ESCUELA DE POSGRADO NEWMAN

MAESTRÍA EN
GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

“Plan Estratégico para la Gestión de la Seguridad de la Información y la Ciberseguridad en la compañía de seguros SECREX”

Trabajo de Investigación
para optar el Grado a Nombre de la Nación de:

Maestro en
Gestión de Tecnologías de la Información

Autores:
Ing. Cohaila Bravo, Oswaldo Manuel

Docente Guía:
Dr. Valderrama Herrera, Roberto Marcel

TACNA – PERÚ

2022

Plan Estratégico para la Gestión de la Seguridad de la Información y la Ciberseguridad en la compañía de seguros SECREX

INFORME DE ORIGINALIDAD

14%	13%	1%	6%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

“El texto final, datos, expresiones, opiniones y apreciaciones contenidas en este trabajo son de exclusiva responsabilidad del (los) autor (es)”

Índice General

Resumen 1

Abstract 3

Introducción 5

Capítulo I Antecedentes del estudio 7

1.1 Título del tema.....7

1.2 Planteamiento del Problema 7

1.3 Objetivos de la investigación 8

1.3.1 Objetivos generales 8

1.3.1 Objetivos específicos 8

1.4 Metodología.....9

1.5 Justificación.....10

1.6 Definiciones.....11

1.7 Alcances y limitaciones 13

1.8 Cronograma 14

Capítulo II Marco Teórico 15

2.1 Conceptualización de las variables o tópicos clave.....15

2.2 Importancia de las variables o tópicos clave 29

2.3 Análisis comparativo 31

2.4 Análisis crítico 32

Capítulo III Marco Referencial 34

3.1 Reseña histórica....34
3.2 Filosofía organizacional....35
3.3 Diseño organizacional....36
3.4 Productos y servicios....38
3.5 Diagnóstico organizacional....42
3.6 Propósito de la compañía....43
Capítulo IV Resultados....45
4.1 Diagnóstico interno y externo....45
4.1.1 Fortalezas....45
4.1.2 Oportunidades....47
4.1.3 Debilidades....48
4.1.4 Amenazas....50
4.2 Diseño o rediseño de la filosofía organizacional....51
4.3 Formulación de estrategias....53
4.3.1 Identificación de la información para la operación....54
4.3.2 Identificación de dispositivos, infraestructura tecnológica y software....57
4.3.3 Identificación de cuentas y permisos a los aplicativos....58
4.3.4 Identificación de vulnerabilidades....60
4.3.5 Establecer un programa de orientación....61
4.3.6 Implementación de línea base para sistemas operativos y aplicaciones....62
4.3.7 Evaluación de actividades aplicables a la autenticación reforzada....63

4.3.8 Programa de Ciberseguridad 64

4.3.9 Estrategias complementarias 67

4.4 Diseño de planes de acción 73

Capítulo V Conclusiones y Sugerencias 76

5.1 Conclusiones 76

5.2 Sugerencias metodológicas y en el marco de actuación 77

5.3 Sugerencias operativas y de seguimiento 78

Bibliografía 80

Índice de tablas

Tabla 1 – Características de la información.....16
Tabla 2 – Fuentes de riesgo.....23
Tabla 3 – Tabla comparativa de conceptos.....31
Tabla 4 – Fortalezas de la compañía SECREX.....46
Tabla 5 – Oportunidades de la compañía SECREX.....48
Tabla 6 – Debilidades de la compañía SECREX.....49
Tabla 7 – Amenazas de la compañía SECREX.....51
Tabla 8 – Información necesaria para el desarrollo de las funciones.....54
Tabla 9 – Información necesaria para el desarrollo de las funciones - muestra.....55
Tabla 10 – Información que se ha procesado o mantiene física o lógicamente 55
Tabla 11 – Información que se ha procesado o mantiene física o lógicamente - muestra.....55
Tabla 12 – Información necesaria para cumplir obligaciones normativas 55
Tabla 13 – Información necesaria para cumplir obligaciones normativas - muestra .56
Tabla 14 – Aplicativos, sistemas, recursos informáticos para realizar actividades....56
Tabla 15 – Aplicativos, sistemas, recursos informáticos para realizar actividades - muestra.....56

Tabla 16 – Matriz de activos de tecnología y red 57

Tabla 17 – Matriz de activos de tecnología y red - muestra 57

Tabla 18 – Matriz de usuarios y roles.....59

Tabla 19 – Matriz de validación de usuarios y roles 59

Tabla 20 – Matriz de vulnerabilidades 60

Tabla 21 – Evaluación de canales y requerimiento de autenticación reforzada 64

Tabla 22 – Evaluación del programa de ciberseguridad.....66

Índice de figuras

Figura 1 – Metodología para la elaboración del Plan Estratégico.....9

Figura 2 – Esquema de un proceso.....24

Figura 3 – Determinación de proporcionalidad.....53

Resumen

El presente trabajo de investigación tiene como objetivo presentar las propuestas sistemáticas con las estrategias para SECREX Compañía de Seguros de Crédito y Garantías, en adelante SECREX o la compañía, en el ámbito de la gestión de la seguridad de la información y la ciberseguridad.

Cabe señalar que se ha identificado lo importante que es para la compañía, el establecimiento de dicho plan que considera las buenas prácticas internacionales y la necesidad de establecer las estrategias y planes operativos que se requieren para mitigar y controlar los riesgos de seguridad y ciberseguridad, en un contexto de incremento de casos de posibles amenazas con daños a la información.

El estudio, ha permitido el análisis situacional de la compañía respecto a las exigencias normativas del sistema de seguros del país, así como recoger las buenas prácticas de gestión de riesgos a nivel internacional tanto en el ambiente interno como externo y, a partir de dicho diagnóstico, formular el Plan Estratégico para la Gestión de la Seguridad de la Información y la Ciberseguridad, el mismo que considera las actividades y planes operativos exigidos en la normativa; el plan además, ha incorporado las actividades para el seguimiento y control de las actividades a desplegar a fin de que se realice un proceso integrado que brinde una mejora sustancial en la gestión de la compañía.

Finalmente, se ha evidenciado que la compañía SECREX está en proceso de adecuación a la exigencia normativa por lo que necesita estructurar y aplicar los lineamientos establecidos en la propuesta de plan estratégico a fin de dar

cumplimiento a la misma; por otro lado, el plan estratégico debe servir como guía directriz para la ejecución de los planes y actividades conducentes a mantener un adecuado control de los riesgos asociados a la disponibilidad, confidencialidad e integridad de la información.

Abstract

This research work aims to present systematic proposals with strategies for SECREX, Credit Insurance and Guarantees Company (hereinafter "SECREX" or "the company"), in the field of information security management and cybersecurity.

It should be noted that it has been identifiedhow important it is, for the company, the establishment of such a plan that considers international good practices, and the need to establish the strategies and operational plans that are required to mitigate and control security and cybersecurity risks, in a context of increasing cases of possible threats with damage to information.

The study has allowed the situational analysis of the company with respect to the regulatory requirements of the country's insurance system, as well as to collect good risk management practices at an international level, both in the internal and external environment and, based on this diagnosis, formulate the Strategic Plan for the Management of Information Security and Cybersecurity, the same that considers the activities and operational plans required in the regulations; The Plan has also incorporated the activities for the monitoring and control of the activities to be deployed in order to carry out an integrated process that provides a substantial improvement in the management of the company.

Finally, it has been shown that SECREX company is in the process of adapting to the regulatory requirement, so it needs to structure and apply the guidelines established in the proposal of the Strategic Plan, in order to comply with it; on the other hand, the Strategic Plan should serve as a guideline for the execution of plans and

activities aimed at maintaining adequate control of the risks associated with the availability, confidentiality and integrity of information.

Introducción

Esta investigación se ha desarrollado mediante la aplicación de la siguiente estructura programática:

Inicialmente se presentarán los antecedentes del estudio en la que se identificará el problema relacionado con la necesidad que tiene la compañía de seguros SECREX para establecer un plan estratégico para la gestión de la seguridad de la información y la ciberseguridad, se detallarán los objetivos relacionados con el establecimiento del referido plan, así como los correspondientes a los componentes operativos asociados. De igual manera en esta sección se presentará la metodología de aplicación, la misma que considera los siguientes aspectos: el análisis interno, la revisión de las exigencias normativas, el análisis de la situación actual respecto las exigencias, la propuesta para cubrir brechas, el despliegue de las acciones ejecutadas y el planteamiento de mecanismos de control y seguimiento. Se completará está primera etapa exponiendo la justificación de la elaboración del plan.

En el segundo capítulo, se presentará el contexto teórico aplicable detallando las principales variables y tópicos relacionados con la seguridad de la información y la ciberseguridad, se presentará la descripción de los principales conceptos como son la disponibilidad, integridad y confidencialidad de la información; los aspectos de ciberseguridad, ciberespacio, canales digitales, servicios en la nube, entre otros. Se describirá la importancia y el análisis crítico de los aspectos mínimos que se requiere conocer para sentar las bases del plan estratégico, así como una revisión de los estándares y buenas prácticas para gestionar la seguridad de la información y la ciberseguridad tanto en el país como a nivel internacional.

La tercera parte describirá a la compañía SECREX, su historia, ámbito de acción, accionistas, productos que ofrece en el mercado, la clasificación y rating de las empresas clasificadoras, así como su posición en el mercado peruano. Se detallará su participación como parte del grupo español CESCE y la descripción de su estructura organizacional donde se buscará enfatizar en las actividades para establecer la función de control de la seguridad de la información y la ciberseguridad.

En el cuarto capítulo se mostrarán los resultados del trabajo de investigación, específicamente se presentará el plan estratégico para la seguridad de la información y la ciberseguridad que incluirá el diagnóstico interno y externo, la propuesta de diseño organizacional aplicable al ámbito de acción, las estrategias, los planes operativos y las actividades conducentes a que la compañía se adecúe a las exigencias normativas. En este capítulo se presentará el resultado formal del trabajo de investigación siendo el principal entregable que será de aplicación en la mejora de la gestión en la compañía.

En el capítulo final, se presentarán las sugerencias y planes de acción para que el despliegue y ejecución del plan estratégico permita a la compañía SECREX un seguimiento adecuado de las estrategias, se verifique su adecuado cumplimiento y se pueda disponer de herramientas para realizar un seguimiento del plan.

Capítulo I Antecedentes del Estudio

1.1. Título del Tema

Plan Estratégico para la Gestión de la Seguridad de la Información y la Ciberseguridad en la compañía de seguros SECREX**.**

1.2. Planteamiento del Problema

SECREX es una compañía de seguros que forma parte del sistema de empresas supervisadas y reguladas por la Superintendencia de Banca, Seguros y Administradoras de Fondos de Pensiones (en adelante La Superintendencia). Como toda empresa que brindar servicios a diferentes grupos de interés, SECREX está expuesta a ataques, amenazas y explotación de vulnerabilidades a la información y los activos que la procesan, por lo que requiere mantener un ambiente operativo donde se implementen y validen los controles para garantizar la seguridad de dicha información. Asimismo, la compañía debe adecuarse y cumplir con las exigencias normativas en materia de seguridad de la información y la ciberseguridad establecidas por dicho órgano regulador en la resolución específica de dicha gestión. Una de las exigencias corresponde al establecimiento de un plan estratégico para la seguridad de la información y la ciberseguridad.

SECREX requiere el desarrollo del correspondiente plan estratégico aplicable a la naturaleza, tamaño y complejidad operativa de sus operaciones el mismo que deberá cumplir con las buenas prácticas internacionales y servir de directriz para las actividades estratégicas y operativas a desplegar en la institución, además que esta exigencia será de continua actualización y seguimiento.

La elaboración del Plan Estratégico para la Gestión de la Seguridad de la Información y la Ciberseguridad permitirá a la compañía cumplir con la implementación de las buenas prácticas de modo que se maximicen los controles y actividades para garantizar la seguridad de la información con la que opera brindando garantía operativa a sus grupos de interés y también cumplir con la exigencia normativa dentro de un marco de cumplimiento normativo y solidez en el sistema de seguros.

1.3. Objetivos de la Investigación

1.3.1. Objetivos Generales

a) Diseñar el plan estratégico para la seguridad de la información y la ciberseguridad en SECREX compañía de seguros siguiendo los requerimientos establecidos por la normativa peruana.

1.3.2. Objetivos Específicos

a) Realizar el diagnóstico situacional de SECREX en relación con el ambiente interno y externo, así como establecer el nivel de adecuación necesario a incluir en el plan estratégico.
b) Formular los planes operativos y actividades necesarias para desplegar las estrategias establecidas en el plan estratégico.
c) Establecer mecanismos de control y seguimiento para la validación del cumplimiento de estrategias y planes operativos del plan.

1.4. Metodología

La metodología que se utilizará corresponde a la de formulación de plan estratégico aplicada y desplegada por la Universidad de Cantabria (2023), la misma que se muestra en la figura 1.

Figura 1

Metodología para la elaboración del Plan Estratégico

Nota: Tomado de la Universidad de Cantabria (2023)

En la fase de situación actual se realizará el análisis interno, la revisión de las exigencias normativas y el análisis del nivel de adecuación respecto las exigencias.

Seguidamente, se realizará la evaluación del entorno externo e interno mediante la determinación de la matriz FODA para el ámbito de la seguridad de la información y la ciberseguridad donde se determinarán los condicionantes para la compañía. En esta fase también se deberá establecer la visión de la compañía en este aspecto considerando detallar hacia donde quiere llegar la compañía.

En la tercera fase, se plantearán las propuestas para cubrir brechas, se establecerán los planes operativos y las actividades para dar cumplimiento a los objetivos y se plantearán los mecanismos de control y seguimiento que permitan evaluar de manera permanente el plan estratégico. Esta fase además incorporará las siguientes tareas: mecanismos y metodología para identificar la información; la identificación de dispositivos, infraestructura tecnológica y software; la identificación de cuentas y permisos de los usuarios; la identificación de vulnerabilidades; la evaluación de autenticación reforzada; la identificación de proveedores; el análisis de servicios en la nube y la definición del programa de capacitación. Como actividad permanente se establecerán los informes de monitoreo continuo.

1.5. Justificación

Este trabajo de investigación formula de manera sistemática, las estrategias que deberá desarrollar SECREX a fin de disponer de un plan estratégico para la seguridad de la información y la ciberseguridad. El plan estratégico se requiere establecer para definir los lineamientos y actividades que aseguren de manera razonable la seguridad de la información y el control de los aspectos de ciberseguridad. En cuanto se conciba el plan estratégico, se cumplirá con la exigencia normativa establecida por el regulador a través de la resolución SBS 504-2021 así como contar con una importante fortaleza ante los grupos de interés y el resto de las empresas del sistema de seguros. En caso no se realizará o desplegará el plan, la compañía se expone a una sanción regulatoria que puede afectar los resultados económicos y la solvencia de la compañía.

A nivel teórico y metodológico, el plan estratégico permitirá sostener la aplicación de los conceptos y métodos empresariales robustos y sólidos que ofrecerán una mejora para la compañía.

1.6. Definiciones

Para efectos del presente trabajo de investigación, deberán considerarse las definiciones establecidas en la normativa de la superintendencia[1] - SBS (2021) las mismas que se basan en el estándar internacional ISO 27000 - Sistemas de gestión de la seguridad de la información y que establecen:

a) **Activo de información:** Información o soporte en que ella reside, que es gestionado de acuerdo con las necesidades de negocios y los requerimientos legales, de manera que puede ser entendida, compartida y usada. Es de valor para la empresa y tiene un ciclo de vida.

b) **Amenaza:** Evento que puede afectar adversamente la operación de las empresas y sus activos de información, mediante el aprovechamiento de una vulnerabilidad.

c) **Autenticación:** Es el proceso que permite verificar que una entidad es quien dice ser, para lo cual hace uso de las credenciales que se le asignan. La autenticación puede usar uno, dos o más factores de autenticación independientes, de modo que el uso sin autorización de uno de ellos no compromete la fiabilidad o el acceso a los otros factores.

   Canal digital: Medio empleado por las empresas para proveer servicios cuyo almacenamiento, procesamiento y transmisión se realiza mediante la representación de datos en bits.

[1] Resolución SBS Nº504-2021: Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad

d) **Ciberseguridad:** Protección de los activos de información mediante la prevención, detección, respuesta y recuperación ante incidentes que afecten su disponibilidad, confidencialidad o integridad en el ciberespacio; el que consiste a su vez en un sistema complejo que no tiene existencia física, en el que interactúan personas, dispositivos y sistemas informáticos.
e) **Confidencialidad:** propiedad mediante la cual la información no se pone a disposición ni se revela a personas, entidades o procesos no autorizados.
f) **Disponibilidad:** propiedad de la información de ser accesible y utilizable bajo demanda por una entidad autorizada.
g) **Entidad:** Usuario, dispositivo o sistema informático que tiene una identidad en un sistema, lo cual la hace separada y distinta de cualquier otra en dicho sistema.
h) **Evento:** Un suceso o serie de sucesos que puede ser interno o externo a la empresa, originado por la misma causa, que ocurre durante el mismo periodo de tiempo.
i) **Factores de autenticación de usuario:** Aquellos factores empleados para verificar la identidad de un usuario
j) **Incidente:** Evento que se ha determinado que tiene un impacto adverso sobre la organización y que requiere de acciones de respuesta y recuperación.
k) **Información:** Datos que pueden ser procesados, distribuidos, almacenados y representados en cualquier medio electrónico, digital, óptico, magnético, impreso u otros, que son el elemento fundamental de los activos de información.
l) **Integridad:** propiedad de la información mediante la cual se garantiza que

sea exacta y completa.

m) **Servicios en nube:** Servicio de procesamiento de datos provisto mediante una infraestructura tecnológica que permite el acceso de red a conveniencia y bajo demanda, a un conjunto compartido de recursos informáticos configurables que se pueden habilitar y suministrar rápidamente, con mínimo esfuerzo de gestión o interacción con los proveedores de servicios.

n) **Procesamiento de datos:** El conjunto de procesos que consiste en la recolección, registro, organización, estructuración, almacenamiento, adaptación, recuperación, consulta, uso, transferencia, difusión, borrado o destrucción de datos.

o) **Vulnerabilidad:** Debilidad que expone a los activos de información ante amenazas que pueden originar incidentes con afectación a los mismos activos de información, y a otros de los que forma parte o con los que interactúa. (p.2)

1.7. Alcances y limitaciones

El Plan Estratégico desarrollado tendrá como ámbito de acción específico a la seguridad de la información y la ciberseguridad que tiene que implementar la compañía SECREX bajo la exigencia de la normativa de la superintendencia dentro del sistema de empresas de seguro del país. El referido plan se aplicará en todas las oficinas de la compañía en Lima y provincias (Trujillo, Arequipa y Huancayo).

Las limitaciones para el desarrollo del Plan Estratégico están relacionadas con el poco conocimiento en los aspectos de base conceptual de las diferentes áreas que proveen o actualizan información y que requieren actualización formativa y de los

términos estándares utilizados. Asimismo, el reducido tamaño de la organización en el equipo técnico de sistemas y proyectos de tecnología son aspectos que se consideran como limitantes para un desarrollo más ágil del proyecto a desarrollar.

1.8. Cronograma

La elaboración del presente trabajo de investigación se regirá bajo el siguiente cronograma de actividades.

Actividad / periodo	May	Jun	Jul	Ago	Set	Oct
Antecedentes del estudio	■					
Marco teórico		■				
Marco referencial – la compañía		■				
Plan estratégico para la SI y la ciberseguridad			■			
Sugerencias			■			
Consolidación del Plan Estratégico				■	■	
Cierre						■

Capítulo II Marco Teórico

2.1 Conceptualización de las variables o tópicos clave

La seguridad de la información es un concepto relativamente nuevo, a partir de los lineamientos de Basilea II donde se mencionan los tópicos de riesgo operacional en el año 1996, se inicia un despliegue importante en el cuidado de la información dado que se van presentando múltiples cambios en el ambiente operativo de las empresas; aspectos como el aumento de operaciones que exigen sistematizar y procesar más operaciones, la aparición de dispositivos con mayor capacidad de almacenamiento, nuevas opciones y servicios de banca y operativa electrónica, el aumento de las capacidades de internet, entre otros rápidos avances, han generado la importante necesidad de mantener adecuados controles internos y externos a la información con la que se realizan las actividades y operaciones empresariales. Mas nuevo todavía es el concepto de ciberseguridad, aplicable recientemente a partir del año 2018 considerando el salto tecnológico que se ha dado en las redes que ya no requieren de ambiente físico para almacén y procesamiento de datos.

En ese contexto, una compañía de seguros mantiene importantes cantidades de información que requiere custodiar, procesar, transportar en el quehacer diario de la prestación de los servicios que brindar a sus clientes, además del control que se requiere cumplir para que se pueda ofrecer confianza a los diferentes grupos de interés con los que interactúa.

A continuación, se presentan los principales tópicos y variables que se han tenido en cuenta para establecer el plan estratégico de seguridad de la información y la ciberseguridad.

a) **La Información**

Partimos de la principal y más relevante variable que es la información, se entiende por información a un conjunto de datos que ha sido organizado y estructurado de tal manera que permita realizar alguna acción con ellos. Por ejemplo, la información de nuestra dirección domiciliaria registra información sobre la calle, el número, el distrito, el código postal. Todos esos datos nos dan en sí una información completa y entendible mediante la cual podemos recibir comunicaciones, recibir un pedido físico o comunicar a otras personas el lugar donde residimos. La información tiene dos importantes características que corresponden al qué podemos hacer con ella y el dónde se mantiene la misma; en el primer caso la información puede ser susceptible de procesarse para efectos de tomar una acción posterior; puede ser entregada a otras personas o puede ser transportada de una locación a otra o puede ser representada de diferentes maneras. En la característica de la ubicación, la información puede ser almacenada de manera física o electrónica, en caso de que sea física, puede estar impresa en un papel y en el caso electrónico se almacena de manera digital o magnética en un repositorio.

En la Tabla 1 se muestra un ejemplo de las características de la información aplicable a un conjunto de datos en una compañía de seguros.

Tabla 1

Características de la información

Característica	Tipo	Detalle o aplicación
Procesamiento	Datos	Se realiza la facturación de las pólizas
Distribución	Datos	Se entrega la información a Contabilidad
Almacenamiento	Datos	Se guarda la información en la base de datos
Medio	Digital	Reporte en la web de cuadro de producción
Medio	Magnético	La tabla de datos donde se guarda la producción
Medio	Físico	Impresión de las pólizas en el certificado a entregar

Nota: Elaboración propia

b) **Activos de información**

La información por si sola se considera un activo importante para una empresa o persona; por tanto, cuando se puede asociar dentro de un mismo concepto a la información en su estructura más básica y al activo que representa como tal. Asimismo, se considera como activo de información a todo aquel dispositivo o repositorio donde la información se encuentra almacenada. Por ejemplo, se considera como activos de información a la base de datos donde reside la información, del mismo modo se considera como activo de información al servidor donde está registrada la base de datos anteriormente indicada; y más aún podemos considerar como activo de información al centro de datos donde se encuentra físicamente el servidor anterior. Quiere decir entonces que dependiendo del nivel o el marco de referencia desde donde se analice la información, podemos encontrarnos con diversos activos de información.

Otra característica importante de los activos de información corresponde a que en la mayoría de los casos puede tener un valor económico. En el caso de los tres activos mostrados anteriormente, una base de datos es más compleja de poder cuantificar; sin embargo, el servidor donde esta reside si tiene un costo que incluso puede registrarse contablemente; a su vez, el centro de datos también tendrá un valor como activo que puede cuantificarse. Estas propiedades de los activos de información hacen que tengan un ciclo de vida y un momento adecuado de valor.

c) **Propiedades de la información**

La información, en el contexto de la seguridad de la información, debe mantener tres propiedades durante cualquier proceso que se ejecute o realice sobre ella.

La primera se denomina *confidencialidad* y se refiere a aquella propiedad en la que la información es utilizada únicamente por personas, procesos, sistemas o entidades que tienen la autorización para poder hacerlo. La confidencialidad según Baca (2016), “se refiere a que en todas las etapas del procesamiento de la información, ésta se encuentra protegida contra accesos no autorizados, los cuales pueden derivar en la alteración o robo de información confidencial” (p.12). Un ejemplo de la confidencialidad de la información es el acceso restringido a nuestro historial médico, en ese sentido solo los médicos, el personal del centro de salud autorizado y nosotros mismos podemos ver la información que allí se encuentra registrada; otro ejemplo en el caso de una empresa sería que los datos de la planilla de los colaboradores, únicamente debe ser revisada por el área encargada de la estimación de pagos y en el caso individual por cada trabajador específicamente la información de su retribución económica. Cualquier acceso no autorizado o cuando cualquier otra persona o entidad puede acceder a la información representa una falla directa en la seguridad de la información.

La segunda propiedad corresponde a la *disponibilidad,* esta corresponde a aquella situación en que la información debe estar disponible y accesible en el momento que sea requerida o cuando se necesite procesar, esta es una propiedad más del tipo cualitativa en la que se espera tener la información lista para desplegar las actividades de procesamiento sin demora de tal modo que permita un tratamiento dinámico y ágil. Esta propiedad, está alineada por lo señalado por Vega (2021), quienes indican que la disponibilidad “se refiere a la capacidad de acceder a nuestros datos cuando los necesitamos” (p.13). En el caso de la disponibilidad un ejemplo directo se daría cuando un usuario solicita los saldos de su cuenta de ahorro e ingresa

con su usuario y clave a la web de su banco, entonces es relevante que en ese preciso momento pueda visualizar dicho saldo; otro ejemplo sería a una persona que solicita una copia de su acta de nacimiento en la autoridad civil y obtenga inmediatamente el documento. De ser el caso que el cliente del banco no acceda a sus saldos o que el usuario no pueda obtener su acta de nacimiento, se generaría una falla en la seguridad de la información.

Finalmente, la tercera propiedad corresponde a la *integridad.* Esta propiedad está relacionada con la calidad de datos y que la información no haya sido manipulada o modificada previamente a su uso, es decir la información debe mantenerse completa y sin variaciones para su efectivo procesamiento, lo que se pretende al garantizar esta propiedad es que los datos y la información sean lo suficientemente confiables para su uso. Precisamente se cumplirá el requisito de integridad cuando “solo el personal autorizado podrá modificar la información, ya que esta debe ser siempre exacta y completa” (Postigo, 2020, p. 8). En el caso de la integridad vamos a entenderla cuando se solicita el detalle de los últimos 20 movimientos en un registro de ventas, debieran aparecer todos y cada uno de los movimientos con la información que se necesita; otro ejemplo de integridad se puede ver en el historial de un registro de inmuebles donde figura toda la información histórica de un predio desde su adquisición, su declaratoria de fábrica, su venta, su independización y otras ventas futuras, un registro completo y adecuado. Cuando la información pierde parte de su contenido o no se puede visualizar de manera completa se genera un problema de seguridad de información.

d) **El Ciberespacio**

El avance tecnológico, la aparición de la internet y los cambios en el ambiente y las plataformas de tecnología a un ritmo realmente sorprendente, han generado un nuevo espacio de interacción, un espacio más complejo donde interactúan personas, empresas, sistemas, aplicaciones, redes y medios de pago. Este espacio que no tiene una locación física o una realidad para su funcionamiento que pueda asociarse a una locación geográfica única se denomina ciberespacio; y es allí donde aparece la necesidad de gestionar actividades para proteger la información.

El ciberespacio es de amplia cobertura, pudiendo incluir servicios y procesamiento para cualquier tipo de sector o rubro económico. En esa línea, Pulido (2016) señala que “en el ciberespacio es normal el uso de herramientas informáticas y telemáticas, aplicaciones y demás elementos que establecen el contacto del usuario con la red” (p.19).

e) **La Ciberseguridad**

Ante la aparición del ciberespacio, se hace necesaria la implementación de medidas de protección para cuidad y preservas la información que ahora se encuentra en este nuevo sistema. Para ello, la ciberseguridad se define como un proceso permanente mediante el cual se realizan actividades de prevención, identificación, atención de incidentes y gestión de la información en el ciberespacio. Todos los procesos que buscan garantizar las tres propiedades de la información (confidencialidad, disponibilidad e integridad) ahora se trasladan al ciberespacio.

Siendo un término relativamente nuevo, puesto que antes del año 2000 no existía un ciberespacio tan complejo como el actual, y donde primaba la estructura física de los grandes computadores, ahora la ciberseguridad pasa a conformar parte de las acciones de control que son buenas prácticas en el mantenimiento de las propiedades de la información.

f) **Fuentes de los riesgos a la información**

Un riesgo es la desviación respecto a un evento o situación esperada. Para el contexto de la seguridad de la información y la ciberseguridad, se considera como riesgo toda desviación respecto a la situación regular del día a día y que afecta operativa o económicamente a personas o empresas. En ese sentido cuando la desviación sea beneficiosa para la empresa o la persona dueña de la información, esa situación no corresponde a un análisis de riesgo; sin embargo, si la desviación es desventajosa, se considerará como un riesgo. Para efectos de analizar el riesgo se consideran las fuentes que originan el riesgo, siendo éstas de dos tipos: las fuentes internas que son denominadas *vulnerabilidades* y fuentes externas, las que se denominan *amenazas.*

Una vulnerabilidad es una debilidad o una falla interna, siendo una situación que puede ser explotada por agentes tanto externos que aprovechan dicha debilidad para intentar generar afectación a las propiedades de la información y obtener algún beneficio.

Por otro lado, se tienen las amenazas, que corresponden a todas las actividades que pueden afectar a los activos de información sea de manera directa a

través de aprovechar una vulnerabilidad o de manera indirecta a través de una afectación que es global o sistémica. En el caso de una amenaza directa se pueden considerar los ataques tecnológicos mediante distintos tipos de ataque como la ingeniería social, el phishing, el malware, el hacking, etc. En el caso de las amenazas indirectas podemos mencionar a los desastres, la indisponibilidad de proveedores, la ausencia de personal que utiliza los sistemas o activos de información.

Cuando se suceden varios sucesos, sean internos (a través de vulnerabilidades) o externos (a través de amenazas), y éstos ocurren durante un periodo de tiempo, estos sucesos se denominan *eventos*. Cuando los eventos generan un efecto económico u operativo a la empresa pasarán a denominarse *incidentes*. En este momento, cuando se presentan incidentes hacia la empresa, a las personas o a los activos de información, entonces será necesario establecer una gestión de atención a fin de que los efectos de su ocurrencia sean reducidos a un nivel razonable de aceptación.

En la Tabla 2, se presenta una lista de fuentes de riesgo, así como una lista de eventos e incidentes en los que se puede identificar la diferencia entre estos conceptos.

Tabla 2

Fuentes de riesgo

Fuente	Evento	Incidente
Vulnerabilidad	Falla en el control biométrico de accesos	Ingreso de personas no autorizadas al edificio con robo de activos de información
Vulnerabilidad	Antivirus desactualizados	Ingreso de virus que daña a un grupo de equipos o servidores
Vulnerabilidad	Caída de firewall	Acceso a servidor y borrado de información de clientes
Amenaza	Ataque cibernético con denegación de servicio	Solicitud de pago de rescate para devolver la liberalidad de base de datos
Amenaza	Falla de servicio de prestación de energía	Gastos importantes en energía alterna o grupos electrógenos para mantener operativa
Amenaza	Robo de oficinas empresariales	Robo por un total específico de dinero con daños a activos que requieren ser repuestos

Nota: Elaboración propia

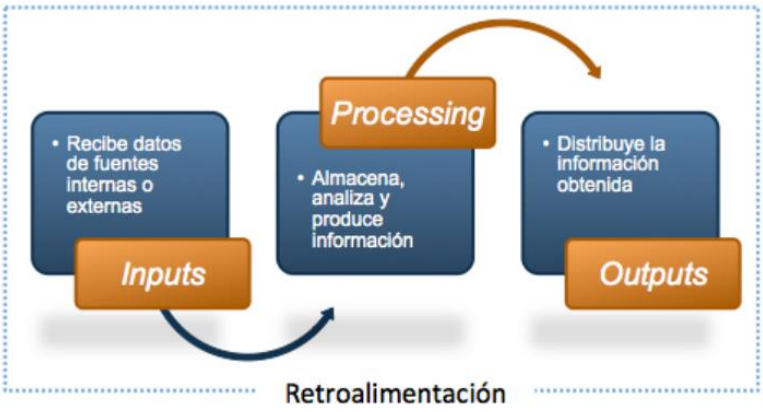
g) **Procesamiento de datos**

En la actividad empresarial o personal se desarrollan procesos y actividades que generan el ciclo operativo o productivo. Un proceso es un conjunto de actividades que integran tres secuencias o pasos; inicialmente existe una fuente o ingreso de insumos, elementos o datos, estos se reciben, se organizan y almacenan para luego pasar a la segunda secuencia que es el procesamiento. En el procesamiento a la información o datos se les da un tratamiento o transformación buscando alcanzar objetivos o beneficios. Finalmente, en la última secuencia los elementos transformados son llevados a un canal de salida donde se distribuyen o almacenan. En la secuencia de tres pasos se obtiene un resultado final con el cual se puede obtener un beneficio producto del procesamiento o se puede tomar una decisión que permita a la persona o empresa obtener un beneficio.

En la Figura 2 se muestra esquemáticamente el proceso con la secuencia de las tres fases indicadas.

Figura 2

Esquema de un proceso



Nota: El esquema muestra las tres secuencias en un proceso: la entrada, el procesamiento y la salida. Tomado de Aliat Universidades http://online.aliat.edu.mx/adistancia/tec_procesos/s2/s2_02.html

En el procesamiento de datos se pueden presentar múltiples actividades dentro de las diferentes fases. A continuación, se detallan las más relevantes dentro de la ejecución de estas:

Recolección: Corresponde al proceso de obtención de datos o insumos para la realización del proceso, por ejemplo, en el caso de obtener datos de clientes esto puede realizarse mediante formularios, encuestas, cuestionarios o mecanismos digitales como enlaces de actualización de datos.

Registro: Corresponde a la actividad mediante la cual la información se ingresa o almacena en un repositorio físico o electrónico a través de registrar la información en dichos repositorios. En el caso de los datos obtenidos estos se ingresan en la base de datos de clientes.

Organización: Corresponde a la actividad en la cual los datos o información mantiene características que permiten segmentar o identificar diversos tipos o agrupaciones. Para el ejemplo que estamos siguiendo, corresponderá por ejemplo organizarlos por zona geográfica, por tipo etario u otras agrupaciones.

Estructuración: Es el proceso mediante el cual los datos o información mantiene un orden de estructura, aquí se podrá identificar los tipos de datos, las cabeceras de los datos, el ancho de estos, entre otros aspectos. Para nuestro ejercicio consideraríamos por ejemplo que los datos de identificación de documento de nuestros clientes deben ser no nulos, con un número único de identificación y con un ancho determinado de dígitos.

Almacenamiento: Es la actividad mediante la cual la información se guarda en un repositorio el mismo que puede ser un disco físico, un disco virtual, un almacén físico o determinado espacio donde mantenga su registro.

Recuperación: Es la actividad mediante la cual se vuelve a obtener los datos previamente almacenados para empezar un proceso de transformación, consulta o explotación. En el caso de nuestro ejemplo se considera la obtención de datos de los clientes para realizar una nueva campaña de comunicación.

Consulta: Se refiere a toda actividad mediante la cual se visualiza o revisa la información recuperada, es un modo de vista donde no se realizan modificaciones, pero si pueden tomarse acciones en relación con la información consultada. En el

ejercicio por ejemplo tomamos los datos de situación de un cliente y obtenemos visualizando sus datos y posición general.

Uso: Es la actividad mediante la cual la información o datos revisados o consultados sirven para tomar una acción determinada. En la secuencia que estamos revisando por ejemplo podemos usar la información para ver si el cliente se encuentra en situación adecuada para ofrecerle nuevos productos.

Transferencia: Corresponde a la actividad de traslado o entrega de información entre distintas entidades, en la transferencia se brinda la información para que otra instancia tome acción en relación con la información. En nuestra secuencia, se puede transferir la información de los clientes a una central consolidadora que agrupa toda la información de diversas fuentes.

Difusión: Es la actividad en la que se presenta información a algún grupo de interés. Por ejemplo, la información de los clientes que no cumplen con cierto requisito, lo cual se debe informar a la central e incluso podría presentarse a una entidad supervisora o de control.

Borrado: Es el proceso mediante el cual se retira de la estructura de la información ciertos valores o datos, en nuestro ejercicio por ejemplo se va a eliminar la información de referidos de los clientes para poder hacer una nueva campaña de prospección y promoción, entonces se borran los datos para ingresar nueva información.

Destrucción: Referido al proceso en el cual se destruye o elimina de manera completa la información, por lo general se aplica cuando pasa un determinado periodo de tiempo y la información ya no requiere ser almacenada. Un ejemplo típico de esta condición se da cuando se destruyen archivos con más de 10 años de almacenamiento.

h) **Entidad**

En el marco de la seguridad de la información, una entidad se refiere a aquel elemento que es único a nivel de identidad, es decir debe mantener características que permitan diferenciarlo de cualquier otro elemento en un grupo. El valor de la entidad hace que se destaque la distinción de entre varios elementos y se pueda separar a un elemento de todo un grupo de elementos.

Cuando se determinan las características de identificación única podemos referirnos a una persona, a un conjunto de datos, a un sistema, a un usuario e incluso a un equipo físico o electrónico. En el caso de las personas, cada una debiera poder identificarse de manera única en un marco de referencia y control para ellos se usan datos biométricos o documentos estándar de identificación. De igual manera, sucede con un equipo electrónico que debe ser posible de identificar de manera única como se hace en el caso de los cajeros automáticos en donde cada máquina tiene un identificador.

i) **Autenticación de entidades**

Tomando en cuenta la característica de identificación única para una entidad, existe un proceso mediante el cual se debe verificar que una entidad es quien dice

ser, ese proceso se denomina *autenticación* y es uno de los procesos más relevantes en el marco de la seguridad de la información dado que darse de manera adecuada se garantiza que una entidad realice las actividades que está autorizada a hacer y también permitirá que se identifique las acciones realizadas dentro de un sistema de entidades. Por ejemplo, cuando una entidad realice el proceso de autenticación podrá acceder a las actividades autorizadas, asimismo el centro de control de entidades podrá hacer seguimiento directo de las acciones que realice una entidad.

Para realizar el proceso de autenticación se utilizan credenciales y factores de autenticación, en el caso de credenciales se relacionan con números de documento, números de tarjeta, códigos de ingreso o cualquier mecanismo brindado a una entidad como registro de identificación. En el caso del factor de autenticación corresponde a aquel elemento que permita verificar la identidad del usuario y que viene relacionado con su credencial. Por ejemplo, podemos mencionar a las claves de ingreso, llaves, elementos generados aleatoriamente como tokens, números de validación, entre otros elementos que hagan posible validar la relación entidad-credencial.

j) **Canal digital**

En la evolución de los diversos tipos de canales para el transporte o circulación de la información, nos encontramos con la definición de canal digital, el mismo que se refiere al medio a través del cual se realiza el procesamiento de la información. Se denomina canal porque a través de él se puede intercambiar información y a través de sus elementos viaja la información de un lugar a otro; y, se denomina digital porque la información se codifica entre valores binarios denominados bits.

Con el avance tecnológico y la rápida explosión del internet de las cosas, el canal digital se ha convertido en la más grande y potente forma de intercambiar información.

k) **La nube y los servicios en nube**

Se denomina nube a aquella infraestructura o plataforma tecnológica donde convergen varios recursos informáticos sin necesidad de una locación física. Estos servicios se pueden configurar y brindar a los usuarios según la demanda que requieran y se pueden habilitar o deshabilitar de manera ágil y sencilla. En la nube, los servicios tradicionales en físico pasan a segundo plano, el procesamiento no depende exclusivamente de un servidor físico, sino que se realiza a través de recursos compartidos con un ambiente separado de los demás y que es altamente parametrizable.

2.2 Importancia de las variables o tópicos clave

La seguridad de la información tanto a nivel de los tópicos tradicionales, como la actual necesidad de cubrir los riesgos de ciberseguridad han tomado importante relevancia a nivel empresarial.

En los últimos años, las empresas han realizado importantes y altamente cuantiosas inversiones para asegurar la calidad de sus datos y de ese modo brindar a sus clientes y contrapartes la tranquilidad para continuar prestando servicios u ofreciendo productos que guarden la debida diligencia en las actividades de procesamiento de información.

Cabe mencionar el caso de robo de información sucedido a JP Morgan, uno de los bancos más grandes de Estados Unidos, cuando en octubre de 2014 tuvo que salir a reconocer en el mercado que información de más de 76 millones de cuentas de clientes, entre la que se podía mencionar datos de nombres, direcciones, correos electrónicos fueron extraídos del banco. A partir de dicho evento, se ha establecido todo el proceso de autenticación doble en las transacciones financieras, control que se ha venido incorporando paulatinamente en los últimos años.

En el Perú, no somos ajenos a los robos de información, sabido es que en los principales mercados negros, es de poca dificultad, la obtención de datos confidenciales de personas y empresas. Incluso esta situación se pudo notar en un caso de robo de información en la autoridad civil.

Tal como recoge la investigación del Diario Gestión (20 de mayo de 2022). *Se detectó que delincuentes cibernéticos, a través de la Plataforma de Interoperabilidad del Estado Peruano (PIDE), infraestructura tecnológica administrada por la Secretaria Gobierno y Transformación Digital de la PCM, accedieron a las cuentas y claves de los usuarios de las instituciones públicas que cuentan con este servicio, las mismas que ya fueron bloqueadas*.

Resulta pues, de amplia importancia establecer los mecanismos que permitan mantener un adecuado control de los riesgos que pueden afectar a los activos de información o exponer a una empresa a situaciones de riesgo.

2.3 Análisis comparativo

En el contexto de comparar los aspectos teóricos, se puede precisar que los mismos vienen siguiendo un mismo patrón puesto que se basan en el estándar internacional ISO 27000 del año 2018, precisamente esa característica ha generado que las prácticas a implementar en materia de seguridad de información y la ciberseguridad guarden un esquema de ejecución robusto y exigible para las empresas.

A continuación, se establece una tabla comparativa entre conceptos a fin de definir las principales características, aspectos y parámetros esenciales de alcance para de cada una de ella de modo que se puede identificar de mejor manera la aplicabilidad que éstas consideran:

Tabla 3

Tabla comparativa de conceptos

Concepto	Parámetro esencial	Principales características
Información	Dato	Datos organizados y estructurados para realizar alguna acción con ellos
Activo de información	Valor	La información por lo que representa y/o los activos donde reside la información
Propiedad de la información	Confidencialidad Disponibilidad Integridad	Son las propiedades esenciales que debe cumplir la información en el contexto de seguridad de la información.
Ciberespacio	Espacio de interacción	Espacio más complejo donde interactúan personas, empresas, sistemas, aplicaciones, redes y medios de pago
Ciberseguridad	Protección	Corresponde a las actividades de prevención, identificación, atención de incidentes y gestión en el ciberespacio.
Fuentes de riesgo	Vulnerabilidad Amenaza	Corresponde a los tipos internos (vulnerabilidad) o externos (amenazas) que son focos u origen de riesgos.
Procesamiento de datos	Procesos	Conjunto de actividades con tres secuencias: ingreso, procesamiento en si y salidas.
Entidad	Distinción	Valor que permite separar a un elemento de un grupo de otros elementos
Autenticación de entidades	Validación	Procedimiento mediante el cual se verifica que una entidad es quien dice ser
Canal digital	Medio binario	Es el camino por donde se intercambia información, es digital porque utiliza codificación binaria (0-1)

Nota: Elaboración propia

2.4 Análisis crítico

Las variables en análisis descritas en el capítulo 2.1 vienen generando un importante impulso cognitivo y de adecuación en las empresas. En los últimos años, la importancia que se le ha dado a los aspectos relacionados con la seguridad de la información y la ciberseguridad van de la mano con el avance tecnológico, la cantidad de información que se procesa y las inmensas cantidades de información que circulan entre diferentes operadores y contrapartes; de allí que resulta muy necesario que las empresas tomen medidas específicas para el control de las fuentes de riesgo a fin de preservar la información y los activos asociados a la misma.

En lo que corresponde a las propiedades de confidencialidad, integridad y disponibilidad, si bien estas mantienen su condición de control desde hace varios años en el sistema de seguros, resultan insuficiente mantener las mismas actividades de control de hace unos 15 o 10 años puesto que, con la aparición del ciberespacio, el espectro de fuentes de riesgo, ha tenido un crecimiento que pone en serio riesgo a las empresas, lo cual no es ajeno a la compañía materia del presente análisis.

En los últimos años, variables como la definición de entidades, los análisis para determinar los niveles de autenticación de contrapartes y los controles sobre los canales digitales con las consecuentes operaciones que hoy allí se realizan; son los nuevos desafíos que las empresas tienen que evaluar y mantener en constante control.

En el componente de la exigencia en relación a la necesidad de implementar un plan estratégico para la seguridad de la información y la ciberseguridad, es

importante precisar que no todas las empresas tienen el mismo tamaño y complejidad en las operaciones por lo que se necesita mejorar la normativa internacional a efecto de establecer niveles escalonados o de aplicación que evidencie una mejora continua puesto que no tendrá el mismo esquema de implementación una empresa pequeña que una empresa grande.

Una variable para poder determinar el alcance de la exigencia es el valor de patrimonio de las empresas o también podría aplicarse el valor de cuota o participación de mercado.

A nivel de la propia compañía SECREX, el ambiente operativo y las áreas responsables de la implementación del plan, resultan ser insuficientes y pequeñas con lo cual la adecuación e implementación podría tomar mayor tiempo de lo requerido.

Capítulo III Marco Referencial

3.1. Reseña histórica

La compañía de seguros SECREX, fue creada en el año 1980 teniendo como primera razón social la denominación Compañía Peruana de Seguro de Crédito a la Exportación, en ese entonces especializada en seguros de crédito con autorización de funcionamiento por parte de la Superintendencia.

En el año 1994, la compañía cambia su razón social a SECREX Compañía de Seguros de Crédito y Garantía ampliando la oferta de sus productos principalmente a los seguros de caución con lo que consolida su posicionamiento, iniciando un proceso de fortalecimiento en los diversos sectores económicos donde presta sus servicios.

A partir de 1995, la compañía ofrece cobertura de seguros para garantías aduaneras, garantías impositivas, obras públicas, obras privadas, prestación de servicios y venta de suministros.

A fines del año 2000, SECREX es adquirida por la Compañía Española de Seguros de Crédito a la Exportación CESCE, empresa especializada en seguros de crédito, con lo cual busca consolidar su posicionamiento en la región. CESCE es la tercera compañía a nivel mundial en participación de seguros de crédito y la primera en el ramo de cobertura por cuenta propia a entidades exportadoras de España.

Entre los años 2001 y 2012, SECREX se consolida como la primera empresa en emisión de primas de seguros de caución y mantiene la participación en el seguro de crédito.

El año 2022, la compañía adopta el nombre comercial CESCE a fin de unificar su imagen internacional, consolidar el posicionamiento de la casa matriz y mantener una estrategia comercial global. El nombre de la compañía se mantiene como SECREX para efectos de registro y tributación, así como denominación social.

Desde el año 2021, SECREX es líder en el mercado de caución en el Perú, con una participación de 28% del mercado, posición que mantiene hasta marzo de 2023. Además, SECREX mantiene contrato de reaseguros con un total de 12 empresas calificadas como reaseguradas de primer nivel en el mundo, lo que brinda un respaldo riguroso y de alta fortaleza para la cobertura de seguros.

3.2. Filosofía organizacional

SECREX mantiene una filosofía de servicio orientada a ofrecer productos de calidad para sus clientes. La misión de la compañía establece la siguiente declaración: “Brindar protección a los asegurados, otorgando coberturas de crédito y caución en condiciones adecuadas y económicamente ventajosas, buscando fortalecer nuestra solvencia y solidez” (SECREX, 2022)

La visión y expectativa de largo plazo es “ser reconocida como líder referente en el mercado asegurador, en los ramos de seguros de crédito y caución, con criterios de crecimiento, rentabilidad, innovación, diversificación y calidad de la gestión” (SECREX, 2022)

SECREX, posee una cultura empresarial orientada al actuar prudente y cumpliendo buenas prácticas de control interno y adecuados lineamientos de un buen gobierno corporativo. La gestión de SECREX se basa en una adecuada política de suscripción, una política de inversiones ajustada a controles de riesgo y a un proceso contractual altamente formal con reaseguradores internacionales de primer nivel.

La cultura de SECREX, además permite una rápida y adecuada adaptación al entorno de negocios en constante cambio, lo que apoya a seguir capitalizando oportunidades de negocio en más grandes y complejos mercados, y también mitigar los riesgos de un entorno volátil y de mayor competencia.

3.3. Diseño organizacional

La Compañía está habilitada para operar en el sistema asegurador peruano, la Superintendencia mantiene la autorización para la prestación y oferta de seguros de crédito y de caución.

SECREX es una empresa que mantiene una organización empresarial basada en principios de buen gobierno corporativo.

El Directorio de la compañía está conformado por profesionales con experiencia y amplios conocimientos del sistema de seguros, finanzas, riesgos y entendimiento de los productos técnicos. A marzo de 2023, el Directorio está conformado por 6 miembros, 3 de los cuales son miembros independientes y 3 de ellos son nombrados por la casa matriz. En este punto cabe mencionar la importancia de la equidad de género puesto que el 50% de los integrantes del Directorio, son damas.

El Directorio tiene como responsabilidad principal la dirección y definición de la estrategia, políticas y procedimientos para el desarrollo de las actividades del negocio en un marco de actuación asociado con el perfil de riesgo que se pueda asumir.

La Gerencia General es nombrada por el Directorio y es responsable de la implementación y seguimiento de la estrategia, los planes operativos y las actividades conducentes a mantener los resultados económicos, financieros y de rentabilidad esperados por la compañía.

El equipo gerencial de la compañía está integrado por profesionales de amplia experiencia, cumpliendo los criterios de idoneidad profesional, académica, económica exigidos por el ente regulador, y se encuentra compuesto de las siguientes gerencias:

a) La Gerencia de Administración y Finanzas: Encargada de la gestión administrativa, contable y financiera de la compañía. Tiene a su cargo los procesos logísticos, de personal, tesorería y administración integral de la empresa.

b) La Gerencia Técnica: Encargada de los procesos para la actividad nuclear de la compañía que es la venta de seguros. Se encarga de la suscripción, emisión, seguimiento y atención de siniestros y recuperaciones.

c) La Gerencia Comercial: Responsable de la venta, prospección y marketing de los productos de la compañía.

d) La Gerencia de Asesoría Jurídica: Responsable de la atención legal, revisiones contractuales, cumplimiento normativo y atención de todo el marco jurídico ante los diferentes grupos de interés.

e) La Gerencia de Riesgos: Responsable de la identificación, evaluación, tratamiento y reporte de los niveles de exposición de riesgo que enfrenta la compañía.

Todos los equipos en la estructura organizacional tienen una contraparte global en CESCE España, por lo cual se desarrollan actividades de manera matricial siguiendo las políticas y estándares de todo el grupo empresarial.

La compañía mantiene una estructura formal, cumple con las obligaciones laborales, asistenciales y previsionales de todo su personal. Cumple con sus obligaciones de reporte y entrega de información requerida por las entidades supervisoras. Adicionalmente a los aspectos formales, SECREX participa en actividades de índole social como parte de su programa de responsabilidad social corporativa, promueve el ahorro energético de agua y electricidad y a nivel de equidad promueve la contratación equilibrada de damas y caballeros.

3.4. Productos y servicios

SECREX ofrece a sus clientes una cartera de productos diversificados enmarcados en dos grandes grupos de negocio, los seguros de crédito y los seguros de caución.

Un seguro de crédito es una cobertura ofrecida por la compañía de seguros a sus clientes cuando venden productos al crédito, a sus propios clientes. Si esas terceras empresas no pagan por la mercadería adquirida al crédito, SECREX cubre hasta por un valor del 93% de la factura impaga. Por ejemplo, SECREX mantiene una póliza de seguro de crédito con su cliente LLANTAS PERÚ que ha vendido 500 llantas a 5 clientes a razón de 100 llantas a cada uno; en el caso que uno de esos 5 clientes no cumpla con pagar a LLANTAS PERÚ, SECREX cubre ese impago.

Un seguro de caución es una garantía ofrecida por una compañía de seguros a sus clientes, quienes son responsables por ejecutar una acción de hacer (realizar una obra, cumplir con una obligación), o de dar (realizar un pago, cumplir con una obligación dineraria). Cuando el cliente de la compañía de seguros no completa o no cumple con su obligación contractual, la compañía de seguros paga el monto garantizado al beneficiario de la póliza. Un ejemplo sería el siguiente: Si la compañía de seguros tiene un cliente que es responsable de realizar una obra para un gobierno municipal, en el caso que dicho cliente no realice la obra, la compañía de seguros pagará al gobierno municipal el monto de la garantía.

En esa línea de productos, SECREX ofrece al mercado las siguientes modalidades de seguro:

a) Seguro de crédito a la exportación: Es un seguro de crédito donde se otorga cobertura para clientes que venden a crédito a clientes fuera del país.

b) Seguro de crédito interno: Es un seguro de crédito donde se otorga

cobertura para clientes que venden a crédito a clientes dentro del país.

c) Seguro de caución para obras privadas: Es un seguro de caución donde se otorga cobertura por la ejecución de obras contratadas entre dos entidades privadas.

d) Seguro de caución para obras públicas: Es un seguro de caución donde se otorga cobertura por la ejecución de obras contratadas bajo el alcance de la ley de contrataciones del estado peruano. En este seguro el beneficiario es una institución pública.

e) Seguro de caución para servicios y suministros: Es un seguro de caución donde se otorga cobertura por la entrega de suministros o por la prestación de algún servicio. En este seguro el beneficiario es una institución pública.

f) Seguro de caución para Fondo Mivivienda: Es un seguro de caución donde se otorga cobertura por la ejecución de obras asociadas a los programas de vivienda del estado peruano pero que son canalizadas a través del Fondo Mivivienda.

g) Seguro de caución para cumplimiento de obligaciones del titular de autorización de casinos o máquinas tragamonedas: Es un seguro de caución a través del cual se brinda cobertura para el cumplimiento de las obligaciones de las empresas de casino, principalmente el pago de los premios y la calidad de las máquinas.

h) Seguro de caución para importación temporal para reexportación: Es un

seguro de caución a través del cual se brinda cobertura para el cumplimiento de las obligaciones de las empresas que importan mercadería de manera temporal y que luego deban reexportarla fuera del país.

i) Seguro de caución para obtención y redención de notas de crédito negociable: Es un seguro de caución a través del cual se brinda cobertura para el cumplimiento de las obligaciones de devolución del saldo a favor materia de beneficio de las empresas exportadoras.

j) Seguro de caución para restitución de derechos arancelarios: Es un seguro de caución a través del cual se brinda cobertura para el cumplimiento de la deuda aduanera por derechos arancelarios.

k) Seguro de caución para régimen suspensivo y tránsito de mercancías: Es un seguro de caución a través del cual se brinda cobertura para el cumplimiento de deuda aduanera para estos regímenes.

l) Seguro de caución para agencias marítimas, fluviales y lacustres: Es un seguro de caución a través del cual se brinda cobertura para el cumplimiento de obligaciones tributarias y aduaneras de este tipo de empresas.

m) Seguro de caución para almacenes y depósitos aduaneros: Es un seguro de caución a través del cual se brinda cobertura para el cumplimiento de obligaciones tributarias y aduaneras de los almacenes y depósitos aduaneros tanto a nivel operativo como a nivel de exigencias aduaneras.

n) Seguro de caución para agencias de aduana: Es un seguro de caución a través del cual se brinda cobertura para el cumplimiento de obligaciones

tributarias y aduaneras de las agencias de aduana en la parte administrativa.

o) Seguro de caución para agentes de carga internacional: Es un seguro de caución a través del cual se brinda cobertura para el cumplimiento de obligaciones tributarias y aduaneras de las empresas de carga.

p) Seguro de caución para empresas de servicio de entrega rápida: Es un seguro de caución a través del cual se brinda cobertura para el cumplimiento de obligaciones tributarias y aduaneras de las empresas de entrega rápida de mercancías.

Todos los productos que ofrece SECREX se encuentran registrados y autorizados para su comercialización en la Superintendencia, esto brinda un respaldo para los contratantes de seguro, así como para los beneficiarios que están cubiertos por las pólizas que se emiten.

3.5. Diagnóstico organizacional

El diagnóstico empresarial que se ha realizado a SECREX, comprende dos frentes. En el primero se muestra el diagnóstico general de la compañía el mismo que se ha realizado aplicando la metodología para la elaboración del Plan Estratégico. En el capítulo 4.1 se muestra el resultado del análisis interno y externo.

El segundo frente será el diagnóstico aplicable al alcance de la compañía en relación con el nivel de cumplimiento de las buenas prácticas en gestión de seguridad de la información y la ciberseguridad, así como el nivel actual de las actividades para

dar cumplimiento a las exigencias establecidas en la normativa de la Superintendencia. De igual modo en el capítulo 4.1 se muestra dicho diagnóstico.

3.6. Propósito de la compañía

SECREX mantiene cifras que lo posicionan como líder referente en el sector del mercado donde realiza sus actividades comerciales (seguros de caución y de crédito). Por ende, la implementación de proyectos, productos y actividades que recogen estándares y buenas prácticas internacionales resulta relevante para mantener una adecuada reputación y reconocimiento tanto de sus grupos de interés como de las entidades supervisoras.

Una de las expectativas fundamentales para la compañía es garantizar y ofrecer una plataforma de información segura y confiable para sus contrapartes, considerando que la mayoría de los beneficiarios de los seguros ofertados por la compañía corresponden a entidades públicas y gubernamentales. En ese sentido el proveer servicios que mantienen una adecuada gestión de la información es relevante para su reputación, su confiabilidad y la aceptación permanente que requiere tener respecto a los organismos de supervisión y con las entidades que son aseguradas.

En esta investigación participan funcionarios especializados de más alto nivel, el espónsor principal de un plan estratégico es el Directorio quien tiene además la responsabilidad explícita de dirigir y establecer la política de gestión de riesgos y seguridad de la información.

El Gerente General a su vez tiene la responsabilidad de implementar la política general y para ello ha desplegado la responsabilidad en la Gerencia Administrativa, la

Unidad de Riesgos, el área de Sistemas y la participación del resto de áreas y gerencias como proveedores y evaluadores de la información en el ámbito que les corresponde.

Capítulo IV Resultados

4.1. Diagnóstico Interno y Externo

Se recoge a continuación el diagnóstico interno y externo de la compañía considerando aplicar la matriz FODA conforme la metodología aplicable:

4.1.1. Fortalezas

Una de las principales fortalezas de la Compañía es contar con personal calificado y que cuenta con una alta experiencia en el manejo de seguros de caución y crédito, lo que a su vez es una ventaja competitiva respecto a las demás aseguradoras.

Asimismo, se considera como fortaleza el haber fidelizado a una importante cartera de clientes, con resultados favorables, permitiendo mejorar la solidez y solvencia financiera de la Compañía.

Otro aspecto importante es que SECREX es parte del grupo internacional CESCE, una de las principales compañías de seguro a nivel mundial.

SECREX cuenta además con reaseguradores de primer nivel, con alta capacidad y rating internacional de grado de inversión y capacidad de respaldo de seguro.

Las clasificadoras locales le dan a SECREX una clasificación de nivel A, lo que es considerado como alta capacidad para cubrir sus obligaciones técnicas y con un nivel de riesgo muy bajo.

La compañía cuenta a su vez con una alta cartera de depósitos en garantía, mitigantes directos para la cobertura de seguro, los depósitos en garantía permiten cubrir los casos en los que la compañía debe pagar los siniestros.

SECREX mantiene una importante relación con su fuerza de ventas externa entre las que destacan más de cien corredores y promotores de seguro.

La compañía mantiene una adecuada gestión de riesgos de inversión y de operaciones técnicas, generando una rentabilidad calzada con el riesgo.

En la Tabla 4, se presentan las fortalezas de la compañía.

Tabla 4

Fortalezas de la compañía SECREX

Fortalezas
Formar parte del Grupo CESCE - Respaldo Internacional
Reaseguradores de primer nivel, con capacidades altas respecto al mercado.
Rentabilidad, solvencia económica y solidez patrimonial
Clasificación de Riesgo A
Amplia cartera en garantías
Adecuada interacción con el Canal Agentes y Corredores
Adecuada gestión de riesgos de inversión y de operaciones técnicas
Personal calificado y con experiencia en los ramos de seguros de crédito y caución.

Nota: Elaboración propia

4.1.2. Oportunidades

Del análisis de la compañía se pueden recoger las siguientes oportunidades:

Un ritmo importante de crecimiento de la cartera de producción de primas en los últimos años, en ambos productos comercializados por la empresa.

La presencia del grupo empresarial CESCE a nivel internacional lo que permite la gestión y venta de seguros a clientes internacionales y de posicionamiento global.

SECREX ha recuperado en los últimos dos años, el primer lugar en producción de seguros de caución en el mercado peruano lo que le brinda un respaldo importante para la venta directa con clientes.

El sector construcción mantiene un nivel de continuidad en la inversión pese a los contratiempos económicos del mercado, se han desarrollado proyectos de inversión, mejora, corrección y atención de emergencias lo que es una oportunidad para un mercado en crecimiento.

La consolidación de las autoridades locales y regionales que han ingresado al espectro político nacional y que tendrá una cartera de obras importantes para los siguientes años.

El sistema financiero, el cual es un competidor indirecto, ya que también emite fianzas, ha tenido una disminución en la participación del mercado. Este aspecto es recogido por las compañías de seguro.

En la Tabla 5, se presentan las oportunidades de la compañía.

Tabla 5

Oportunidades de la compañía SECREX

Oportunidades
Crecimiento de la cartera de clientes en ramos de Crédito y caución
Presencia Internacional de Grupo CESCE que permite gestionar clientes Globales
Recuperación de liderazgo en el ramo de caución e incremento en la cuota de mercado en el ramo de crédito
Continuidad de inversión en obras públicas para reducir la brecha de infraestructura.
Desarrollo de proyectos de reconstrucción nacional y crecimiento del sector construcción en los últimos meses
Consolidación de los gobiernos regionales y locales para los siguientes años y la consecuente ejecución de obras.
Disminución de participación de emisión por parte del sistema financiero
Sólida posición en el mercado asegurador

Nota: Elaboración propia

4.1.3. Debilidades

Se ha recogido el análisis de las debilidades de la compañía, las mismas que se muestran a continuación:

El crecimiento en la producción y el aumento de las primas emitidas ha generado una recarga importante, que no se ha cubierto, en la parte operativa y técnica.

La compañía tiene un limitado acceso a instrumentos de inversión dado que es un mercado pequeño y hay poco análisis en la expectativa de inversiones más allá de las tradicionales.

En lo que respecta a la planta de recursos humanos, se ha identificado debilidades en la atención de cuellos de botella generados por el aumento de la carga operativa en las actividades de la empresa.

La compañía no cuenta con una amplia red de oficinas, cuenta únicamente con posicionamiento en las ciudades de Arequipa y Trujillo, recientemente ha consolidado una nueva oficina en Huancayo.

Existe retraso en la implementación de nuevos aplicativos y herramientas para las operaciones core de negocios lo que perjudica la labor operativa y de comercialización.

En la Tabla 6, se presentan las debilidades de la compañía.

Tabla 6

Debilidades de la compañía SECREX

Debilidades
Recarga operativa por incremento de operaciones
Limitado acceso a instrumentos de inversión en el mercado local por el bajo monto demandado.
Recursos humanos y técnicos insuficientes para atender el mayor crecimiento proyectado y la consecuente mayor carga operativa
Ausencia de red a nivel nacional
Retraso en implantación de nuevos sistemas integrados de gestión y contable.

Nota: Elaboración propia

4.1.4. Amenazas

A continuación, se muestra el análisis de las amenazas recogido en la compañía SECREX.

La situación económica a nivel global, la misma que genera incertidumbre en el tema de inflación, precios internacionales y crisis energética lo que puede afectar al sector.

Ingreso de nuevos competidores a un mercado creciente lo que puede afectar la producción y generar caída en la participación, en el último año han ingresado dos nuevos competidores al mercado.

Excesiva y mayor regulación por parte del organismo supervisor (SBS) en lo que respecta a mayores controles y exigencias normativas lo que genera afectación a la parte operativa por dedicación y atención de estos.

Contracción del sector construcción debido a crisis económico, social y política.

En los últimos meses se ha identificado en el mercado, la aparición de fianzas falsificadas, a través de serias y muy elaboradas mafias que ofrecen fianzas falsas a entidades lo que afecta la reputación y los productos.

Se han iniciado acciones judiciales de investigación fiscal a clientes constructoras que puede afectar la reputación de la compañía considerando que algunas empresas son clientes.

Existe una permanente exposición a cambios en la legislación de la ley de contrataciones del estado debido al ambiente político que es vulnerable.

En la Tabla 7, se presentan las amenazas a la compañía.

Tabla 7

Amenazas a la compañía SECREX

Amenazas
Contracción de la economía y crisis mundial por incremento de la inflación, guerras y crisis energética
Pérdida de participación de mercado por el ingreso de nuevos competidores o por estrategias agresivas de mayor riesgo en el ramo de caución y de seguro de crédito.
Nuevas regulaciones de organismos de control que incrementen la carga operativa así como las exigencias de solvencia y patrimonio
Crisis político social que puede generar contracción del sector construcción
Situaciones de fraude y falsificación de pólizas que pueden afectar la operativa y reputación.
Inclusión de clientes en procesos de investigación que detengan la ejecución de obras y puedan poner en riesgo la liquidez de la compañía al cubrir eventos inesperados.
Distorsión en el mercado por emisión de documentos no autorizados a empresas de seguro
Posibilidad de cambios en la legislación

Nota: Elaboración propia

4.2. Diseño o rediseño de la filosofía organizacional

Tomando en consideración que la filosofía de la compañía está orientada a ofrecer productos de calidad a sus clientes. El plan estratégico para la seguridad de la información y la ciberseguridad permitirá que se robustezca la posición de

administración de información de la compañía, el cuidado de la información, los mecanismos de seguridad y el despliegue de las estrategias planteadas en la presente investigación incrementarán la filosofía empresarial.

Sabido es que una empresa es medida por los resultados a sus clientes y beneficiarios, entonces la implementación de las prácticas a través de la ejecución de actividades enmarcadas en un plan estratégico coadyuvará a que la perspectiva de la compañía sea más sólida y confiable. Por tanto, lo que busca el plan estratégico es reforzar la filosofía empresarial.

El diseño de la filosofía organizacional se debe enmarcar en los alcances del plan estratégico materia de esta investigación, es decir a las actividades de rediseño orientadas a cubrir la seguridad de la información y la ciberseguridad en SECREX.

En primer lugar, se planteará establecer un marco de actuación base para la gestión de seguridad de la información y la ciberseguridad que analice y verifique la aplicación de las exigencias establecidas en la normativa de la SBS.

En línea con lo indicado, la compañía deberá establecer un sistema de gestión de seguridad de la información y ciberseguridad en función al tamaño de la organización, su naturaleza y la complejidad de sus operaciones. Además, incorporará lo establecido en el marco regulatorio vigente que exige determinar periódicamente la proporcionalidad de la exigencia normativa.

Para ello, deberá realizar la siguiente evaluación en cada periodo anual la misma que debe estar aprobada por el Directorio de la compañía:

a) Recopilar el volumen de activos de los tres (3) últimos ejercicios anuales
b) Determinar el promedio de dichos volúmenes de activos
c) Evaluar si el promedio es mayor a S/ 450 millones. De ser así, la proporcionalidad estará comprendida en el régimen general, de lo contrario en el régimen simplificado.

Como base para la determinación de la proporcionalidad, se muestra la aplicación para el año 2022 la misma que deberá aplicarse, como se indica, de manera anual.

Figura 3

Determinación de proporcionalidad

Año	Ejercicios considerados	Volumen de activos	Promedio	Evaluación y determinación	Fecha de informe a Comité
2022	2019	111,598,968.81	147,733,195.94	Monto promedio menor a S/ 450 millones corresponde **régimen simplificado**	Febrero 2022, informado en sesión de Comité
	2020	162,878,006.33			
	2021	168,722,612.67			
	2022	194,076,824.74			

Nota: Elaboración propia con datos de la SBS

4.3. Formulación de estrategias

Dentro del marco de actuación, se plantean las diferentes estrategias a seguir a fin de mantener un sistema de gestión de seguridad de la información y la ciberseguridad robusto, razonable y que le permita a la compañía cumplir con los lineamientos y exigencias normativos.

4.3.1. Identificación de la información para la operación

En esta estrategia, la compañía deberá elaborar y mantener actualizado el registro de la información y activos de información distintos a la infraestructura tecnológica que utiliza para realizar las actividades. Cada unidad organizativa deberá identificar cuatro tipos de datos:

a) Información necesaria que se requiera para el desarrollo de las funciones (información recibida).
b) Información que el usuario va a procesar o haya procesado y mantiene física o lógicamente en el desarrollo de sus actividades
c) Información necesaria para cumplir con obligaciones normativas.
d) Aplicativos, sistemas o recursos informáticos lógicos que necesita para desarrollar sus actividades

Para desarrollar esta estrategia, la compañía deberá hacer uso de las plantillas para identificar la información para la operación. A continuación, se muestran las tablas que deben llenar y completar las diferentes áreas de la compañía y un ejemplo de llenado con un primer recojo de información aplicable a una de las áreas que sirve de base para completar esta estrategia.

Tabla 8

Información necesaria para el desarrollo de las funciones

#	Área	Nombre	Tipo de fuente (interna/externa)	Tipo de información	Descripción de la información	Fuente u origen	Importancia	Clasificación

Tabla 9

Información necesaria para el desarrollo de las funciones – muestra

#	Área	Nombre	Tipo de fuente (interna/externa)	Tipo de información	Descripción de la información	Fuente u origen	Importancia	Clasificación
1	Area Tecnica	Alisson Elizabeth Tamara Garcia	Externa	Documento lógico	Informacion de los clientes, experiencias, eeff, obras y todo para evaluar las operaciones.	Comercial	Alta	Información restringida
2	Area Tecnica	Ibar Ivan Prieto Desulovich	Externa	Documento físico	Formulario de liberación de garantías	Cliente	Alta	Información confidencial
3	Area Tecnica	Ibar Ivan Prieto Desulovich	Externa	Documento lógico	Estatus del proyecto	Cliente - Contraloria	Alta	Información pública
4	Area Tecnica	Ibar Ivan Prieto Desulovich	Interna	Base de datos	Posición del cliente	Sistema de Gestion	Alta	Información restringida
5	Area Tecnica	Ibar Ivan Prieto Desulovich	Interna	Documento lógico	Confirmación de descarga de fianza	Operaciones	Alta	Información restringida
6	Area Tecnica	Ibar Ivan Prieto Desulovich	Interna	Documento lógico	Confirmación de cobro de cheques	Legal	Alta	Información restringida
7	Area Tecnica	Ibar Ivan Prieto Desulovich	Interna	Documento lógico	Confirmación de envío de fianzas	Operaciones - Contabilidad	Alta	Información restringida

Tabla 10

Información que se ha procesado o mantiene física o lógicamente

#	Área	Nombre	Tipo de información	Ubicación de almacenamiento (físico/lógico)	Descripción de la información	Importancia	Lugar almacenamiento

Tabla 11

Información que se ha procesado o mantiene física o lógicamente - muestra

#	Área	Nombre	Tipo de información	Ubicación de almacenamiento (físico/lógico)	Descripción de la información	Importancia	Lugar almacenamiento
1	Area Tecnica	Alisson Elizabeth Tamara Garcia	Base de datos	Lógico	Registros de actas	Alta	Sistema Tecnico de Gestion
2	Area Tecnica	Ibar Ivan Prieto Desulovich	Documento Lógico	Lógico	Liberación de garantías: correo de aprobación / rechazo / observación	Alta	Correo electronico
3	Area Tecnica	Ibar Ivan Prieto Desulovich	Documento Lógico	Lógico	Informes varios: fondo mi vivienda, seguimiento de operaciones fuera del limite de retención, resumen de casos en fideicomiso o administracion de fondos, reducción de prima	Alta	Carpetas compartidas
4	Area Tecnica	Ibar Ivan Prieto Desulovich	Documento Lógico	Lógico	Compensación de garantías: correo de aprobación	Alta	Correo electronico

Tabla 12

Información necesaria para cumplir obligaciones normativas

#	Área	Nombre	Tipo de información	Descripción de la información	Entidad	Descripción de la obligación

Tabla 13

Información necesaria para cumplir obligaciones normativas – muestra

#	Área	Nombre	Tipo de información	Descripción de la información	Entidad	Descripción de la obligación
1	Area Tecnica	Alisson Elizabeth Tamara Garcia	Documento lógico	Reporte	SBS	Si se cumple con los parametros al momento de registrar las operaciones
2	Area Tecnica	Luis Miguel Goicochea Hernández	Documento lógico	Equifax u otros informes comerciales	Secrex Cesce	Evaluación de riesgos
3	Area Tecnica	Luis Miguel Goicochea Hernández	Documento lógico	Estados financieros de deudores	Secrex Cesce	Evaluación de riesgos
4	Area Tecnica	Luis Miguel Goicochea Hernández	Documento lógico	Cesnet/Acuario	Secrex Cesce	Evaluación de riesgos
5	Area Tecnica	Claudia Pacheco Vasi	Documento lógico	Sistema de gestión	SBS	Data del sistema Gestión para preparar Anexo correspondiente a Resolución 19514 y 26528

Tabla 14

Aplicativos, sistemas, recursos informáticos para realizar actividades

#	Área	Nombre	Nombre del app, sistema o recurso informático	Descripción de las principales funcionalidades que utiliza en el recurso	Indique quien le brinda soporte o atención del app	Importancia

Tabla 15

Aplicativos, sistemas, recursos informáticos para realizar actividades – muestra

#	Área	Nombre	Nombre del app, sistema o recurso informático	Descripción de las principales funcionalidades que utiliza en el recurso	Indique quien le brinda soporte o atención del app	Importancia
1	Area Tecnica	Alisson Elizabeth Tamara Garcia	Sistema Tecnico de Gestion	Registro de actas	Sistemas	Alta
2	Area Tecnica	Alisson Elizabeth Tamara Garcia	CESNET	Revisión de techos	Sistemas	Alta
3	Area Tecnica	Alisson Elizabeth Tamara Garcia	Carpeta Interna L	la la información de las operaciones a rev	Comercial	Alta
4	Area Tecnica	Ibar Ivan Prieto Desulovich	Sistema Tecnico de Gestion	Liberaciones, compensaciones	Sistemas	Alta

El llenado de estas tablas y archivos deberá ser realizado por cada unidad de negocio de la compañía y además actualizarse y revisarse cuando menos una vez al año o cuando se presenten cambios importantes en la información. La Unidad de Riesgos o la Unidad de Sistemas serán responsables de dicho seguimiento.

4.3.2. Identificación de dispositivos, infraestructura tecnológica y software

En esta estrategia, la compañía deberá elaborar y mantener actualizado el inventario de todos los recursos, dispositivos y equipos asociados con la seguridad de la información, la ciberseguridad y los activos que dan soporte a estas actividades.

Se deberá identificar los activos tecnológicos, software, infraestructura y dispositivos que se conecten a la red interna.

Para el despliegue y ejecución de esta estrategia, deberá aplicarse la matriz de identificación mostrada en la siguiente tabla donde además se muestra una tabla adicional con un modelo de recojo de algunos activos iniciales.

Tabla 16

Matriz de activos de tecnología y red

N°	Categoría del activo	Activo Descripción	Cantidad	Clasificación (Ver tabla 2)	Propietario del Activo	Criticidad	Estado

Tabla 17

Matriz de activos de tecnología y red – muestra

N°	Categoría del activo	Activo Descripción	Cantidad	Clasificación (Ver tabla 2)	Propietario del Activo	Criticidad	Estado
1	Servidor	Servidor Secrex8 (Windows Server 2003)	1	Información confidencial	Hewlett Packard	Alto	Activo
2	Comunicaciones	central telefónica Rainbow Alcatel (en nube)	1	Información restringida	ALE International	Alto	Inactivo
3	Software	firewall fortinet 60e	1	Información confidencial	Fortinet, Inc.	Alto	Activo
4	Red	domain server, active directory, dns, print server	1	Información confidencial	Hewlett Packard	Alto	Activo

El llenado de estas matrices deberá ser realizado por el área de sistemas de la empresa y además actualizarse y revisarse cuando menos una vez al año o cuando se presenten cambios importantes en la información. La Unidad de Riesgos o la Unidad de Sistemas serán responsables de dicho seguimiento.

4.3.3. Identificación de cuentas y permisos a los aplicativos

En esta estrategia, se deberán identificarán las cuentas de usuario y los permisos de accesos habilitados, además de las que poseen privilegios administrativos y mantener el principio de mínimos privilegios otorgados.

En esta etapa, deberá listarse inicialmente los principales aplicativos y sistemas de la compañía, luego revisar la aplicación de roles y perfiles establecidos en las mismas y cruzar dicha información con cada uno de los usuarios (una matriz de usuarios y perfiles).

Determinada la matriz de usuarios y perfiles, cada responsable de unidad en calidad de propietario de la información deberá validar la matriz y realizar las actualizaciones correspondientes dependiendo de cada situación. En este caso, el usuario responsable deberá:

a) Modificar los permisos de los usuarios dependiendo si se han producido cambios en las actividades o funciones.
b) Revocar permisos
c) Incluir nuevos permisos

Para el despliegue y ejecución de esta estrategia, deberá aplicarse en primer lugar la recopilación de usuarios y perfiles de los aplicativos. Para ello, se utilizará la matriz indicada en la siguiente tabla:

Tabla 18

Matriz de usuarios y roles

ID_USUARIO	NOMBRE_USUARIO	SISTEMA	AREA	NOMBRE_ROL	DESCRIPCION_ROL	FECHA_CREACION	ESTADO

Seguidamente, se deberá preparar una matriz de validación para los usuarios cruzando la información de la matriz de usuarios con la matriz de roles de modo que los usuarios validen cada acceso a las herramientas. En este caso, hay que tener en cuenta que el usuario que va a realizar la validación es el propietario o dueño de la información en el aplicativo.

Tabla 19

Matriz de validación de usuarios y roles

Usuario	Areas	Aplicativos base			Aplicativos / Software de negocio														
		Microsoft Windows	Microsoft Office	Browser navegador		SG - ADMINISTRA BROKER	SG - ADMINISTRACION OFERTA POLIZA	SG - ATENCION AL CLIENTE	SG - CONST_GARANTIAS_VIEW	SG - CONSULTA CLIENTES	SG - EJECUTIVO COMERCIAL	SG - FIANZAS_VIG_FECHA	SG - VISUALIZA_BROKER	SG - VISUALIZAR SINIESTROS		Workflow - Atencion Al Cliente	Workflow - Gerente	Workflow - Ejecutivo Comercial	Workflow - Recepcion
A	Comercial	x	x	x				x								x			
B	Comercial	x	x	x			x				x								
C	Comercial	x	x	x				x										x	
D	Comercial	x	x	x		x	x		x		x							x	
E	Comercial	x	x	x		x		x	x		x							x	
F	Comercial	x	x	x				x								x			

El llenado de la matriz de usuarios y roles deberá ser preparado por la Unidad de Riesgos de la empresa. En tanto la matriz de validación deberá ser realizada por cada responsable de aplicativo o área. Ambas matrices deberán actualizarse y revisarse cuando menos una vez al año o cuando se presenten cambios importantes

en la información. La Unidad de Riesgos o la Unidad de Sistemas serán responsables de dicho seguimiento.

4.3.4. Identificación de vulnerabilidades

En esta estrategia, se deberá identificar las vulnerabilidades y amenazas que puedan afectar a la seguridad de información y ciberseguridad; para aquellas que sean críticas, se deberá establecer planes de acción correctivos o mitigantes.

Para realizar la identificación de vulnerabilidades y amenazas, se aplicará la evaluación como escenarios que pueden afectar la seguridad de la información y la ciberseguridad. Para dicho despliegue la compañía aplicará la matriz de vulnerabilidades y amenazas se seguridad que se muestra en la tabla siguiente:

Tabla 20

Matriz de vulnerabilidades

IDENTIFICACIÓN		EVALUACION DE LAS VULNERABILIDADES Y AMENAZAS	ESTADO	
Categoría	**Sub-Categoría**	**Nivel de madurez**	**Estado Actual**	**Acciones por mejorar**
Evaluación de riesgos (V1): La organización entiende el riesgo de ciberseguridad para las operaciones de la organización (incluida la misión, las funciones, la imagen o la reputación), los activos de la organización y las personas.	**V1.1.** Las vulnerabilidades de los activos están identificadas y documentadas			
	V1.2. La inteligencia de amenazas cibernéticas se recibe de foros y fuentes de intercambio de información			
	V1.3. las amenazas, vulnerabilidades, probabilidades e impactos se utilizan para determinar el riesgo			

IDENTIFICACIÓN		EVALUACION DE LAS VULNERABILIDADES Y AMENAZAS	ESTADO	
Categoria	**Sub-Categoria**	**Nivel de madurez**	**Estado Actual**	**Acciones por mejorar**
Evaluación de riesgos (V1): La organización entiende el riesgo de ciberseguridad para las operaciones de la organización (incluida la misión, las funciones, la imagen o la reputación), los activos de la organización y las personas.	**V1.1.** Las vulnerabilidades de los activos están identificadas y documentadas	Nivel 1: Parcial	No se evidencia que se realizan y analizan pruebas de vulnerabilidad en los activos críticos de la organización	- Se debe asegurar que la gestión de vulnerabilidades técnicas sea oportuna definiendo su la frecuencia de aplicación de parches de seguridad para minimizar el riesgo que las vulnerabilidades sean explotadas. - Considerar actualizaciones de firmware y parches de seguridad. - Tener un inventario de activos actualizado y completo para una adecuada gestión de vulnerabilidades técnicas. - Verificar que Se realicen las actualizaciones de manera oportuna
	V1.2. La inteligencia de amenazas cibernéticas se recibe de foros y fuentes de intercambio de información	Nivel 1: Parcial	Están suscrito a una lista de informes de amenazas de la empresa Secure Soft. Reciben notificaciones de Microsoft con respecto a vulnerabilidades.	Se debe considerar estar suscrito para recibir información de una organización de intercambio de información sobre amenazas y vulnerabilidades como por ejemplo FS-ISAC, Kaspersky Threat Intelligence, FireEye iSIGHT Intelligence, entre otros.
	V1.3. las amenazas, vulnerabilidades, probabilidades e impactos se utilizan para determinar el riesgo	Nivel 1: Parcial	Se realiza por procesos la evaluación, no hay una matriz de amenazas y vulnerabilidades. Se ha identificado un escenario de problemas de indisponibilidad de servidores.	La evaluación de riesgos debe identificar las amenazas y vulnerabilidades internas y externas, la probabilidad y el daño potencial asi como los controles existentes para mitigar el riesgo asociado.

El llenado de la matriz de vulnerabilidades debe ser evaluado por la Unidad de Riesgos o por la Unidad de Sistemas. En cada categoría de evaluación existen subcategorías donde se detalla un conjunto de vulnerabilidades. Al respecto, se debe analizar el contexto de la situación actual (en modo descriptivo) y luego en caso de que el nivel de madurez sea distinto a implementado, la compañía deberá establecer un plan de acción para corregir la actividad. El detalle de los planes de acción y el procedimiento para su implementación se detalla en el capítulo 4.4: Diseño de planes de acción.

4.3.5. Establecer un programa de orientación

La estrategia asociada al programa de orientación busca establecer un marco de concienciación, capacidad técnica operativa y conocimiento en los aspectos relacionados con las diversas actividades. Se deberán implementar tareas de formación, inducción, capacitación y orientación a todo el personal relacionado a las prácticas seguras de seguridad de información.

Las actividades podrán realizarse utilizando cualquiera de las siguientes alternativas:

a) Charlas o actividades presenciales
b) Charlas o actividades virtuales
c) Inducciones grabadas
d) Sesiones de trabajo remoto
e) Entrega de material por correo electrónico
f) Comunicaciones recordatorias remitidas por correo electrónico
g) Acceso a recursos compartidos de la casa matriz.

Los temas serán establecidos dentro de los tópicos de seguridad de información.

Se deberá guardar evidencia de la realización de las charlas sea en físico o digital y evaluar el nivel de aprehensión.

4.3.6. Implementación de línea base para sistemas operativos y aplicaciones

En esta estrategia, se establecerán las actividades de seguridad y vigilancia en ciberseguridad para los sistemas operativos y las aplicaciones core del negocio de seguros.

Esta actividad está a cargo del área de sistemas y se completará realizando las siguientes actividades:

a) Vigilancia de servidores y sus sistemas operativos
b) Vigilancia de estaciones de trabajo de los usuarios

c) Vigilancia de equipos de seguridad, red y dispositivos de comunicación

d) Procedimiento de seguimiento de servicios críticos

e) Procedimiento de backup y restauración

Para todos los casos, el área de sistemas debe emitir cada 6 meses un informe de mantenimiento y control de línea base de la plataforma tecnológica.

4.3.7. Evaluación de actividades aplicables a la autenticación reforzada

Para el desarrollo de esta estrategia, se analizarán los recursos informáticos y aplicaciones puestas a disposición de clientes o beneficiarios en las que se evaluarán:

a) Si se pueden generar operaciones fraudulentas

b) Abusos de servicio en perjuicio de clientes

c) Evaluar aplicaciones que impliquen pagos o transferencias de fondos, registros de beneficiarios, modificación de condiciones de producto, contratación de seguros, modificación de límites o condicionados.

En el desarrollo del presente plan estratégico, se ha relevado con las áreas de la compañía, el siguiente análisis respecto a la aplicación de la autenticación reforzada. Cabe indicar que esta estrategia debe ser revisada anualmente.

En la tabla 21, se muestra el esquema de evaluación de la compañía.

Tabla 21

Evaluación de canales y requerimiento de autenticación reforzada

Exigencia Normativa (art 19)	Análisis de las operaciones y servicios realizados en SECREX	Observaciones o anotaciones adicionales	Evaluación
Pagos o transferencias de fondos a terceros	La compañía no ofrece a sus clientes alternativas para pago o transferencia de fondos a terceros, tampoco solicita realizar transferencias por canales que no sean los ofrecidos por el sistema financiero. Nuestra operativa comercial no establece ni exige realizar transacciones o transferencias entre nuestros clientes y terceras personas, empresas o servicios	Los clientes utilizan canales digitales o físicos ofertados por el sistema financiero para transferir fondos a nuestra Compañía, los que cuentan con la autenticación correspondiente ofrecida por dichas instituciones.	No aplicable
Registro de un beneficiario de confianza	La compañía no ofrece a sus clientes alternativas para registrar mediante canales digitales a beneficiarios de confianza, tampoco exige a sus clientes realizar registros por canales digitales. Todas las transacciones en las que se registre beneficiarios de seguro se realizan de manera presencial en nuestras oficinas físicas y presentando la documentación correspondiente.		No aplicable
Modificación de productos se seguro contratados	La compañía no ofrece a sus clientes alternativas digitales para realizar cambios o modificaciones en los productos contratados. Las modificaciones contractuales se realizan de manera coordinada y siguiendo los principios de conducta de mercado.		No aplicable
Modificación de productos de ahorro/inversión contratados	La compañía no comercializa productos de ahorro o inversión, tampoco ofrece seguros que estén asociados a alternativas de ahorro o inversión para sus clientes		No aplicable
Contratación de un producto o servicio	La compañía no ofrece a sus clientes alternativas digitales para contratar un producto o servicio. Toda contratación se realiza mediante la presentación de expedientes de aprobación en las oficinas o mediante correo, pero en todos los casos la contratación se completa con la participación de los ejecutivos o promotores comerciales.		No aplicable
Modificación de límites y condiciones	La compañía no ofrece a sus clientes alternativas digitales para realizar cambios o modificaciones en líneas de garantías o de productos		No aplicable

4.3.8. Programa de Ciberseguridad

La compañía deberá establecer un programa de ciberseguridad que cubra los siguientes servicios en análisis:

a) Para las operaciones o servicios que se brinden a los usuarios por canales digitales.
b) Para los servicios significativos provistos por terceros

Se elaborará un Informe de capacidad de ciberseguridad que será presentado a Directorio con una frecuencia anual.

En relación con esta estrategia, se ha realizado un primer ejercicio de aplicación con la información de la compañía. No obstante, este análisis inicial requiere ser revaluado con frecuencia anual.

Para las operaciones o servicios que se brindan a los usuarios por canales digitales, la compañía realizó un Informe de evaluación de operaciones por canales digitales, donde se evaluaron las operaciones tecnológicas y los canales en las que estas se ejecutan a fin de determinar si alguna de ellas está inmersa en la exigencia normativa de requerir autenticación reforzada.

Tomando en consideración los aspectos indicados en la normativa, relativos a posibles acciones donde se puedan originar operaciones fraudulentas u otro abuso del servicio en perjuicio del cliente, así como en la operativa actual de la compañía, se observó que, en el barrido inicial, no se cuentan con operaciones en canales digitales que puedan requerir el desarrollo de proyectos de autenticación reforzada.

Respecto a los servicios significativos provistos por terceros, en este otro aspecto, de la evaluación realizada, se ha identificado para el año 2022, un total de

13 servicios provistos por terceros que tienen un nivel de riesgo alto por lo que su prestación se considera de carácter significativo. Al respecto, se presenta en la tabla 22 una muestra de dichos servicios, así como la aplicación de los criterios del programa de ciberseguridad aplicable según la exigencia que la compañía requiere evaluar. Esta estrategia debe mantenerse actualizada de manera dinámica por cuanto cada año, los proveedores de la compañía cambian, se actualizan, concluyen servicios o prestaciones lo que lo convierten en un trabajo que requiere actualización dinámica y permanente.

Tabla 22

Evaluación del programa de ciberseguridad

CRITERIOS DEL PROGRAMA DE CIBERSEGURIDAD - 2022					
Proveedor	**Activos de información**	**Esquema de protección ante amenazas**	**Detección de incidentes de ciberseguridad**	**Respuesta con medidas de mitigación**	**Recuperación de capacidades**
BBVA Continental - recaudación	Transferencias, ordenes de pago, cobro de garantías, pago de primas	BBVA es el segundo banco más importante del Perú, se encuentra regulado por la SBS y dadas las características de su entorno empresarial (grupo económico, tipo de empresa, robustez empresarial, etc) se desprende que su esquema de continuidad de negocios y seguridad de información permite garantizar la atención a amenazas externas.	No se han presentado durante el año	No se han presentado durante el año	No se han presentado durante el año
BCP - Recaudación	Transferencias, ordenes de pago, cobro de garantías, pago de primas	BCP es el principal banco del Perú, se encuentra regulado por la SBS y dadas las características de su entorno empresarial (grupo económico, tipo de empresa, robustez empresarial, etc) se desprende que su esquema de continuidad de negocios y seguridad de información permite garantizar la atención a amenazas externas.	No se han presentado durante el año	No se han presentado durante el año	No se han presentado durante el año
Bloomberg	Precios Bloomberg, Información de mercado de instrumentos	Bloomberg ofrece como alternativa de contingencia a su servicio, la posibilidad de utilizar las funcionalidades de bloomberg en modo web sin usar la terminal habilitado o si no se tiene acceso a ella. Bloomberg es un proveedor internacional por lo que se desprende también un esquema de atención robusto.	No se han presentado durante el año	No se han presentado durante el año	No se han presentado durante el año
Century Link (Level 3)	Red de fibra óptica para salida a internet (dual)	Century Link consiguió la certificación de ISO 20000, permitiendo obtener servicios bien planificados, diseñados, administrados y entregados. En definitiva, solo mediante una gestión de servicios de TI de alta calidad evitaremos que los proyectos de TI tengan fallos reiterados o rebasan el presupuesto por costes mal calculados difíciles de administrar y que nos pueden conducir a un fracaso en el negocio.	No se han presentado durante el año	No se han presentado durante el año	No se han presentado durante el año

4.3.9. Estrategias complementarias

Considerando las buenas prácticas internacionales para la gestión de la seguridad de la información y la ciberseguridad, y de manera adicional a las estrategas presentadas previamente, el presente plan estratégico considera prudente y necesario establecer un conjunto adicional de estrategias complementarias:

a) **Control de accesos**: La compañía deberá aplicar un procedimiento formal de control de accesos para los usuarios. Para ello, deberán seguirse las siguientes políticas de seguridad:

1. Se prohíbe todo derecho, acceso y privilegio sobre los servicios informáticos en tanto no tengan una autorización.

2. Los identificadores de usuarios deben cumplir lo siguiente:
   - El nombre de usuario debe estar formado por el nombre del usuario más las primeras letras de sus apellidos paterno y materno. En caso de repetición, se agregarán identificadores individuales como la primera letra del segundo nombre
   - El identificador es válido durante su periodo laboral.

3. El usuario tendrá como máximo tres (3) intentos para ingresar / digitar correctamente su contraseña para el acceso a la red. En caso exceda dichos intentos, la cuenta deberá bloquearse de manera automática.

4. Las contraseñas de los usuarios deben ser iguales o mayores de 8

caracteres alfanuméricos (letras, números y uso de mayúsculas minúsculas).

5. Las contraseñas de acceso a la red deben modificarse dentro de un periodo que no exceda los 90 días. El cambio de la contraseña es obligatorio y no podrán utilizarse las 5 últimas contraseñas anteriormente ingresadas. Los usuarios deberán de cambiar las contraseñas en el plazo determinado, en caso expire y el usuario tendrá 5 operaciones adicionales para realizar el cambio.

6. No debe otorgarse una cuenta de usuario ni privilegios para utilizar las computadoras o los sistemas de información de la Compañía, a las personas que no tengan vínculo laboral con la Compañía a menos que se obtenga la autorización escrita del Gerente General.

7. El usuario deberá bloquear manualmente el acceso a su computadora cuando abandone temporalmente su zona de trabajo. El bloqueo de pantalla automático debe ser programado a los 5 minutos de inactividad.

8. El usuario deberá bloquear manualmente el acceso a su computadora cuando abandone temporalmente su zona de trabajo. El bloqueo de pantalla automático debe ser programado a los 5 minutos de inactividad.

b) **Seguridad del personal**: La compañía deberá aplicar los siguientes controles para la seguridad del personal, así como aplicar las siguientes políticas:

1. Todos los colaboradores deberán cumplir con la normativa establecida para la seguridad de la información, el desconocimiento no exime de responsabilidades.

2. La compañía debe establecer los roles, responsabilidades y funciones de cada colaborador a efecto que se determine los alcances sobre la información que le será asignada y con la cual desarrollará sus tareas.
3. Esa asignación se incorpora en el Manual de Organización y Funciones de la Compañía.

4. Las personas que trabajan en la compañía sean cual fuere su modalidad de trabajo, deberán hacer uso adecuado de los activos de información asignados.

5. El personal externo, outsourcing o terceros deberán cumplir con la normativa que la compañía establezca.

6. Durante la selección de personal, la compañía debe realizar las comprobaciones necesarias sobre la veracidad de la información brindada.

7. Las personas que trabajan o brindan sus servicios a la compañía

deberán firmar los acuerdos de confidencialidad de información, así como de autorización de tratamiento de información laboral que se requiera.

8. Los activos de información entregadas a cada colaborador deberán ser devueltos al momento de la finalización del vínculo laboral, salvo deterioro, renovación o cambio que debe ser registrado.

9. Todo el personal deberá participar en las actividades de concienciación que la compañía programe.

c) **Procedimientos de respaldo y restauración**: La compañía deberá aplicar los siguientes controles para almacén y backup de la información, los procedimientos de restauración de ser el caso, así como aplicar las siguientes políticas:

1. La Compañía debe implementar un procedimiento formal para el respaldo y recuperación de la información. Los procedimientos de respaldo y recuperación deberán ser coherentes con la estrategia de continuidad de la empresa.

2. La Compañía ha establecido una estrategia de almacenamiento de información, recursos, datos y bases de datos de manera diaria como frecuencia global de almacenamiento de información.

3. Los medios de respaldo deberán ser almacenados en ambientes adecuados conforme las especificaciones de los fabricantes. Se debe

probar regularmente su funcionalidad.

4. Se deberá comprobar y probar regularmente los procedimientos de recuperación para asegurar que son eficaces y que pueden cumplirse en el tiempo establecido.

5. Los respaldos deberán estar almacenado en una locación a distancia suficiente para escapar de cualquier daño en el local principal o en espacios de la nube con las debidas medidas de seguridad.

6. Todo acceso a los dispositivos de almacenamiento debe ser gestionado por el Departamento de Sistemas.

7. Toda la información de la compañía deberá por defecto gestionarse en las carpetas de red, en este caso, las copias serán diarias y de manera automática.

d) **Gestión de incidentes**: La compañía deberá aplicar los siguientes controles para atender los incidentes asociados a seguridad de la información, así como aplicar las siguientes políticas:

1. Todos los colaboradores están obligados a reportar al Departamento de Sistemas o a la Unidad de Riesgos, los incidentes o vulnerabilidades de seguridad identificados o asociados a cualquier activo de información de la Compañía.

2. El Departamento de Sistemas coordinara con las áreas involucradas

las medias que permitan dar una respuesta adecuada a los incidentes y vulnerabilidades de seguridad que hayan sido reportados.

3. Todo incidente originado intencionalmente o reincidente será elevado a la Unidad de Riesgos para que defina las medidas disciplinarias pertinentes según lo establecido en el Reglamento Interno de Trabajo de la Compañía. Las acciones disciplinarias no se limitarán sólo a la pérdida de privilegios de los recursos de procesamiento de información y pueden considerar la cancelación de contratos u otras acciones apropiadas establecidas en dicho Reglamento.

4. En caso el incidente implique una acción legal, se elevará la evidencia al área Legal para que tome las acciones necesarias en la jurisdicción correspondiente.

5. El Departamento de Sistemas tendrá un registro de incidentes de seguridad en hoja Excel el mismo que tendrá información sobre fecha y hora de ocurrencia, usuario que reporta, detalle del incidente, recurso comprometido, así como las acciones tomadas para su seguimiento y solución.

6. Las incidencias menores que no aplican como incidente de seguridad de la información, es decir que no ponen en riesgo la confidencialidad, integridad o disponibilidad de la información, se gestionarán de manera directa sin llevar un registro específico, no obstante, si alguna incidencia menor es repetitiva o constante o le ocurre a más de 5 colaboradores deberá ser incluida en el registro correspondiente.

4.4. Diseño de planes de acción

Con la revisión de la situación de la empresa y analizando las estrategias a seguir en el plan estratégico que permitirá dar cumplimiento a las exigencias establecidas en la normativa de la SBS y la adecuación de buenas prácticas, se proponen los siguientes planes de acción aplicables al seguimiento y cumplimiento de las actividades.

A) Actualizar el nivel de proporcionalidad de la gestión de seguridad de la información de manera anual. Para ello, deberá seguirse el procedimiento de cálculo establecido en la norma.

B) Actualizar de manera anual la información para la operación, completando los cuatro tipos de datos que permiten la identificación total de la información y los activos de información. En este contexto es de importante necesidad que se culmine el primer recojo de información y eventualmente guardar dicha información en un repositorio para que las subsecuentes evaluaciones sean más sencillas de aplicar.

C) Actualiza de manera anual los inventarios de dispositivos, infraestructura tecnológica y software. En este aspecto, dada las condiciones de limitación de personal del área de sistemas indicada en las limitaciones de la investigación, la compañía debería establecer un presupuesto para la actualización de inventario mediante la participación de una empresa externa.

D) Actualizar anualmente la matriz de usuarios y perfiles, considerando que los

movimientos de ingreso, salida, cambio de funciones de los colaboradores de la compañía es bastante dinámica, se requieres actualizar y revisar esta estrategia para mantener ciclos de control de permisos.

E) Respecto a la matriz de vulnerabilidades, es necesario completar dicha matriz y en todos los casos donde se identifique un nivel de madurez menor a la cumplimentación de los controles, se deberá priorizar los más altos (mayor vulnerabilidad) y buscar que se implemente controles para los más relevantes.

F) Sobre el programa de capacitación, realizar las mismas y guardar evidencia de convocatoria, material utilizado, exámenes o controles sobre las materias infundidas. En este sentido, se recomienda utilizar las charlas que periódicamente pueden desarrollarse dentro de la organización para contar con participación masiva.

G) Finalmente, sobre las actividades de autenticación reforzada y el programa de ciberseguridad, se debe realizar actualización anual de los informes.

La recomendación fundamental es que el presente plan estratégico sea un documento vivo y con contenido que sea revisado y actualizado de manera permanente para que cumpla con el objetivo de la adecuación y exigencia normativa y sea buena práctica aplicada por la compañía.

La compañía no ha realizado un análisis de servicios en la nube, esta es una brecha que debe completar para lo cual, se debe aplicar una serie de pasos que incluya:

- Determinar si posee o realiza procesamiento operativo en algún canal en la nube.
- De ser el caso, para cada servicio identificar: la plataforma o servicio contratado, la locación donde reside el servicio y si esta está en nube o no
- Para los casos que estén en la nube: una reseña con la descripción del servicio, cumplimiento de las prácticas internacionales como ISO 27001, HIPAA, HDS; evaluación de redes segregadas; evaluación de logs, capacitación de servicios en la nube; seguimiento de calidad y performance del servicio.

Capítulo V Conclusiones y Sugerencias

5.1. Conclusiones

Finalmente, con relación a los objetivos detallados en el presente trabajo de investigación, se establecen las siguientes conclusiones:

- Se ha establecido el plan estratégico para la gestión de la seguridad de la información y la ciberseguridad en la Compañía SECREX, el mismo que ha considerado el análisis de compañía y el establecimiento de las estrategias y planes de acción conducente a cumplir con las exigencias y requisitos establecidos por la normativa peruana.

- Se ha realizado el diagnóstico situacional en relación con el ambiente interno y externo, el análisis integral de la Compañía y su filosofía, así como el nivel de adecuación que debe cumplir tomando en consideración los parámetros de complejidad y tamaño de operación basado en el tamaño de su patrimonio.

- El Plan Estratégico ha logrado establecer los procedimientos, planes operativos, herramientas a utilizar y metodologías o procesos para poder cumplir con el nivel de adecuación, la compañía ya tiene recogidas y mapeadas las actividades conducentes a mantener un plan dinámico y permanentemente actualizado.

- Finalmente, se han formulado las actividades, la periodicidad y ejecución de

puntos de control para que el plan estratégico sea continuamente actualizado y validado a efecto que mantenga su vigencia de manera permanente.

5.2. Sugerencias metodológicas y en el marco de actuación

En lo que corresponde a sugerencias metodológicas que sean de aplicación, es importante que la compañía permanentemente:

- Revise las prepublicaciones, publicaciones y boletines de las entidades generadoras de buenas prácticas como ISO, Basilea, las asociaciones financieras y de seguros y la SBS en calidad de regulador, a fin de mantener de manera permanente, el seguimiento de las exigencias que se requieren implementar.

- Mantener una revisión, cuando menos anual, de los documentos, procedimientos o manuales que se elaboren para implementar las estrategias de seguridad y ciberseguridad.

- Requerir en las evaluaciones de auditoría y control interno, que se revisen los procedimientos y el marco de actuación de seguridad de la información y la ciberseguridad a fin de determinar posibles brechas o mejoras en la implementación del plan estratégico.

- Para el caso de quienes tienen bajo responsabilidad la implementación y seguimiento de las estrategias como primera línea de defensa, la compañía

debiera establecer un presupuesto especial para capacitación, actualización y mantenimiento permanente de conocimientos.

5.3. Sugerencias operativas y de seguimiento

Por otra parte, respecto a las condicionantes operativas y de seguimiento, la compañía debe:

- Mantener registro de las tablas, matrices y herramientas aplicadas en cada una de las estrategias indicadas, esto para supervisión de auditorías y guardar evidencia de la ejecución.

- Consolidar la participación de las diferentes áreas puesto que la implementación de las estrategias es un trabajo coordinado con participación del personal. La seguridad de la información es un contexto que hoy requiere participación e interiorización.

- En relación con la brecha y limitación detectada en la compañía sobre la poca capacidad operativa y de recursos de la compañía, la misma debe orientar a optimizar los recursos y de ser el caso contratar para algunas revisiones a empresas externas con criterio de objetividad. Los recursos y presupuestos para estas actividades debieran ser gestionados por la Unidad de Sistemas con el debido sustento donde puede apoyarse en la obligatoriedad y exigencia normativa como principal patrón de respaldo. En este caso debe destacar que el incumplimiento en la implementación puede decantar en sanciones o multas regulatorias.

- Finalmente, en lo que respecta a presentación de informes, los mismos deben ser elevados a instancias de toma de decisión relevantes como son la Gerencia General, Comités especializados o el Directorio de la compañía.

De manera general, el seguimiento del plan estratégico debe contar con un conjunto dinámico de control, además es importante recomendar que de haber algún cambio en la parte normativa, de manera forzosa la compañía deberá hacer una actualización de las actividades operativas puesto que el regulador realizará una actualización de sus listas de chequeo de control y la compañía debiera estar al mismo tiempo, actualizando sus procesos de control.

Bibliografía

BACA, G. (2016). Introducción a la seguridad informática. Grupo editorial Patria.

BERTOLIN, J. (2008). Seguridad de la información: redes, informática y sistemas de información. Paraninfo.

CALDER, A. (2009). Information security based en ISO 27001/ISO 27002 a management guide (2nd edition). Wilco.

CHOQUE, R. (2012). Nuevas competencias tecnológicas en información y comunicación (2da edición). Infodem.

DIARIO GESTIÓN (20 de mayo de 2022). *Filtración de datos personales: Reniec informó las acciones tomadas tras denuncia de Asbanc.* https://gestion.pe/peru/filtracion-de-datos-personales-reniec-informo-las-acciones-tomadas-tras-denuncia-de-asbanc-estado-pcm-rmmn-noticia/

GALLO, F. (2011). Inseguridad informática (2da edición). Cooma.

GARCÍA-CERVIGNON, A. & ALEGRE, M. (2011). Seguridad Informática. Paraninfo.

GOMEZ, A. (2014). Enciclopedia de la seguridad informática (2da edición). RAMA editores.

HUIDOBRO, J. & ROLDÁN, D. (2005). Seguridad en redes y sistemas informáticos. Paraninfo.

INTERNATIONAL ORGANIZATION OF STANDARDIZATION. (2018). Information security management systems – Overview. (ISO)

KAMBERG, M. (2018). Ciberseguridad. The Rosen Publishing Group Inc.

MARTIN, I. & ALBERTO, I. (2020). Ciencia de datos para la ciberseguridad. RAMA Editorial.

MIGUEL, J. (2015). Protección de datos y seguridad de la información: guía práctica para ciudadanos y empresas (4ta edición). RAMA Editorial.

MOODY'S (2022). Informe de calificación de riesgo SECREX.

PACIFIC CREDIT RATING (2022). Informe de calificación de riesgo SECREX.

PISTORIOUS, M. (13 de mayo de 2023). La nube y ciberseguridad: guía rápida. https://www.google.com.pe/books/edition/La_Nube_Y_Ciber_Seguridad_Gu%C3%ADa_R%C3%A1pida/1VQ6DwAAQBAJ?hl=es&gbpv=1&dq=seguridad+en+la+nube&printsec=frontcover

PLATINI, M.; DEL PESO, E. & DEL PESO, M. (2008). Auditoría de tecnologías y sistemas de información. RAMA Editorial.

POSTIGO, A. (2020). Seguridad informática. Paraninfo.

PULIDO, N. (2016). Seguridad y ciberseguridad: realidad y práctica del documento electrónico. Universidad de La Salle.

Resolución SBS N.º 504-2021. Reglamento para la gestión de la seguridad de la información y la ciberseguridad (19 de febrero de 2021). Normas Legales, Nº 1929393-1. Diario Oficial El Peruano, 23 de febrero de 2021.

SAINZ, J. (2017). El plan estratégico en la práctica (5ta edición). ESIC

UNIVERSIDAD DE CANTABRIA (12 de mayo de 2023). Metodología para la elaboración del plan. https://web.unican.es/plan-estrategico/anexos/anexo-2-metodologia-para-la-elaboracion-del-plan

VEGA, E. (2021). Seguridad de la Información. España: 3 Ciencias