UNIVERSIDAD PERUANA DE CIENCIAS APLICADAS

FACULTAD DE NEGOCIOS

PROGRAMA ACADÉMICO DE ADMINISTRACIÓN DE EMPRESAS

Análisis de la preparación de las organizaciones Mapfre Perú Seguros y Kallpa Corredora de Seguros ante las amenazas de seguridad de la información en el medio empresarial y que podrían impactar en sus operaciones de negocio

TESIS

Para optar el título profesional de Licenciado en Administración de Empresas

AUTORES

Beteta Lazarte, Juan Enrique (0000-0001-9744-9522)

Narva De la Cruz, Miluska de Jesús (0000-0001-7035-8639)

ASESOR

Jorge Ruiz, Marisol (0000-0003-0949-2876)

Lima, 18 de julio de 2018

DEDICATORIA

*A mi padre por su ejemplo de compañerismo, apoyo incondicional y modelo de tenacidad
a lo largo de mi vida.*

Miluska de Jesús Narva De La Cruz

A mi padre, que se lo debo todo.

Juan Enrique Beteta Lazarte

AGRADECIMIENTOS

Este proyecto es el resultado de nuestro esfuerzo y el apoyo absoluto de nuestro amigo Javier Niquén quien gracias a sus conocimientos y experiencia nos ha orientado y dado soporte a lo largo del desarrollo de la tesis.

Así mismo, queremos agradecer muy especialmente a la Sra. Julie Beteta Lazarte de la empresa Mapfre Perú y al Sr. Dante Reyna Terrones de la empresa Kallpa corredores de seguro por las facilidades, disponibilidad y estrecha colaboración tanto de ellos y sus colaboradores; para el logro de la investigación y el cumplimiento de nuestra meta académica.

EPIGRAFE

“Las organizaciones gastan millones de dólares en firewalls y dispositivos de seguridad, pero tiran el dinero porque ninguna de estas medidas cubre el eslabón más débil de la cadena de seguridad: La gente que usa y administra los ordenadores”.

Kevin Mitnick

RESUMEN

El presente trabajo de investigación analizará cómo están preparadas Mapfre Perú Seguros y Kallpa corredora de seguros, ante las amenazas de seguridad de la información que podrían impactar en sus operaciones de negocio, con la finalidad de proponer una guía base de controles para mitigar los riesgos.

En el capítulo uno se expondrá el marco teórico respecto al impacto de los cambios tecnológicos y las definiciones de la terminología utilizada; también articularemos temas como tendencias de las ciberamenazas, problemática de la información, resiliencia en las organizaciones y ciberseguridad industrial.

Para el segundo capítulo presentaremos el marco metodológico de la investigación y las herramientas usadas en el proceso; así como el propósito de la investigación, tipo de investigación, descripción del contexto interno y externo, establecimiento de la guía de preguntas, la identificación de los segmentos y categorías, codificación, determinación de la muestra y la matriz de procesamiento de la información.

Posteriormente, en el tercer capítulo se efectuará el análisis de la información, permitiendo interpretar en base a los datos recogidos de las entrevistas a profundidad, la observación a través de la bitácora y la experiencia de los entrevistados.

En lo que respecta al cuarto capítulo se precisarán los hallazgos, barreras y brechas identificadas a lo largo de la investigación y entrevistas realizadas.

Finalmente, en el quinto capítulo se brindan las conclusiones y recomendaciones para mitigar los riesgos de seguridad de la información en Mapfre Perú Seguros y Kallpa Corredora de Seguros.

Palabras clave: Ciberseguridad, amenazas, seguridad, seguros.

Analysis of the preparedness of Mapfre Perú Seguros and Kallpa insurance broker organizations in the face of information security threats in the business environment that could have and impact on their business operations

ABSTRACT

The present investigation paper will analyze how prepare the companies Mapfre Perú Insurance and Kallpa Insurance Brokers, are against the information security threats that may impact their business operations, with the intention to propose a guideline of controls to mitigate the risks.

On the First chapter we will expose the theoretical framework in regards to the impact of the technological developments and the definitions of the terminology used on this paper; as well we will articulate subjects such as trends of cyberthreats, resilience in the organization and industrial cybersecurity.

In the Second chapter we will present the investigation methodological framework and the tools used in the investigation process; as well as the purpose of the investigation, type of investigation, description of the internal and external context, establishment of the question guide, the segment identification and categories, codification, sample determination y finally the information processing matrix.

On the Third chapter we will realize the information analysis, allowing us to interpret the data gather in the depth interviews, observation based on the binnacle and finally the experience of the interviewed professionals.

Along the Fourth chapter we will be specifying our findings, barriers and gaps identified along the investigation and conducted interviews.

Finally, on the Fifth chapter we will be given the final conclusion and recommendation to mitigate the information security risks in Mapfre Perú Insurance and Kallpa Insurance Broker.

Keywords: Cybersecurity, threats, security, insurance.

TABLA DE CONTENIDO

TABLA DE CONTENIDO	VII
INDICE DE FIGURAS	X
INDICE DE TABLAS	XI
CAPITULO 1. MARCO TEÓRICO	17
1.1 Gestión de la información en un mundo globalizado.....	17
1.1.1 Tendencias de ciberamenazas en Europa	17
1.1.2 Problemática de la información.....	18
1.1.3 Preparando organizaciones con resiliencia	20
1.1.4 Ciberseguridad Industrial en Perú	21
1.2 Definiciones de seguridad de la información	23
1.2.1 Información	23
1.2.2 Seguridad de la Información	24
1.2.3 Seguridad Informática	24
1.2.4 Ciberseguridad	26
1.2.5 Amenazas a la información	26
1.2.6 Ransomware	27
1.2.7 Phishing	27
1.2.8 Vulnerabilidad de seguridad.....	27
1.2.9 Gestión de Riesgos	27
1.2.10 Riesgo del Negocio	27
1.2.11 Riesgo Operacional	28
1.2.12 Riesgos de la información	28
1.2.13 Políticas de Seguridad	28
1.2.14 Controles de seguridad	28
1.2.15 Servicios esenciales (Críticos)	29
1.2.16 Incidentes de seguridad	29
1.2.17 Impactos de los incidentes de seguridad	29
1.2.18 Plan de Contingencias	29

1.2.19 Planes de Recuperación ante desastres (DRP)	30
1.2.20 Internet de las cosas (IoT)	30
1.2.21 Resiliencia	30
1.3 Estándares Internacionales para sostener la guía de controles	30
1.3.1 Seguridad de la Información – ISO/ IEC 27001: 2013	30
1.3.2 Protección y seguridad de los ciudadanos y Sistema de Continuidad de Negocio- ISO 22301:2012	31
1.4 Incidentes de Seguridad de la Información en el Perú	31
1.5 Sistema Financiero Peruano	34
1.6 Sistema de Seguros Peruano	36
1.6.1 Definiciones del sector del negocio	38
1.7 Regulaciones del Sector de seguros	39
1.7.1 Circular N° G-140-2009 Gestión de la seguridad de la información	39
1.7.2 Circular N° G-139-2009 Gestión de la continuidad del negocio	40
1.7.3 Resolución SBS N° 2116-2009 Reglamento para la gestión de riesgo operacional	40
1.7.4 Resolución SBS N° 272- 2017 Reglamento de gobierno corporativo y de gestión integral de riesgos.....	41
1.8 En Perú- Ley N° 29733 Ley de protección de datos personales.	41
1.9 Mapfre Seguros	42
1.10 Kallpa Corredores de Seguros.....	47
CAPITULO 2. METODOLOGÍA DE LA INVESTIGACIÓN	49
2.1 Planteamiento de la Investigación	49
2.1.1 Propósito de la Investigación	49
2.2 Tipo de Investigación	49
2.2.1 Preguntas de la investigación	50
2.3 Contexto	51
2.3.1 Descripción del contexto interno y externo.....	51
2.4 Muestra.....	53
2.4.1 Descripción de la muestra	53
2.5 Diseño o abordaje principal.....	53

2.5.1 Identificación de la estructura de la entrevista o focus	53
2.5.2 Guía de preguntas.....	53
2.5.3 Segmentos	54
2.5.4 Categorías.....	54
2.5.5 El instrumento de Investigación.....	55
2.6 Procedimiento.....	55
2.6.1 Matriz de procesamiento : Segmento - Categoría	56
2.6.2 Matriz de procesamiento de información – Aspectos positivos y negativos	58
CAPITULO 3. ANÁLISIS DE DATOS Y RESULTADOS	61
3.1 Principales preguntas que cubren los objetivos planteados	61
CAPITULO 4. DISCUSIÓN DE RESULTADOS	80
4.1 Hallazgos.....	80
4.2 Barreras	81
4.3 Brechas.....	81
CAPITULO 5. CONCLUSIONES.....	82
CAPITULO 6. RECOMENDACIONES	84
REFERENCIAS	85
ANEXOS.....	87

INDICE DE FIGURAS

Figura 1. Escenarios cambiantes ante el avance de las nuevas tecnologías.	32
Figura 2. Instituciones que conforman el Sistema Financiero Peruano donde se aprecian las entidades que regulan y supervisa la SBS.	35
Figura 3. Primas de Seguros Netas por Compañía- 2017.	38
Figura 4. Distribución Organizacional Estratégica de Mapfre Perú.	43
Figura 5. Distribución Organizacional Táctica de Mapfre Perú.	44
Figura 6. Participación del Mercado sin Rentas de Jubilación, Previsionales y Renta Particular.	45
Figura 7. Participación de Mercado por Agrupación de Riesgos- Vida.....	46
Figura 8. Organigrama de la empresa Kallpa corredores de seguros.	47
Figura 9. Ranking por año de la empresa Kallpa corredores de seguros donde se aprecia que en el año 2015 obtuvo el primer lugar en su sector.	48

INDICE DE TABLAS

Tabla 1 Principales sectores de la industria que fueron encuestados.....	33
Tabla 2 Amenazas y vulnerabilidades que han aumentado el riesgo en los cuatros últimos años.	33
Tabla 3. Principales riesgos asociados al uso creciente de los dispositivos móviles	34
Tabla 4. Total prima de seguros	36
Tabla 5 Productos que ofrece Mapfre Perú.....	44
Tabla 6.Informe del Mercado asegurador peruano al mes de marzo del 2018	45
Tabla 7.Las líneas de negocio de Kallpa corredores de seguros:.....	48

INTRODUCCIÓN

La información es uno de los activos más importantes con los que cuentan las organizaciones y es por ello que requiere ser protegida para evitar pérdidas en términos de ventaja competitiva, financiera, comercial y legal que originen impactos negativos en la operatividad de los distintos negocios.

Debido a la constante innovación tecnológica nos encontramos interconectados con el mundo en cada instante y este escenario genera que la información se transmita, remita y reciba más ágilmente, así también permite incrementar la eficiencia y rentabilidad mejorando la cadena de valor de las organizaciones, sin embargo, siempre debe ser controlada para garantizar el uso y/o manejo a las personas o entidades autorizadas.

En la actualidad la automatización de la industria, la transformación digital, el internet de las cosas, la tecnología móvil y otras tendencias; facilitan la conexión a sistemas de información desde el auto, la casa, el celular o desde cualquier punto del mundo. Este escenario viene ocasionando impacto en las actividades de las organizaciones debido a que no siempre la información es protegida contra de daños, pérdidas o robo; principalmente por la falta de conocimiento del impacto y la falta de mecanismos de control.

En este sentido, las organizaciones requieren de tres elementos base para el sostenimiento de sus servicios críticos como son: el hardware, el software y los datos; siendo esta última la que contiene la información de mayor valía para los distintos sectores y se convierte en un activo para la organización.

En el contexto de nuestro país, en una primera etapa el gobierno a través del Comité Técnico de Normalización de Codificación e intercambio electrónico de datos elabora la norma técnica peruana NTP-ISO/IEC 27001:2008 Tecnología de la información. Técnicas de seguridad. Sistema de Seguridad de la Información, utilizando como antecedente la ISO/IEC 27001:2005 Sistema de Gestión Seguridad de la Información, con el objetivo de implementar controles de seguridad de la información en las instituciones públicas; para resguardar la información y mantener los pilares de la confidencialidad, integridad y disponibilidad.

Al año siguiente el sector financiero adopta estas medidas a través de la Superintendencia de Banca y seguros (SBS) quien regula a la banca, seguros y AFPs en este sector y se efectúa a través de la Circular N° G-140-2009 Gestión de la seguridad de la información donde se brinda todo el marco de trabajo, definiciones y controles que se deben implementar en este sector con el mismo objetivo común de garantizar el resguardo de la información tanto de personas naturales como jurídicas.

Posteriormente, en el año 2015 se aprueba la Ley N° 29733 Ley de protección de datos personales y a través del Ministerio de Justicia se empezó la implementación de la normativa tanto en empresas privadas como públicas; las cuales se vieron obligadas a seguir adoptando medidas de control y concientización respecto de la seguridad de la información con la finalidad de reducir los riesgos que se podrían originar ante un uso indebido de la información tanto de personas naturales como jurídicas.

La presente investigación se realiza con el propósito de analizar la forma en la cual las empresas del sector financiero peruano Mapfre Perú Seguros, que ofrece seguros vida y seguros generales ante el riesgo de pérdida o deterioro en los bienes o patrimonios y Kallpa Corredora de Seguros, que comercializa contratos de seguro a través de servicios de intermediación; mantienen la confidencialidad, integridad y disponibilidad de la información con enfoque en el mercado de seguros en el Perú.

Es por este motivo que identificamos el siguiente problema de investigación: ¿Cómo están preparadas Mapfre Perú Seguros y Kallpa Corredora de Seguros ante las amenazas de seguridad de la información en el entorno empresarial que podrían impactar negativamente en sus operaciones de negocio?

La hipótesis general a partir de la cual se desarrolla esta investigación es que Mapfre Perú Seguros y Kallpa Corredora de Seguros desarrollan la gestión de la seguridad de la información, las políticas y procedimientos de seguridad de la información y planes de continuidad de negocio para estar preparadas ante las amenazas de seguridad de la información en el entorno empresarial que podrían afectar negativamente sus operaciones.

El objetivo general de la presente investigación es analizar la preparación de Mapfre Perú Seguros y Kallpa Corredora de Seguros, ante las amenazas de seguridad de la información en el entorno empresarial y que podrían impactar en sus operaciones de negocio.

En relación al objetivo general, se identificaron los siguientes objetivos específicos para la investigación:

1. Identificar los servicios críticos de la organización.
2. Identificar los principales riesgos de seguridad de la información a las que están expuestas.
3. Identificar cómo se gestiona la información, las políticas de seguridad y los planes de recuperación.
4. Proponer la guía de controles base para mitigar los riesgos de seguridad de la información.

Tal como hemos mencionado, la justificación para efectuar esta investigación está estrechamente ligada a la información como valor que manejan las organizaciones para efectuar las operaciones de negocio y en el caso de sufrir algún tipo de pérdida o daño causaría impactos en términos financieros, legales, comerciales y reputacionales, principalmente; por lo cual las organizaciones deberían estar preparadas y ser resilientes ante ataques disruptivos que podrían afectar sus activos de información.

Con la introducción de constantes innovaciones tecnológicas se están concibiendo nuevas amenazas, así pues, con el intercambio de información y la facilidad de acceso a través del internet de las cosas (IoT), las empresas están siendo más vulnerables a los ataques cibernéticos. Es por ello que las organizaciones deben definir políticas e implementar controles orientados a proteger la información, con enfoque estratégico y relacionado con el entorno que considere las necesidades y expectativas de las partes interesadas. En este sentido, es importante tener en cuenta que la seguridad de la información es un tema que debe ser tratado a nivel de gobierno corporativo y no solo a nivel tecnológico.

La relevancia de esta investigación se fundamenta en que actualmente las organizaciones son reactivas ante los incidentes de seguridad de la información tal como sostiene el estudio realizado por la auditora EY a través de su reciente “Encuesta Global de Seguridad de la Información 2016-17”, la cual indica que solo el 64 % de un total de 1,735 organizaciones encuestadas a nivel mundial no tienen o sólo tienen un sistema

informal de inteligencia contra amenazas. (Acosta, 2017, p.123); esto significa que no están preparadas para atender incidentes de seguridad de la información.

Si bien es cierto todas las organizaciones tienen incidentes recurrentes de índole operativa, cuando nos referimos a seguridad de la información estamos hablando de la información que está expuesta en términos de confidencialidad, integridad y disponibilidad y sostenida bajo una plataforma tecnológica y las telecomunicaciones.

Los acontecimientos relacionados con la seguridad de la información durante el 2017, según la encuesta de la auditora EY, revelaron que tanto las personas como las organizaciones han sido incapaces de adaptarse rápidamente a los cambios tecnológicos. Sin embargo, ello también ha ocasionado la apertura de nuevos escenarios de exposición de la información sensible o privada. Tal es así que se prevé que las estafas digitales y las amenazas informáticas seguirán incrementándose.

En este sentido, la relevancia de esta investigación se sostiene en los niveles social, práctico y académico. En lo social debido a que uno de los factores en los que se sostienen las organizaciones es a través de su información y al ser esta confiable concebirá nuevas oportunidades para otros negocios, y esta a su vez traerá consigo nuevos puestos laborales. En el nivel práctico porque la investigación impacta en términos económico, organizacional y reputacional; nos referimos al termino económico en relación a que la información debe ser protegida bajo ciertos controles, para evitar pagar multas o penalidades por la falta parcial o total de ella. Respecto al ámbito organizacional porque la información se alberga en el equipamiento tecnológico sea de hardware o software para agilizar tiempos y reducir costos, pero hay que considerar que éstos pueden tener vulnerabilidades y estar expuestos a ciberamenazas, que aunque hoy se han considerado, se deben definir controles para mantener siempre disponibles los servicios; y por otro lado, en términos de reputación porque al presentarse alguna pérdida de información la organización afecta en confianza y credibilidad con sus clientes, accionistas, proveedores u otros, los cuales al tomar conocimiento buscarán enseguida cambiarse a la competencia, que sí les puede garantizar proteger su información. Y finalmente, también es relevante a nivel académico porque el aporte de esta investigación es base de otras investigaciones, pues permitirá entender la importancia de proteger la información del negocio tan igual como se gestionan los recursos administrativos, financieros, logísticos, entre otros; dado que la información exacta, confidencial y disponible permite a las empresas tomar

decisiones acertadas para las partes interesadas, llámese accionistas, colaboradores, proveedores, entidades relacionadas y otros, los que podría ser afectados; por lo cual se debe entender que la información representa un elemento estratégico para el desarrollo de su misión y debe ser tratada bajo ese enfoque.

Respecto a la viabilidad, esta toma sentido en cuanto el aporte académico a través de la guía de controles base que se proyecta plantear a las organizaciones de seguros y corredores de seguros para mitigar los riesgos de seguridad de la información; lo que ayudará a que el impacto sea menor.

CAPITULO 1. MARCO TEÓRICO

1.1 Gestión de la información en un mundo globalizado

1.1.1 Tendencias de ciberamenazas en Europa

Debido al constante cambio tecnológico, y el incremento en el uso de la tecnología para efectuar actividades de índole personal y organizacional, cada vez son más los usuarios constantemente conectados a internet, tal es así que, el Centro Criptológico Nacional señala en su informe Ciberamenazas y tendencias Edición 2018 el servicio de internet es usado por más del cincuenta por ciento de los habitantes del planeta e igualmente identifica como hallazgos que el internet de las cosas ha puesto más vulnerable el internet originando diversos ataques de manera disruptiva, y el otro hallazgo es la capacidad de recuperación de las organizaciones ante el incremento de las ciberamenazas, lo que hace necesario una resiliencia digital.

Asimismo, se menciona que no siempre los costos y beneficios de la ciberseguridad recaen en el usuario pues en muchas ocasiones afecta a terceros ya que en el caso del internet de las cosas en diversas oportunidades se originaron ataques a través de ellos, debido a que los diversos dispositivos móviles que se ofrecen en el mercado no cuentan las debidas actualizaciones de seguridad.

En lo que respecta a las organizaciones y ciudadanos revela que las medidas adoptadas todavía son limitadas para mejorar la resiliencia digital y está por debajo de las amenazas existentes.

En otro punto del informe se identifica las tendencias más probables que podrían afectar a las organizaciones a través de ciberincidentes sofisticados. A continuación, se listan algunas tendencias con mayor impacto y probabilidad de ocurrencia:

- Incremento de las brechas de seguridad: ataques de ciberseguridad a través de la explotación de vulnerabilidades a nivel de aplicación, ocasionando pérdidas económicas. Ejemplo: Uber y Equifax.

- Amenazas móviles: infección de malware en las aplicaciones móviles del sistema operativo Android y es probable que haya sido el primer ransomware móvil.
- La regulación de Internet de las cosas (IoT): precisa que la creciente utilización comercial de los dispositivos IoT produce el interés para los atacantes.
- Ataques contra redes sociales: el desarrollo de formas accesibles para los atacantes para lo cual se sugiere planes de formación y concientización a los empleados sobre el uso de las redes y la creación de planes de respuesta.
- El mayor uso de los Proveedores de Servicios Gestionados de Seguridad: al contar con mayor experiencia, personal y herramientas adecuadas generan confianza para las organizaciones. (p.5-82-84-85).

Según lo expuesto, damos a conocer el panorama de tendencias que se están gestando a nivel europeo, para conocer esta información y tomar medidas apropiadas que permitirá estar preparados para la resiliencia tecnológica ante la exposición latente de ciberamenazas.

A continuación, se describe la problemática de la información, la cual nos ayudará a comprender de una manera más pragmática el contexto actual, tomando en cuenta el análisis realizado por ESET, una de las compañías más importantes en la industria de la seguridad de la información.

1.1.2 Problemática de la información

ESET fundada desde el año 1992 es una compañía global de soluciones de software de seguridad que provee protección de última generación contra amenazas informáticas. Desde el 2004, ESET opera en Latinoamérica, en Argentina, donde dispone de profesionales y un laboratorio de investigación focalizado en el descubrimiento proactivo de diversas amenazas informáticas, asimismo contribuye al portal web WeLiveSecurity en español, el portal de noticias de seguridad en internet, opiniones y análisis, buscando satisfacer a todos los niveles de conocimiento. ESET, (2017).

Para la presente investigación se ha considerado el estudio realizado sobre Tendencias de ciberseguridad 2018: El costo de nuestro mundo conectado que nos indica que el ransomware es una gran amenaza, que origina cobros por información secuestrada en las

organizaciones alrededor del mundo, y esto se ha incrementado de manera exponencial causando alarma en relación a los controles de la seguridad de la información. (2018)

Las infecciones masivas no fueron los únicos incidentes de seguridad, se afectaron organizaciones como Equifax o el ataque de HBO filtrando información privada respecto a las producciones, guiones y los actores; así también Yahoo admitió que durante el año 2013 fue vulnerada, exponiendo información como: direcciones de correo electrónico, fechas de nacimiento, contraseñas y otros; mostrándose la debilidad y exposición de las organizaciones globales. (ESET,2018)

Durante el mismo año, también se habló de acusaciones de interferencia rusa durante las elecciones presidenciales que se realizó en los Estados Unidos durante el año 2016, por vulnerabilidades del sistema de cifrado que dejaba inseguras las conexiones de WiFi.

Como se puede apreciar, si bien los avances de la tecnología han facilitado a reducir costo y tiempo en las operaciones de las organizaciones, a su vez han originado incidentes y escenarios críticos para los cuales los sectores no están preparados; los casos mencionados en el ámbito internacional nos indican que muchos de los sistemas y protocolos se trazaron sin considerar la seguridad de la información, ya que no fueron concebidos considerando la conexión de internet.

De lo mencionado anteriormente, podemos precisar que todos estamos obligados a comprender el valor de la información y que esta debería ser gestionada adecuadamente, todo depende de cada uno de nosotros para mantenerla segura; así también, es necesario identificar las principales amenazas a las que estamos expuestos para formular las medidas que protejan la disponibilidad, integridad y confidencialidad de la información, tanto de las personas como de las organizaciones afín de reducir el impacto de los riesgos que podrían suscitarse.

A continuación, presentamos el tratamiento de la problemática de la información desde el punto de vista organizacional, para lo cual citaremos a EY, una de las mayores firmas de servicios profesionales a nivel corporativo y organizacional.

1.1.3 Preparando organizaciones con resiliencia

EY es una de las mayores firmas de servicios profesionales del mundo, que incluyen auditoría, impuestos, finanzas, contabilidad, servicios de cálculos y estudios actuariales y asesoramiento en la gestión de la empresa. Así también realiza estudios de análisis y tendencias de los distintos sectores.

En las organizaciones, al no siempre emplear controles adecuados para resguardar la información confidencial y al aprovechar por ejemplo el internet de las cosas (IoT) permite que los trabajadores utilicen dispositivos móviles como celulares, tablests o laptop las cuales podrían presentar riesgos de seguridad como aplicaciones maliciosas (malware) incrementando la probabilidad que puedan contener brechas de seguridad y por otro lado, vulnerabilidades de aplicaciones que son desplegadas por la organización con acceso a información corporativa que pueden tener debilidades de seguridad, ambos escenarios podrían impactar en los principales servicios o productos que se brindan. Es decir, no siempre se implementan controles que mitiguen probables riesgos que conllevan los cambios tecnológicos, por ejemplo: divulgación de información sensible, hackers que descifran datos confidenciales, plataformas con mayor acceso a virus, software malicioso, secuencias de comandos en páginas cruzadas y suplantación de identidad en la web.

Bajo este contexto es necesario establecer controles que permitan mitigar los impactos en las organizaciones y disminuir las pérdidas que podrían generarse.

Para esta investigación hemos obtenido información de EY (2017) en su encuesta a nivel mundial que nos muestra que, si bien en los resultados globales se aprecia que un 50% de encuestados indican estar en capacidad de predecir y detectar un ataque cibernético, solo un 36% tiene un programa formal para detectar las amenazas cibernéticas y en nuestro país este porcentaje sólo alcanza el 10%.

En este sentido, el socio líder de la consultoría de EY señala que debemos encontrarnos preparados “los constantes cambios en los mercados, el desarrollo tecnológico y la globalización de la economía generan nuevos riesgos y oportunidades para las empresas y con ello nuevas regulaciones y tendencias” (Acosta, 2017, p.3)

Según los estudios Tendencias de ciberseguridad 2018: El costo de nuestro mundo conectado y la Encuesta global de seguridad de la información 2016-17, efectuados por

ESET y EY respectivamente; se aprecia que tanto instituciones como las organizaciones no están preparadas para sostener pérdidas de información ante ataques cibernéticos y no cuentan con metodologías como buena práctica para realizar análisis de riesgos u otro tipo de análisis, originando que su información se encuentre expuesta a ciertas amenazas latentes y que su respuesta ante un incidente se desarrolla de forma reactiva; causando pérdidas de datos, tiempo, económicas, legales y otras; lo que también podría conllevar a una mala imagen acerca de su reputación ante la probable caída de sus operaciones .

Debido a la situación que se repite en distintos sectores, se hace necesario diseñar estrategias a fin de que las organizaciones establezcan acciones estándar que permitan mitigar los impactos en sus operaciones en caso de ocurrencia.

A continuación, describiremos la situación de la ciberseguridad en el Perú, tomando como referencia al Centro de Ciberseguridad Industrial (CCI).

1.1.4 Ciberseguridad Industrial en Perú

El Centro de Ciberseguridad Industrial (CCI) es una organización independiente, sin ánimo de lucro, cuya misión es impulsar y contribuir a la mejora de la Ciberseguridad Industrial, en un contexto en el que las organizaciones de sectores como el de fabricación o el energético juegan un papel crítico en la construcción de la sociedad actual, como puntales del estado del bienestar.

El CCI desarrolla actividades de investigación y análisis, generación de opinión, elaboración y publicación de estudios y herramientas, e intercambio de información y conocimiento, sobre la influencia, tanto de las tecnologías, incluidos procesos y prácticas, como de los individuos, en lo relativo a los riesgos -y su gestión- derivados de la integración de los procesos e infraestructuras industriales en el Ciberespacio.

En el contexto peruano el Estudio sobre el estado de la Ciberseguridad industrial en Perú realizado en noviembre del 2017 por CCI nos indica que se analizaron los sectores: tecnologías de la información, sistema financiero y tributario, y los servicios eléctricos, gas y petróleo; así como la administración pública, ingenierías, alimentación, industria farmacéutica, entre otros y nos revela que el desafío de las organizaciones es que las tecnologías que soportan la operación, control y mantenimiento de los equipos industriales han sido diseñadas para garantizar el procesamiento y comunicación en

tiempo real, sin considerar la seguridad de la información que se comparte. Esta situación se empeora cuando el marco regulatorio es incipiente y se efectúan desarrollos de proyectos de automatización industrial sin contemplar requisitos de seguridad y más aun con la ausencia de un equipo de respuesta ante incidentes. (CCI,2017)

Al mismo tiempo, la interconexión de las redes industriales de operación con las redes corporativas de la organización es donde el riesgo se incrementa en manera exponencial. Las redes corporativas están diseñadas para soportar grandes volúmenes de procesamiento adicional para sus funciones, permitiendo agregar controles de seguridad sin que representen un problema en su rendimiento ni funcionamiento. En contraste, la red industrial, las operaciones diarias de un negocio, es completamente diferente: la tecnología no puede soportar carga adicional a la que fue diseñada impidiendo implementar controles de seguridad porque el rendimiento y la operación de los equipos puede verse afectado, y como consecuencia, ocasionar una parada en la operación de las empresas industriales. CCI (2017).

Por otro lado, las conclusiones del estudio de CCI (2017) nos informa que:

la hiperconectividad y las iniciativas de transformación digital tiene como uno de sus principales pilares la ciberseguridad, y las organizaciones industriales no son ajenas a ella, por lo que se debe empoderar al responsable de ciberseguridad para la conceptualización y diseño de las soluciones, de tal manera que no se vea afectada la seguridad de la organización. (p.30)

Cabe señalar que CCI (2017) señala que “el gobierno peruano ha solicitado la asistencia técnica de la Organización de Estados Americanos (OEA) para desarrollar y adoptar un Plan Nacional de Ciberseguridad” (p.8). En coordinación con el Banco Interamericano de Desarrollo; donde se indica que, a pesar de no existir una estrategia nacional de ciberseguridad, se denota que se han adoptado algunas normas de seguridad y la gestión se efectúa un tanto de manera informal.

En este sentido, podemos precisar que se hace necesario establecer un marco de referencia que permita enfrentar los incidentes que afectan a los servicios críticos de las organizaciones no sólo desde un ámbito tecnológico sino también a nivel organizacional.

Del mismo modo en el 2017 Digiware, empresa con más de 20 años dedicada a la generación de estrategias integrales en seguridad de la información en Latinoamérica,

informaba a través de Galindo su *chieff business delevopment officer* que el Perú registraría pérdidas por aproximadamente de US \$ 4,782 millones por ciberdelitos debido a los cientos de ataques de malware que se suscitan diariamente e indicaba también que suelen ser los bancos pequeños los principales blancos de ataques por la falta de protección y que las dos vulnerabilidades más evidentes son: acceder al sistema de un banco a través de la tercerización de servicios y a través de las apps móviles bancarias o sus portales web; ocasionando hackear al tercero, y así ingresar al sistema del banco. (Galindo, 2017).

En consecuencia, se concluye que el sector financiero es uno de los más expuestos y afectados de manera constante por el *hackeo* de información a través de sus propios colaboradores, por el uso constante de sus aplicaciones móviles que facilitan sus actividades personales, pero que finalmente terminan infectando el equipamiento de la organización; así pues, ambas partes son víctimas de robo de información personal y organizacional.

Así también, se precisa que se ha incrementado el robo de información y constantes fraudes, lo que podría causar indisponibilidad de los servicios y en consecuencia grandes pérdidas económicas para las organizaciones.

1.2 Definiciones de seguridad de la información

A continuación, citaremos las principales definiciones que se emplearán en el presente trabajo de investigación y nos ayudarán a tener un mejor entendimiento de los temas presentados.

1.2.1 Información

De acuerdo con la norma ISO 27000 “la información es un activo que, como otros activos comerciales importantes, es esencial para el negocio de una organización y en consecuencia necesita estar adecuadamente protegida”. (p.6)

Asimismo, nos precisa que ésta puede ser almacenada de muchas formas, como: “forma digital: archivos de datos almacenados en medios electrónicos u ópticos, forma del material: en papel, así como información no representada que está en el conocimiento de los empleados”

Además, también nos indica que puede ser transmitida por diferentes medios: mensajería, comunicación electrónica o verbal; siempre teniendo la protección adecuada. (ISO 27000:2014, 3.2.2)

1.2.2 Seguridad de la Información

Tal como se refiere el ISO 27000 (2014, 3.2.3) indica:

La seguridad de la información garantiza la confidencialidad, disponibilidad e integridad de la información. Así también, “implica la aplicación y gestión de controles apropiados que implican considerar una amplia gama de amenazas, con el objetivo de garantizar el éxito empresarial, la continuidad, y minimizar las consecuencias de los incidentes de seguridad de la información”. (p. 15)

Cabe señalar que se espera que dichos controles importantes de seguridad de la información se integren de manera adecuada y perfecta con un proceso de negocio de la organización”. (ISO 27000:2014, 3.2.3)

1.2.3 Seguridad Informática

Tal como señala Gómez (2011), podemos definir la seguridad informática como cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, siendo que estos efectos puedan conllevar a daños sobre la información, o comprometer su confidencialidad, autenticidad o integridad, así como disminuir el rendimiento de los equipos o bloquear el acceso de usuarios autorizados al sistema.

Es importante señalar, que toda acción detectada no autorizada a un sistema o red informática es fundamental para prevalecer los principios básicos de la seguridad informática; mantener la confidencialidad y el acceso a usuarios autorizados.

Entre los principales objetivos de la Seguridad Informática podemos distinguir los siguientes:

- Minimizar y gestionar los riesgos y detectar los posibles problemas y amenazas a la seguridad.
- Garantizar la adecuada utilización de los recursos y las aplicaciones del sistema.

- Limitar las pérdidas y conseguir la adecuada recuperación de un sistema en el caso de un incidente de seguridad.
- Cumplir con el marco legal y con los requisitos impuestos por los clientes en sus contratos. (Gómez, 2011).

Así también indica Costas (2010), la mira central de este análisis radica en poder reducir los riesgos de las empresas, limitando las pérdidas que pueda ocasionar un incidente de seguridad; la seguridad informática está teniendo una importancia cada vez mayor; cada uno de los usuarios de cada institución y/o empresa debe de saber y custodiar que el correcto funcionamiento de sus sistemas dependerá directamente la medida de la seguridad de vuestras empresas.

La seguridad informática busca poder asegurar los recursos del sistema para que se utilicen fundamentalmente de manera única por las personas acreditadas manteniendo los límites y autorizaciones correspondientes; la seguridad es un problema integral, no puede ser tratado de manera aislada; siendo que con mayor incidencia, a través de engaños, los inducen a los usuarios a evidenciar sus passwords; es por eso, que se hace necesario la educación de cada uno de los usuarios ya que de nada serviría si estos a su vez, no están secundados por parte de los directores; dirigiendo de esta manera la cultura organizacional para el cumplimiento de logros de objetivos. (Costas, 2010).

Lo principal a proteger en cada empresa, institución, o sistema informático es el software, hardware y los datos. El hardware entendemos como el conjunto formado por todos los elementos físicos de un sistema informático, CPU, terminales, cableado, medios de almacenamiento secundario; por software, al conjunto de programas lógicos que hacen funcionar el hardware, tanto los sistemas operativos como por ejemplo las aplicaciones; finalmente tenemos los datos como el conjunto de información lógica que manejan el software y el hardware, en ese sentido, podemos argumentar que los datos se constituyen como el principal elemento de los tres a custodiar; debido a que estos representan la información del negocio tanto del ámbito comercial, financiero y legal de las organizaciones. (Costas, 2010).

Por otro lado, podemos verificar que las amenazas se pueden clasificar en amenazas provocadas por: personas, amenazas lógicas y amenazas físicas. Es de vital importancia crear una concientización de riesgos, para evitar pérdida de información de valor; siendo

los datos los de mayor relevancia debido a que es información crítica que sostiene la disponibilidad de los servicios en las organizaciones, por lo tanto, deben ser controlados y protegidos; constituyéndose la seguridad de la Información, como un activo más propio de la organización, por lo tanto, se está más expuesto a amenazas y vulnerabilidades.

Tal como menciona la NTP-ISO/IEC 17799, (2007) la información se presenta de diversas formas, impresa, electrónica, por correo, en videos, entre otros, debiéndose protegerse en cualquier de sus diferentes presentaciones, siendo la seguridad de la información la protección a las diferentes amenazas que permitan minimizar los daños y maximizar el retorno de las inversiones, implementando políticas y diversas prácticas y procedimientos que puedan asegurar el cumplimiento de los objetivos de la seguridad de la información.

1.2.4 Ciberseguridad

Tal como señala García (2015) podemos mencionar que la ciberseguridad es un conjunto de diferentes herramientas, políticas, conceptos, diversas directrices, gestiones de riesgo que de hecho se podrían utilizar para proteger todos y cada uno de los activos de una organización y también a los usuarios de los mismos en su ciberentorno, tales como claves, compras, datos personales, entre otros.

Asimismo, tal como se refiere también (Merino, M y Pérez, J., 2008) la ciberseguridad se ha convertido en algo primordial e indispensable dado que brinda establecer los diferentes controles para garantizar los diversos riesgos de la información reduciéndolos mitigándolos o transfiriéndolos.

1.2.5 Amenazas a la información

De acuerdo a lo indicado por (Gómez, 2011) define la amenaza como distintos eventos de manera intencionada o por accidente, que podrían acarrear algún impacto en términos informáticos, ocasionando algún tipo de pérdida material o de finanzas que afecten de alguna manera a la organización.

De igual forma el Instituto de Recuperación de Desastres (DRI) lo define como una “situación o condición natural u ocasionada por el hombre que puede causar una interrupción de las operaciones o servicios de una organización”. (p.7)

1.2.6 Ransomware

Borghello (2009) menciona “Aplicaciones orientadas a “secuestrar” el sistema operativo o documentos del usuario para luego cobrar una “recompensa” por su recuperación. (p.18).

1.2.7 Phishing

Se puede entender, según lo mencionado por Lara y Albán (2017) como “Las personas consiguen información confidencial mediante el envío de un correo electrónico en el que engañan al beneficiario pidiéndole sus datos o claves para actualización de datos. (p.18).

1.2.8 Vulnerabilidad de seguridad

Tal como define Gómez (2011) se relaciona con cualquier debilidad y/o fallos en el sistema informático físico y/o lógico que posibilitará a las amenazas causar daños y producir pérdidas en la organización. Así también, se presentan por defectos de ubicación, instalación, configuración y mantenimiento en cualquiera de los equipos; que pueden estar ligados a cualquier aspecto de la organización, a las faltas de las políticas de seguridad; así como a los recursos humanos o a los distintos equipos, programas y herramientas de los diversos sistemas, a la infraestructura y condiciones ambientales del sistema.

1.2.9 Gestión de Riesgos

Sea cual fuera el tipo de empresa o institución está expuesta a diversos riesgos; en tal sentido, menciona Instituto de recuperación de desastres (DRI, 2015) “el desarrollo estructurado y aplicación de la cultura de gestión, a través de políticas, procedimientos y prácticas por medio de la definición de actividades para la identificación, análisis, evaluación y control de los riesgos. (p.12).

1.2.10 Riesgo del Negocio

Tal como ha concluido el Instituto de Recuperación de Desastres (DRI, 2015) los productos, servicios de las organizaciones que ellos brindan, se podrían ver afectados por diversos factores tanto internos como externos, que podrían generar una disminución de sus ventas o servicios; la misma que generaría directamente y en forma inesperada un impacto económico y financiero para la institución.

1.2.11 Riesgo Operacional

De igual forma el riesgo de operaciones se constituye como un factor importante en la organización, en ese sentido el Instituto de Recuperación de Desastres (DRI, 2015) señala:

Riesgo de pérdida resultante de controles y procedimientos inadecuados o fallidos. Incluye la pérdida por eventos relacionados con tecnología e infraestructura, fallas, interrupciones de negocios, problemas relacionados con el personal y eventos externos, tales como los cambios regulatorios. Se basa en el riesgo de la operación, independientemente del riesgo del negocio en particular. (p.26).

1.2.12 Riesgos de la información

Tal como lo refiere Gómez (2011) el riesgo es toda aquella posibilidad de que aparezca una amenaza y se concrete sobre una vulnerabilidad en el sistema informático, generando un impacto en la organización; determinando las vulnerabilidades del sistema, las amenazas y su posible impacto se establecerá nivel del riesgo.

Asimismo, el Instituto de Recuperación de Desastres (DRI, 2015) señala al riesgo como:

Probabilidad de que se presente un evento que pudiera causar daños o pérdidas o afectar la capacidad para alcanzar los objetivos del negocio, asociado a la vulnerabilidad de la organización ante esa amenaza. En el contexto de gestión del riesgo corporativo, riesgo se refiere al potencial de que el resultado de una acción o actividad (incluyendo la no acción) resulte en un resultado diferente. (p.25).

1.2.13 Políticas de Seguridad

Las políticas de seguridad son las directrices que aplican dentro del contexto interno de la organización. Tal como indica ISO 27000 (2016, 2.6) “lineamientos para la dirección de una organización tal como lo expresa formalmente la alta dirección” (p.9)

1.2.14 Controles de seguridad

Hoy en día los controles de seguridad se han convertido en una de las mayores preocupaciones de toda institución; sobre lo dicho señala el Instituto de Recuperación de Desastres (DRI, 2015):

Procedimientos de gestión, operativos y técnicos, implementados para un sistema de información con el fin de proteger la confidencialidad,

integridad y disponibilidad del sistema y su información. En español, el término se puede utilizar además en relación con la seguridad física y la protección de las personas. (p.6).

1.2.15 Servicios esenciales (Críticos)

Los servicios críticos es parte esencial de la seguridad de la información, en ese sentido tal como lo refiere DRI (2015):

Servicios de infraestructura sin los cuales un edificio o área estarían inutilizados e impedidos para proporcionar sus servicios normales de operación; típicamente incluye: servicios (agua, gas, electricidad, telecomunicaciones) y también pueden incluir sistemas de respaldo de electricidad y de control ambiental. (p.26).

1.2.16 Incidentes de seguridad

Como nos indica Gómez (2011) un incidente de seguridad es cualquier evento que podría ocasionar la interrupción de los servicios en el sistema informático ocasionando pérdidas físicas, en sus activos o en sus finanzas.

Asimismo, el Instituto de Recuperación de Desastres (DRI,2015) lo define como el “suceso que tiene el potencial para generar una interrupción, alteración, pérdida, emergencia, crisis, desastre o catástrofe”.

1.2.17 Impactos de los incidentes de seguridad

Podemos definir el impacto como la medición y la valoración del daño que podría producirse en cualquier organización ante un incidente de seguridad. Para verificar el alcance de estos es necesario considerar los daños tangibles, así como el cálculo de los intangibles dentro de la compañía. (Gómez, 2011).

1.2.18 Plan de Contingencias

El Instituto de Recuperación de Desastres (DRI, 2015) se refiere “Documento que contiene un conjunto de acciones y procedimientos definidos previamente, que serán utilizados en incidentes menores que afecten únicamente la operación (no a las personas) cuya duración sea menor al RTO (Recovery Time Objective). (p.20).

1.2.19 Planes de Recuperación ante desastres (DRP)

Los planes de recuperación se constituyen como fundamentales frente a cualquier incidente de seguridad de la Información, menciona el Instituto de Recuperación de Desastres (DRI, 2015) “Documento que contiene un conjunto de acciones y procedimientos definidos previamente, con responsabilidades claramente establecidas, para la recuperación del componente tecnológico, sistemas y servicios de telecomunicaciones. (p.21).

1.2.20 Internet de las cosas (IoT)

El internet puede ser también como una plataforma para dispositivos que se comunican de manera electrónica, que se comparte información y datos con el mundo que los rodea. En ese sentido, Salazar y Silvestre (2016) indican “es una arquitectura emergente basada en la Internet global que facilita el intercambio de bienes y servicios entre redes de la cadena de suministro y que tiene un impacto importante en la seguridad y privacidad de los actores involucrados” (p.7)

1.2.21 Resiliencia

La resiliencia es un término importante que permite poder afrontar algún momento de adversidad en las organizaciones. Sobre lo dicho se refiere el Instituto de Recuperación de Desastres (DRI, 2015) “Capacidad de una organización para mantener sus funciones y su estructura críticas ante cualquier cambio interno o externo y regresar a un nivel aceptable de rendimiento en un periodo mínimo después de una interrupción”. (p.26).

1.3 Estándares Internacionales para sostener la guía de controles

En este punto queremos precisar los distintos estándares, metodologías o buenas prácticas que permitan cumplir con el objetivo de proponer la guía de controles base para mitigar los riesgos de seguridad de la información.

1.3.1 Seguridad de la Información – ISO/ IEC 27001: 2013

Tal como se indica en la ISO 27001:2013 el sistema “conserva la confidencialidad, integridad y disponibilidad de la información al aplicar un proceso de gestión de riesgo y les entrega confianza a las partes interesadas cuyos riesgos son gestionados de manera

adecuada”. Así también define los “requisitos para la evaluación y tratamiento de los riesgos de la seguridad de la información que se adapta a la organización”. (p.1)

1.3.2 Protección y seguridad de los ciudadanos y Sistema de Continuidad de Negocio- ISO 22301:2012

La organización internacional de estandarización a través de la ISO 22301:2012 nos indica que:

Esta norma internacional sobre la gestión de la continuidad del negocio, especifica los requisitos para la planificación, el establecimiento, la implantación, la operación, la supervisión, la revisión, el mantenimiento y la mejora continua de un sistema de gestión documentado, a fin de que el negocio esté protegido contra incidentes disruptivos, así como reducir la probabilidad de ocurrencia de éstos, estar preparado contra, responder a, y recuperarse de ellos cuando se presentan. (p.9)

1.4 Incidentes de Seguridad de la Información en el Perú

El avance de la tecnología conlleva el incremento de las amenazas cada año y las organizaciones tienen un horizonte cambiante con lo cual están aprendiendo a defenderse tomando medidas básicas o efectuando procesos especializados; por lo que definitivamente deben estar en la capacidad de defenderse y establecer controles de protección. A continuación, los distintos escenarios que se presentan ante la evolución de nuevas tecnologías:

Figura 1. Escenarios cambiantes ante el avance de las nuevas tecnologías.

Adaptado de “El camino hacia la resiliencia cibernética”, por EY, 2017.

Bajo este contexto antes mencionado, hemos tomado como referencia la 19ª encuesta global de seguridad de la información realizada por EY que se emitió en marzo del 2017 y se efectuó a nivel mundial con participación de empresas peruanas; en este sentido queremos mostrar cuales son los principales sectores que participaron de esta encuesta y donde se podrá apreciar que el sector de seguros es el segundo.

Por otro lado, queremos precisar según lo referido en la mencionada encuesta que, aunque las organizaciones han mejorado sus habilidades resistiendo los ataques informáticos y han salido airoas; los ataques o ciberamenazas son cada vez más complejos, con lo cual se precisa cuáles son las principales vulnerabilidades y amenazas en las organizaciones.

A continuación, según la encuesta de EY: la tabla N°1 principales sectores participantes, y la tabla N° 2 vulnerabilidades y amenazas más frecuentes.

Tabla 1 Principales sectores de la industria que fueron encuestados.

Encuestados por sector de la industria	
Banca y mercado de capitales	20%
Seguros	7%
Tecnología	7%
Productos de consumo	6%
Gobierno y sector público	6%
Productos industriales diversos	5%
Energía y servicios públicos	5%
Minoristas y mayoristas	4%
Telecomunicaciones	4%
Salud	4%
Medios de comunicación y entretenimiento	3%
Otros	29%
	100%

Nota: Se ha realizado el desagregado del porcentaje de participantes en la encuesta por sector realizada por la consultora EY. Adaptado de “El camino hacia la resiliencia cibernética.”, por EY, 2017.

Tabla 2 Amenazas y vulnerabilidades que han aumentado el riesgo en los cuatros últimos años.

	2013	2014	2015	2016
Vulnerabilidades				
Empleados descuidados o desinformados	53%	57%	44%	55%
Controles de seguridad o arquitectura de información desactualizada	51%	52%	34%	48%
Acceso no autorizado	34%	34%	32%	54%
Amenazas				
Malware	41%	34%	43%	52%
Suplantación de identidad (Phishing)	39%	39%	44%	51%
Ataques cibernéticos para robar información financiera	46%	51%	33%	45%
Ataques cibernéticos para robar Ips o datos	41%	44%	30%	42%
Ataques internos	28%	31%	27%	33%

Nota: Se ha realizado el desagregado de vulnerabilidades y amenazas más frecuentes. Adaptado de “El camino hacia la resiliencia cibernética”, por EY, 2017.

En la tabla N° 2 podemos apreciar que la principal vulnerabilidad en las organizaciones son los mismos empleados por las acciones descuidadas que pudieran realizar; seguidamente de los controles de seguridad. Por otro lado, de forma externa las principales amenazas son los malware y la suplantación de identidad (Phishing) y en tercer lugar los ataques cibernéticos para robar información financiera.

En este sentido, podemos deducir que conforme se viene incrementando la transformación digital y el Internet de las cosas (I o T), ambos conllevan beneficios y oportunidades tales como reducción de costos, tiempo, seguridad y protección, infraestructura mejorada, potencial crecimiento de los ingresos empresariales y también ampliar oportunidades de negocio; igualmente se presentan retos que afectan los servicios de las organizaciones.

No obstante, como indica EY en la mencionada encuesta, el Internet de las cosas también afectará a distintos sectores; tal como los servicios financieros, salud, telecomunicaciones y educación. Así mismo, se muestra en la tabla N° 3 Principales riesgos asociados al creciente uso de dispositivos móviles, son los desafíos de seguridad a los que están expuestas las organizaciones.

Tabla 3. Principales riesgos asociados al uso creciente de los dispositivos móviles

Riesgos asociados con el creciente uso de dispositivos móviles	
Pobre conciencia / comportamiento de los usuarios	73%
La pérdida de un dispositivo no solo significa la pérdida de información, sino también puede significar la pérdida de la identidad	50%
Secuestro de dispositivos	32%
Los ingenieros no utilizan el mismo firmware o software	31%
Los criminales cibeméticos venden hardware con troyanos o backdoors (puertas traseras) ya instalados	27%
Indefinición de ataques Zero-day ocultos o desconocidos	19%
Problemas de interoperabilidad a nivel hardware de los dispositivos.	16%
Otros	3%

Nota: Se aprecia el detalle los riesgos asociados al uso de dispositivos móviles. Adaptado de “El camino hacia la resiliencia cibernética”, por EY, 2017.

1.5 Sistema Financiero Peruano

En el Perú existe dentro del marco del sistema de financiero peruano, el organismo de supervisión financiero llamado Superintendencia de Banca, Seguros y AFP (SBS), encargado de regular y supervisar los Sistemas Financieros, de Seguros y del Sistema Privado de Pensiones, así como de prevenir y detectar el lavado de activos y financiamiento del terrorismo. Tiene como objetivo primordial preservar los intereses de los depositantes, asegurados y afiliados al Sistema Privado de Pensiones.

La SBS es una institución de derecho público cuya autonomía funcional está reconocida por la Constitución Política del Perú. Sus objetivos, funciones y atribuciones están establecidos en la Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca, Seguros y AFP (Ley 26702) (www.sbs.gob.pe,2018)

Del mismo modo, la SBS pone énfasis en aplicar métodos que permitan identificar, medir, controlar y monitorear sus riesgos de una manera eficiente. “Las empresas tienen a su vez libertad para implementar los sistemas que crean más convenientes, pero la SBS establece los parámetros mínimos que deben cumplirse para garantizar un manejo prudente de los riesgos”.

Cabe señalar que la SBS realiza una “supervisión especializada con enfoque por tipo de riesgo lo que implica contar con personal especializado en la evaluación de los diversos tipos de riesgo, tales como riesgo crediticio, de mercado, de liquidez, operacional y legal; permitiendo orientar una supervisión integral” (www.sbs.gob.pe,2018)

A continuación, las instituciones que conforman el sistema financiero peruano:

Figura 2. Instituciones que conforman el Sistema Financiero Peruano donde se aprecian las entidades que regulan y supervisa la SBS.

Adaptado de la página web de la Superintendencia de Banca y Seguros, SBS, 2018.

Además, deseamos mostrar el ranking de primas de seguros neta por ramos, lo cual permite apreciar cuantas aseguradoras existen en el sector y la ubicación de cada una de ellas, la data es al corte de Abril 2018.SBS

Tabla 4. Total prima de seguros

N°	Empresa	Participación %
1	Rímac	30.51
2	Pacífico Seguros	26.24
3	Mapfre Perú	9.59
4	Interseguro (1)	6.91
5	La Positiva	6.7
6	Mapfre Perú Vida	5.11
7	La Positiva Vida	4.41
8	Protecta	2.09
9	Chubb Seguros	1.85
10	Cardif	1.84
11	Otros	4.76
Total		100

Nota: Se ha realizado el detalle de la participación porcentual de cada una de las aseguradoras. Adaptado de la página web de la Superintendencia de Banca y Seguros, SBS, 2018.

En lo referente a las Corredores de seguros como Personas Jurídicas la SBS emite el control de la información financiera en ese sentido Kallpa Corredores de seguros SAC al corte de diciembre del 2016 se encuentra en la posición 26 de un total de 310 corredoras.

1.6 Sistema de Seguros Peruano

De acuerdo con el informe de clasificación de riesgo de Class & Asociados S.A. emitido el 27 de marzo de 2018 “el sistema asegurador al mes de diciembre de 2017 contó con 21 empresas: ocho dedicadas exclusivamente a brindar cobertura de seguros generales, siete a brindar coberturas de riesgos de vida, y seis para operar en ambos rubros”; en lo que

respecta al 2018 se espera una nueva fusión, debido a la adquisición de Seguros Sura por el Grupo InterCorp con la debida adscripción por Interseguro.

El mercado asegurador local es regulado por la Superintendencia de Banca y Finanzas (SBS) y supervisado por la Superintendencia de Mercado de Valores (SMV), de acuerdo a sus respectivas competencias.

Tal como reseña Class y Asociados S.A. (2018) “las coberturas de seguros generales, se conocen también como seguros patrimoniales, indemnizan al asegurado ante un daño sucedido a su propiedad” y respecto a “las coberturas de seguros de vida cubren los riesgos condicionados al bienestar y a la existencia del asegurado”.

Asimismo, la mencionada clasificadora de riesgos indica que el mercado asegurador nacional presenta una gran perspectiva de crecimiento “dada la baja penetración del sector de seguros (1.8% del PBI vs alrededor de 4.0% en promedio de otros países de Latinoamérica)” así también porque en los nichos del mercado se muestran oportunidades”. De la misma forma refiere que “el ingreso de nuevos operadores en el sistema asegurador nacional ha estado influenciado por el potencial en las coberturas de ramos específicos, algunos relacionados con regulaciones” e igualmente “por la existencia de mercados con poca profundidad y oportunidad en la especialización, permitiendo el desarrollo de productos con nuevas y diversas coberturas”. (p.7)

Por otra parte, la clasificadora nos ilustra indicando que no obstante “el ingreso de nuevas compañías reaseguradoras, así como por la poca profundización del mercado, el sistema asegurador peruano presenta alta concentración”, siendo Rímac y Pacífico las principales en el periodo 2017 y entre ambas registraron el 57,34% de las primas de seguros netos.

Y también nos indica que “las obligaciones patrimoniales y técnicas del sistema asegurador nacional están adecuadamente cubiertas por la cartera de inversiones financieras e inmobiliarias, lo que permite que la gestión financiera genere rendimientos positivos, los cuales cubren las pérdidas operativas y técnicas”. (p.7)

Finalmente, precisa que cerca del 90% de las primas de seguros netos son canalizadas a través de cinco principales grupos de empresas de seguros: Rímac, Pacífico Seguros, el grupo Mapfre, el grupo La Positiva e Interseguro y Sura.

Figura 3. Primas de Seguros Netas por Compañía- 2017.

Adaptado de “Informe de clasificadora de riesgo- Class & Asociados S.A. – Sesión de comité N°12/2018: 27 de marzo 2018”

En la actual investigación realizaremos el enfoque de nuestra indagación a través de las empresas Mapfre Perú y Kallpa corredora de seguros que pertenecen al mercado de seguros y corredores de seguros respectivamente.

1.6.1 Definiciones del sector del negocio

1.6.1.1 Seguros

Tal como lo señala Castelo y Guardiola (2008) el concepto de seguro es una contraprestación en la cual el asegurado se hace acreedor mediante un pago (prima); de una prestación que habrá que satisfacer la otra parte (el asegurador) en caso se produzca un siniestro; asimismo, desde un punto de vista general, puede también entenderse como una actividad de servicio económica financiera de transformación de riesgos de diversa naturaleza que están sometidos los patrimonios, a un gasto periódico presupuestable.

Pero hay que señalar también que el seguro supone otros servicios tales como ayuda para el ahorro, asistencia médica, o servicios de responsabilidad civil.

1.6.1.2 Reaseguros

El reaseguro sirve para distribuir entre otros aseguradores los excesos de los riesgos; tal como lo indica Castelo y Guardiola (2008) “el instrumento técnico del que se vale una entidad aseguradora para conseguir la compensación estadística que necesita, igualando u homogenizando los riesgos que componen su cartera de bienes asegurados mediante la cesión de parte de ellos a otras entidades” (p.383).

1.6.1.3 Corredores de seguro

Los corredores de seguro informan sobre las condiciones del contrato; además, durante la duración del mismo prestan asistencia y asesoramiento. Al respecto Castelo y Guardiola (2008) señalan:

Persona física o jurídica que realiza la actividad mercantil de mediación de seguros privados sin mantener vínculos contractuales que supongan afección con entidades aseguradoras, y que ofrece asesoramiento independiente, profesional e imparcial a quienes demanden la cobertura de los riesgos a que se encuentran expuestos sus personas, sus patrimonios, sus intereses o responsabilidades (p.128 – 129).

1.7 Regulaciones del Sector de seguros

1.7.1 Circular N° G-140-2009 Gestión de la seguridad de la información

La mencionada circular N° G-140-2009 en su artículo 3° nos indica que se debe implementar un sistema de gestión de seguridad de la información con las siguientes actividades mínimas:

- a. Definición de una política de seguridad de información aprobada por el Directorio.
- b. Definición e implementación de una metodología de gestión de riesgos, que guarde consistencia con la gestión de riesgos operacionales de la empresa.
- c. Mantenimiento de registros adecuados que permitan verificar el cumplimiento de las normas, estándares, políticas, procedimientos y otros definidos por la empresa, así como mantener pistas adecuadas de auditoría. (G-140-2009, art.3)

En otro punto de la circular, específicamente en el artículo N° 5 se acota los controles mínimos de seguridad de la información, con respecto a los siguientes puntos:

- 5.1 Seguridad lógica
- 5.2 Seguridad de personal
- 5.3 Seguridad física y ambiental
- 5.4 Inventario de activos y clasificación de la información
- 5.5. Administración de las operaciones y comunicaciones
- 5.6. Adquisición, desarrollo y mantenimiento de sistemas informáticos
- 5.7. Procedimientos de respaldo
- 5.8. Gestión de incidentes de seguridad de información
- 5.9. Cumplimiento normativo
- 5.10. Privacidad de la información

1.7.2 Circular N° G-139-2009 Gestión de la continuidad del negocio

La presente circular N° G-139-2009 en su artículo 3° describe a la gestión de la continuidad del negocio como un proceso que realiza tanto el Directorio, la Gerencia y el personal, para que ante la ocurrencia de un evento que genere interrupción o desequilibrio en las operaciones; la organización pueda estar en la capacidad de salvaguardar los intereses de todas las partes e implementar respuestas efectivas que permitan seguir operando.

1.7.3 Resolución SBS N° 2116-2009 Reglamento para la gestión de riesgo operacional

En esta resolución se acota en el artículo N° 3 la definición del riesgo operacional como:

“Entiéndase por riesgo operacional a la posibilidad de ocurrencia de pérdidas debido a procesos inadecuados, fallas del personal, de la tecnología de información, o eventos externos. Esta definición incluye el riesgo legal, pero excluye el riesgo estratégico y de reputación”. (p.5)

En la misma resolución en el artículo N°4 se consideran como factores que originan el riesgo operacional a los siguientes: procesos internos, personal, tecnología de información y eventos externos. (p.5)

1.7.4 Resolución SBS N° 272- 2017 Reglamento de gobierno corporativo y de gestión integral de riesgos

En el artículo N°22 la resolución define la gestión integral de riesgos como:

Proceso efectuado por el directorio, la gerencia y el personal aplicado a toda la empresa y en la definición de su estrategia, diseñado para identificar potenciales eventos que pueden afectarla, gestionarlos de acuerdo a su apetito por el riesgo y proveer una seguridad razonable en el logro de sus objetivos. (p.14)

Y en el artículo N°23 enumera una lista de diversos tipos de riesgos a la que están expuestas las organizaciones y se deben considerar: Riesgo de crédito, de lavado de activos y del financiamiento del terrorismo, de liquidez, de mercado, de reputación, técnico, de reaseguro, estratégico y operacional. (p.15)

1.8 En Perú- Ley N° 29733 Ley de protección de datos personales.

Según lo indicado por la (Ley 29733,2011, art.1) respecto al Objeto de la Ley considera lo siguiente:

La presente Ley tiene por objeto garantizar el derecho fundamental a la protección de los datos personales, previsto en el artículo 2 numeral 6 de la Constitución Política del Perú, a través de su adecuado tratamiento, en un marco de respeto de los demás derechos fundamentales que en ella se reconocen.

Del mismo modo precisa el ámbito de la aplicación de la siguiente manera:

La presente ley se aplica a los datos personales contenidos o destinados a ser contenidos en bancos de datos personales, cuya administración es de carácter público o privado y cuyo tratamiento se realiza en el territorio nacional. (Ley 29733,2011, art.3)

Y en lo que compete al flujo transfronterizo de datos personales indica lo siguiente:

El titular y el encargado del banco de datos personales deben realizar el flujo transfronterizo de datos personales solo si el país destinatario mantiene niveles de protección adecuados conforme a la presente Ley.

En caso de que el país destinatario no cuente con un nivel de protección adecuado, el emisor del flujo transfronterizo de datos personales debe

garantizar que el tratamiento de los datos personales se efectúe conforme a lo dispuesto por la presente Ley. (Ley 29733,2011, art.15)

Por otro lado, nos reseña Seguridad del tratamiento de datos personales precisando:

Para fines del tratamiento de datos personales, el titular del banco de datos personales debe adoptar medidas técnicas, organizativas y legales que garanticen su seguridad y eviten su alteración, pérdida, tratamiento o acceso no autorizado. (Ley 29733,2011, art.16)

Y finalmente nos habla sobre la Confidencialidad de datos personales

El titular del banco de datos personales, el encargado y quienes intervengan en cualquier parte de su tratamiento están obligados a guardar confidencialidad respecto de los mismos y de sus antecedentes. Esta obligación subsiste aun después de finalizadas las relaciones con el titular del banco de datos personales. (Ley 29733,2011, art.17)

El uso de los estándares internacionales que se aplican a cualquier organización de ámbito global nos permitirán identificar cuáles son las mejores prácticas que se pueden plantear en las organizaciones del sector seguros y reaseguros para establecer el marco de trabajo que brindará las facilidades para poder mitigar los impactos en caso de ocurrencia de algún ataque de ciberamenazas o que impacte la seguridad de la información. Asimismo, identificando el marco legal y normativo que aplica al sector, nos permitirá evidenciar si hay alguna brecha que no ha sido considerada, y ante los escenarios de transformación digital e incremento de la automatización, traen consigo nuevas vulnerabilidades que aún no han sido identificadas, pero que debemos proyectar para que el impacto en las organizaciones sea el menor posible.

1.9 Mapfre Seguros

Tal como nos informa Class & Asociados S.A. en su informe de clasificación de riesgos “el principal accionista de Mapfre Perú Vida es Mapfre internacional S.A., holding propietario de inversiones en entidades aseguradoras y en sociedades con actividades afines al negocio de seguros en el continente americano, como parte del Sistema Mapfre (España).” (p.3)

Negocios

Mapfre Perú Vida brinda cobertura de seguros en los ramos de seguros de vida, de seguros de desgravamen, de seguros de deceso y de SCTR Pensión. Sus operaciones se complementan con los servicios brindados por Mapfre Perú, que ofrece cobertura de seguro en los ramos generales, y con la integración de los servicios relacionados con la cobertura de seguros de SCTR Salud, a través de Mapfre Perú EPS.

Cabe indicar que también cuenta con diseños de centros médicos Mapfre y las boticas “Farmapfre” que complementan la oferta de servicios a clientes de estratos emergentes. Así también los seguros de decesos se con la prestación de servicios de sepelio, a través de la corporación funeraria y la administración de cinco cementerios.

Estrategia corporativa

Mapfre Perú realiza una constante evaluación del desenvolvimiento de su cartera de primas, con el apoyo del comité de siniestros quien tiene amplia experiencia en el mercado asegurador peruano y un sistema de información moderno el cual permite tomar decisiones de manera eficiente, así como; implementar medidas correctivas en los ramos de seguros que viene operando.

También, la compañía viene optimizando sus procesos operativos orientados a incrementar la calidad del servicio a sus clientes; a través de su red de atención y de tele venta, las cuales han incrementado su nivel de actividad. Además, a ello, Mapfre Perú aprovecha las sinergias operativas que le brindan sus empresas relacionadas por medio de las cuales resalta su imagen y solidez en el mercado.

Figura 4. Distribución Organizacional Estratégica de Mapfre Perú.

Adaptado de Mapfre Perú, 2018.

Figura 5. Distribución Organizacional Táctica de Mapfre Perú.

Adaptado de Mapfre Perú, 2018.

Productos y operaciones

Tal como lo menciona Class & Asociados S.A – Clasificadora de riesgo (2018) indican que la empresa Mapfre Perú Vida se encuentra actualmente en el mercado en una expectante y prometedora consolidación de mercado.

Es una empresa de seguros especializada en brindar cobertura en los ramos de vida, de sepelios y de rentas vitalicias, alcanzando actualmente 4.98% del total de primas de seguros netos en el mercado. Sus operaciones se complementan con las de Mapfre Perú, que proporciona cobertura en los ramos de seguros generales y de accidentes personales, alcanzando a diciembre del 2017 la tercera posición en el sistema de seguros nacional. El Grupo Mapfre, ha ampliado sus actividades a la prestación de servicios de sepelio, a la administración de cementerios, a la prestación de servicios de salud, a través de Mapfre Perú EPS y al establecimiento de centros médicos y boticas, ofreciendo de este modo, una completa gama de servicios y de coberturas a personas naturales. (p.1)

Tabla 5 *Productos que ofrece Mapfre Perú*

Seguros de salud	Seguros Patrimoniales
EPS	Automóviles
Riesgos del trabajo	Seguro de transporte
Accidentes	Seguro de robo y asalto
Enfermedad	Responsabilidad Civil
Vida y Decesos	Multirisgos
Funeraria y Cementerios	Reaseguro y coaseguro

Nota: Se ha realizado el detalle de los seguros que ofrece Mapfre Seguros. Adaptado “Informe de clasificadora de riesgo- Class & Asociados S.A. – Sesión de comité N°12/2018: 27 de marzo 2018”

Posición Competitiva

A marzo 2018, Mapfre Perú se ubica en la cuarta posición dentro del sistema asegurador peruano con una participación de 14.81%, considerando las cinco compañías más grandes, es la que más ha incrementado su market share. Del total de empresas dedicadas a los ramos generales, accidentes y enfermedades; cuatro compañías concentran el 89.93%: Rímac (30.80%), Pacífico Seguro Generales (26.60%), Mapfre Perú (14.81%), La Positiva (11.01%) e Interseguro-Sura (6.47%).

Tabla 6. Informe del Mercado asegurador peruano al mes de marzo del 2018

N°	Compañía	Marzo, 2017	Marzo, 2018
1	Rímac	31.77 %	30.80%
2	PPS	25.7 %	26.60%
3	Mapfre	13.26 %	14.81%
4	La Positiva	10.85 %	11.81%
5	Interseguro+SURA	8.76 %	6.47%
6	Chubb Seguros	1.81 %	1.82%
7	Secrex	0.41 %	0.44%
8	Cardif	2.28 %	1.76%
9	Protecta	1.16 %	2.04%
10	Otros	3%	4.24%
Total		100%	100%

Nota: Se aprecia la participación del mercado de Mapfre seguros. Adaptado de la Superintendencia de Banca, Seguros y AFP, SBS, 2018.

Figura 6. Participación del Mercado sin Rentas de Jubilación, Previsionales y Renta Particular.

Adaptado de Mapfre Perú, 2018.

Figura 7. Participación de Mercado por Agrupación de Riesgos- Vida.

Adaptado de Mapfre Perú, 2018.

Administración de Riesgos

Mapfre Perú está familiarizada con la gestión de los riesgos y así lo menciona Class & Asociados (2018) en ese sentido “cuenta con un equipo de funcionarios responsables de Riesgo Operacional Continuidad del Negocio y Control Interno (ROCC’s) quienes además de sus labores de sus áreas, contribuyen al control interno en toda la compañía.” (p.13). Además, menciona “el comité de riesgos por su parte, es responsable de aprobar las políticas para la gestión integral de riesgos, así como de establecer las políticas correctivas necesarias. ”...” Las políticas y los procedimientos para la administración de riesgos son definidas en función a los lineamientos del Sistema Mapfre para todas las empresas de América Latina”. (Class & Asociados, 2018, p.13).

Gestión de Riesgo Operacional.

La administración del riesgo operacional es uno de los pilares del Sistema de Gestión de Riesgos del Sistema Mapfre, que cuenta con variables y parámetros presentes en todas las compañías a nivel mundial, consolidando datos de todas para un manejo integral.

El riesgo de la operación, se trabaja en el Riskmap, a través de una valoración “alto”, “medio” y “bajo”; con la implantación del modelo COSO, el área de riesgos puede medir

el impacto económico del riesgo operacional, a fin de potenciar la gestión de riesgos y controles.

Como herramienta complementaria se cuenta con una base de eventos de pérdida que permite la identificación y la cuantificación, de manera de generar medidas correctivas. Class & Asociados (2018).

1.10 Kallpa Corredores de Seguros

A partir del año 2011 se inician las actividades de la corredora de seguros como persona natural y posteriormente en el año 2015, empieza como persona jurídica la empresa Kallpa corredora especializada en seguros corporativos bajo el concepto de brindar protección integral a las familias peruanas; brindando asesoramiento técnico, apoyando en caso suceda un siniestro y defendiendo los intereses del asegurado ante las compañías de seguros.

En el año 2015 ocupa el primer lugar en el ranking de la SBS de Personas Naturales, y en el 2016 obtiene el puesto 26 en el ranking SBS de Personas Jurídicas, de 360 empresas que existen en el mercado. La empresa está enfocada en la captación de los asegurados del estrato socio económico C para lo cual cuenta con tres líneas de negocio: seguros de salud, seguros de vida y seguro patrimonial; destacando en su organización los seguros de vida para la institución policial, el cual representa el 80% de sus ingresos. (Kallpa,2018).

Figura 8. Organigrama de la empresa Kallpa corredores de seguros.

Adaptado de Kallpa corredores de seguros, 2018.

Tabla 7. Las líneas de negocio de Kallpa corredores de seguros:

Seguros de salud:	Seguros de vida:	Seguro Patrimonial:
Seguro accidentes personales	Seguro vida 20 años	Seguro vehicular
Seguros oncológicos	Seguro académico	Seguro responsabilidad civil
SCTR	--	Seguro de transporte
--	--	Seguro de robo y asalto

Nota: Se ha realizado el detalle de los servicios que ofrece Kallpa corredores de seguros.

Adaptado de Kallpa corredores de seguros, 2018.

Figura 9. Ranking por año de la empresa Kallpa corredores de seguros donde se aprecia que en el año 2015 obtuvo el primer lugar en su sector.

Adaptado de Kallpa corredores de seguros, 2015.

CAPITULO 2. METODOLOGÍA DE LA INVESTIGACIÓN

2.1 Planteamiento de la Investigación

2.1.1 Propósito de la Investigación

El propósito de esta investigación es analizar la preparación de las empresas de seguros y reaseguros ante los riesgos de seguridad de la información presente en el entorno empresarial actual.

En ese sentido, determinamos que la investigación tiene un alcance descriptivo debido a que se busca conocer y describir el contexto en el cual las organizaciones manejan sus procesos de seguridad de la información; asimismo validar cómo se gestiona la información, las políticas de seguridad y los planes de recuperación; y finalmente poder aportar en el sector financiero , con enfoque en las empresas de seguros y corredores de seguros con una guía práctica de controles que es base para mitigar los riesgos de seguridad de la información que podrían impactar en el negocio.

2.2 Tipo de Investigación

Según el enfoque de nuestro trabajo la investigación es de corte cualitativo de tipo descriptivo, pues es abierta y busca explicar y describir los detalles de la investigación. Está basada en el diseño de la teoría fundamentada, ya que se han analizado los datos obtenidos en las entrevistas a profundidad, las cuales fueron codificadas para finalmente obtener una respuesta al problema planteado. Por otro lado, es de tipo descriptiva porque nos permite profundizar, analizar y entender lo que sucede en las empresas del tema de investigación y describe los hechos como son observados. Por último, es explicativa porque busca exponer las causas que originaron el problema investigado y dar soluciones al mismo.

Estas entrevistas se realizaron a los segmentos establecidos, las mismas que fueron analizadas y codificadas, para obtener una respuesta al problema planteado.

2.2.1 Preguntas de la investigación

A través del presente trabajo de investigación se buscará responder las siguientes preguntas, que se relacionan con los objetivos específicos.

- ¿Cuáles son los servicios críticos de las empresas de seguros Mapfre Perú y Kallpa corredores de seguros?
- ¿Cuáles son los principales riesgos de seguridad de la información a las que están expuestas la asegurada Mapfre Perú y Kallpa corredores de seguros?
- ¿Cómo se gestiona la información, las políticas de seguridad y los planes de recuperación en la aseguradora Mapfre Perú y Kallpa corredores?
- ¿Qué controles existen para mitigar los riesgos de seguridad en la asegurada Mapfre Perú y Kallpa corredores de seguros?

2.3 Contexto

2.3.1 Descripción del contexto interno y externo

Las entrevistas a profundidad realizadas, así como la observación del contexto en los que se desarrollaron, nos permitieron obtener mayor información para el análisis de la investigación. A continuación, se muestra la bitácora de contexto interno y externo, donde se describen nuestras observaciones de los diversos contextos o escenarios antes, durante y después de cada entrevista realizada.

Contexto/ Segmento	Segmento 1 Representantes	Segmento 2 Jefe de riesgos y tecnología	Segmento 3 Oficial de cumplimiento	Segmento 4 Analistas	Segmento 5 Consultores
Observaciones antes de la entrevista Interno	Los locales fueron similares respecto a su buena iluminación infraestructura orden; y se presentaron diferencias respecto al tamaño de los locales y oficinas. Se mostró interés por parte de las dos empresas de llevar a cabo la investigación. La edad de la representante de Mapfre Perú oscila entre 45 y 48 años mostró una gran especialización y experiencia; el representante de Kallpa tiene una edad aproximada entre 45 y 50 años. También muestran una amplia experiencia en el rubro de seguros.	Los entrevistados mostraron puntualidad. Las entrevistas se coordinaron con anticipación y los profesionales mostraron buena actitud para el apoyo de la investigación. También mostraron amabilidad y un adecuado conocimiento del tema.	Para lograr las citas con los oficiales de cumplimiento se tuvo que reprogramar a fin de no afectar en la fecha de los cierres financieros pues trabajan en conjunto con estas áreas.	Para el segmento de analista se observó inicialmente un poco de desconfianza sobre la entrevista y no permitieron que se grabara la conversación. Se coordinaron hasta en 3 oportunidades las reuniones, se mostró que eran profesionales con experiencia en el caso de Mapfre. Nos recibieron en su puesto de trabajo y, además, durante la entrevista mostraron una conversación fluida y amigable.	Se observó interés por parte de los consultores de llevar a cabo la investigación. Para el caso de algunos consultores las entrevistas se realizaron en cafés, restaurantes, hotel e inclusive en casa de uno de los integrantes de la investigación. A pesar de estos inconvenientes hubo disponibilidad por parte de los consultores; estos mostraron una gran experiencia en el campo de seguridad de la información y en el sector de seguros, todas mostraron buena actitud e interés en la investigación.
Observaciones antes de la entrevista Externo	Las entrevistas se coordinaron con anticipación; una fue en Miraflores y la otra en la Victoria; la avenida principal a Mapfre Perú es la Av. 28 de julio N° 873 – Miraflores es concurrida de mucho tráfico y tránsito de personas. En el caso de Kallpa corredora de seguros se encuentra en el distrito de la Victoria cerca al óvalo Arriola y también es una calle concurrida con poca iluminación eléctrica.	Al ingreso de sus instalaciones de ambas empresas tenían controles de seguridad física Se aprecia más trabajadores en Mapfre respecto de Kallpa. La infraestructura de la empresa Mapfre Perú es amplia, con una serie de mecanismos de seguridad; y su local bien iluminado. En Kallpa se presenta un ambiente más pequeño y reducido pero ordenado, iluminado y limpio.	Ambas entrevistas se realizaron en las mismas instalaciones de Mapfre y Kallpa que se mencionaron anteriormente. Se aprecia una buena estructura de los locales, así como un cálido clima laboral para las 2 empresas. Se cumplieron los horarios de la entrevista.	Para el tema de los horarios en las entrevistas de Mapfre Perú fue un poco complicado la disponibilidad referente a los horarios, se tuvo que esperar el término de unas funciones para la atención. Las entrevistas se realizaron en los distritos de Miraflores y la Victoria que se mencionaron anteriormente. Se aprecia que ambos distintos tienen mucha congestión de tránsito para el acceso a sus instalaciones, el entorno se nota que es limpio y ordenado.	El Café, restaurant, hotel donde se realizaron las entrevistas fueron en los distritos de San Isidro, Miraflores y Surco respectivamente, son zonas seguras, comerciales de alto tránsito; normalmente se realizaron en las noches cuando los consultores tenían mayor disponibilidad de tiempo.
Observaciones durante la entrevista	Los entrevistados mostraron amplia experiencia en su rubro, además presentaron un alto de grado de interés frente a las preguntas que les hacíamos de acuerdo a nuestra investigación. Asimismo, mostraron diferencias respecto a la magnitud de sus operaciones; se encontró similitud en el buen trato e interacción. En Mapfre Perú se vieron espacios colaborativos de los puestos de trabajo en la distribución de los colaboradores. Los representantes pidieron a sus secretarias que no los interrumpieran durante una hora. Ambos entrevistados aceptaron se grabara la entrevista.	Los entrevistados mostraron amplia experiencia y trayectoria en el sector; mostraron un alto grado de interés y participación; todos fueron puntuales y se mostraron buena predisposición a la entrevista. Se apreció un buen clima laboral en ambas empresas, en el caso de Mapfre se observó paneles con fotos de cumpleaños de las áreas de trabajo. Para el caso de Kallpa se apreció que todos se conocían de una forma muy amical al ser un grupo pequeño. Durante la entrevista los profesionales apagaron los celulares. Uno de los profesionales no permitió que se grabara.	Ambos profesionales mostraron puntualidad y atención en las entrevistas, uno de ellos no permitió grabar la entrevista. Se mostró mucho conocimiento respecto a fraudes, estafas, lavado de activos, riesgos y otros. Mantuvieron sus celulares apagados y nos atendieron en salas privadas. Se nos solicitó que tuviéramos nuestros celulares apagados. Ambas personas mostraron puntualidad y buen trato; así como apertura a los diversos temas tratados.	Durante la entrevista se mostró similitud en el trato, en el lenguaje y en el interés acerca de la investigación a tratar; así también, los tiempos durante las mismas entrevistas fueron adecuados, siendo Kallpa la empresa que mostró mayor disponibilidad. El entrevistado de la empresa Mapfre Perú estuvo algo apurado debido a sus labores y/o trabajos cotidianos pues los visitamos en cierre de mes que es cuando presentan informes de cierre de gestión.	Los entrevistados mostraron amplia experiencia en su rubro, además presentaron un alto de grado de interés frente a las preguntas que les hacíamos de acuerdo a nuestra investigación. Asimismo, se encontraron que la mayoría tenían trayectoria profesional en la especialidad. El consultor de Rímac nos explicó ampliamente sobre las tecnologías emergentes y sobre el incremento de las ciberamenazas; asimismo comentó que la SBS aún no contempla controles en estos cambios tecnológicos. Por otro lado, el consultor de la Management Secure nos precisó que la transformación digital va acompañada de un cambio de cultura en las organizaciones.

					El consultor de La Positiva nos indicó que el internet de las cosas si bien trae facilidades para sus usuarios también conllevan a nuevos riesgos que deben ser analizados por la organización. La mayoría nos solicitaron que les informáramos respecto al resultado de la investigación.
Observaciones después de la entrevista	Ambos ejecutivos al momento de la despedida manifestaron su disposición para absolver otras futuras consultas de nuestra investigación.	Los entrevistados brindaron sus correos y celulares para futuras consultas, se mostraron muy amigables e interesados con el tema de la investigación.	Ambas personas mostraron que tenían mucha experiencia respecto al lavado de activos, fraudes, pero a su vez mostraron mucha cautela en la información que nos brindaron, además, nos referenciaron a otro profesional de la organización para que nos brinden mayor información.	Se observaron diferencias respecto al momento del término de las entrevistas. Se evidenció apuro por parte de los analistas de Mapfre Perú, brindando más disponibilidad los analistas de Kallpa; tiempo referente a Kallpa. Ambos analistas de las empresas nos desearon éxito en el tema a investigar.	Aunque las mayorías de las entrevistas se dieron en lugares públicos, y en horarios nocturnos, todos mostraron interés en el tema y debido a que la mayoría viaja por trabajo y brinda capacitaciones nos indicaron que nos podríamos comunicar con ellos posteriormente por correo o por whatsapp.
Conclusion general por segmento	<p>Ambas empresas mostraron interés y disponibilidad a nuestra investigación, estuvieron interesados en nuestras consultas. Se observó una conducta ética respecto a escenarios que se vivieron en la organización.</p> <p>Se observó diferencia en el tamaño de las oficinas, no obstante, ambos ambientes eran modernos y cálidos y se apreció en ambas organizaciones buen clima laboral.</p>	<p>En la empresa Mapfre los especialistas contaban con mayor trayectoria respecto a seguridad de la información y a los sistemas de tecnología. Para el caso de Kallpa sus profesionales eran más jóvenes en el sector.</p> <p>Las entrevistas se realizaron en salas de reuniones con buena iluminación e infraestructura; no se presentaron interrupciones durante las mismas,</p>	<p>Los especialistas en cumplimiento mostraron experiencia en detectar fraudes, estafas, lavado de activos entre otros. Mantuvieron mucha reserva a la hora de brindar la información; nos recomendaron ahondar con otro colega de la compañía.</p> <p>El trato fue sobrio y formal, no se permitió las grabaciones y ambas partes mantuvimos los celulares apagados.</p> <p>Se mostró puntualidad en las entrevistas.</p>	<p>En este segmento se evidenció que la mayoría de los entrevistados estuvo un poco desconfiada en brindar una cita para las entrevistas por el tema a tratar y por la carga laboral que tienen.</p> <p>Sin embargo, mostraron conocimiento del tema y mostraron un trato amable, aunque no todos permitieron que se grabara las reuniones.</p> <p>El que la reunión se haya agendado a fin de mes cuando hacen la entrega de sus informes no facilitó que nos brindaron más tiempo para repreguntas.</p>	<p>Los expertos mostraron conocimiento en tecnología emergentes, robotización, internet de las cosas, y en el incremento de las ciberamenazas. Así también, nos informaron en la nueva tendencia del servicio de seguros “insuretech”, seguros con tecnología.</p> <p>Todas las entrevistas se realizaron en ambientes como restaurantes, cafés, casa de integrante de la investigación; presentaron una gran disposición y experiencia, a pesar del ruido que existió en algunos locales. En todo momento facilitaron las entrevistas y mostraron un gran profesionalismo.</p>

2.4 Muestra

2.4.1 Descripción de la muestra

Nuestra muestra no es de corte probabilístico porque es una investigación descriptiva que está ligada al tipo cualitativo; hemos considerado entrevistar aquellos actores fundamentales de la seguridad de la información de Mapfre Perú y Kallpa, así como representantes de las organizaciones y consultores de la especialidad que nos permitan tener una visión con mayor precisión de la información como valor; según los factores de Sampieri se ha considerado por el entendimiento del fenómeno, su naturaleza y la saturación de las respuestas en la categoría; confirmando lo que se ha fundamentado y se tomó una muestra de 16 entrevistas a los siguientes roles:

Segmentos de entrevistas	Cantidad
Representantes de organización	02
Jefe de Riesgos /Jefe de Tecnología	04
Oficial de cumplimiento	02
Analistas de Riesgos/ Seguridad de la Información /Analista de TI	04
Consultor / Especialista de Seguridad	04
Total de entrevistados	16

2.5 Diseño o abordaje principal

2.5.1 Identificación de la estructura de la entrevista o focus

Para esta investigación se efectuaron entrevistas a profundidad en base a una guía de preguntas semiestructuradas, permitiendo que los entrevistados manifiesten de una manera profunda sus puntos de vista, conocimientos y experiencia.

2.5.2 Guía de preguntas

Aquí se presenta una muestra de preguntas realizadas en las entrevistas a profundidad, tomando como base los objetivos específicos de la presente investigación, así como de las categorías y segmentos:

- ¿Cuáles son los servicios críticos de la organización y que tratamiento se les ha dado?
- ¿Qué líneas de negocio tiene la empresa y que productos ofrece al mercado?
- ¿Cómo se gestiona los riesgos de seguridad de la información que se han identificado?
- ¿Cómo guardan la información crítica y cómo aseguran que la información no sea manipulada o alterada?
- ¿Se tienen políticas de seguridad establecidas y quiénes la aprueban?
- ¿El personal involucrado con el manejo de la información recibe capacitación o inducción en las políticas de seguridad?
- ¿Cómo se gestionan incidentes o incumplimiento que se dan entorno a la política y como se retroalimentan las políticas?
- ¿Considera usted que el IoT (Internet de las cosas) incrementa los riesgos en las organizaciones?

La guía de preguntas por cada segmento se encuentra en el Anexo 1.

2.5.3 Segmentos

Los segmentos seleccionados para el levantamiento de la información son los que se mencionan en la siguiente tabla, dentro de los cuales definimos un número determinado de entrevistados, como se detalla a continuación:

Mapfre Perú/Kallpa Corredores de Seguros
Representante de la organización
Jefe de Riesgos/ Jefe de Tecnología
Oficial de cumplimiento
Analistas de Riesgos/ Seguridad de la Información /Analista de TI
Consultor / Especialista de Seguridad

2.5.4 Categorías

El presente trabajo de investigación al tener una metodología cualitativa y utilizar entrevistas a profundidad para obtener información, definimos las categorías o grandes temas que abordamos en ellas en base a nuestros objetivos planteados y los conceptos indicados en el marco teórico. Dichas categorías permitieron organizar los resultados o descubrimiento relacionados con el tema de investigación.

Se agruparon las categorías de la siguiente manera los temas que se abordaron con los entrevistados son:

CATEGORIAS:

- Modelo de la aseguradora y corredora de seguros
- Líneas de negocio y productos/servicios
- Gestión de los riesgos de la organización: identifica, análisis, evalúa y tratamiento.
- Controles para mitigar riesgos
- Custodia de la información
- Políticas de seguridad
- Planes de recuperación
- Tendencias y cambios tecnológicos

2.5.5 El instrumento de Investigación

En base a los objetivos de la investigación, se llevaron a cabo entrevistas a profundidad con una guía de preguntas semiestructuradas, lo que nos permitió recopilar datos y analizarlos para obtener indicadores cualitativos que brinden mayor confiabilidad a la investigación a los dos miembros del equipo, principal instrumento de investigación

2.6 Procedimiento

El trabajo de campo fue desarrollado en las oficinas y /o lugares de trabajo de los entrevistados. En la mayoría de los segmentos entrevistados se localizaban en los distritos de Miraflores, La Victoria y Lince. El equipo de investigación estuvo conformado por dos participantes, uno realizaba la entrevista y el otro participante, tomaba nota de cómo se observaba el contexto.

Previamente a iniciar las grabaciones, se les solicitaba autorización a los entrevistados para no tener inconvenientes durante nuestra reunión.

2.6.1 Matriz de procesamiento : Segmento - Categoría

	CATEGORIAS	PREG	Segmento 1 Representante de empresa	Segmento 2 Jefe de riesgos/ Jefe Tecnología	Segmento 3 Oficial de cumplimiento	Segmento 4 Analistas de Riesgos, Seguridad de la Información y de tecnología	Segmento 5 Consultores
OBJETIVO 1 SERVICIOS CRITICOS	Modelo de aseguradora y corredora Líneas de negocio y productos y servicios	1	Mapfre Perú independientemente del seguro que ofrece sostiene su información en la plataforma tecnológica y las telecomunicaciones los cuales brindan el sostenimiento para la venta a través de la red digital, siendo estos componentes sensibles a ser vulnerados por las ciberamenazas. Kallpa corredora de seguros solo lleva su información guardada en un centro de cómputo interno y a través de formatos Excel. Como tiene captado al 80% de las fuerzas policiales, debe proteger con minuciosos controles de seguridad la información que guarda	Para Mapfre Perú es de suma importancia la plataforma tecnológica para la atención a sus usuarios de seguros vida y seguros generales. Así mismo, las telecomunicaciones para su atención en redes digitales. En Kallpa, al ser un intermediario, sostiene su información en archivos Excel y están en fase de migración a una plataforma tecnológica.	En Mapfre Perú, para este segmento los servicios críticos son la atención al usuario a través de las redes digitales y sus líneas de negocios principales son salud, vida, sepelio, autos, seguros médicos y planes de jubilación; los cuales se brindan a los sectores c y d con más fuerza. En Kallpa se considera como servicio crítico a las telecomunicaciones como internet y telefonía. Las líneas de negocio son seguros vida y seguros generales y se concentran en el nivel C.	Para los analistas de Mapfre los servicios críticos son las bases de datos que resguarda Mapfre así como la fuga de información y el uso de dispositivos electrónicos. Respecto a los principales servicios indican que son riesgo, salud, vida, EPS, fraudes, entre otros. Se brindan atención a los segmentos a, b, c y d. En Kallpa, su servicio crítico es almacenar información en archivos Excel sin control de accesos lógicos lo que podría generar fuga de información. La mayor atención a sus usuarios es en el sector C con los seguros de vida.	Los principales productos que se ofrecen seguros vida y seguros generales. Los principales clientes son las personas naturales, luego empresas y pymes, no se realiza diferencia del NSE. Como servicios críticos identifican a las bases de datos, data centers, aplicaciones y plataformas tecnológicas que sostienen los servicios.
		2					
		3					
OBJETIVO 2 GESTIÓN DE LOS RIESGOS	Identificación, análisis, evaluación y tratamiento. Controles para mitigar riesgos Custodia de la información confidencial	4	En Mapfre Perú se realiza una gestión integral de riesgos periódicamente y a través del Disma del área de riesgo, los que a su vez implementan los controles necesarios para mitigar los riesgos. Así mismo, establecen las políticas para custodiar la información. En el caso de Kallpa corredores, se efectúa el análisis de riesgos según lo solicitado por la SBS y la información de su negocio está resguardada en el servidor de la empresa.	En Mapfre Perú, se gestionan los riesgos de la compañía tanto riesgos operativos, financieros, lavados de activos, reputación, liquidez y tecnológicos, de acuerdo a lo indicado por la SBS y alineado a lo gestionado por la casa matriz. En Kallpa corredores, se han implementado controles básicos como control de accesos físicos y control de accesos lógicos.	Mapfre Perú cumple con una gestión integral de riesgos en aspectos de resguardo de información, tecnología, lavado de activos, operativos, liquidez, entre otros. Según lo indicado por la SBS. Los riesgos son canalizados a través de un comité, pero lo correspondiente al lavado de activos y financiamiento de terrorismo también es notificado a la entidad supervisora. En Kallpa se realizan controles básicos y se aprecia que tienen vulnerabilidades al sostener la información en el google drive.	En Mapfre se ha identificado ataques de ransomware los cuales no han generado impacto a la organización debido a que se realizaron los parches oportunamente. En caso de tener algún impacto en los servicios estos son escalados al comité de riesgos. En Kallpa, los principales incidentes que se han presentado son el spam y el phishing los cuales han sido mitigados por el área de sistemas, no se realizan escalamiento para la resolución,	Los consultores precisan que se llevan controles de riesgos de acuerdo con lo indicado por la reguladora SBS que supervisa al sector de seguros, reaseguros y corredores. En este sentido estas organizaciones deben cumplir con gestionar los riesgos de su organización en el ámbito estratégico, operativo, financiero, lavado de activos, mercado, reputación, liquidez y tecnológicos. Los incidentes de seguridad de la información son tratados a nivel interno a través de las áreas de riesgos y los comités correspondientes, estos no son reportados a la SBS. Así mismo, estas organizaciones custodian la información de sus clientes, colaboradores, proveedores, según lo indicado por la LPDP.
		5					
		6					

OBJETIVO 3 POLITICAS DE SEGURIDAD Y PLANES DE RECUPERACIÓN	Políticas de seguridad	7	Mapfre Perú cuenta políticas de seguridad de la información respecto a acceso lógico, control de activos, acceso físico, respaldo de información, redes y continuidad de negocio.	Mapfre Perú cuenta con políticas de seguridad de la información a través de un sistema de gestión liderado por el área de gestión de riesgos y la alta dirección, involucrado a las partes interesadas proveedores, clientes, accionistas, entre otros.	En Mapfre Perú cuentan políticas de seguridad de la información respecto a control de accesos físicos, control de accesos lógicos, respaldo de información, continuidad y otros.	La aseguradora Mapfre Perú tiene implementada políticas de seguridad de la información que son informadas al ingreso de cada colaborador y en las capacitaciones periódicas que realiza el área de gestión de riesgos para la organización, por lo menos, una vez al año.	En las organizaciones del sector de seguros y corredores se definen políticas de seguridad de la información aprobadas por la alta dirección o quien la represente, además se realizan programas de concientización y cuentan con áreas de riesgos o comités para canalizar el tratamiento y control de los mismos para mitigar los riesgos. Así mismo, se llevan a cabo programas de auditorías internas, y cuando apliquen auditorías externas, así como planes de cumplimiento para el logro de los objetivos.
		8					
	Planes de recuperación	9					
		10	Respecto a Kallpa corredores, no cuenta con políticas de seguridad de la información a la fecha.	La corredora Kallpa no cuenta con políticas de seguridad de la información.	En Kallpa no se han implementado políticas de seguridad aún.	Para el caso de Kallpa, se brindan charlas ocasionales a las áreas de la organización sobre ciertos cuidados tecnológicos, pero no existen políticas de seguridad formales.	
		11	Mapfre Perú realiza planes de recuperación y pruebas una vez al año que están a cargo del área de Gestión de Riesgos.	Mapfre Perú realiza planes de recuperación y pruebas una vez al año, que están a cargo del área de Gestión de Riesgos. Las pruebas de continuidad se realizan entre el data center principal de EE.UU. y el data center secundario en Brasil simulando una caída de uno de ellos.	En Mapfre Perú, se realizan planes de recuperación y las pruebas correspondientes anualmente a cargo del área de gestión de riesgos.	Mapfre realiza planes de recuperación de la plataforma tecnológica por cada uno de sus componentes y un ejercicio completo de sus data center una vez al año.	Las organizaciones de este sector deben tener planes de recuperación y realizarlos por lo menos 1 vez al año y emitir los informes de las pruebas realizadas, esto es una exigencia de la entidad supervisora, SBS.
		12					
		13					
		14	Por el lado de Kallpa, no se realizan planes y pruebas de recuperación.	Por el lado de Kallpa, no se realizan planes de recuperación.	En Kallpa, aún no se han implementado planes de recuperación.	En Kallpa aún no se ha implementado planes de recuperación.	
OBJETIVO 4 GUIA DE CONTROLES	Tendencias y cambios tecnológicos	15	El Internet de la cosas (IoT) y otras nuevas tecnologías son evaluadas por el área de Gestión de Riesgos de Mapfre Perú.	En Mapfre Perú debido a los constantes cambios tecnológicos y tecnologías emergentes, se evalúan los riesgos cuando se realizan cambios en la organización y para cada uno de sus productos nuevos, esta evaluación está a cargo del área de riesgos.	N.A.	N.A.	Respecto al internet de la cosas (IoT), nos indican que cualquier dispositivo que sume en el ecosistema de la red puede ser una potencial fuente de vulnerabilidad que podría comprometer la seguridad y las operaciones, por lo cual se debe establecer controles para evitar que la información que se comparte sea vulnerada por las ciberamenazas. En lo que respecta a la transformación digital indican que esta trae beneficios a las organizaciones en cuanto a reducción de costo y tiempos así como automatización de los procesos pero a su vez conlleva a nuevas amenazas de ciberseguridad que podrían generar fugas de información, extorsión, y interrupción de servicios. Con el crecimiento de las tecnologías emergentes se deben plantear programas de ciberseguridad liderados por alta dirección concientizando a los colaboradores de las organizaciones para generar un cambio de cultura, a fin de mitigar los impactos de las ciberamenazas.
		16					
		17					
		18	En Kallpa corredores, estos cambios tecnológicos aún no han sido analizados ni contemplados.	En la corredora Kallpa aún no se realiza evaluación de cambios tecnológicos.			

2.6.2 Matriz de procesamiento de información – Aspectos positivos y negativos

MATRIZ DE PROCESAMIENTO DE INFORMACIÓN	
MODELO LÍNEAS DE NEGOCIO, PRODUCTOS Y SERVICIOS	
ASPECTOS POSITIVOS	ASPECTOS NEGATIVOS
Tanto las empresas aseguradoras y corredoras de seguros tienen la opción de pertenecer a asociaciones a fin de estar fortalecidas en el sector; para el caso de Mapfre Perú pertenece a la asociación peruana de empresas de seguro (APESEG) que es una institución sin fines de lucro que agrupa y representa a todas las compañías de seguro y reaseguros del país. Así también la corredora de seguros pertenece a la asociación peruana de corredores de seguros APECOSE, institución sin fines de lucro que vela por que la compra-venta de seguros sea un buen negocio para todos los que intervienen en ella: clientes, compañías, agentes y corredores de seguros; convencidos de que los seguros son parte del motor que mantiene la continuidad de negocios e instituciones en el Perú. Entre ambas asociaciones trabajan también por la protección de información y siendo líderes en el sector podrían efectuar controles en común respecto a la seguridad de la información.	El avance de la tecnología sobre pasa los controles establecidos en la empresa de seguros Mapfre Perú. Para el caso de Kallpa tendría un mayor impacto debido a que aún no están evaluando las tecnologías emergentes, que ya se están implementando en el sector.
La compañía de seguros Mapfre Perú tiene una plataforma tecnológica que permite resguardar la información del negocio, de sus clientes, proveedores y otros; así como facilitar el acceso de su red digital para el beneficio de sus servicios.	Si bien la empresa Mapfre Perú ya empezó a atender a sus clientes por la red digital, también debería familiarizar a sus usuarios respecto al impacto de la ingeniería social – phishing, ransomware y otros -, al hacer uso de las App y que pueda conllevar algún riesgo en los servicios de Mapfre Perú.
La corredora de seguros Kallpa viene implementando un sistema para su información lo que permitirá tener mayor seguridad y custodia de la misma. La migración de la información de excel a un sistema integrado, logrará mitigar los riesgos de pérdida o robo de información tecnológica para sus principales líneas de negocio.	
Mapfre fomenta la concientización de la seguridad de la información de manera periódica a todos los niveles de la organización.	

IDENTIFICACIÓN, ANÁLISIS , EVALUACIÓN TRATAMIENTO DE CONTROLES PARA MITIGAR RIESGOS	
ASPECTOS POSITIVOS	ASPECTOS NEGATIVOS
La empresa corredora de seguros Kallpa y Mapfre Perú tienen un buen control del manejo de lavado de activos y financiamiento para el terrorismo, en ese sentido, los filtros para acceder como clientes a esta organización son bien gestionados.	Existen oportunidades en que a través de la compra de seguros se cometen fraudes para realizar lavado de activos o financiamiento del terrorismo.
Las compañías de seguros efectúan una gestión de riesgos integral desde la alta dirección hasta las áreas operativas de la organización; asimismo, mantienen la alineamiento con la casa matriz de España.	La corredora de seguros Kallpa al mantener información en excel tiene expuesta la información de la organización debido a que es de fácil acceso de cualquiera de los miembros de la empresa, por más que tenga ciertos controles básicos.
La Superintendencia de Banca y Seguros (SBS) a través de sus circulares intenta controlar y orientar a las empresas del sector con la identificación y tratamiento de los riesgos; así como de asegurar la disponibilidad de sus servicios para la atención de sus clientes.	En la actualidad Kallpa no realiza o no efectúa una gestión de riesgo de seguridad de la información, se estima que una vez que implante su plataforma tecnológica evaluará los riesgos que esta conlleva.
Mapfre y Kallpa ambas manejan un buen control de accesos físicos a sus instalaciones, pues a través de fotochecks se identifica al personal de la organización y los pases de visita para el personal externo, lo que permite que personas desconocidas no accedan a sus locales.	Ambas empresas deberían contemplar dentro de sus riesgos el servicio de red digital, a fin de evitar robos o secuestro de información, ransomware o phishing que podrían presentarse a través de ella.
En cuanto a los accesos lógicos a sus aplicaciones, ambas organizaciones han establecido perfiles para sus usuarios, a fin de establecer la trazabilidad de las actividades de cada uno de sus usuarios en las plataformas tecnológicas, reduciendo así los riesgos de la seguridad de la información.	
Mapfre cuenta con herramientas tecnológicas para identificar amenazas como spam, phishing, ransomware y otros los mismos que son controlados por el área de gestión de riesgos de la organización evitando pérdidas o robos, o inclusive caída de los servicios; de tal forma que permita mitigar el impacto de las ciberamenazas.	
Se evidenció que Mapfre Perú cuenta con un área encargada de efectuar la evaluación de riesgos integrales y, asimismo, ha establecido un comité de riesgos que ayuda a implementar nuevos controles o lineamientos en beneficio de la organización y sus clientes.	

POLÍTICAS DE SEGURIDAD Y PLANES DE RECUPERACIÓN	
ASPECTOS POSITIVOS	ASPECTOS NEGATIVOS
Las políticas establecidas por parte de la empresa Mapfre Perú permite poder mitigar los riesgos de seguridad de la información, es decir, disminuir el impacto de las mismas.	La corredora de seguros Kallpa no cuenta con políticas de seguridad de la información lo que origina que no contempla la protección para la información confidencial de la organización; lo que más adelante podría traer pérdidas económicas.
La empresa Mapfre Perú realiza planes de recuperación permitiendo proyectarse a cualquier incidente o contingencia para la no afectación de sus servicios y el cuidado de la información.	La falta de mayor conciencia frente a incidentes de ciberseguridad pueden generar robo, secuestro o fraude de la información; viéndose reflejado directamente en la recuperación del servicio, afectación a sus clientes y activos de la compañías.
Además, Mapfre Perú realiza periódicamente pruebas de contingencia con la ayuda de sus centros de cómputo en Miami y Brasil, así también realiza informes de las mismas para identificar los tiempos que le tomaría establecer sus servicios.	En la actualidad Kallpa no realiza planes de contingencia para mantener disponible sus servicios, este escenario lo expone a estar vulnerable ante ciberamenazas.
TENDENCIAS Y CAMBIOS TECNOLÓGICOS	
ASPECTOS POSITIVOS	ASPECTOS NEGATIVOS
Mapfre Perú tiene diversas áreas de manejo y custodia de la información tales como Disma- Dirección de seguridad y medio ambiente-; área de tecnología y el área de riesgos operativos; donde de manera integral plantean lineamientos que permitan implementar nuevos controles de acuerdo con las tecnologías emergentes.	Mapfre Perú está empezando a robotizar procesos operativos de su organización para atender de manera oportuna a sus clientes, pero esta nueva tecnología trae consigo ciberamenazas que podrían afectar sus servicios.
La compañía de seguros Mapfre Perú cuenta con un sistema integrado de proveedores, clientes, accionistas lo cual custodia y protege de mejor manera la información, permitiendo tener sistemas integrados de comunicación, interacción, y eficacia a través de alcances tecnológicos que demanda la era digital.	La compañía Kallpa aún no está preparada para la era digital, el internet de las cosas, como nuevas formas de manejo y custodia de la información de productos, venta de servicios, entre otros; lo cual podría ocasionar riesgos frente al crecimiento tecnológico.
La transformación digital y las tecnologías emergentes traen consigo beneficios como reducción de tiempos, costos, ahorros económicos y nuevas oportunidades de negocio para las organizaciones Mapfre y Kallpa.	Frente a la era digital, tecnologías emergentes, internet de las cosas y otros, podrían generarse amenazas que a un mediano plazo podrían generar pérdidas económicas, financieras, legales y hasta en su reputación.

CAPITULO 3. ANÁLISIS DE DATOS Y RESULTADOS

3.1 Principales preguntas que cubren los objetivos planteados

En el presente capítulo se analizará la información obtenida de las entrevistas realizadas a los segmentos identificados, con el fin de validar nuestra hipótesis planteada en la presente investigación.

1. ¿Cuáles son los servicios críticos de las empresas de seguros Mapfre Perú y Kallpa corredores de seguros?

Según las entrevistas realizadas y el análisis efectuado se han identificado como servicios críticos las telecomunicaciones y la infraestructura tecnológica, que dan soporte a la entrega de los servicios que ofrecen tanto la aseguradora como la corredora de seguros, cabe indicar que la complejidad de su equipamiento dependerá de la envergadura de la organización.

Al margen del servicio que se ofrece, del nivel socio económico de sus clientes y del tipo de la información que se maneja, estas organizaciones custodian información sensible de cada uno de sus asegurados.

Estos registros son almacenados y muchas veces compartidos con distintas entidades vinculadas al sector, así como: Superintendencia de Banca y Seguros, centros de salud, funerarias, empresas de servicios automotriz, entre otras.

Siendo que este sector está en crecimiento debido a la oferta de más productos y servicios y además de la misma especialización del campo de seguros; las organizaciones pretenden diversificar los canales de comunicación para facilitar el acceso a sus clientes, y para lograrlo demanda de la tecnología que permitirá reducir costos, simplificar procesos, disminuir los tiempos de atención, diferenciarse de la competencia y mejorar la satisfacción del cliente; entre otros.

En este contexto, donde las tecnologías de información tendrán un rol de suma importancia para el desarrollo de los negocios; la seguridad de la información y más específicamente la ciberseguridad deberá incorporarse a las prácticas de gestión empresarial lo cual demandará establecer estrategias, destinar recursos y todo lo necesario para custodiar la información de valor.

Todos estos servicios, recursos y sistemas se demandan con mayor magnitud de manera digital, obligando a los sectores a adaptarse a los cambios que trae consigo la transformación digital.

Se ha verificado, en lo anteriormente expuesto, que la empresa Mapfre Perú tiene como uno de sus servicios críticos la emisión masiva de pólizas para estas operaciones, la empresa de seguros viene implementando el servicio de emisión de pólizas a través de robots, lo que permitirá efectuar una mayor cantidad de pólizas y a su vez reducir trabajos operativos; estas operaciones son conocidas “puestos masivos de la nueva tecnología”; en ese sentido, adicionalmente a las actividades de verificar la programación, el mantenimiento y supervisión de los robots, se va requerir gestionar los riesgos de ciberseguridad en torno al funcionamiento de los robots, evitando de esta manera posibles afectaciones a la operatividad de los servicios críticos; principalmente debido a ataques informáticos y cibernéticos. Al respecto la representante comercial de la referida empresa nos menciona:

...Mapfre siempre esta aperturando nuevos ramos, por ejemplo, ya ahora estamos trabajando con los robots los que van a hacer trabajos operativos como las emisiones de pólizas, los puestos masivos la nueva tecnología...
(Julie B. - Sub Gerente Recursos Humanos Mapfre Perú.).

Podemos apreciar, que efectivamente parte actual de los servicios críticos de la empresa Mapfre Perú se encuentra en una etapa de transición hacia la automatización ya que se demuestra que la incorporación de nueva tecnología como el internet de las cosas y la robótica conllevará hacia una transformación digital la misma que se traduce en ser eficientes teniendo un acercamiento personalizado y en tiempo real con el cliente a la par con las nuevas demandas del mercado.

Por otro lado, se ha comprobado que uno de los servicios críticos de la empresa Kallpa corredora son los seguros de vida que actualmente representa el 80 % de su fuerza de

venta de la referida empresa; pues brinda este servicio a instituciones como la Policía Nacional del Perú con una cuota aproximada de 20 mil asegurados.

...el negocio fuerte de la corredora es el de vida representando un 80 – 20, Pareto ...tenemos más de 20 mil asegurados en la policía, por ejemplo, que es nuestro principal cliente... (Dante. R. - Gerente General de Kallpa).

Del mismo modo, se precisa que la información de los asegurados es de carácter sensible dado que se registra datos personales de sus asegurados en repositorios de información no apropiadas como hojas de cálculo, reporte manuscrito, y otros similares, entendiéndose que este tipo de medios carecen de medidas de seguridad efectivas.

Así pues, se evidencia que la información correspondiente a los servicios críticos de la corredora de seguros requiere de controles efectivos para preservar la confidencialidad, integridad y disponibilidad de la información de sus clientes, proveedores y demás partes interesadas de la organización. Es así que tomaron la decisión de migrar a un sistema informático con mejores prestaciones para la seguridad de la información, teniéndose en cuenta que la información es el principal activo para la empresa, tal como lo menciona:

...acá tenemos un área de operaciones que se encarga de registrar las solicitudes que son las que llenan los asesores es un formato una solicitud que contiene los datos completos del contratante se registran en nuestra base de datos lo ordenamos y se envía a la compañía de seguros para que se emita la póliza (...) yo le doy la data, ambos tenemos la misma base de datos que incluye toda la información nombres, fecha de nacimiento, DNI, teléfonos, celulares, correo electrónico, beneficiarios y toda información de su salud como se encuentra. (Dante. R - Gerente General de Kallpa).

...ahora hemos comprado un sistema y estamos mudando toda nuestra data para que sea más fácil toda la operatividad... (Dante. R. - Gerente General de Kallpa).

Además de la importancia de la información de los clientes hay otro aspecto a cubrir que son las sanciones económicas, pues en el contexto del sector de seguros la Superintendencia de Banca y Seguros (SBS) exige a las corredoras una póliza por responsabilidad civil para dar cobertura a alguna mala praxis que entre otras cosas podría tener como causa un uso indebido de la información del asegurado, tal como lo indica Kallpa.

...La Superintendencia de Banca y Seguro regula el mercado de corredores de seguro; exigencias tales como pólizas de responsabilidad civil para cada

corredor ante una mala praxis con sus clientes. (Dante. R. - Gerente General de Kallpa).

En el sector se aprecia que algunas empresas de seguros y reaseguros tercerizan los servicios de data center implicando que la información del negocio sea gestionada por sus proveedores y algunos casos fuera del ámbito nacional. Este escenario demanda un mayor nivel de supervisión y protección de la información en vista de la aplicación de la Ley N° 29733 - Ley de protección de datos que regula protección de datos y aspectos relacionados con su transferencia a terceras partes ya sea en el ámbito nacional o internacional.

En la prueba se busca ser capaces de que la data center de Brasil este en capacidad de funcionar como principal; se simula la caída y del Data center USA y se activa el plan de contingencia y/o continuidad a Brasil. (Carlos B. - Director de Seguridad de la Información - Mapfre Perú)

Todas las solicitudes de las pólizas de los asegurados por parte de la empresa Kallpa se realizan a través del área de operaciones, quien es la encargada de ingresar toda la información de los asegurados; nombres, dirección, tarjetas de pago, fechas de nacimiento, DNI, celulares, beneficiarios, salud, enfermedad, entre otros; esta información constituye un gran valor para los servicios que ofrece la corredora; es decir, representa un activo para la empresa. Dicha información es archivada físicamente y escaneada; además ingresada a una base de datos en excel y remitida a la empresa de seguros correspondiente; tanto la empresa de seguros como la corredora de seguros mantienen esta información clave y confidencial para ambas compañías. Actualmente, la corredora está implementando un sistema donde la base de datos será migrada con la finalidad de poder tener un mejor control, manejo y apropiada seguridad de la información.

Hemos comprobado que Kallpa corredora de seguros maneja toda su información en base de datos excel y la comparte a las demás empresas de seguros sus bases de datos; por tratarse de información confidencial de los clientes de la empresa, pólizas, costos, entre otros; se considera que está muy expuesta a tener algún robo de información, siendo más fácilmente vulnerable tanto para el acceso de información, por infecciones u posibles ataques.

Por otro lado, un nuevo servicio crítico para la compañía Mapfre Perú es la red de ventas digital, que es el medio por el cual se realizan la mayor cantidad de ventas; lo que conlleva al incremento de la emisión de nuevas pólizas de seguros. Sin lugar a dudas, en este nuevo y exigente escenario la aseguradora está más vulnerable y expuesta. En esta etapa el mercado exige la venta de productos y servicios on line, pues por medidas de seguridad ya muy pocos clientes te reciben en sus domicilios.

...por eso creamos esta red que inclusive ganó un premio a la innovación a nivel mundial en el limra esta red lo que hace es vender igual que nuestros vendedores, pero a nivel digital (...) los porcentajes de crecimiento están en el orden del 150 % ahora solamente estamos creciendo por la red digital... (Sub directora de Recursos Humanos Mapfre Perú – Julie B.)

En ese sentido, la seguridad de la información busca poder proteger, a través de controles los sistemas actuales de la empresa de seguros, la información digital en estos nuevos ambientes interconectados puede ser vulnerable con cualquier tipo de ataques en red con mucho más impacto que los sistemas tradicionales de ventas.

Asimismo, se convierte en un servicio crítico para la organización Mapfre Perú cuando hay eventos de siniestros ocasionados por la naturaleza, como: terremotos, maremotos, inundaciones, huaicos y otros, ya que la compañía tiene asegurado a distintas empresas de diversos sectores. Debido a este escenario en alguna oportunidad la aseguradora a colapsado tanto en sus sistemas como en sus archivos físicos, al intentar efectuar sus atenciones de siniestro, en ese sentido, la estrategia a seguir es enviar equipos de trabajo a la zona afectada.

...cuando hubo el terremoto de pisco hace 10 año fue tanta la demanda de atención por los canales tradicionales que de frente se enviaron personas porque no hay formas de que el sistema pueda cubrir... (Sub directora de Recursos Humanos Mapfre Perú – Julie B.)

Frente a estos escenarios críticos, lo que busca Mapfre Perú es poder mantener la disponibilidad de sus servicios, por eso establece medidas preventivas y correctivas en sus sistemas tecnológicos y garantizar la seguridad de su información.

2. ¿Cuáles son los principales riesgos de seguridad de la información a las que están expuestas la asegurada Mapfre Perú y Kallpa corredores de seguros?

Entre los principales riesgos de seguridad de la información que se han identificado en la empresa de seguros y corredora de seguros están las ciberamenazas que se vienen

incrementando día a día, debido a la demanda de la tecnología para el sostenimiento de las operaciones en las empresas Mapfre Perú y Kallpa corredores; en ese sentido, los equipos tecnológicos y las telecomunicaciones han tomado mayor relevancia y autonomía para el desarrollo de los nuevos servicios o productos que se han ido incrementando según las necesidades del mercado.

En la empresa de seguros con mayor frecuencia se han registrado amenazas, como el phishing; una técnica de ingeniería social utilizada por los delincuentes para obtener información confidencial como nombres de usuario, contraseñas, información de los asegurados y del propio negocio, haciéndose pasar por una comunicación de mensajería electrónica confiable y legítima. Así también, se ha identificado un ataque de ransomware en la empresa Mapfre Perú que pudo haber ocasionado el secuestro de toda la información contenida en las computadoras de la organización el cual no tuvo la oportunidad de lograr su cometido porque se efectuaron la configuración de diversos parches oportunos en los sistemas.

...Los incidentes de seguridad son diarios; se encuentran phishing; spam, virus, o archivos con adjuntos maliciosos que infectan los equipos. lo que se evita para ser vulnerados y pedir rescates por la información. (Álvaro – Analista de seguridad Mapfre Perú)

Asimismo, se encontró:

...robo de datos de clientes, robo de datos estratégicos, ransomware. (Consultor del sector - Carlos V.).

Tal como podemos apreciar vemos que los riesgos de seguridad de la información se presentan a diario, tanto en la empresa Mapfre Perú como en la corredora de seguro Kallpa, diariamente se detectan intentos por pescar datos, es decir, intentos por ver quien “muerde el anzuelo”, tal como se refiere la palabra en inglés phishing que significa pesca; a través de correos electrónicos fraudulentos intentan infectar los equipos informáticos de manera sistemática; esto representa una vulnerabilidad constante para la información de las empresas mencionadas.

Así también podemos apreciar, que otro de los riesgos más comunes que se encuentran en las organizaciones es el uso de teléfonos celulares de los colaboradores, los cuales contienen diversas aplicaciones propias de los servicios que utilizan para poder realizar

sus transacciones bancarias, ver videos, escuchar música, entre otros, y en caso de ser conectados a los equipos de la organización podrían generar diferentes infecciones.

En relación a los riesgos, los consultores mencionan que las organizaciones están expuestas a los siguientes escenarios:

...Robo de información, eventos disruptivos en los sistemas y ataques a la ciberseguridad. (Consultor - Alcides H.)

...fugas de información, extorción a funcionarios, pérdida de datos, disrupción de servicios... (Consultor- Devis R.)

...robo de datos de clientes, robo de datos estratégicos, ransomware... (Consultor - Carlos V.)

Además, se verificó que diferentes apps instaladas al celular pueden generar el control del equipo y estos a su vez generar un robo de información a otras aplicaciones propias de la empresa de seguros Mapfre Perú:

...una aplicación maliciosa o un juego que tu instalas que está en el Play Store en alguna tienda Apple o Android puede tomar el control de tu celular y a través de esa aplicación puede saltar a otra aplicación que puede ser una app de la compañía y cuando hay transacción por ejemplo uno paga por las apps de los bancos, ahora ya no necesito ir al banco yo pago todo por el celular entonces esas transacciones pueden ser vulnerables a que alguien pueda aprovechar alguna debilidad que tenga esa aplicación y empezar a meterse de ese modo... (Carlos B. - Director de Seguridad de la Información - Mapfre Perú)

En la empresa Mapfre Perú se ha encontrado diversos casos en donde, a través de los smartphones o android, se han visto infectados por diversos virus que apuntaban directamente a tomar el control de manera imperceptible inicialmente del teléfono móvil o celular, y luego, el control o intromisión a las computadoras personales de los colaboradores con la única intención de tener acceso a la información confidencial de la compañía de seguros.

...Como tenemos apps tenemos que ver que esas aplicaciones antes que salgan a las tiendas al Apple Store o Play Store que sean aplicaciones seguras para que otra aplicación no pueda tomar el control y que, si el celular está controlado, no pueda meterse, si es que no tiene un usuario y una contraseña... (Carlos B. - Director de Seguridad de la Información - Mapfre Perú)

Se busca, de esta manera, ante las evidentes vulnerabilidades cada vez más constantes por la tendencia digital que, bajo ciertos parámetros de seguridad tales como usuario y contraseña, se pueda filtrar cada uno de estos riesgos de la seguridad de la información al dar acceso controlado a las personas autorizadas de la compañía de seguros.

Se ha verificado que hay un riesgo común tanto para Mapfre Perú como para Kallpa como es el resguardo de los activos de información debido a las constantes bases de datos que manejan.

Para el caso de la corredora, se ha observado que vienen migrando las bases de datos, que se encontraban en un excel, a un sistema donde se pueda salvaguardar de mejor manera toda la información de la compañía.

...manejamos varias bases de datos en excel y en google drive, estamos ya próximos a implementar un sistema de información y trabajando la migración de la información de hojas de cálculo ahora a un motor de base de datos a un sistema de información... (Gerente de Tecnología de la Información de la empresa Kallpa).

Se evidencia que la información de la corredora Kallpa presenta vulnerabilidades en el almacenamiento de su información y esto es un riesgo en el ámbito de sistemas; si bien es cierto, actualmente tienen la información en el google drive, ésta no garantiza los protocolos de confidencialidad que se requieren. En ese sentido, vienen implementando una plataforma confiable para sostener la información, tal como afirma el Gerente de TI de Kallpa:

...el proveedor tenía una plataforma de seguros genérica para todos, lo que hemos hecho en Kallpa es requerir también la parte de soporte para que desarrolle ciertos módulos que se acomoden a la organización... (Gerente de Tecnología de la Información de la empresa Kallpa).

...ahorita nos encontramos en una red de dominio, es decir, un servidor en el cual se administra las cuentas de usuarios también está el servidor de archivos en donde se administra las carpetas por áreas o también carpetas individuales por usuario... (Gerente de Tecnología de la Información de la empresa Kallpa).

Siendo parte esencial de la administración de sistemas dentro de la organización de Kallpa, lo que se busca es controlar el acceso a la información y evitar riesgos posteriores por lo cual en la actualidad se ha restringido el acceso al servidor, a la base de datos, así

como a la administración de carpetas, de tal manera que se pueda tener personalizado los privilegios de los acceso para asegurar la custodia de la información, sin embargo, se verifica que estas acciones recién se vienen implementando para disminuir el riesgo frente a acceder a contenidos no autorizado; como bloqueos de puestos y otros según indica el Gerente de TI:

...Se han bloqueado los puertos USB y filtrado también el tema de las páginas webs y un servidor proxy para que no puedan acceder a contenido que no está autorizado... (Gerente de Tecnología de la Información de la empresa Kallpa).

Por otro lado, también se ha identificado que la corredora de seguros Kallpa utiliza el sistema de correo electrónico gratuito de Google, que no necesariamente garantiza los protocolos de seguridad requeridos, puesto que, al ser un servicio gratuito, no se tienen acuerdos contractuales formales para el sostenimiento del servicio, lo que podría ocasionar alto riesgo sobre la información y gran impacto para la organización por las vulnerabilidades de ciberamenazas a la que está expuesta en la nube , aquí tenemos la versión del representante de TI:

...en cuanto a correos en el servidor no lo tenemos. Los correos lo tenemos mediante google drive que se encarga de darle soporte a nuestros correos, entonces ellos cumplen con todos sus estándares para que no llegue tanto spam, o también es configurable a pedido del usuario, yo también podría bloquear ciertos dominios... (Gerente de Tecnología de la Información de la empresa Kallpa).

Algo que se ha podido observar de la empresa Mapfre Perú y de la corredora de seguros Kallpa es que en ambos casos el riesgo informático se ha vuelto más creciente, inclusive en este año 2018 se espera a nivel global un ataque más agresivo respecto a las ciberamenazas. Cada vez salen nuevos ataques, vulnerabilidades y amenazas informáticas, llamadas “día cero”, es decir, que durante más tiempo se mantenga vigente una aplicación sin actualización de parches, se genera un riesgo de vulnerabilidad en las organizaciones, tal como lo manifiesta el Gerente TI- Mapfre

...hay personas que se dedican a encontrar fallas y las hacen públicas mientras más tiempo tenga más fallas va a tener por eso se recomienda que se realicen revisiones periódicas porque las marcas van encontrando vulnerabilidades... (Carlos B. - Director de Seguridad de la Información - Mapfre Perú)

...la seguridad no es estática la seguridad puede estar controlada o razonablemente segura pero mañana no sabemos porque hay vulnerabilidades que aparecen de un día para otro, que se llaman vulnerabilidades del día cero... (Carlos B. - Director de Seguridad de la Información - Mapfre Perú)

Estos riesgos son peligrosos debido a que no se conocen parches, actualizaciones (up grade) o soluciones concretas, dado que aparecen de un momento a otro con el transcurrir del tiempo. En este contexto, tanto la empresa de seguros como la corredora de seguros se mantienen alertas frente a este tipo de amenazas; para lo cual con sus respectivos equipos de TI realizan la programación de las respectivas actualizaciones a nuevas versiones, de tal manera se pueda mitigar el riesgo a la seguridad de la información.

3. ¿Cómo se gestiona la información, las políticas de seguridad y los planes de recuperación en la aseguradora Mapfre Perú y Kallpa corredores de seguros?

En esta pregunta queremos precisar si las organizaciones tienen un marco de gobierno con políticas, procedimientos, planes de contingencia que permitan garantizar la protección de los datos, hardware y software crítico para que, ante un incidente de seguridad, la empresa logre mantener la disponibilidad de sus operaciones.

En este sentido, hemos podido observar a través de los analistas de seguridad de la información de la empresa Mapfre Perú quienes indican que las políticas de seguridad se difunden periódicamente por diversos medios como inducciones al personal, charlas de concientización, con comunicados vía correo electrónico; así también vía intranet corporativa se difunden las diferentes normativas y lineamientos a la organización, tal como indica:

...Las políticas de seguridad se difunden a través de correos electrónicos de seguridad; charlas, inducciones al personal nuevo de la empresa y también se usa la intranet corporativa para transmitir la normativa, las informaciones por área; entre otros. (Álvaro – Analista de seguridad Mapfre Perú)

Así también, al ingresar un personal nuevo a la organización se le ofrece una inducción organizacional donde se le familiariza con las políticas de seguridad de la información y posteriormente, se realizan talleres de formación teórico práctico una vez al año a todo el personal, programadas por el área de riesgos, con la finalidad de crear conciencia y cultura en los colaboradores.

...cuando ingresas a la compañía hay una inducción en parte de esa inducción le contamos un poco de estas cosas que pasan, que han robado identidades que cuando exponen o postean cosas en Facebook las puede ver cualquier persona y pueden deducir cosas que recomendamos que no posteen cosas de la oficina de la compañía que sean cuidadosos con su usuario y contraseña... (Carlos B. - Director de Seguridad de la Información - Mapfre Perú)

Por otro lado, también pudimos confirmar que en la aseguradora se realizan pruebas de recuperación; la periodicidad de las mismas es anual, y varía el alcance según el programa. Estas actividades se efectúan en conjunto con los proveedores de las data center, uno de los cuales se encuentra en la ciudad de Miami – Estados Unidos siendo el data center principal de Mapfre -, y el otro desde el país de Brasil. Para realizar todas estas actividades de prueba se tienen procedimientos documentados de cómo actuar mientras se realizan estas pruebas de recuperación. Para poner en práctica estos planes de recuperación se simula la caída del sistema de Mapfre en Lima y se busca que el data center de la ciudad de Brasil funcione como data center principal; se realizan las actividades para asegurar que tienen respaldo en caso de una caída y que las operaciones se mantengan disponible para las partes interesadas, tal como lo manifiesta el Gerente TI-Mapfre:

... los planes de recuperación son las pruebas de continuidad o contingencia que se realizan 1 vez al año; en USA esta una data center principal y en Brasil el de contingencia y se aplica el plan frente a cualquier emergencia, desastre; etc. En la prueba se busca ser capaces de que la data center de Brasil este en capacidad de funcionar como principal; se simula la caída y del Data center USA y se activa el plan de contingencia y/o continuidad a Brasil. (Carlos B. - Director de Seguridad de la Información - Mapfre Perú)

...nuestro sistema principal está en EE.UU. y nuestra contingencia está en Brasil la prueba de continuidad es que seamos capaces de ver que Brasil siempre esté funcionando o que funcione cuando hagamos la prueba... (Carlos B. - Director de Seguridad de la Información - Mapfre Perú)

En el caso de Kallpa corredores no se pudo validar que realizaran planes de recuperación y esto quizás es debido a que a la fecha recién se van a sostener su información en un sistema.

Para el caso de los ejecutivos de la empresa corredora específicamente para el caso del Gerente General, toda la información se tiene una copia de seguridad tanto en el servidor físico del centro de cómputo como el google drive.

...lo que sí está respaldado al 100 % es la información del gerente general, él está acostumbrado a grabar toda la información en su carpeta y lo de el sí está respaldado en google drive (...) y aparte como está en la nube tiene copia de seguridad de google...(Gerente de Tecnología de la Información de la empresa Kallpa – Corredora de Seguros).

Asimismo, para el caso de la aseguradora como de la corredora se ha podido comprobar, que la concientización respecto a la seguridad de la información es un tema que toma tiempo en calar en los colaboradores. En algunas oportunidades es por la existencia de un cambio generacional y de gestión; pero el contexto del sector se sostiene a través de tecnología y se prioriza la red digital; en ese sentido el mayor problema que se origina es con el propio factor humano; es más dificultoso el entendimiento para cada uno de ellos de cumplir con los protocolos o controles que se les indica, es más factible establecer controles en la administración de la plataforma; tal como lo indica, el representante de TI Kallpa

...cambiarles ese chip, no piensan en lo que podría pasar buscan más sus facilidades lo que es más rápido, tienen su orden en el escritorio entonces no lo quieren hacer (...) la barrera de los usuarios es lo más complicado que administrarles bien la plataforma... (Gerente de Tecnología de la Información de la empresa Kallpa – Corredora de Seguros).

...una vez se intentó e inclusive redacté una manual de políticas de seguridad de la información que también incluye políticas de los usuarios, (...) creo que lo han tomado desde la gerencia hasta los usuarios como algo secundario... (Gerente de Tecnología de la Información de la empresa Kallpa – Corredora de Seguros).

Respecto de la gestión de los riesgos de seguridad de la información en estas organizaciones, solo logramos comprobar que en Mapfre están muy familiarizados y organizados bajo una gestión integral de riesgos, adicionalmente a la exigencia de la Superintendencia de banca y seguros con su circular N° 140, tal como indicó el Gerente TI- Mapfre

...este sistema de gestión tiene una serie de controles, tiene objetivos de control que tratan diferentes cosas de seguridad ...la base para cuidar la información es aplicar esos 114 controles dentro de la compañía, se aplican

de diferentes maneras y, además, que esos controles tendrían que tener un sistema de medición de efectividad, que tan efectivo son... (Carlos B. - Director de Seguridad de la Información - Mapfre Perú)

...nosotros aplicamos el cuidado de la información por lo que te decía que la información está en papel está en los discos duros, ah yo no dejo que entren USB porque se infecta, se pueden llevar la información; yo no puedo publicar a internet cosas porque por ahí pueden entrar puedo exponer cosas que puedan ser confidenciales, o comerciales o de propiedad intelectual(...) Estamos alineados a la SBS porque además la superintendencia nos lo exige con la circular 140...(Carlos B. - Director de Seguridad de la Información - Mapfre Perú)

Para el caso de la empresa de seguros Mapfre Perú se puede observar que dentro de la gestión de controles de seguridad de la información cada vez que lanzan al mercado un nuevo producto y en varias ocasiones es a través de apps, se efectúan análisis de riesgos para evitar riesgos en las transacciones de sus clientes y se realizan pruebas de validación de seguridad y si es necesario el cifrado de la información y canales de comunicación entre otros.

...queremos un seguro de autos para mujeres... ¿Dónde vas a instalar esa aplicación esa aplicación va a tener una app? esa aplicación va a tener una transacción de datos personales? (...) tiene que estar en celular tiene que estar encriptado, además, las cookies deshabilitadas... (Carlos B. - Director de Seguridad de la Información - Mapfre Perú)

Cada producto nuevo que la empresa Mapfre Perú ingresa al mercado en esta etapa digital tiene un alto riesgo por las diversas vulnerabilidades de las distintas aplicaciones informáticas; se ha verificado que la compañía de seguros aplica diferentes medios de seguridad para garantizar que no se presente un posible daño o robo de los datos a través de los móviles o apps.

Por otro lado, en las entrevistas con los consultores del sector nos indicaron y coincidieron en que bajo la exigencia de la SBS estas entidades deben realizar pruebas de continuidad y contar con lugares alternos para brindar los servicios a sus usuarios, esto lo indica la circular N° 139 Continuidad del Negocio, bajo este sustento sólo podemos afirmar que a aseguradora cumple con estas exigencias

...Si se cuenta con planes de recuperación es una obligación por parte de la SBS; se cuenta con un centro alternativo de negocios; además, con una oficina principal y con otra de contingencia; puntos de red, módulos para lo básico; si se cae el servicio. (Javier N. - Consultor seguridad).

... Se tienen planes de acuerdo a la normativa vigente. (Carlos V.- Consultor Seguridad)

...si se cuentan con planes de recuperación y continuidad de acuerdo a las normativas (Devis R.- Consultor Seguridad)

4. ¿Qué controles existen para mitigar los riesgos de seguridad en la aseguradora Mapfre y Kallpa corredores de seguros?

En este punto pretendemos dar respuesta si las organizaciones realmente han implementado controles de seguridad de la información y como los gestionan al interior de ellas con la finalidad de prevenir o evitar daños en el software, hardware o datos; así como anticiparse al riesgo de pérdida de información.

En este contexto se ha validado que la empresa Mapfre Perú ha implementado los siguientes controles en distintos aspectos, como:

Al pertenecer a la planilla de la organización se le solicita al colaborador antecedentes penales, policiales y su estado crediticio financiero en el sector bancario, esta información es almacenada en el sistema y se mantiene en su legajo personal en archivo físico y se le hace entrega de un fotocheck para que pueda identificarse y acceder a las instalaciones de la empresa, lo que permite que se controle el acceso físico. Adicionalmente por la Ley de Protección de Datos tanto colaboradores como clientes firman un documento formal al respecto:

...nosotros cuando entra un colaborador a Mapfre le hacemos firmar un documento sobre la ley de protección de datos y lo mismo a los clientes cuando se le entrega las pólizas se le hace llegar un documento también y esto está archivado... (Julie B - Sub Directora Recursos Humanos –Mapfre Perú).

Por otro lado, también se crean accesos lógicos con un usuario y contraseña para que pueda acceder a la red Mapfre Perú, así mismo se le brinda un perfil de usuario para diferentes sistemas de información: atención al cliente, emisión de pólizas, reclamos, según el servicio o necesidad de acceder a información para desarrollar su labor diaria; lo que permite identificar la trazabilidad del uso, ingreso y cambios que pudiera realizar en la información.

...los accesos están basados en roles y perfiles por ejemplo hay un perfil de ejecutivo de atención al cliente tiene diferentes roles en los distintos sistemas (...) puede haber un perfil de emisor, de caja, de cobranzas; dentro de las áreas hay diferentes roles y perfiles por función (...) cada responsable de unidad es el que define los roles y perfiles que se tiene que tener... (Director de Seguridad de la información y medio ambiente – Carlos B Mapfre Perú).

Otro aspecto que se controla es el uso de los dispositivos con los que trabajan los colaboradores para realizar sus actividades, como: tablets, celulares y otros, para lo cual en el caso de pérdida o robo constituye es riesgo alto debido al mal uso que le pueden dar, para este escenario se ha considerado el bloqueo de los mismos a través de gadgets, aplicación que permite bloquear los equipos en el caso de pérdida y son monitoreados por el área de sistemas con la objetivo de defender los activos de la compañía Mapfre Perú, tal como nos afirma el Gerente TI:

...los riesgos de seguridad se controlan a través de gestiones; por ejemplo, el control de acceso físico a las instalaciones es a través de fotochecks para nuestros trabajadores. Respecto a las tablets y celulares que se les asigna y tienen instalado una aplicación que permite bloquearlo en caso de pérdida. (Carlos B. - Director de Seguridad de la Información - Mapfre Perú).

De la misma forma, nos indicaron que hay ocasiones en que se había realizado el préstamo de contraseñas por la necesidad de no desatender a un cliente y como el colaborador no tenía el perfil para aprobar siniestros y la persona responsable estaba de vacaciones o licencia se suscitaba la situación, lo cual se prestaba a muchas suspicacias de fraude o irregularidad; pudiendo ocasionar alguna pérdida para la compañía, por no mantener los controles de seguridad de la información a través de los perfiles, claves, contraseñas y/o usuarios; ahora se realiza un nuevo perfil en caso de ausencia del aprobador, lo confirma Gerente TI:

...tenemos casos en los que, por vacaciones, enfermedad... (...) una cosa fortuita que no pueda venir la persona que aprueba un control...le crearemos un perfil a otro usuario con las opciones que necesita para no prestarse la contraseña y no meterse en un problema, la compañía también que apruebe un siniestro o un fraude... (Carlos B. - Director de Seguridad de la Información - Mapfre Perú)

Bajo estos sustentos, podemos confirmar que la empresa aseguradora mantiene controles en prevención de pérdida de información que podría afectar a las operaciones de la

organización, clientes, accionistas y otros; con la premisa de mantener la integridad, disponibilidad y confidencialidad de la misma. De esta manera busca poder generar mecanismos de seguridad reduzcan el impacto que las vulnerabilidades y amenazas traen consigo.

Asimismo, este sector está regulado por la Superintendencia de Banca y Seguros y bajo los oficiales de cumplimiento, referente al tema de lavado de activos y financiamiento de terrorismo, en estos aspectos también existen regulaciones y controles para las empresas del sector, como indican:

...dentro de las normas legales del oficial de cumplimiento tienen que cumplir con ciertas referencias ve todo lo que es el lavado de activos y financiamiento de terrorismo... (...) la SBS exige que el oficial de cumplimiento estudie administración de seguros en APECOSE (Asociación Peruana de corredores de seguro) ... (David C. – Oficial de cumplimiento - Kallpa)

...las compañías de seguros no sé cómo hacen yo he mandado a emitir una póliza a veces a un cliente y me han dicho, no, no procede, me llaman por teléfono no me lo dicen por escrito, y yo digo: ¿Qué pasó? Y me dicen tiene una denuncia por corrupción por lavados de activos... (David C. – Oficial de cumplimiento - Kallpa)

...la SBS te puede venir a supervisar cuando le da la gana, lo normal es que venga 1 vez al año; y revisa todas las cosas que pueda revisar... (Carlos B. - Director de Seguridad de la Información - Mapfre Perú)

Asimismo, bajo la experiencia del consultor de TI nos indica que el uso claves o contraseñas es fundamental para llevar un buen control de acceso lógico a los sistemas, es decir, no utilizar usuarios genéricos de administrador sino usuarios únicos. De esta manera se busca controlar los accesos a la información, quienes son los que acceden y la trazabilidad de las acciones para así evitar de robo de información. Por otro lado, indicó que es importante la implementación de enlaces alternos para no perder comunicación y tener dos proveedores alternos para obtener redundancia, permitiendo estos controles reducir los riesgos de seguridad de la data e información.

...Normalmente se mantenían usuarios genéricos una de las medidas es personalizar los accesos lógicos, de administrador (genérico) a jbeteta (lógico huella). Además, se ha implementado los canales alternos de comunicación enlaces de contingencia, contratan a 2 proveedores de los servicios empresariales (movistar, claro, entel, betel, entre otros) fibra óptica, router, etc. (Javier N. – Consultor de Seguridad de la información.)

Bajo la experiencia de los consultores se señala que ante el crecimiento del internet de las cosas (IoT) hay una exposición más acentuada a los diversos riesgos cibernéticos, ya que los distintos procesos de negocios dependen de la tecnología y las telecomunicaciones, con más demanda en esta etapa de transformación digital; donde el sector debe alinearse a la demanda de los consumidores y lograr que obtengan experiencias digitales simples e integradas a través de los numerosos canales de servicio; esto se puede lograr a través de los siguientes controles:

...Programa de ciberseguridad aprobado por la alta gerencia y un proceso continuo de gestión de riesgos tecnológicos y de seguridad de la información... (Carlos V. – Consultor seguridad)

...Con una organización liderada desde el más alto nivel de la empresa, una robusta evaluación y tratamiento de riesgos, personal capacitado y comprometido con la seguridad, una robusta gestión de incidentes de seguridad y planes de continuidad de negocios. (Alcides H. – Consultor independiente).

Adicional a lo que vivimos, las empresas deberán afianzar su seguridad en el ciberespacio, porque los ataques se dan y se darán con mayor frecuencia desde este frente. (Alcides H. – Consultor de seguridad)

Cambio de cultura hacia una cultura más ágil y que se centre en el cliente. (Sergio C. – Consultor de seguridad TI)

...en el sentido que la organización tiene una gestión de seguridad de la información robusta y madura, el IoT se verá sólo como servicios adicionales que deberán contar con controles, evaluación de riesgos, capacitaciones al personal, etc... (Alcides H. – Consultor de seguridad)

al llevar todo al mundo digital se deben tener responsables de la gestión de la seguridad en este nuevo frente además que podemos ser propensos a incidentes que en el mundo físico no ocurrían (Devis R. – Consultor de seguridad)

Los consultores también nos indican que a pesar de todas las regulaciones que se vienen implementando como medidas de control por la Superintendencia de Banca y Seguros vemos que en esta nueva era digital vienen siendo insuficientes, es más, la tendencia apunta al incremento de los riesgos de ciberamenazas debido a que cada vez se automatizan los procesos sobre todo para el desarrollo de la venta digital, con lo cual cuestionan lo siguiente:

... ¿Estamos preparados para llegar a ese nivel regulatorio de madurez de las compañías? Si analizas la normativa como tal la circular 140, 139, la 2560, todas las que están relacionadas a la gestión de riesgos...tienen controles muy básicos... (Carlos B. - Director de Seguridad de la Información - Mapfre Perú)

...El sector de seguro hasta donde está yendo, es hacia la transformación digital eso mismo te dice la insurtech que tiene una visión de cómo el negocio va a evolucionar y en ese evolucionar del negocio todo va a ser tech, el tema de ciberseguridad va a ser crítico... (Carlos V. – Consultor de Seguridad de la Información)

...el sector asegurador mientras vaya creciendo se va a volver mucho más sensible a que a ataques cibernéticos como aseguramos finalmente los temas de seguridad... (Carlos B. - Director de Seguridad de la Información - Mapfre Perú)

En ese sentido, podemos determinar que el sector seguro, cada vez se va a volver más vulnerable puesto que forma de captar clientes va ser e medio digital y el sostenimiento de las operaciones va ser netamente en infraestructura tecnológica y las telecomunicaciones, lo que por ende hace inferir que estaremos más expuestos a los ciberataques o ciberamenazas.

...el sector asegurador mientras vaya creciendo se va a volver mucho más sensible a que a ataques cibernéticos como aseguramos finalmente los temas de seguridad... (Carlos V. - Consultor de seguridad)

Todo nueva tecnología o dispositivos que se suman al ecosistema de la red puede ser potencialmente una fuente de vulnerabilidades que puede comprometer la seguridad. (Carlos V. Consultor de seguridad)

...si ya que al ser una tecnología emergente tiene muchas brechas de seguridad y asimismo el entorno no está preparado para gestionar esta brecha en dispositivos poco conocidos... (Carlos V.-Consultor de seguridad)

El IoT nos permite conectar con los afiliados para poder atenderlos de forma más rápida, pero hay información que viaja con el que si no es protegida o tratada adecuadamente se puede generar demandas. (Sergio C. - Consultor de seguridad)

La digitalización de la información y el uso de la tecnología para agilizar / transformar procesos generará una mayor exposición de las compañías a los ciberataques. (Carlos V. – Consultor seguridad)

Las razones expuestas por nuestros entrevistados sobre el rol de la seguridad de la información en las organizaciones y sobre todo en el sector de seguros donde se manejan muchas bases de datos de los clientes, nos indican que ambas empresas Mapfre Perú y Kallpa deben tomar medidas correctivas y de prevención para cubrir las vulnerabilidades técnicas que se presentan en sus sistemas informáticos, debido a que el sostenimiento de sus servicios empresariales se efectuará haciendo un uso intensivo de plataformas tecnológicas y telecomunicaciones.

CAPITULO 4. DISCUSIÓN DE RESULTADOS

4.1 Hallazgos

Se identificaron los siguientes hallazgos:

- En las organizaciones que tienen el respaldo con casa matriz a nivel internacional ya están empezando a implementar procesos de automatización a través de robots, lo cual no pensábamos encontrar aun en la presente investigación.
- Por otro lado, otro aspecto que también se está implementando es el Teletrabajo, en este tipo de organizaciones corporativas la cual tiene otro marco legal regulatorio muy distinto al tradicional y que debe asegurar también la seguridad de la información, lo que hace intuir que en un mediano plazo se incrementará este tipo de labor; como se viene dando en otros países del extranjero, lo que también podría analizarse a nivel de impacto organizacional.
- Entre los consultores entrevistados encontramos que uno de ellos no hizo mención del nuevo enfoque para el sector e identificaron la terminología “Insurtech” que es la unión de insurance (seguros) y technology (tecnología), lo que significa el tránsito a la transformación digital y en ese contexto, las compañías tradicionales de seguros adaptadas al nuevo entorno tecnológico y ofreciendo nuevos productos digitales; para lo cual consideran aspectos de cambios de mentalidad de la gente, asegurar no solo objetos sino estilos de vida y así también, incluyen a la penetración de distintos modelos económicos.
- Otro hallazgo que encontramos en nuestra investigación es el “Gobierno de datos” que el caso de Mapfre seguros esta manejado a través del área CRM- Calidad quienes analizan la información de cada uno de sus clientes de acuerdo a su perfil de gustos y preferencias para fidelizarlo a través de ciertos beneficios; a la vez que es analizada y gestionada esta información también se considera el marco legal y el aseguramiento de la custodia de la misma, lo cual puede ser relevante para futuras investigaciones.

4.2 Barreras

- Lograr las autorizaciones para acceder a las entrevistas, es lo que complicó los tiempos y que todo pudiera fluir adecuadamente para el análisis de la información.
- Las citas que nos brindaron en su mayoría fueron en horario de oficina, lo cual dificultó los permisos de ambos participantes en sus centros laborales.
- Para lograr entrevistar a los consultores expertos en el tema y sector, se efectuaron dichas entrevistas fuera del horario de oficina y también fuera de las instalaciones de sus oficinas; al punto de tener que realizar las referidas entrevistas en diversos lugares públicos como restaurantes u hoteles, debido a que varios de ellos luego del horario de oficina brindan charlas o capacitaciones a instituciones.
- Se encontró pocos estudios de la región en términos de seguridad de la información, datos, estadísticas, resultados de estudios, estos análisis se desarrollan con mayor frecuencia en Europa y américa del norte – Estados Unidos.
- Inicialmente se estimó entrevistar a un representante de la empresa supervisora, es decir, Superintendencia de Banca y Seguros (SBS), pero no se tuvo oportunidad de efectuarla, sería propicio para otras investigaciones obtener información de cómo ellos efectúan la validación del cumplimiento de las circulares con las que realizan la supervisión.

4.3 Brechas

- No se encontraron brechas en el proceso de investigación.

CAPITULO 5. CONCLUSIONES

1. La empresa aseguradora Mapfre Perú cumple con la hipótesis planteada dado que tiene un sistema de gestión de seguridad de la información, que incluye metodología para la gestión de riesgos, políticas, procedimientos y realiza planes de recuperación; mientras que la empresa Kallpa corredora de seguros no cumple con la hipótesis planteada dado que sólo utiliza algunos controles básicos de seguridad que no incluyen políticas, procedimientos y planes de recuperación; por lo que la hipótesis se cumple parcialmente y no en todos sus extremos.
2. Se invierte en seguridad de la información en las empresas grandes como es el caso de la aseguradora Mapfre Perú, debido a que es consciente que mantiene múltiples bases de datos, sistemas, aplicaciones con información sensible para el negocio que realiza; y de sufrir algún tipo de pérdida, secuestro o daño la información podría impactar severamente en términos operativos, financieros, legales y de reputación. Lo cual no ocurre en las empresas pequeñas como Kallpa corredora de seguros debido a que sus procesos y servicios de negocio son menos complejos y/o de menor ámbito respecto a la aseguradora, sin embargo, también maneja información sensible y requiere se implemente una gestión de seguridad de la información con sus respectivos controles.
3. Mapfre Perú soporta las operaciones de su negocio en un conjunto de sistemas de información lo que permite automatizar sus procesos y servicios los cuales se sostienen en la infraestructura tecnológica y las telecomunicaciones, siendo estos últimos considerados servicios críticos para la organización. Estos sistemas traen muchas ventajas en términos de productividad, pero también traen consigo riesgos que se pueden materializar por la acción de las ciberamenazas, las cuales cada vez son más sofisticadas y mantienen abiertas una serie de brechas de control por la hiperconectividad, que exigen ser implementadas para proteger la información.
4. En el corto plazo los principales canales de información para las empresas del sector seguros, Mapfre Perú y Kallpa estarán soportados en el internet de las cosas (IoT), la automatización, robotización y otras tecnologías emergentes; en este nuevo entorno se incrementarán las vulnerabilidades y amenazas por los ataques de ciberseguridad, como: phishing, ransomware, infecciones masivas y otros.

5. Un factor clave de éxito para la gestión de la seguridad de la información es el cambio cultural de los colaboradores de la corredora Kallpa y el reforzamiento en la organización Mapfre, de manera que estas empresas se enfoquen en la prevención más que en la reacción; a través de inducciones, programas de concientización, capacitaciones y otras actividades dirigidas a sus trabajadores.
6. En materia de seguridad de la información la Superintendencia de Banca y Seguros sólo establece normativas que no son actualizadas periódicamente y es de suma importancia esta renovación, debido a que el contexto tecnológico no es estático y su evolución es constante, originando la apertura de nuevas brechas de ciberseguridad; que traen consigo las nuevas tecnologías emergentes, sobre la cual se soportan los servicios del sector.

CAPITULO 6. RECOMENDACIONES

1. Se sugiere el uso de una guía de controles base que permitirá brindar la orientación para establecer los principales lineamientos respecto a la gestión de la seguridad de la información (Ver guía de control en el Anexo N°3).
2. Queremos precisar que el internet de las cosas (IoT), la transformación digital y las tecnologías emergentes traen consigo brechas y vulnerabilidades, y en ese sentido, el entorno todavía no está preparado para gestionarlas adecuadamente; por lo cual se deben adoptar controles de ciberseguridad para que la información no sea vulnerada en términos de confidencialidad, integridad y disponibilidad, trabajando soluciones integradas y a nivel estratégico, no únicamente como si la solución fuera responsabilidad del área de tecnología.
3. Se aconseja que la inversión en seguridad de la información se priorice en los procesos clave del negocio.
4. La mejora continua deberá considerar la inclusión de otros procesos al modelo de gestión de la seguridad de la información, según las necesidades de la organización.
5. Es fundamental, que se realicen campañas de concientización y sensibilización con el compromiso de la Alta dirección a los colaboradores para desarrollar un cambio de cultura, y que conozcan de las consecuencias de la hiperconectividad cuando la organización no establece controles de seguridad de la información, así mismo explicarles como pueden ser sorprendidos en distintas modalidades por la ingeniería social y ocasionar pérdidas por robo de información, extorsión y otros.

REFERENCIAS

- Abanto, J. & Asensio, S. (2017). Centro de Ciberseguridad Industrial. *Estudio sobre el estado de la Ciberseguridad Industrial en Perú*. ISACA. Recuperado de: https://www.cci-es.org/web/cci/detalle-actividad/-/journal_content/56/10694/452983;jsessionid=26CDA3DBD58CAAC3FDA5B73BD2D9359C [Consulta: 7 de diciembre 2017]
- Acosta, J. (2017). *El camino hacia la resiliencia cibernética. Encuesta Global de Seguridad de la información 2016-17*. Recuperado de [http://www.ey.com/Publication/vwLUAssets/EY-el-camino-hacia-resiliencia-cibernetica/\\$FILE/EY-el-camino-hacia-resiliencia-cibernetica.pdf](http://www.ey.com/Publication/vwLUAssets/EY-el-camino-hacia-resiliencia-cibernetica/$FILE/EY-el-camino-hacia-resiliencia-cibernetica.pdf) [Consulta: 4 de diciembre de 2017]
- Borghello, C. (2009). *Crimeware: el crimen del Siglo XXI*. Recuperado de: https://www.welivesecurity.com/wp-content/uploads/2014/01/crimewarecrimen_siglo_xxi.pdf [Consulta: 8 de enero de 2018]
- Castelo, J. & Guardiola A. (2008). *Diccionario Mapfre de seguros. 4ª ed.* España: Fundación Mapfre. Instituto de Ciencias del Seguro.
- Centro Criptológico Nacional (2018) *Ciberamenazas y Tendencias Edición*. Recuperado de: <https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2835-ccn-cert-ia-09-18-ciberamenazas-y-tendencias-edicion-2018-1/file.html> [Consulta: 20 de mayo 2018]
- Class & Asociados S.A (2018). *Informe de clasificación de riesgo Mapfre Perú Vida Compañía de Seguros y Reaseguros*. Recuperado de: <http://www.smv.gob.pe/ConsultasP8/temp/MPV311217.pdf> [Consulta: 16 de abril 2018]
- Congreso de la República del Perú. (03 de julio de 2011). Ley de Protección de Datos Personales. [Ley N° 29733]. Recuperado de <http://www.leyes.congreso.gob.pe/Documentos/Leyes/29733.pdf> [Consulta: 07 de marzo de 2018]
- Costas, J. (2010). *Seguridad Informática*. Malaga, España : Editorial Ra-Ma.
- Disaster Recovery Institute International (DRI). “s.f.”. Permanent Committee Members. *International Glossary for Resiliency (Glosario en Español)*
- Garcia, D. (3 de julio de 2015). *Ciberseguridad: qué es y para qué sirve*. Obtenido de <https://www.ucavila.es/blog/2015/07/03/ciberseguridad-que-es-y-para-que-sirve/>

- Gestión. (10 de agosto de 2017). *Perú registrará US\$ 4,782 millones en pérdidas por ciberdelitos en 2017*. Recuperado de <https://gestion.pe/tecnologia/peru-registrara-us-4-782-millones-perdidas-ciberdelitos-2017-141411>
- Gómez, A. (2011). *Enciclopedia de la seguridad informática*. (2 ed.). RA-MA EDITORIAL. Recuperado de: <http://www.ra-ma.es/libros/ENCICLOPEDIA-DE-LA-SEGURIDAD-INFORMATICA-2-EDICION-ACTUALIZADA/28627/978-84-9964-036-5>
- International Organization for Standardization (ISO). (2016). ISO 27000:2016 Information technology – Security techniques- Information security management systems- Overview and vocabulary. 4a ed. Suiza. ISO. Org.
- International Organization for Standardization (ISO). (2012). *ISO 22301:2012. Protección y Seguridad de los Ciudadanos. Sistema de gestión continuidad de negocio. Especificaciones*. España. AENOR
- Laboratorio de investigación ESET *Tendencias de ciberseguridad 2018: El costo de nuestro mundo conectado*. Recuperado de : <https://www.welivesecurity.com/la-es/articulos/reportes/> [Consulta: 06 de marzo de 2018]
- Merino, M y Pérez, J. (2008). *Definición de seguridad informática*. Recuperado de: <https://definicion.de/seguridad-informatica> [Consulta: 19 de febrero de 2018]
- Norma Técnica Peruana (NTP).(2007): NTP-ISO/IEC 17799:2007 . *EDI.Tecnología de la información. Código de buenas prácticas para la gestión de la seguridad de la información*. 2ª ed. Perú: INDECOPI.
- Salazar, J & Silvestre. “s.f.” *Internet de las cosas - Tech Pedia*. Recuperado de: https://upcommons.upc.edu/bitstream/handle/2117/100921/LM08_R_ES.pdf [Consulta: 27 de marzo de 2018].
- Superintendencia de Banca y Seguros (SBS). (2 de abril 2009). *Gestión de la seguridad de la información* [Circular N° G - 140 - 2009].
- Superintendencia de Banca y Seguros (SBS). (2 de abril 2009). *Gestión de la continuidad del negocio* [Circular N° G - 139 - 2009].
- Superintendencia de Banca y Seguros (SBS). (2 de abril 2009). *Reglamento para la Gestión del Riesgo Operacional* [Resolución SBS N° 2116 - 2009]
- Superintendencia de Banca y Seguros (SBS). (18 de enero 2017) *Reglamento de Gobierno Corporativo y de la Gestión Integral de Riesgos* [Resolución SBS N° 272 - 2017]

ANEXOS

Anexo 1. –Guía de preguntas por Segmento

	CATEGORIAS	PREGUNTAS	Segmento 1 Representante de empresa	Segmento 2 Jefe de riesgos/ Jefe Tecnología	Segmento 3 Oficial de cumplimiento	Segmento 4 Analistas de Riesgos, Seguridad de la Información y de tecnología	Segmento 5 Consultores
OBJETIVO 1 SERVICIOS CRITICOS	Modelo de aseguradora y corredora	Preg 1	¿Cuáles son los servicios críticos de la organización y que tratamiento se les ha dado?	¿Cuáles son los servicios críticos de la organización y que tratamiento se les ha dado?	¿Cuáles son los servicios críticos de la organización y que tratamiento se les ha dado?	¿Cuáles son los servicios críticos de la organización y que tratamiento se les ha dado?	¿Cuáles son los servicios críticos de la organizaciones del sector financiero, como aseguradora o corredora de seguros?
	Líneas de negocio y productos y servicios	Preg 2	¿Qué líneas de negocio tiene la empresa y que productos ofrece al mercado?	¿Qué líneas de negocio tiene la empresa y que productos ofrece al mercado?	¿Qué líneas de negocio tiene la empresa y que productos ofrece al mercado?	¿Qué líneas de negocio tiene la empresa y que productos ofrece al mercado?	¿Si tuvo la oportunidad de atender alguna empresa de seguros, sabe cuáles son los principales tipos de seguro?
		Preg 3	¿A qué tipos de clientes está dirigido el negocio y en qué porcentaje?	¿A qué tipos de clientes está dirigido el negocio y en qué porcentaje?	¿A qué tipos de clientes está dirigido el negocio y en qué porcentaje?	¿A qué tipos de clientes está dirigido el negocio y en qué porcentaje?	¿A qué tipos de clientes está dirigido el negocio y en qué porcentaje?
OBJETIVO 2 GESTIÓN DE LOS RIESGOS	Identificación, análisis, evaluación y tratamiento.	Preg 4	¿Cómo se identifican y gestionan los riesgos de seguridad de la información?	¿Cómo se gestiona los riegos de seguridad de la información que se han identificado?	¿Cómo se gestiona los riegos de seguridad de la información que se han identificado?	Cuáles han sido sus principales incidentes tecnológicos entorno a la información de los datos del negocio	¿Cómo se gestiona los riesgos de seguridad de la información que se han identificado?
	Controles para mitigar riesgos	Preg 5	¿Cuándo fue la última vez que han tenido una pérdida de información como consecuencia de un riesgo no identificado o mal gestionando?	¿Qué medida se han tomado para tratar los riesgos en la organización y como se escalan los casos o incidentes ?	¿Qué medida se han tomado para tratar los riesgos en la organización y como se escalan los casos o incidentes ?	¿Qué medida se han tomado para tratar los riesgos en la organización y como se escalan los casos o incidentes ?	¿Cuándo fue la última vez que han tenido una pérdida de información como consecuencia de un riesgo no identificado o mal gestionando y como se escalan los incidentes?
	Custodia de la información confidencial	Preg 6	¿Cuál es la información más sensible o de carácter confidencial para la empresa y Cómo garantizas la confidencialidad	¿Cómo guardan la información crítica y cómo aseguran que la información no sea manipulada o alterada?	¿Cómo guardan la información crítica y cómo aseguran que la información no sea manipulada o alterada?	¿Cómo guardan la información crítica y cómo aseguran que la información no sea manipulada o alterada?	¿Cuál es la información más sensible o de carácter confidencial para la empresa y Cómo garantizas la confidencialidad

OBJETIVO 3 POLITICAS DE SEGURIDAD Y PLANES DE RECUPERAC IÓN	Políticas de seguridad	Preg 7	Se tienen políticas de seguridad establecidas y quiénes la aprueban?	Se tienen políticas de seguridad establecidas y quiénes la aprueban?	Se tienen políticas de seguridad establecidas y quiénes la aprueban?	Se tienen políticas de seguridad establecidas y quiénes la aprueban?	Se tienen políticas de seguridad establecidas y quiénes la aprueban?
		Preg 8	El personal involucrado con el manejo de la información recibe capacitación o inducción en las políticas de seguridad	El personal involucrado con el manejo de la información recibe capacitación o inducción en las políticas de seguridad	El personal involucrado con el manejo de la información recibe capacitación o inducción en las políticas de seguridad	El personal involucrado con el manejo de la información recibe capacitación o inducción en las políticas de seguridad	El personal involucrado con el manejo de la información recibe capacitación o inducción en las políticas de seguridad
		Preg 9	Hay un responsable o área encargado de su implementación y cumplimiento	Hay un responsable o área encargado de su implementación y cumplimiento	Hay un responsable o área encargad de su implementación y cumplimiento	Hay un responsable o área encargad de su implementación y cumplimiento	Hay un responsable o área encargad de su implementación y cumplimiento
		Preg 10	Como se gestionan incidentes o incumplimiento que se dan entorno a la política y como se retroalimentan las políticas	Como se gestionan incidentes o incumplimiento que se dan entorno a la política y como se retroalimentan las políticas	Como se gestionan incidentes o incumplimiento que se dan entorno a la política y como se retroalimentan las políticas	Como se gestionan incidentes o incumplimiento que se dan entorno a la política y como se retroalimentan las políticas	Como se gestionan incidentes o incumplimiento que se dan entorno a la política y como se retroalimentan las políticas
	Planes de recuperación	Preg 11	¿Se tienen planes de recuperación de la plataforma tecnológica?	Se tienen planes de recuperación de la plataforma tecnológica?	Se tienen planes de recuperación de la plataforma tecnológica?	Se tienen planes de recuperación de la plataforma tecnológica?	Se tienen planes de recuperación de la plataforma tecnológica?
		Preg 12	¿Con que frecuencia se revisan o actualizan estos planes?	¿Con que frecuencia se revisan o actualizan estos planes?	¿Con que frecuencia se revisan o actualizan estos planes?	¿Con que frecuencia se revisan o actualizan estos planes?	¿Con que frecuencia se revisan o actualizan estos planes?
		Preg 13	¿Con que frecuencia realizan pruebas de estos planes?	¿Con que frecuencia realizan pruebas de estos planes?	¿Con que frecuencia realizan pruebas de estos planes?	¿Con que frecuencia realizan pruebas de estos planes?	¿Con que frecuencia realizan pruebas de estos planes?
		Preg 14	¿En caso de hacerse pruebas se informan los resultados?	¿En caso de hacerse pruebas se informan los resultados?	¿En caso de hacerse pruebas se informan los resultados?	¿En caso de hacerse pruebas se informan los resultados?	¿En caso de hacerse pruebas se informan los resultados?
OBJETIVO 4 GUIA DE CONTROLES	Tendencias y cambios tecnológicos	Preg 15	Considera Ud. que el IoT (Internet de las cosas) incrementa los riesgos en las organizaciones? ¿Porque?	¿Considera Ud. que el IoT (Internet de las cosas) incrementa los riesgos en las organizaciones? ¿Porque?	N.A.	N.A.	¿Considera Ud. que el IoT (Internet de las cosas) incrementa los riesgos en las organizaciones? ¿Porque?
		Preg 16	Si bien la transformación digital trae nuevas oportunidades de negocio , que amenazas se deberían considerar a futuro?	Si bien la transformación digital trae nuevas oportunidades de negocio , que amenazas se deberían considerar a futuro?	N.A.	N.A.	Si bien la transformación digital trae nuevas oportunidades de negocio , que amenazas se deberían considerar a futuro?
		Preg 17	N.A.	¿Qué debilidades o vulnerabilidades son más frecuentes en las organizaciones?	N.A.	N.A.	¿Qué debilidades o vulnerabilidades son más frecuentes en las organizaciones?
		Preg 18	N.A.	Bajo su experiencia como cree Ud. que se pueden reducir estas vulnerabilidades en las organizaciones.	N.A.	N.A.	Bajo su experiencia como cree Ud. que se pueden reducir estas vulnerabilidades en las organizaciones.

Anexo 2. Codificación

	CATEGORIAS	CODIFICACIÓN	DEFINICIÓN
OBJETIVO 1 SERVICIOS CRITICOS	Modelo de aseguradora y corredora	SC_VID	Seguros vida
		SC_GENE	Seguros generales
		SC_EMP	Empresas
		SC_NAT	Naturales
	Líneas de negocio y productos y servicios	SC_NSE	Nivel socio economico
		SC_OPER	Operativos
		SC_TEC	Tecnologicos
		SC_TEL	Telecomunicaciones
OBJETIVO 2 GESTIÓN DE LOS RIESGOS	Identificación, análisis, evaluación y tratamiento. Controles para mitigar riesgos Custodia de la información confidencial	SC_FFPP	Fuerzas Policiales
		GR_SBS	SBS
		GR_ESTR	Estrategico
		GR_OPE	Operativos
		GR_FIN	Financieros
		GR_CUS	Custodia información
		GR_LAV	Lavado activos
		GR_MER	Mercado
		GR_REP	Reputación
		GR_LIQ	Liquidez
		GR_TEC	Tecnologicos
		CON_LOG	Logico
		CON_FIS	Fisico
		CON_PER	Personal
		CON_RES	Respaldo
		CON_CON	Concientización/
		CON_IND	Inducción
		CON_OPE	Operaciones
		CON_COM	Comunicaciones
		CON_DES	Desarrollo

	CATEGORIAS	CODIFICACIÓN	DEFINICIÓN
OBJETIVO 3 POLITICAS DE SEGURIDAD Y PLANES DE RECUPERACIÓN	Políticas de seguridad	POL_ACC	Acceso logico
		POL-ACT	Activos
		POL_FIS	Fisico
		POL_RESP	Respaldo información
		POL_COM	Comunicación(red)
		POL_CONT	Continuidad
	Planes de recuperación	POL_PROV	Proveedores
		PR_CORR	Correo electronico
		PR_TEL	Telefonia
		PR_APLI	Aplicaciones
		PR_EQUI	Equipos : Servidores, PC
		PR_PER	Personas
OBJETIVO 4 GUIA DE CONTROLES	Tendencias y cambios tecnológicos	TC_CIB	Ciberseguridad(robot)
		TC_AUTO	Automatización
		TC_SER DIG	Servicios digitales (insurtech)
		TC_EMER	Tecnologías Emergentes

Anexo 3. Guía de controles base para mitigar riesgos de seguridad de la información

- Toda organización debe definir sus servicios críticos de los complementarios, es decir, que sin esos servicios no se puede garantizar la disponibilidad de sus operaciones.
- El siguiente paso es establecer los riesgos a los que están expuestos los servicios críticos y esto se puede identificar de las ocurrencias operativas que se hallan presentado a lo largo de un periodo y también por juicio de expertos del área.
- En este proceso también se identificarán los recursos que los sostienen y definitivamente se incluye el soporte tecnológico y las telecomunicaciones, que son algunos de los soportes para las operaciones.
- La metodología de gestión de riesgos que deseen aplicar dependerá de la organización, se sugiere orientar de la Norma ISO/IEC 31000: Gestión de riesgo que les brinda el enfoque de cómo gestionarlos a través de un sistema.
- Posteriormente se debe revisar la Norma ISO 27001:2013 Sistema de gestión de la seguridad de la información y específicamente el Anexo A donde se precisa 14 dominios de control y 114 controles específicos, que dependiendo de los servicios críticos identificados se deban priorizar según el impacto que pueda ocasionar a la organización.
- Consideramos también que para facilitar la identificación de los servicios críticos podrían desarrollar un análisis de impacto del negocio (BIA) y relacionarlo tanto con los recursos, las dependencias con áreas internas y con proveedores.