras actividades, pero también ha significado la apertura de nuevos riesgos que deben de ser gestionados a través de medidas de mitigación y de prevención.

El desarrollo de las TIC ha propiciado el desarrollo, en gran magnitud, de la economía digital. Entendiendo que negocios tradicionales, como son los servicios financieros, han pasado a ser digitalizados a través del uso de los TIC´s, los cuales brindan un entorno apropiado para el procesamiento, administración y distribución de servicios o información mediante dispositivos tecnológicos.

Dentro de las ventajas que trae consigo la economía digital, está la posibilidad de acceder de forma libre y rápida a diversos mercados, estos servicios involucran educación, comercio, servicios financieros, entre otros. En términos generales las TIC´s han impactado de forma positiva en el crecimiento y desarrollo de la economía digital, hecho que ha impulsado el desarrollo de aplicaciones y sistemas de información.

En el caso específico de los servicios financieros, gracias a la digitalización de sus servicios, se ha logrado tener acceso a un mayor número de clientes, las distancias geográficas ya no son un problema para realizar transacciones de envío o depósito de dinero, incluso gracias al desarrollo de diversas aplicaciones y sistemas es que se puede promover la inclusión financiera, llegando incluso a las comunidades más alejadas.

Sin embargo, pese a la gama de beneficios que ha traído consigo la digitalización de servicios financieros, también ha significado la apertura de una brecha de riesgos que inciden de forma directa con los activos de las empresas de este sector, siendo necesaria la adopción de acciones inmediatas y oportunas que prevengan y mitiguen estos riesgos.

Números estudios han demostrado que la incidencia de ciberataques cada vez es más grande, los ataques son más sofisticados y dichos incidentes son generadores de perdidas monetarias. Al año 2018 ocasionaron a nivel mundial la perdida de al menos 45 millones de dólares.

En ese sentido, los casos estudiados nos permiten afirmar que incidentes como los ocurridos en Chile y México han demostrado que no se tienen adecuados sistemas de gestión de riesgos digitales, que existe debilidad en la normativa de uso general como la normativa interna de cada empresa, además de verificar que las empresas no destinan los recursos monetarios ni de personal necesarios para la detección y prevención de este tipo de riesgos, generando la falta de atención sobre el tema.

En el caso específico del HSBC, a raíz de la filtración de datos sobre procedimientos irregulares que realizaba el banco, como es su participación en el lavado de dinero proveniente de la venta de drogas, ha puesto de realce la importancia de contar con un sólido sistema de gestión de riesgos, debido que su mala gestión además de incidir de forma directa en la reputación de una empresa, incide de forma directa en sus activos, desencadenando más problemas que podrían poner en peligro la existencia de una empresa.

El caso HSBC nos permite entender la importancia que tiene la alta dirección en la adopción de modelo de gestión de riesgos, los mismos que deben de ser adecuados e idóneos de acuerdo al nivel de apetito y tolerancia por el riesgo que tengan las empresas. Se debe entender que la adopción de modelos de gestión no debe de ser tomado como mero cumplimiento de la ley.

Es preciso recalcar que la correcta gestión de riesgos requiere la participación activa en la adopción de políticas, controles, evaluaciones por parte de la alta gerencia.

El caso de Chile en la actualidad resulta ser referente para la correcta gestión de riesgos digitales. Es a raíz del ciberataque que tuvo lugar el 24 de mayo que genero la pérdida de más de 10 millones de dólares, que se pueden apreciar una serie de cambios dentro de la estructura orgánica de dicha entidad, además de cambios dentro del gobierno central de Chile.

Pese a que antes del ciberataque el banco incluyó como parte de la gestión de riesgos el tema de ciberseguridad, se puede comprobar que las medidas no fueron suficientes frente al impacto que tuvieron.

Con el caso del Banco de Chile y caso HSBC se reafirma el rol trascendental que tiene la alta dirección en la adopción de medidas, políticas, controles y demás medidas que gestionen los riesgos que son inherentes a las empresas, de acuerdo a su naturaleza y tamaño.

En el caso del Banco de Chile, se ha podido corroborar mayor compromiso de la alta dirección en la gestión de riesgos digitales a través de la adopción de políticas en ciberseguridad que han sido incluidas en su código de gobierno, además de ello, el banco ha reforzado la gestión de ciberseguridad a través de la creación de una gerencia especializada en ciberseguridad y la realización de diversas capacitaciones que van desde la alta dirección, colaboradores y clientes, proyectándose como una entidad ciber-resiliente.

En el caso de México, se registró el impacto a cinco entidades de su sistema financiero, teniendo una pérdida de más de 14 millones de dólares, en merito a ello que las autoridades implementaron nuevos protocolos y nuevos controles para la gestión de ciberataques, que incluyen el envío de señales de alerta y la activación de forma inmediata de planes de contingencia.

A pesar de los esfuerzos realizados por México, se ha podido corroborar que las medidas adoptadas no son suficientes frente al nivel de incidencia de los ciberataques, en diversos estudios realizados, México se encuentra dentro del top 10 de países que registran más incidentes de este tipo.

Como se puede apreciar, los resultados obtenidos no han sido los mismos, hecho que nos permite tener una idea de que medidas resultan ser las más idóneas y eficaces frente a la gestión de riesgos.

En el caso de nuestro país, se ha podido verificar que no existe ningún tipo de reglamento o normativa que regule de forma expresa la gestión de riesgos digitales, por el contrario, el tema sigue siendo tratado de forma superflua. El ente regulador solo se ha limitado a requerir que las empresas que se encuentran bajo su ámbito de control tengan que gestionar los riesgos que les son inherentes dependiendo al tamaño y naturaleza de la empresa, entendiendo que el sistema financiero peruano está conformado por bancos, EDPYMES, CMAC´s cooperativas, etc.

Asimismo, se ha determinado que nuestra normativa actual no está preparada para la gestión de riesgos digitales, sin embargo, este hecho no es un impedimento para que las empresas que forman parte del sistema financiero puedan adoptar medidas eficaces para la correcta gestión de riesgos. En ese entender, es preciso recalcar que la implementación de prácticas de buen gobierno corporativo constituyen medidas idóneas para lograr la protección de activos de la empresa, lograr mayor rentabilidad, promover cultura institucional además de permitir una correcta delegación de funciones y responsabilidades.

No obstante a que a la fecha no existe un marco normativo específico sobre la gestión de riesgos digitales, la SBS ha reconocido que el uso de las nuevas tecnologías ofrecen una gama de productos y servicios, pero que estos representan el aumento de riesgos a los cuales se encuentran expuestas las empresas del Sistema Financiero Peruano, precisando que la sofisticación, frecuencia y persistencia de riesgos digitales son cada vez más peligrosos y diversos, y que ponen en peligro el normal desarrollo del sistema financiero, es en merito a ello que la SBS ha desarrollado una "*Hoja de Ruta de Ciberseguridad"* que comprende cinco pilares, tal como se puede apreciar en el siguiente esquema:

Figura 14. Hoja de ruta de ciberseguridad SBS

El desarrollo de esta hoja de ruta, comprende el desarrollo del marco regulatorio como extension del marco legal aplicable; sin embargo hasta la fecha no se tiene ningun tipo de actualizacion y/o desarrollo normativo por parte de la SBS (Boletin Semanal SBS), siendo preciso indicar, que pese

a que constituye una necesidad que se determine de forma expresa los aspectos sobre la correcta gestion de riesgos digitales, es importante que las empresas que forman parte del Sistema Financiero Peruano, puedan adoptar medidas de prevencion y mitigacion de forma autonoma, según la naturaleza y tamaño de las empresas.

En ese entender, considerando que existe la necesidad de una adecuada gestión de riesgos digitales, que nuestro país no cuenta con las medidas necesarias y que como una buena práctica de gobierno corporativo se pueden adoptar medidas que hagan frente al problema, se comprueba la necesidad de contar con un programa de cumplimiento en ciberseguridad.

Según el estudio de los casos del HSBC, Banco de Chile y Banco de México, el programa de cumplimiento en ciberseguridad, mínimamente deberá estar estructurado de la siguiente forma:

- Primero, se deberá de establecer cuál es la estrategia a adoptar en el marco de gestión de riesgos digitales y ciberseguridad de forma aislada a la gestión de riesgo operacional, considerando que el tema de ciberseguridad y riesgos digitales requieren de mayor especialización y sofisticación de sistemas.

  Se debe tener en cuenta que la estrategia deberá ser fijada de acuerdo al nivel de apetito por el riesgo de la empresa.

  Es importante que todos los órganos de gobierno estén involucrados en la gestión de riesgos digitales, en ese sentido será importante determinar cuáles serán los roles y las responsabilidades que permitirán cumplir de manera eficaz la estrategia adoptada por la empresa.
- Será conveniente realizar cambios dentro de la organización de la empresa, para garantizar la existencia de un área especializada en el tema, además de demostrar el compromiso del directorio en la gestión de riesgos digitales, es conveniente tener una política de riesgos digitales.
- Se deberán determinar actividades de supervisión, primero para determinar la efectividad de las medidas adoptadas, para prever cualquier tipo de contingencia y para evaluar los cambios que se deberán de realizar, entendiendo que cada vez los ataques son más sofisticados y es necesario tener un sistema actualizado.
- Se deberán definir cuáles son los riesgos a los que está expuesto la empresa y definir controles. En este punto será importante desarrollar una matriz de riesgos para determinar el nivel de

complejidad del riesgo, además del desarrollo de señales de alerta que nos permitan conocer el nivel de riesgo, pudiendo ser bajo, moderado o alto, y en base a ello tomar decisiones.

- Monitorear de forma constante los controles implementados para garantizar su efectividad y detectar cualquier tipo de amenaza.
- Desarrollar planes de contingencia ante un ciberataque.
- Capacitar de forma constante a todos los colaboradores de la empresa.
- Evaluar de forma periódica el sistema de cumplimiento.

Asimismo, a fin de que exista mayor claridad sobre los aspectos que debe contener el programa de cumplimiento, se pone en consideración los siguientes esquemas que deberán ser utilizados para la gestión de riesgos digitales, resaltando que estos han sido elaborados tomando en consideración los modelos de gestión desarrollados en el presente trabajo de investigación (ISO 31000, IRM, COSO) y que muestran con mayor precisión y claridad los aspectos que deben ser tomados en cuenta en orden de correlación e importancia, en ese sentido, se deberán considerar los siguientes aspectos:

- **Objetivos Estratégicos de la Organización**

Brindar lineamientos dirigidos al cuidado de la confidencialidad, integridad y disponibilidad de los activos de la información de XXX S.A expuestos en el ciberespacio, como parte de la gestión de ciberseguridad, como parte de los pilares de la empresa.

De forma previa, se ha determinado la importancia de contar con el apoyo y participación constante de los miembros de la Alta Dirección, para la adopción de políticas, reglamentos, manuales, etc, que gestionen los riesgos que son inherentes a la empresa. En el caso específico del Banco de Chile, a pesar de realizar la modificación de su estructura orgánica a través de la creación de un área especializado en ciberseguridad, el banco implementa como uno de sus pilares la gestión de riesgos digitales, en ese sentido, las empresas deberían considerar lo siguiente:

- **Valoración de Riesgos**

1. Identificación de Riesgos

Para esta etapa, según lo desarrollado en los modelos de gestión de riesgo, se deben de identificar o reconocer aquellos riesgos a los cuales se encuentra expuesta la empresa, debiendo identificar si son internos o externos, como pueden suceder, si pueden generar daños en la empresa o si se tratan de oportunidades de mejora, básicamente se trata de realizar una descripción completa y detallada. Para ello, se ha construido el siguiente esquema:

Tabla 1

Identificación del Riesgo

IDENTIFICACIÓN DEL RIESGO							
Descripción de la situación	Causas que dieron origen	Origen		Tipo de evento		Efectos	Vulnerabilidades
		Interno	Externo	Riesgo	Oportunidad de mejora		

Todos estos datos podrán ser obtenidos a través del estudio de todos los procesos de la empresa, a través de información obtenida por los colaboradores, o teniendo en consideración los criterios establecidos por otras empresas a través de un benchmarking.

2. Descripción de Riesgos

El objetivo de esta actividad, es poder exponer como la incidencia de los riesgos que han sido identificados, podrían afectar a la empresa, en ese sentido, se deberá tomar en cuenta la probabilidad, impacto, resultados del riesgo que se ha identificado, interesados, acciones a desarrollar, así como los mecanismos de control aplicables.

Tabla 2

Descripción de Riesgos

DESCRIPCIÓN DE RIESGOS								
Probabilidad			Impacto			Interesados	Acciones a desarrollar	Mecanismos de control
Improbable	Probable	Muy probable	Bajo	Medio	Alto			

Para la determinación de estos valores, el área encargada de la gestión de riesgos digitales, deberá proponer a Directorio, la aprobación de los límites para determinar los niveles de probabilidad, por ejemplo, se podrán considerar los siguientes aspectos:

Tabla 3

Probabilidad

Probabilidad	
Improbable	Riesgo, cuya probabilidad de ocurrencia es muy baja, entre 1% a 49%
Probable	Riesgo, cuya probabilidad de ocurrencia es media, entre 50% a 79%
Muy Probable	Riesgo, cuya probabilidad de ocurrencia es muy alta, entre 80% a 100%

Tabla 4

Impacto

Impacto	
Bajo	La materialización del riesgo no generará pérdidas o tendrá un impacto menor en la empresa.
Medio	La materialización del riesgo generara un impacto moderado en la empresa.
Alto	La materialización del riesgo generara pérdidas, teniendo un impacto significativo en la empresa además de obstruir los objetivos de la empresa.

Los pasos descritos previamente, además de brindar una visión integral sobre los riesgos a los cuales se encuentra expuesta una empresa, ayudan a tener un panorama completo sobre su origen, sus causas, las implicancias que tiene, así como el impacto y probabilidad de ocurrencia.

- **Evaluación de Riesgos**

En base a los datos recolectados previamente, por medio de esta etapa se podrán decidir si el riesgo identificado podrá ser aceptado, tratado o mitigado, para ello, se ha considerado, que se deberán tomar en cuenta los siguientes aspectos:

Tabla 5

Riesgo Identificado

Riesgo identificado	
Costo de tratamiento	Se deberá evaluar si se debe recurrir a la contratación de una consultoría, implementación de software o si solo se debe reforzar alguna actividad en la empresa haciendo uso de recursos propios.
Riesgos asociados	Evaluar si la incidencia del riesgo identificado puede desencadenar en la incidencia de otros

	riesgos. Por ejemplo, la ocurrencia de un ciberataque generara riesgos reputacionales en la empresa.
Revisión de normativa	En caso la gestión de los riesgos identificados deba tener en consideración algún aspecto normativo o si se deben de cumplir con determinados aspectos señalados por la ley.

- **Tratamiento de Riesgos**

Implica que se determinen cuáles serán las acciones a implementar para tratar o mitigar el riesgo identificado, para ello, se deberá de garantizar que la estructura orgánica de la empresa sea la adecuada, es decir que exista un área especializada en la gestión de riesgos digitales; que la empresa cuente con procedimientos establecidos y que por ende existan controles internos.

- **Monitoreo y control**

A través de esta etapa se deberá de verificar que los riesgos identificados y de forma consiguiente, que los planes de acción y los controles aplicados para su tratamiento, actúen de manera eficaz. En caso se determine que las medidas implementadas no funcionan de la manera adecuada se deberán de reforzar las acciones o implementar otros mecanismos.

Dependiendo del nivel de probabilidad o de impacto, se debe determinar la periodicidad de monitoreo y control.

Asimismo, es preciso recordar que la gestión de riesgos debe ser dinámica.

Finalmente, para que todas estas etapas puedan ser llevadas a cabalidad, es imprescindible que la empresa cumpla con los siguientes aspectos:

1. Que la empresa cuente con una política de gestión de riesgos digitales, la misma que debe enmarcar de forma clara el nivel de apetito por el riesgo, así como las responsabilidades que surgen de la gestión de este tipo de riesgos.

2. Una vez más se recalca que debe existir el compromiso de la alta dirección, ello se podrá vislumbrar a través de la creación de un área especializado, la destinación de recursos (financieros, tecnológicos y humanos), asignación de responsabilidades, según se puede apreciar en el siguiente esquema:

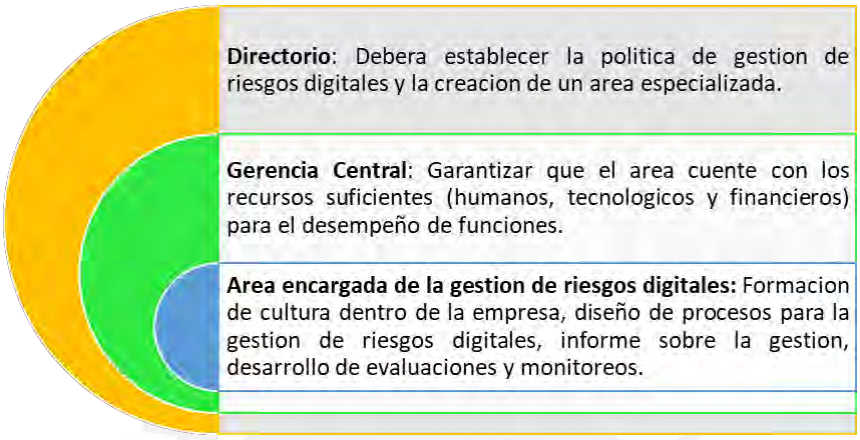

Figura 15. Asignación de responsabilidades.

Finalmente, es preciso indicar que los aspectos desarrollados previamente, forman parte de los aspectos mínimos que deberán considerar las empresas que forman parte del sistema financiero peruano para fortalecer e implementar de manera adecuada la gestión de riesgos digitales. Es oportuno mencionar que estas medidas deberán ser implementadas según la naturaleza y tamaño de las empresas.

CONCLUSIONES

El desarrollo del presente trabajo de investigación nos ha permitido profundizar en la importancia de las Tecnologías de la Información y la Comunicación, y con ello la importancia de la economía digital dentro del mercado actual, lo cual nos ha conducido a determinar que gracias a su desarrollo, la prestación de servicios se ha vuelto más ágil pero a su vez ha significado la apertura de riesgos digitales, sobre todo para las entidades que forman parte del Sistema Financiero Peruano; hecho que nos ha permitido determinar la necesidad de implementar un sistema de cumplimiento de ciberseguridad en las entidades que forman parte del Sistema Financiero Peruano, para lo cual se ha tomado en consideración la experiencia en el HSBC, Banco de Chile y Banco de México, entidades que nos han presentado distintas realidades y que nos permiten plantear el modelo de programa. En base a esas premisas, hemos arribado a las siguientes conclusiones:

En primer lugar, el avance las tecnologías de la información y de la comunicación han coadyuvado, en gran magnitud, al desarrollo de diversas actividades, propiciando que estas puedan ser realizadas de una forma más dinámica y que se encuentran al alcance de más personas. Es preciso indicar que el avance de las TICs ha tenido una relación estrecha con el desarrollo de la economía digital, la misma que incide de forma directa en la forma de llevar a cabo los negocios tradicionales, incluyendo a las entidades que forman parte del sector financiero.

En segundo lugar, gracias a datos ofrecidos por el Foro Económico Mundial, Price Waterhouse Cooper y otras empresas que han sido tomadas en consideración para el desarrollo del presente trabajo, se ha determinado que el avance de la economía digital ha propiciado que las entidades que forman parte del sistema financiero puedan ofrecer sus servicios a más personas y ha ayudado a la inclusión financiera; no obstante, también ha significado el incremento de ciberataques, demostrando que en la actualidad, el sector financiero es uno de los sectores más contingentes y que los ataques son más frecuentes y sofisticados.

En ese entender, ha resultado bastante didáctico estudiar la experiencia en HSBC, Banco de Chile y Banco de México; entidades que nos han dado un panorama sobre como los riesgos digitales indicen de forma directa en los activos de las empresas, cual es la importancia de la gestión de este tipo de riesgos y cuáles serían las medidas más idóneas a implementar en el caso peruano.

El caso de HSBC, nos brinda un panorama claro y preciso, sobre la importancia de contar con un adecuado sistema de gestión de riesgos y fortalece la idea de que estos sistemas deben de ser monitoreados y supervisados de forma constante, teniendo siempre en cuenta que la gestión de riesgos es dinámica.

En el caso del Banco de Chile, nos ha brindado un panorama más amplio sobre la gestión de riesgos digitales, los cambios realizados en el banco han sido determinantes para entender que la gestión de riesgos digitales requiere el compromiso de los miembros de la alta dirección, así como de un área especializado que se encargue de la gestión de este tipo de riesgos. Mientras que, en el caso del Banco de México, a pesar que se implementaron diversos tipos de controles y planes de mitigación, los resultados no han sido tan exitosos; sin embargo, también nos dan una idea de las medidas que pueden ser aplicadas en las entidades del sector financiero peruano.

En tercer lugar, se ha podido verificar que nuestro país no cuenta con algún tipo de reglamento o normativa que regule de forma expresa la gestión de riesgos digitales, a la fecha solo se tiene un marco de gestión de riesgos operacionales. Asimismo, la SBS ha reconocido que existe un incremento de incidentes de riesgos digitales que perturban el desarrollo de las entidades del sector financiero, en merito a lo cual, ha desarrollado una hoja de ruta que consta de 05 pilares dentro de los cuales se encuentra el compromiso de la SBS de desarrollar un marco normativo especializado en la gestión de ciberseguridad, este hecho nos permite incidir en la importancia de adoptar medidas autorregulatorias.

En cuarto lugar, considerando que nuestro país no tiene ningún tipo de normativa que regule de forma expresa la gestión de riesgos digitales y que los ciberataques son más frecuentes y sofisticados, existe la necesidad de implementar un programa de cumplimiento de ciberseguridad en las entidades que forman parte del sector financiero peruano, como una práctica de buen gobierno corporativo teniendo en cuenta que su adopción incide de forma directa en la generación de valor, solidez y eficiencia, propiciando que exista una mejor gestión de riesgos, en este caso, digitales.

Finalmente, la implementación del programa de cumplimiento de ciberseguridad brindara mayor confianza sobre la gestión de riesgos digitales, brindara un apoyo importante en la organización y sobre todo, actuara de forma directa en la prevención y mitigación de riesgos identificados por las empresas del sector financiero dependiendo de su tamaño y naturaleza.

REFERENCIAS BIBLIOGRÁFICAS

Alfaro, M. (2008) Apuntes sobre el gobierno corporativo en el Perú". Foro Jurídico. Lima, número 08, pp. 96-104.

Andina (2020, 04 de mayo) Coronavirus: Perú sufrió más de 433 millones de intentos de ciberataques en 2020. Recuperado de https://andina.pe/agencia/noticia-coronavirus-peru-sufrio-mas-433-millones-intentos-ciberataques-2020-795751.aspx

Artaza Varela, (2014) Programas de cumplimiento. Breve descripción de las reglas técnicas de gestión del riesgo empresarial y su utilidad jurídico-penal", en MIR, CORCOY, GÓMEZ (dirs.), Responsabilidad de la empresa y compliance, B de F, 2014, pp. 231-271.

Asobancaria. Riesgo Cibernético y el futuro de la rentabilidad financiera. Semana Económica, Edición 1178, 2019, pp. 1-12.

Asociación Española de Compliance, (2017) Libro Blanco sobre la Función de Compliance,

Astudillo, G. (2015) Programas de Cumplimiento como Mecanismo de lucha contra la corrupción: Especial referencia a la Autorregulación de las Empresas. Derecho & Sociedad, numero 45, pp.63 – 73

Banco de Chile (2019) Código de Conducta.

Banco de Chile (2017) Memoria Anual.

Banco de Chile (2018) Memoria Anual.

Banco de Chile (2019) Memoria Anual.

Banco de México (2018) Informe anual sobre infraestructuras de los Mercados Financieros.

BBC (17 de julio 2012) Las claves del escándalo del HSBC. Recuperado de https://www.bbc.com/mundo/noticias/2012/07/120717_hsbc_escandalo_claves

BBVA (2015) Situación Economía Digital. Recuperado de: https://www.bbvaresearch.com/wpcontent/uploads/2015/05/Situacion_Economia_Digital_1.pdf

Boletín Semanal SBS (2019) Ciberseguridad: Una hoja de ruta para su desarrollo en los sistemas supervisados. Recuperado de: https://www.sbs.gob.pe/boletin/detalleboletin/idbulletin/88

Cattrysse, (2005) Reflections on Corporate Governance and the role of the Internal Auditor, Roularta Media Group, pp. 1-64

Comisión Económica para América Latina – CEPAL (2013) Economía Digital para el cambio estructural y la igualdad.

Committee of Sponsoring Organizations' (COSO) Recuperado de: https://www.coso.org/Pages/aboutus.aspx

Congreso de la República (06 de diciembre 1996) Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros. (Ley N°26702). Recuperado de http://www.sbs.gob.pe/Portals/0/jer/ley_general_sistema_financiero/20171109_Ley-26702.pdf

Cuesta, Carmen. (2015) Situación Economía Digital. BBVA Research

Deloitte. Los Retos de la función de Compliance. Recuperado de: https://www2.deloitte.com/es/es/pages/governance-risk-and-compliance/articles/retos-de-la-funcion-compliance.html

Del Águila, A. (2001) La economía digital y su impacto en la empresa: bases teóricas y situación en España. Boletín Económico de ICE N°2705.

Decisio. Caso HSBC – Parte II: Riesgo Reputacional, Sanciones por Lavado de Dinero Impacto, Consecuencias y la Gestión del Riesgo) Recuperado de https://www.decisiola.com/articulos/caso-hsbc-2-parte.pdf

Dey, Aiyesha (2019) Regtech at HSBC. Harvard Business School

Diario El Comercio (2016, 12 de agosto). ¿Cuántas perdidas generan ciberataques en Latinoamérica? Recuperado de https://elcomercio.pe/economia/mundo/perdidas-generan-ciberataques-latinoamerica-398244-noticia/

Diario El Economista (2019, 23 de octubre) Perú es el tercer país con más ciberataques en América Latina. Recuperado de https://www.eleconomistaamerica.pe/telecomunicacion-tecnologia-pe/noticias/10157538/10/19/Peru-es-el-tercer-pais-con-mas-ciberataques-en-America-Latina.html

Diario Gestión (2018, 20 de agosto). Ciberataques a empresas peruanas aumentaron 600% en los últimos 12 meses. Recuperado de https://gestion.pe/economia/empresas/ciberataques-empresas-peruanas-aumentaron-600-ultimos-12-meses-242114-noticia/?ref=gesr

Duarte, F. (2010) Economía digital, sitios web y PYMES del sector artesanías en el Perú. Pontificia Universidad Católica del Perú. Recuperado de http://revistas.pucp.edu.pe/index.php/contabilidadyNegocios/article/view/209/203

El Economista. Uno de cada cinco ataques cibernéticos, en contra de instituciones financieras. (26/02/2019). Recuperado de https://www.eleconomista.com.mx/tecnologia/Uno-de-cada-cinco-ataques-ciberneticos-en-contra-de-instituciones-financieras-20190226-0071.html

Etchichury, H. (2016) Riesgo y Derechos Sociales: La visión del Banco Mundial y su impacto en Argentina. Revista Jurídica de los Derechos Sociales Lex Social. Vol. 6 núm 1.

Federation of European Risk Management Asociations (2002) Estandares de Gerencia de Riesgos.

Forbes Mexico (2019) La ciberseguridad: el reto de México. Recuperado de https://www.forbes.com.mx/la-ciberseguridad-el-reto-de-mexico/

Ganguly, Saptarshi (2017) Digital Risk: Transforming risk management for the 2020s. McKinsey&Company

Garat, M. (2018) El Compliance de las empresas: un instrumento para el cumplimiento normativo y una garantía para los derechos fundamentales. Revista de la Facultad de Derecho de México. Tomo LXVIII, número 271, pp.555 – 575

Garcia Zavallos (2017) Economía digital en América Latina y el Caribe: Situación actual y recomendaciones. Banco Interamericano de Desarrollo.

Hartmann, Philipp (2003) The euro – area financial system: Structure, integration and policy initiatives, Oxford review of economic policy, vol.19, N°1

Instituto Peruano de Economía. Recuperado de: https://www.ipe.org.pe/portal/sistema-financiero/

ISO 27001 – Sistema de Gestión de Seguridad de la Información. Recuperado de http://www.iso27000.es/download/doc_sgsi_all.pdf

Kshetri, N. (2016) The Quest to Cyber Superiority: Cybersecurity Regulations, Frameworks and Strategies of Major Economies. Springer

Management Society, (2015, 10 de febrero) ¿Cómo el HSBC "ayudo" a millonarios a evadir impuestos?) Recuperado de https://www.managementsociety.net/2015/02/10/como-el-hsbc-ayudo-a-millonarios-a-evadir-impuestos/

Mendiola, A (2015) Sostenibilidad y rentabilidad de las cajas municipales de ahorro y crédito (CMAC) en el Perú. Universidad ESAN

Murillo, S. (2008). Colonizar el dolor. La interpelación ideológica del Banco Mundial en América Latina.

Naciones Unidas (2019) Informe sobre la economía digital 2019. Creación y captura de valor: Repercusiones para los países en desarrollo – Panorama General. Recuperado de: https://unctad.org/es/PublicationsLibrary/der2019_overview_es.pdf

Organización de los Estados Americanos. (2018) Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe. (pp.1-186) Recuperado de https://www.oas.org/es/sms/cicte/sectorbancariospa.pdf

Perrotta, Jeronimo J. (2012) HSBC: El Lavado de Activos, las debilidades y las implicancias del caso. DECISIO

Portocarrero, F. (2003) Microfinanzas en el Perú. Experiencias y Perspectivas. Centro de Investigación de la Universidad Pacifico. Lima

Rapid7 (2018) National Exposure Index. Recuperado de https://www.rapid7.com/globalassets/_pdfs/research/rapid7-national-exposure-index-2018.pdf

RFI (2018, 19 de diciembre) Hervé Falciani, pesadilla del HSBC, explica los secretos de la optimización fiscal. Recuperado de http://www.rfi.fr/es/economia/20181114-entrevista-con-herve-falciani

Samuelson, Paul A. (2006) Economía, Mc Graw Hill. Colombia

Seminario, Fabiola (2020) Coronavirus y ciberseguridad bancaria: Auge de ciberataques ponen a prueba la seguridad. Recuperado de: https://iupana.com/2020/04/27/covid-19-ciberseguridad-bancaria-auge-ciberataques-ponen-prueba-seguridad/

Soler, S. Ciberseguridad y Compliance. Recuperado de: http://www.worldcomplianceassociation.com/1440/noticia-ciberseguridad-y-compliance.html

Solís, Joseph (29/10/2018) ¿Cómo ocurrieron los ciberataques a la banca en Chile y México? Recuperado de http://blog.cobiscorp.com/ciberataques-banca-chile-mexico

Stiglitz, Joseph E. (2006) El malestar en la globalización. Taurus. México.

Superintendencia de Banca, Seguros y AFP (2009). Gestión de la seguridad de la información.

Superintendencia de Banca, Seguros y AFP (2009). Reglamento para la Gestión del Riesgo Operacional.

Superintendencia de Banca, Seguros y AFP (2017). Reglamento de Gobierno Corporativo y Gestión Integral de Riesgos. Recuperado de: https://intranet2.sbs.gob.pe/dv_int_cn/1708/v2.0/adjuntos/272-2017.r.pdf

Superintendencia del Mercado de Valores. Gobierno Corporativo. Recuperado de https://www.smv.gob.pe/Frm_VerArticulo?data=4BF937842B3A0A085D942F2E13337DDFBC24C632B6F12BACB5B8E999596EC99368B9819C22

Unión Internacional de Telecomunicaciones. (2008) Serie X: Redes de Datos, Comunicaciones de Sistemas Abiertos y Seguridad. Seguridad en el ciberespacio - Ciberseguridad – Aspectos Generales de la Ciberseguridad. Recuperado de https://www.itu.int/rec/T-REC-X.1205-200804-I/es

UNE Normalización Española (2018) Norma Española UNE ISO 31000 Gestión del Riesgo Directrices. Madrid.

ANEXO A


Francisco Spröhnle @fsprohnle · 24 may.
Atención!! a raíz de los problemas de los sistemas del Banco de Chile @bancodechile #BancodeChile están enviando correos fraudulentos a los cliente ⚠ No abrir links que contiene el correo!
PAGO RETENIDO DESDE SU CUENTA POR MOTIVOS DE SEGURIDAD - (455754110123)
24 de mayo de 2018 10:20
De: banco-chile@bancochile.cl
DETALLES
Banco en Línea
bancochile.cl
Apreciado(a) Cliente :
Te informamos que acabas de realizar un Pago desde su cuenta, el cual se encuentra retenida debido a anomalias que el sistema observo en su cuenta. La importancia por la seguridad e integridad de nuestros servicios es la primera, por lo tanto, nos vemos obligados a retener esta transferencia hasta que usted verifique su estado de cuenta, para ello, por favor, haga clic en el siguiente enlace y siga las instrucciones que se le indican a continuacion para poder procesar con exito la transferencia.
Es necesario que ingrese a nuestra banca por internet para poder verificar su informacion en nuestra base de datos o de lo contrario su TRANSFERENCIA QUEDARA RETENIDA y sera necesario acudir a nuestra sucursal mas cercana para el desbloqueo de su cuenta.
Para iniciar el proceso de Verificacion de Identidad ingrese a su cuenta haciendo clic en el siguiente enlace web
Haga clic aqui: https://www.BancoChile.cl
3
18
6

ANEXO B

Banco de Chile

DECLARACION PÚBLICA

24 de mayo de 2018, El Banco de Chile informa que el día de hoy detectó la presencia de una falla que afectó nuestra normal atención en sucursales, banca telefónica y algunos servicios puntuales. Esto generó la activación de nuestro protocolo de contingencia diseñado para mantener la continuidad de los servicios, no viéndose en ningún caso afectada la seguridad de los productos y transacciones de nuestros clientes.

Los portales internet, aplicaciones móviles y cajeros automáticos han operado con normalidad. Los clientes pueden consultar sus productos y efectuar transferencias de fondos a través de estos canales con total seguridad.

Seguimos trabajando para solucionar esta situación. Lamentamos los inconvenientes que esto pudiese haber causado. Una vez más, hacemos un llamado a informarse a través de los canales oficiales del Banco de Chile, donde estaremos actualizando la información disponible.