DISEÑO DE UN PLAN ESTRATÉGICO DE SEGURIDAD DE INFORMACIÓN (PESI) PARA UNA COMPAÑÍA DEL SECTOR ASEGURADOR

TRABAJO DE GRADO

MARISOL LOZANO OLAVE

COD. 9812049299

INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO
FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS
ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN
2017

DISEÑO DE UN PLAN ESTRATÉGICO DE SEGURIDAD DE INFORMACIÓN (PESI) PARA UNA COMPAÑÍA DE SEGUROS

TRABAJO DE GRADO

MARISOL LOZANO OLAVE

COD. 9812049299

Asesor
Alejando Castiblanco Blanco

INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO
FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS
ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN
2017

Nota de aceptación

_____
_____
_____
_____
_____
_____

_____

_____

_____

Firmas de los jurados

Ciudad, Fecha

CONTENIDO

ILUSTRACIONES

TABLAS

INTRODUCCION

La Compañía aseguradora busca afrontar los retos del negocio con una infraestructura digital moderna, robusta y segura, capaz de sacar provecho de la llamada cuarta revolución industrial "La transformación digital". En general, el cambio inexorable desde la simple digitalización (la tercera revolución industrial) a la innovación basada en combinaciones de tecnologías (la cuarta revolución industrial) está obligando a las empresas a reexaminar la forma de hacer negocios. El resultado final, sin embargo, es el mismo: los líderes de negocios y altos ejecutivos necesitan entender su entorno cambiante, desafiar las suposiciones de sus equipos, y sin descanso innovar continuamente, esto significa que el talento, la cultura y las formas de organización tendrá que ser reconsiderada.[1]

Es claro que las Compañías del sector asegurador se encuentran inmersas en medio del desarrollo de la era digital y de las tecnologías, donde se ha transformado la forma de acceder a la información, de desarrollar negocios, y el consumo de tecnologías, requiriendo cada vez más presencia en entornos digitales para ser más competitivos.

Es así como, CapGemini, empresa de consultoría en tecnología y seguridad de la información, ha elaborado una lista con 10 tendencias claves para el sector asegurador en el 2017, entre ellas, cita la "*creación de nuevos productos y servicios por parte de las aseguradoras para dar respuesta a las demandas que propicia la economía colaborativa. Ésta empuja a pólizas más especializadas, más cortas y más personalizadas. Serán más frecuentes los acuerdos de colaboración entre las aseguradoras y las empresas de negocios colaborativos, por ejemplo, para ofrecer seguros de coche por kilómetros recorridos o seguros de vivienda mediante contratos inteligentes"*.

También destaca la "*mayor penetración del Internet de las Cosas (IoT). Las propias aseguradoras incentivarán el uso de dispositivos por parte del consumidor para poder personalizarle su oferta, ayudarle a reducir precios y ampliar los servicios ante reclamaciones. Por ejemplo, con el seguro de vida se incentivará el uso de sensores para monitorizar la salud. Igualmente, las compañías incrementarán el análisis de datos en tiempo real*".

Otra tendencia será la "*mayor aplicación de tecnologías emergentes como los drones —por ejemplo, para recabar información sobre una vivienda tras una catástrofe— y la realidad aumentada —por ejemplo, con fines educativos sobre medidas de seguridad y protocolos*".

Asimismo, indica que la "*inclusión de propuestas móviles y digitales para promover comportamientos más seguros y saludables por parte de los clientes. Por ejemplo,*

[1] http:// www.weforum.org/agenda/2016/01/the-fourth-industrialrevolution-what-it-means-and-how-to-respond.

apps que utilizan gamificación para dejar de fumar y así reducir el coste de un seguro o móviles que comparten consejos a los conductores en determinados escenarios. Se trata de propuestas orientadas a una gestión proactiva del riesgo para reducir los incidentes, que generarán una mayor interacción entre aseguradora y cliente, y generarán datos. Fundamentalmente serán desarrollos de Insurtechs".[2]

Todas estas circunstancias y nuevas tecnológicas, generan gran incertidumbre para la Compañías, tal y como lo señala el informe de Allianz Risk Barometer, causadas por la creciente preocupación sobre los desarrollos políticos, legales y regulatorios alrededor del mundo. Según el Allianz Risk Barometer, la interrupción del negocio resulta la principal preocupación de las empresas debido a que no alcanzan a predecir las pérdidas económicas que podrían generarse producto de cambios políticos, nuevas regulaciones, fugas de información y catástrofes naturales, entre otras variables. Si bien las pérdidas ocasionadas por el cambio climático e incendios son las más temidas, la naturaleza del riesgo está variando hacia eventos que no generan daños materiales pero que sí ocasionan grandes pérdidas, como pueden ser los incidentes cibernéticos o el impacto del terrorismo.[3]

Es importante mencionar, que las Compañías del sector asegurador de Colombia están vigiladas por la Superintendencia Financiera de Colombia (SFC), la cual permanentemente dicta disposiciones para garantizar los tres pilares de la seguridad de la información, por lo que el cumplimiento legal, regulatorio y normativo debe ser una prioridad dentro de la estrategia de seguridad. Igualmente, disposiciones recientes emitidas por la Superintendencia de Industria y Comercio (SIC) en torno a la protección de datos personales, en cuanto a la implementación de controles de seguridad, para garantizar un adecuado tratamiento de los datos personales de clientes, proveedores y empleados.

Para mitigar los impactos que conllevan la materialización de los riesgos de seguridad a los que está expuesta la Compañía debido al uso de las nuevas tecnologías, se hace necesario formular un plan estratégico de seguridad de la información con una proyección a tres (3) años, identificando y priorizando el portafolio de proyectos de seguridad de la información que permitirá contribuir al cumplimiento del logro de los objetivos de negocio, siendo cada vez más competitivos a nivel del sector asegurador a través de la aplicaciones de las nuevas tendencias en tecnologías, estando cada vez más empoderados para ingresar a la nueva era de transformación digital.

OBJETIVO

Identificar el portafolio de proyectos a ser desarrollados por la Compañía Seguros, del periodo comprendido entre los años 2018 al 2020, que permitirá a la

[2] https://www.es.capgemini.com/biblioteca/10-tendencias-para-el-sector-seguros-en-2017%20
[3] https://www.agcs.allianz.com/assets/PDFs/Reports/Allianz_Risk_Barometer_2017_EN.pdf

Organización cumplir con el objetivo de seguridad de la información que es proteger los activos de información de la organización, el plan deberá está alineado con los objetivos estratégicos, la gestión de riesgos empresariales, optimización de recursos, entrega de valor, medición del desempeño y la integración del aseguramiento del proceso.

A continuación, se relacionan los objetivos específicos a cumplir en la elaboración del plan estratégico de seguridad de la información:

- Realizar un diagnóstico de la situación actual de seguridad de la información.
- Desarrollar un análisis que permita priorizar las iniciativas.
- Definir el portafolio de proyectos de seguridad de la información
- Elaborar el plan estratégico de seguridad de la información

ALCANCE

El alcance del proyecto abarca la formulación del Plan estratégico de Seguridad de la Información (PESI) para la Compañía de Seguros, el cual debe estar alineado con los objetivos estratégicos de la Organización, y debe contemplar la identificación del portafolio de proyectos de seguridad de la información con su correspondiente priorización a 3 años. El portafolio de proyectos de seguridad de la información deberá cubrir los aspectos relacionados con gobierno, gestión de riesgos, desarrollo y gestión del programa de seguridad de la información y gestión de incidentes.

1. RESUMEN EJECUTIVO

Actualmente la Compañía aseguradora tiene el propósito de fortalecer su sistema de gestión de seguridad de la información, sin embargo, cree necesario iniciar con la formulación de un Plan Estratégico de Seguridad de la Información (PESI), que se encuentre alineado con el cumplimiento de los objetivos estratégicos del negocio, ya que existen iniciativas aisladas que no permiten articular de manera adecuada los conceptos de gobernabilidad, gestión de riesgos, desarrollo y gestión del programa de seguridad de la información y el cumplimiento de los marcos normativos, legales y regulatorios que existen en materia de seguridad de la información y privacidad de datos personales para el sector financiero, buscando que la organización alcance sus objetivos misionales, dentro de un marco de valores corporativos, transparencia e integridad de la información.

Con respeto a lo indicado, toma relevancia formular un Plan Estratégico de Seguridad de la Información, para que de forma organizada y adecuada se establezcan las iniciativas y proyectos que garanticen el cumplimiento del objetivo de seguridad de la información que es proteger, asegurar y minimizar el daño que

pueda sufrir la Compañía debido a una situación adversa sobre sus activos de información.

La Compañía está expuesta, continuamente a la materialización de los riesgos de Seguridad de la información debido a la criticidad de la información que maneja y la complejidad de los sistemas de información que la procesan y almacenan, que hace que la Compañía sea más sensibles ante cambios e incidentes que se producen en su entorno, y también por eventos que se generan en su interior, por lo que se hace necesario mejorar el nivel de madurez del actual modelo de seguridad de la información a través de la formulación y ejecución de una estratégico de seguridad de la información que apalanque los objetivos del negocio y los intereses de la Compañía.

Aparte de eso, el plan estratégico de seguridad de la información debe contemplar los siguientes lineamientos[4]:

- Tiempo real: Considerar que el factor tiempo es fundamental para la toma de decisiones.
- Adaptativo: Los sistemas de información y la seguridad deben adaptarse a los cambios y necesidades del negocio, favoreciendo y facilitando su ejecución.
- Eficiencia Operacional: Los controles de seguridad deben armonizar y facilitar la operación de la compañía
- Orientado al Cumplimiento: El cumplimiento legal, regulatorio y normativo es una de las entradas a considerar en todo momento, es una realidad en la que actualmente estamos inmersos en un entorno cambiante en ese aspecto.
- Gestión de riesgos: La gestión de riesgos es el pilar fundamental de la seguridad de la información.
- Resiliencia: La resiliencia es la capacidad de afrontar la adversidad, debido a la dependencia tecnológica y el potencial impacto que las nuevas ciberamenazas pueden causar en las organizaciones, pueden derivar situaciones que afecten la operatividad de la compañía[5].
- Visibilidad: Tener la capacidad de conocer que sucede en el entorno tecnológico de la compañía, para así anticiparse a situaciones que puedan afectarla.
- Mejores prácticas: Las buenas prácticas de seguridad de la información son un instrumento que permiten desarrollar de manera consciente las estrategias en la compañía.
- Defensa en profundidad: Identificar los controles necesarios para proteger la información.

Para elaborar y formular el plan estratégico de seguridad se adelantarán las siguientes etapas; conocimiento de la organización, diagnóstico, alineación de los objetivos, modelo de seguridad de la información, para terminar en la definición del plan estratégico de seguridad de la información donde se analizan y priorizan las

[4] http://www.digiware.net/?q=es/consultoria
[5] http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO35-2015_Ciber-resiliencia_LuisdeSalvador.pdf

iniciativas y se establece el portafolio de proyectos de seguridad de la información. Todo esto con el fin de plantear la propuesta de un estado de madurez a tres (3) años, que es el estado deseado, el cual es requerido para contribuir con el logro de los objetivos de negocio y salvaguardar la información de la organización.

Culminadas estas etapas, se presenta un plan estratégico de seguridad de la información que expone la planificación estratégica de seguridad de la información para el periodo comprendido entre los años 2018 al 2020, que pretende orientar los esfuerzos relacionados con la función de apoyo de la Gestión de la seguridad de la información al resto de los procesos estratégicos, misionales y de apoyo de la organización, conduciendo a la preservación de la confidencialidad, integridad, disponibilidad de la información.

- Como resultado de la implementación del plan estratégico de seguridad de la información la Compañía puede lograr los siguientes beneficios:

- Tener una visibilidad sobre el nivel de madurez del modelo de seguridad de la información.
- Establecer un portafolio de proyectos de seguridad adecuados y apalancados con los objetivos estratégicos corporativos.
- Establecer los controles de forma organizada, adecuada y priorizada.
- Adoptar y apropiar las políticas necesarias para salvaguardar la información de la aseguradora, mediante la prevención y disminución del impacto de los incidentes de seguridad garantizando la seguridad y continuidad de los activos de información que soportan los procesos críticos del negocio,
- Mayor competitivos a nivel del sector asegurador a través del uso y apropiación de las nuevas tecnologías, y cada vez más empoderados con la nueva era de transformación digital donde el cliente es el epicentro de los servicios.
- Mayor tranquilidad para los clientes y accionistas.
- Ofrecer servicios seguros que superen las expectativas de sus clientes.
- Ser referente en el mercado por mantener la seguridad de la información de sus clientes como prioritaria.
- Mayor captación de mercado.
- Dar cumplimiento a la normatividad vigente sobre los lineamientos regulatorios emitidos por la Superintendencia Financiera de Colombia y Superintendencia de Industria y comercios en cuanto a seguridad y privacidad de la información.

2. JUSTIFICACIÓN

Es claro que las Compañías del sector asegurador se encuentran inmersas en medio del desarrollo de la era digital y de las tecnologías, donde se ha transformado la forma de acceder a la información, de desarrollar negocios, y el consumo de tecnologías, requiriendo cada vez más presencia en entornos digitales para ser más competitivos.

Este incremento se puede evidenciar en los resultados presentados en el informe de operaciones del segundo semestre del 2016 por la Superintendencia Financiera de Colombia, donde señala que el sistema financiero colombiano realizó 4.926 millones de operaciones durante el año 2016, con un incremento del 14% frente a 2015; 2.559 millones monetarias por valor de $7.056,8 billones con un incremento del 5% frente a 2015, y 2.366 no monetarias, esta última con un incremento del 22% frente a 2015. Siendo el 32.8% el número de operaciones financieras (monetarias y no monetarias) en Colombia mediante el canal Internet.[6]

Lo que demuestra un incremento del uso de las tecnologías que conlleva una serie de beneficios que ayudan a fortalecer las organizaciones y a desarrollar nuevas oportunidades de negocios. No obstante, es ampliamente conocido que la era digital trae consigo una serie de riesgos derivados de la actividad delictiva en el ciberespacio, y por eso se hace necesario que las organizaciones establezcan planes estratégicos de seguridad de la información, que permitan afrontar estos nuevos retos, de forma organizada y consciente, de manera que se puedan establecer las medidas necesarias para garantizar la confidencialidad, disponibilidad y continuidad de los sistemas de información de la compañía[7]. Asimismo, realizar la alineación de los objetivos de seguridad con los objetivos estratégicos corporativos permitirán que los mismos sean visibles y medibles en cuanto a la generación de valor para la organización.

Todas estas circunstancias generan gran incertidumbre para la Compañías, tal y como lo señala el informe de Allianz Risk Barometer, causadas por la creciente preocupación sobre los desarrollos políticos, legales y regulatorios alrededor del mundo. Según el Allianz Risk Barometer, la interrupción del negocio resulta la principal preocupación de las empresas debido a que no alcanzan a predecir las pérdidas económicas que podrían generarse producto de cambios políticos, nuevas regulaciones, fugas de información y catástrofes naturales, entre otras variables. Si bien las pérdidas ocasionadas por el cambio climático e incendios son las más temidas, la naturaleza del riesgo está variando hacia eventos que no generan daños materiales pero que sí ocasionan grandes pérdidas, como pueden ser los incidentes cibernéticos o el impacto del terrorismo.

[6] https://www.superfinanciera.gov.co/jsp/loader.jsf?lServicio=Publicaciones&lTipo=publicaciones&lFuncion=loadContenidoPublicacion&id=61066

[7] http://www.isaca.org/Knowledge-Center/Research/Documents/innovation-insights_whp_eng_0615.pdf

Top 10 business risks by region in 2017: Americas

	Top 10 business risks		2016 Rank	Trend
1	Business interruption (incl. supply chain disruption, and vulnerability)	43%	1 (58%)	-
2	Cyber incidents (cyber crime, IT failure, data breaches, etc.)	31%	2 (46%)	-
3	Natural catastrophes (e.g. storm, flood, earthquake)	28%	3 (37%)	-
4	Market developments (volatility, intensified competition/new entrants, M&A, market stagnation, market fluctuation)	26%	4 (35%)	-
5	Changes in legislation and regulation (goverment change, economic sanctions, protectionism, etc.)	19%	5 (28%)	-
6	Fire, explosion	15%	6 (25%)	-
7	Macroeconomic developments (austerity programs, commodity price increase, deflation, inflation)	15%	8 (20%)	▲
8	Loss of reputation or brand value	14%	6 (25%)	▼
9	New technologies (e.g impact of increasing interconnectivity, nanotechnology, artificial intelligence, 3D printing, drones, etc.)	12%	NEW	▲
10	Theft, fraud, corruption	12%	9 (20%)	▼

Source: Allianz Global Corporate & Specialty. Figures represent a percentage of all relevant responses. 398 respondents. More than one risk selected.

Ilustración 1- Los 10 principales riesgos empresariales por región en 2017:Américas

Con respecto a 2016, aumentaron su posición en el ranking la introducción de nuevas tecnologías, que puedan ocasionar fugas de información o ataques cibernéticos; la posibilidad de riesgos catastróficos, que dañen la operación del negocio; y los daños colaterales, producto de los actos de violencia política (como guerras e incidentes terroristas)[8].

Por ejemplo, el informe presenta los principales riesgos empresariales en 2017 por industria, siendo para el sector financiero los siguientes:

Financial Services			2016 Rank	Trend
1	Market developments (volatility, intensified competition/new entrants, M&A, market stagnation, market fluctuation)	41%	1 (44%)	-
2	Cyber incidents (cyber crime, IT failure, data breaches, etc.)	40%	2 (44%)	-
3	Changes in legislation and regulation (goverment change, economic sanctions, protectionism, etc.)	36%	3 (37%)	-
4	Macroeconomic developments (austerity programs, commodity price increase, deflation, inflation)	33%	4 (29%)	-
5	Political risks and violence (war, terrorism, etc.)	23%	NEW	▲

Ilustración 2- Principales riesgos empresariales en 2017 por industria

Para mitigar los impactos que conllevan la materialización de los riesgos de seguridad a los que está expuesta la Compañía, se hace necesario formular un plan estratégico de seguridad de la información con una proyección a tres (3) años, identificando y priorizando el portafolio de proyectos de seguridad de la información que permitirá contribuir al cumplimiento del logro de los objetivos de negocio, siendo cada vez más competitivos a nivel del sector asegurador a través del uso y

[8] https://www.agcs.allianz.com/assets/PDFs/Reports/Allianz_Risk_Barometer_2017_EN.pdf

apropiación de las nuevas tecnologías, cada vez más empoderados en la nueva era de transformación digital.

En otras palabras, establecer el Plan Estratégico de Seguridad de la Información (PESI), permitirá a la aseguradora, identificar el conjunto de responsabilidades, prácticas y acciones a ser desarrolladas por la Compañía con miras a propender que los riesgos de la información sean apropiadamente administrados, mediante la definición de un modelo de seguridad de la información alineado con las mejores prácticas y estándares internacionales como la ISO27001:2013 y ISO27002:2013, lo anterior, con el fin de plantear una propuesta de un estado de madurez a 3 años, que es el estado deseado, el cual es requerido para contribuir con el logro de los objetivos estratégicos del negocio.

3. MARCO TEÓRICO Y REFERENCIAS

Se han identificado las siguientes etapas para la elaboración y formulación de un plan estratégico en seguridad de la información; conocimiento de la organización, diagnóstico, alineación de los objetivos, modelo de seguridad de la información, para terminar en la definición del plan estratégico de seguridad de la información donde se analizan y priorizan las iniciativas y se establece el portafolio de proyectos de seguridad de la información. Todo esto con el fin de plantear la propuesta de un estado de madurez a tres (3) años, que es el estado deseado, el cual es requerido para contribuir con el logro de los objetivos de negocio y salvaguardar la información de la organización.

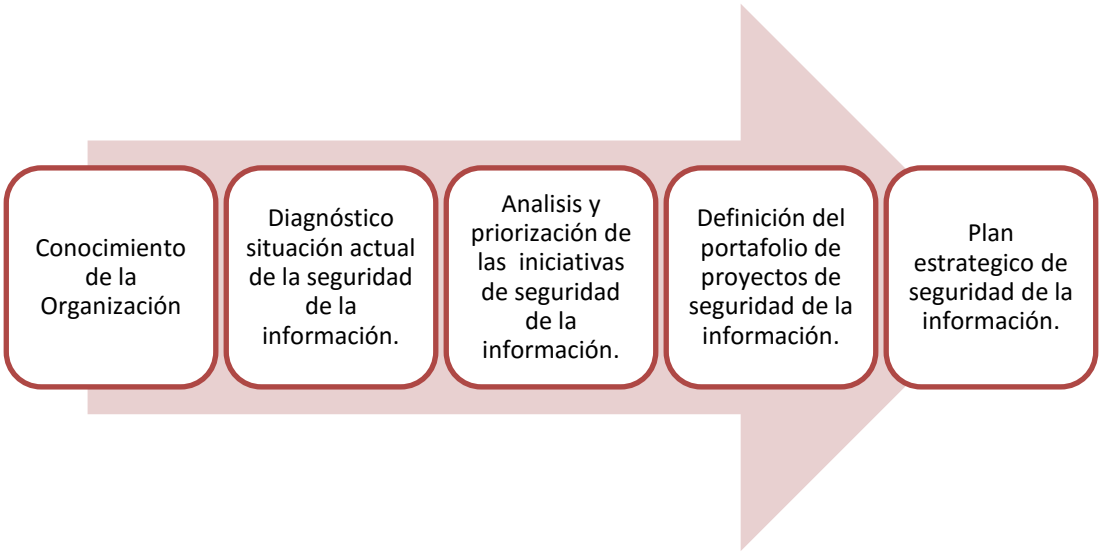

Ilustración 3- Construcción del plan estratégico de seguridad de la información

3.1 Conocimiento de la Organización

Mediante entrevistas a personas claves dentro de la organización y la revisión del plan estratégico corporativo existentes, se llevó a cabo la contextualización y el conocimiento de la Compañía, con el propósito de identificar los objetivos y necesidades que tienes las áreas de negocio frente a la seguridad de la información y a la aplicación, uso y apropiación de las nuevas tecnologías.

Como insumo se cuenta con el plan estratégico corporativo de la aseguradora, que a continuación se presenta:

Ilustración 4. Matriz objetivos estratégicos corporativos

Se aplica una encuesta que permite determinar las necesidades de cada uno de los procesos estratégicos, misionales y de apoyo en cuento a las tendencias e incorporación de nuevas tecnologías, como:

- Analítica Big Data
- Móviles
- Computación en la nube
- Aprendizaje automático (Inteligencia artificial).
- Internet de las Cosas
- Cursos masivos On line
- Redes Sociales
- Modelo de negocios Digitales
- Ciberseguridad
- Moneda Digital (Criptomonedas)

El resultado de la encuesta permite establecer los requerimientos del negocio en cuanto a la aplicación, uso y apropiación de nuevas tecnologías, las cuales deben ir acompañadas del establecimiento de buenas prácticas de seguridad de la información y de proyectos de seguridad que mitiguen los riesgos asociados a estas nuevas tecnologías.
Durante esta etapa se realiza la alineación de objetivos, a través de entrevistas con partes interesadas; se establece el entendimiento de los objetivos estratégicos de la organización, para así identificar los objetivos de seguridad de la información que aportarán al desarrollo del plan estratégico de seguridad de la información de la aseguradora.

3.2 Diagnóstico seguridad de la información

Determinar el estado actual de la seguridad de la información en la organización, usando como marco de referencia las normas internacionales 27001:2013 y para los controles la 27002:2013, mediante los cuales se identificó el ambiente de seguridad de la información existente y su nivel de cumplimiento.

Igualmente, a través de este diagnóstico se puede evidenciar el nivel de madurez del modelo de seguridad de la información que es un pilar importante del plan estratégico, a partir de este modelo, se establece el gobierno de seguridad de la información y se identifican las iniciativas propias de seguridad de la información requeridas por las áreas de negocio para cumplir los requisitos, para establecer, implementar, mantener y mejorar el sistema de gestión de seguridad de la información (SGSI), de acuerdo con la norma ISO/IEC 27001:2013.

3.3 Análisis y priorización de iniciativas.

Teniendo en cuenta el resultado anterior, se identifican las iniciativas de seguridad de la información, los cuales deben estar alineadas al plan estratégico, y a las necesidades que se identificaron en los procesos del negocio, conforme al resultado de las entrevistas.

De otra parte, es importante que las iniciativas estén enmarcadas dentro de los controles sugeridos para garantizar una adecuada arquitectura de seguridad de la información y un esquema de defensa a profundidad utilizando soluciones y tendencias de seguridad de la información y de tecnología.

3.4 Definición del portafolio de proyectos de seguridad de la información

En esta etapa, después del análisis y priorización de iniciativas, se define el portafolio de proyectos del plan estratégico, agrupados en proyectos relacionados con:

- Gobierno o modelo de seguridad de información
- Gestión de riesgos de Seguridad
- Desarrollo y gestión del programa de seguridad de la in formación.
- Gestión de incidentes de seguridad de la información.

3.5 Plan estratégico de seguridad de la información

Se presenta el plan estratégico de seguridad de la información, cuyos objetivos de Seguridad de la información están alineados con los objetivos estratégicos de la Compañía. Asimismo, se establecen las restricciones a la estrategia, donde se identificar las restricciones asociadas a la situación geográfica, cultural y de presupuesto. Por último, se presenta el portafolio de proyectos priorizado durante el periodo de tiempo comprendido entre los años 2018 al 2020.

3.6. MARCO CONCEPTUAL (GLOSARIO DE TERMINOS)

Activo de información: aquello que es de alta validez y que contiene información vital de la empresa que debe ser protegida. Amenaza: Es la causa potencial de un daño a un activo de información.

Análisis de riesgos: Utilización sistemática de la información disponible, para identificar peligros y estimar los riesgos. Causa: Razón por la cual el riesgo sucede.

Controles: Son aquellos mecanismos utilizados para monitorear y controlar acciones que son consideradas sospechosas y que pueden afectar de alguna manera los activos de información.

Disponibilidad: Propiedad de determina que la información sea accesible y utilizable por aquellas personas debidamente autorizadas.

Propietario del riesgo sobre el activo: Persona responsable de gestionar el riesgo.

Impacto: Consecuencias de que la amenaza ocurra. Nivel de afectación en el activo de información que se genera al existir el riesgo.

Incidente de seguridad de la información: Evento no deseado o inesperado, que tiene una probabilidad de amenazar la seguridad de la información.

Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos.

Probabilidad de ocurrencia: Posibilidad de que se presente una situación o evento específico.

Responsables del Activo: Personas responsables del activo de información.

Riesgo: Grado de exposición de un activo que permite la materialización de una amenaza.

Riesgo Inherente: Nivel de incertidumbre propio de cada actividad, sin la ejecución de ningún control.

Riesgo Residual: Nivel de riesgo remanente como resultado de la aplicación de medidas de seguridad sobre el activo.

PSE: Proveedor de Servicios Electrónicos, es un sistema centralizado por medio del cual las empresas brindan a los usuarios la posibilidad de hacer sus pagos por Internet.

Seguridad de la Información: Preservación de la confidencialidad, la integridad y la disponibilidad de la información (ISO 27000:2014).

SGSI: Siglas del Sistema de Gestión de Seguridad de la Información. Sistema de Gestión de Seguridad de la información SGSI: permite establecer, implementar, mantener y mejorar continuamente la gestión de la seguridad de la información de acuerdo con los requisitos de la norma NTC-ISO-IEC 27001:2013.

Vulnerabilidad: Debilidad de un activo o grupo de activos de información que puede ser aprovechada por una amenaza. La vulnerabilidad de caracteriza por ausencia en controles de seguridad que permite ser explotada.

Amenaza: Es todo aquella acción o elemento capaz de atentar contra la seguridad de la información.

Antivirus. Software encargado de detectar, bloquear y eliminar virus informáticos o código malicioso.

Ataque: Es la acción de interrumpir o dañar un activo de información con el objetivo de causar problemas de confiabilidad, disponibilidad e integridad. O también se puede afirmar que es cuando se materializa una amenaza de seguridad.

Código malicioso: Software diseñado para ejecutar acciones maliciosas (como provocar daños al software de la computadora, robar información almacenada en un sistema informático, aprovechar recursos informáticos para efectuar otras acciones perjudiciales para el usuario) y que incluye programas como virus, gusanos, troyanosy spyware. Puede utilizar como vía de diseminación, el correo electrónico, sitios de internet, redes, dispositivos móviles, dispositivos removibles (por ejemplo, pen-drives).

Estándar de seguridad: Conjunto de normas o modelos diseñados con la finalidad de brindar soluciones de sistemáticas a un área del conocimiento específico.

Firewall: Un firewall o también llamados corta fuego, es un software o hardware que restringe el acceso a sitios web o una red sin autorización de acceso

Incidente de seguridad: Un incidente de seguridad es cualquier acción que atente contra la confiabilidad, disponibilidad e integridad de la información.

Ingeniería social: es la secuencia de acciones que tienen como finalidad la obtención de información, el fraude o el acceso no autorizado a sistemas informáticos, y que ha implicado en algún momento la manipulación psicológica de personas.

Intrusos: Es una Persona que intenta acceder a un sistema informático sin autorización, a través de técnicas y/o métodos informáticos que se lo permitan.

ISO: (International Organization for Standardization). Organización internacional de estándares

Metodología: Es un conjunto de reglas o métodos organizados de forma sistémica con el objetivo de lograr el cumplimiento de una norma o un estándar.

Phishing: Suplantación de identidad de una página o sitio Web.

Plan de contingencia: Es un tipo de plan preventivo, predictivo y reactivo. Presenta una estructura estratégica y operativa que ayudará a controlar una situación de emergencia y a minimizar sus consecuencias negativas.

Riesgos: Es la posibilidad de que una amenaza aproveche una vulnerabilidad y dañe un activo de información. Departamento de seguridad.

Repudio: Denegación, por una de las entidades implicadas en un a comunicación, de haber participado en la totalidad o en parte de dicha comunicación.

Seguridad lógica: Conjunto de medidas de seguridad y herramientas informáticas de control de acceso a los sistemas informáticos.

Seguridad física: Controles externos al ordenador, que tratan de protegerlo contra amenazas de naturaleza física como incendios, inundaciones, entre otros.

SGSI: Sistema de gestión de la seguridad de la información,

Teletrabajo: El teletrabajo es un nuevo sistema de organización del trabajo en que la persona trabajadora desarrolla una parte importante de su trabajo fuera de la empresa y por medios telemáticos.

Vulnerabilidad: Una vulnerabilidad de seguridad es un fallo o debilidad en el diseño, la implementación, la operación o la gestión de un sistema, que puede ser explotado con el fin de violar la política de seguridad del sistema. UOC. Guillermo Navarro Arribas. Introducción a las vulnerabilidades.

Wi-Fi (wireless fidelity o fidelidad sin cables): Es una red de ordenadores sin utilización de cables equivalente a la tecnología inalámbrica 802.11 para comunicación a distancia.

Wi-phishing: Wi-phishing, sustracción de datos personales a través de falsas redes públicas de acceso Wi-Fi

DMZ: Una DMZ o una zona desmilitarizada, es un segmento de red específico, en el cual se ubican servicios específicos de red que son públicos a redes poco seguras como Internet.

Red de Datos: Es aquella infraestructura o red de comunicación que se ha diseñado específicamente a la transmisión de información mediante el intercambio de datos.

Diseño de Red Segura: Definición de un esquema de red aplicando medidas de seguridad informática, que una vez implementadas minimizan los riesgos de una intrusión.

Red Privada virtual VPN: Sistema de telecomunicación consistente en una red de datos restringida a un grupo cerrado de usuarios, que se construye empleando en parte o totalmente los recursos de una red de acceso público, es decir, es una extensión de la red privada de una organización usando una red de carácter público.

4. METODOLOGÍA

Las normas y buenas prácticas en seguridad que se tienen en cuenta para el levantamiento de información, se detallan a continuación:

4.1 Norma ISO/IEC 27001:2013

Establece los requisitos necesarios para establecer, implementar, mantener y mejorar continuamente el Sistema de Gestión de Seguridad de la Información dentro del contexto de la organización. Busca lograr que los riesgos y problemas asociados a la Seguridad de la Información sean conocidos por la organización, puedan minimizarse y existan procesos de gestión para resolverlos adecuadamente o lograr que afecten lo mínimo posible a la Organización. La numeración de las cláusulas en todas las normas serán idénticas, constando de cuatro (4) cláusulas informativas (0-3), y siete (7) cláusulas que determinarán los requerimientos (4-10)

Los aspectos evaluados durante esta fase se describen a continuación:

DOMINIO	DESCRIPCION
4. Contexto de la Organización	Entendimiento de la Organización
	Expectativa para interesadas
	Alcance del Sistema de Gestión de Seguridad de la Información
5. Liderazgo	Liderazgo y compromiso de la Alta Dirección
	Política de seguridad general (alto nivel)
	Roles, responsabilidades y autoridades
6. Planeación	Valoración de riesgos
	Tratamiento de riesgos
	Declaración de aplicabilidad
	Objetivos de seguridad
7. Soporte	Recursos
	Competencias
	Conciencia
	Comunicación
	Información documentada
8. Operación	Evaluación de riesgos de Seguridad de la información
	Tratamiento de los Riesgos
	Procesos necesarios para cumplir con los objetivos de seguridad

9. Evaluación de desempeño	Seguimiento, medición, análisis y evaluación
	Auditoria interna
	Revisión por la Dirección
10. Mejora Continua	No conformidades y acciones correctivas
	Mejora continua

Tabla 1. Dominios de la norma ISO/IEC 27001:2013

4.2 Norma ISO/IEC 27002:2013

La norma ISO 27002:2013 es el código de prácticas de seguridad de la información el cual tiene como objetivo proveer una guía para la implementación de controles que apoyen la implementación del Sistema de Gestión de Seguridad de la Información. Los aspectos evaluados durante esta fase se describen a continuación:

- **Políticas de seguridad de la Información:** Establece la necesidad de definir un conjunto de políticas aplicadas a todas las actividades relacionadas con la gestión de la seguridad de la información dentro de la Organización, con el propósito de proteger la misma contra las amenazas presentes en el entorno.

- **Organización de la seguridad de la información:** Sugiere diseñar una estructura para la gestión de la seguridad de la información dentro la Organización que establezca los roles y responsabilidades con la seguridad de la información a lo largo de la misma.

- **Seguridad del Recurso Humano:** Establece la necesidad de educar e informar a los empleados actuales y potenciales sobre lo que se espera de ellos en materia de seguridad y confidencialidad de la información que manejan. También determina cómo incide el papel que desempeñan los empleados como co-responsables de la seguridad de la información.

- **Gestión de Activos:** Detalla los elementos de la Organización (servidores, PCs, medios magnéticos, información impresa, documentos, etc.), que deben ser considerados para establecer un mecanismo de seguridad que permita garantizar un nivel adecuado de protección.

- **Control de acceso:** Establece la importancia de monitorear y controlar el acceso a la red y los recursos de aplicación para protegerlos contra los abusos internos e intrusos externos. Asimismo, establece los diferentes tipos de accesos o privilegios a los recursos informáticos (sistema operativo, aplicaciones, correo electrónico, Internet, comunicaciones, conexiones remotas, etc.) que requiere cada empleado de la Organización y el personal externo que brinda servicios, en concordancia con sus responsabilidades. Esto permitirá identificar y evitar acciones o actividades no autorizadas, garantizando los servicios informáticos.

- **Cifrado:** Garantiza el uso adecuado y eficaz del cifrado para proteger la confidencialidad, autenticidad y/o integridad de la información.

- **Seguridad física y ambiental:** Responde a la necesidad de proteger las áreas, los equipos y los controles generales. El objetivo principal es la prevención de accesos no autorizados a las instalaciones de la Organización, con especial atención a todos los sitios en los cuales se procesa información (centros de cómputo, PC de usuarios críticos, equipos de los proveedores de servicios, etc.), y áreas en las cuales se recibe o se almacena información (magnética o impresa) sensitiva (fax, áreas de envío y recepción de documentos, archivadores, etc.), minimizando riesgos por pérdidas de información, hurto, daño de equipos y evitando la interrupción de las actividades productivas.

- **Seguridad de las operaciones:** Define las políticas, procedimientos y responsabilidades para asegurar la correcta operación de las instalaciones de procesamiento de información.

- **Seguridad de las comunicaciones:** Define las políticas y procedimientos para asegurar la protección de la información en las redes y sus instalaciones de procesamiento de información.

- **Adquisición, desarrollo y mantenimiento de los sistemas de información:** Establece la necesidad de implantar medidas de seguridad y aplicación de controles de seguridad en todas las etapas del proceso de desarrollo y mantenimiento de los sistemas de información. Además, considera los mecanismos de seguridad que deben implantarse en el proceso de adquisición de todos los sistemas o aplicaciones de la Organización, para prevenir pérdidas, modificaciones, o eliminación de los datos, asegurando así la confidencialidad e integridad de la información.

- **Relación con proveedores:** Permite asegurar la protección de los activos de información que son accedidos por proveedores.

- **Gestión de Incidentes de Seguridad:** Establece la necesidad de desarrollar una metodología eficiente para la generación, monitoreo y seguimiento de eventos e incidentes de seguridad.

- **Aspectos de seguridad de la información en la gestión de la continuidad del negocio:** Considera el análisis de todos los procesos y recursos críticos del negocio, y define las acciones y procedimientos a seguir en casos de fallas o interrupción de los mismos, evitando la pérdida de información y la no disponibilidad de los procesos productivos de la Organización, lo que podría provocar un deterioro de la imagen de la Organización, una posible pérdida de clientes o incluso una dificultad severa que impida continuar operando.

- **Cumplimiento:** Imparte instrucciones a las organizaciones para que verifiquen si el cumplimiento con la norma técnica ISO/IEC 27002:2013, concuerda con otras leyes, reglamentos, normatividad y obligaciones contractuales o cualquier requerimiento de seguridad, tales como propiedad intelectual, auditorías, contrato de servicios, entre otros. Esta sección también requiere una revisión a las políticas de seguridad, al cumplimiento y las consideraciones técnicas; asimismo, busca garantizar que las políticas de seguridad y privacidad de la información sean acordes a la infraestructura tecnológica de la Organización.

4.3 Nivel de madurez del modelo de seguridad de la información

Una vez analizada la información, se procede a determinar el nivel de madurez del modelo de seguridad de la información para cada uno de los controles de la norma ISO/IEC 27001:2013 y ISO/IEC 27002:2013, para lo cual se toma como referencia el modelo de madurez establecido por el Framework Cobit 4.1.[9]

Escala	Puntaje	Descripción
No Aplica	N/A	No aplica.
Inexistente	0	Total, falta de cualquier proceso reconocible. La Organización ni siquiera ha reconocido que hay un problema a tratar. No se aplican controles.
Inicial	1	Hay una evidencia de que la Organización ha reconocido que existe un problema y que hay que tratarlo. No hay procesos estandarizados. La implementación de un control depende de cada individuo y es principalmente reactiva.
Repetible	2	Los procesos y los controles siguen un patrón regular. Los procesos se han desarrollado hasta el punto en que diferentes procedimientos son seguidos por diferentes personas. No hay formación ni comunicación formal sobre los procedimientos y estándares. Hay un alto grado de confianza en los conocimientos de cada persona, por eso hay probabilidad de errores.
Definido	3	Los procesos y los controles se documentan y se comunican. Es poco probable la detección de desviaciones.
Gestionado	4	Los controles se monitorean y se miden. Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas de acción donde los procesos no estén funcionando eficientemente.
Optimizado	5	Las buenas prácticas se siguen y automatizan. Los procesos han sido redefinidos hasta el nivel de mejores prácticas, basándose en los resultados de una mejora continua.

Tabla 2. Modelo de nivel de madurez Framework Cobit 4.1.

[9] http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/COBIT-4-1.aspx

El nivel de madurez permitirá establecer las bases para la mejora continua del proceso de Seguridad de la Información de la aseguradora, e identificar las iniciativas de seguridad de la información, los cuales deben estar alineadas al plan estratégico y a las necesidades que se identificaron en los procesos del negocio.

4.4 Priorización del portafolio de proyectos[10]

Una vez identificadas las iniciativas y los proyectos con base en el resultado de diagnóstico de la situación actual de la aseguradora en seguridad de la información y teniendo en cuenta el resultado de las necesidades del negocio, es necesario priorizar las soluciones, para lo cual se construyeron las siguientes categorías de prioridad que permiten evaluar y determinar una secuencia sistemática para el desarrollo del Plan Estratégico de seguridad de la Información (PESI):

Prioridad	Descripción
0	Elaboración del presente Plan Estratégico de Seguridad de la Información
1	Estrategia de la Dirección de seguridad de la información: Incluye las iniciativas que soportan la implementación de la estrategia de la Oficina de seguridad de la información y apalancan su reconocimiento y posicionamiento como un área estratégica y de servicio dentro de la aseguradora.
2	Riesgos Operacionales: Hace referencia a los proyectos y actividades que mitigan los riesgos de seguridad de la información catalogados como relevantes, garantizando salvaguardar la información en su confidencialidad, disponibilidad e integridad.
3	Misional: Identifica aquellos proyectos que favorecen el cumplimiento de la estrategia y metas de la aseguradora y que soportan la gestión o ejecución de las actividades de los procesos misionales de la aseguradora.
4	Desempeño: Soportan el adecuado desempeño de las funciones de la aseguradora. No generan impactos críticos, pero es deseable contar con estas soluciones para mejorar los indicadores de gestión de algunos procesos.

Tabla 3. Criterios para priorización de proyectos

5. RESULTADOS Y DISCUSIÓN

Los resultados obtenidos de este trabajo se derivan del desarrollo de los procesos definidos y los lineamientos metodológicos indicados con el fin de poder dar

[10] Se toma de la metodología presentada en el informe Diseño del Plan Estratégico de tecnologías de información y comunicaciones y la estrategia de información (PETIC) para el MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE. - http://www.minambiente.gov.co/images/tecnologias-de-la-informacion-y-comunicacion/pdf/Petic_mads_2013.pdf

cumplimiento a los objetivos específicos que corresponde al conocimiento de la organización, el diagnostico de las situación actual de seguridad, la iniciativas de seguridad de la información, para concluir con el portafolio de proyectos de seguridad de la información, alcanzado el objetivo general del proyecto, que corresponden a la elaboración del Plan Estratégico de Seguridad de la Información.

Para el desarrollo de estas actividades se utilizaron diferentes métodos o instrumentos de recolección de información, como, entrevistas, cuestionarios, formularios en excel, evaluación con base en la experiencia del autor, documentos físicos y electrónicos, documentos publicaciones en la WEB, entre otros. Esto métodos fueron aplicados y posteriormente analizados detalladamente con el fin de alcanzar el resultado óptimo del proyecto.

6. CONCLUSIONES

El diseño de un plan Estratégico para la Gestión de Seguridad de la Información basado en un modelo de mejoras prácticas y lineamientos de seguridad, como es la Norma internacional ISO/IEC 27001:2013 y la ISO/IEC 27002:2013, y el alineamiento del plan estratégico corporativo con los objetivos estratégicos de seguridad de la información, es un herramienta de gran ayuda que permite identificar los diferentes proyectos de seguridad de la información que debe adelantar la Compañía de manera organizar para cumplir con el objetivo de seguridad de la información que es salvaguardar la información de la compañía garantizando la confidencialidad, integridad de disponibilidad de la información, todo lo anterior, se cumple si se logra establecer un modelo de seguridad de la información, para lograr forjar en el tiempo un adecuado y sostenible Sistema de Gestión de Seguridad de la Información, nuestro objetivo es viable y conforme a los planteado en el desarrollo de este trabajo.

Ahora es muy importante contar desde el inicio con el apoyo y la aprobación de la alta dirección de la empresa y con el compromiso de todas las áreas involucradas en el proceso, el portafolio de proyectos que tendrá el plan estratégico deben ser desarrollados y ejecutados para lograr un sistema de seguridad de la información conforme a los más altos estándares de seguridad, cumpliendo los requisitos y temas regulatorios y lo más relevante, lograr apalancar el cumplimiento de los objetivos estratégicos de la compañía.

7. BIBLIOGRAFÍA

[1] ICONTEC, NTC-ISO-IEC 27001, 2013. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI). Requisitos

[2] ICONTEC, NTC-ISO-IEC 27002, 2013. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI). Controles.

[3] España. El portal de ISO 27001 en español. [En línea]. Disponible: http://www.iso27000.es/

[4] Klaus Schwab, Reunión Anual en Davos, Cuarta Revolución Industrial, enero 2016. [En línea]. Available: http:// www.weforum.org/agenda/2016/01/the-fourth-industrialrevolution-what-it-means-and-how-to-respond.

[5] Capgemeni, 10 tendencias para el sector seguros en 2017, diciembre 2016. [En línea]. Available: https://www.es.capgemini.com/biblioteca/10-tendencias-para-el-sector-seguros-en-2017%20

[6] Allianz, Allianz Risk Barometer Top Business Risks 2017, diciembre 2016. [En línea]. Available: https://www.agcs.allianz.com/assets/PDFs/Reports/Allianz_Risk_Barometer_2017_EN.pdf

[7] Luis de Salvador Carrasco, CIBER-RESILIENCIA, 03 de abril de 2015. [En línea]. Available: http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO35-2015_Ciber-resiliencia_LuisdeSalvador.pdf

[8] Superintendencia Financiera de Colombia, Informe de Operaciones Segundo Semestre de 2016, marzo 13 de 2017. [En línea]. Available: https://www.superfinanciera.gov.co/jsp/loader.jsf?lServicio=Publicaciones&lTipo=publicaciones&lFuncion=loadContenidoPublicacion&id=61066

[9] IT Governance Institute, Cobit 4., Maturit y Models, 2017. [En línea]. Available: http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/COBIT-4-1.aspx

[10] ISACA, Top Digital Technology Trends That Affect Strategy, julio 2015. [En línea]. Available: http://www.isaca.org/Knowledge-Center/Research/Documents/innovation-insights_whp_eng_0615.pdf

[11] Dinero, Las aseguradoras se suben al bus del big data para no perder dinero, febrero 2017. [En línea]. Available:

http://www.dinero.com/empresas/articulo/aplicacion-del-big-data-y-analitica-en-el-sector-asegurador/240722

[12] Encar Ferreiro, Canal Asegurador Marketing, Influencia del Marketing Móvil en el Sector Asegurador, 2014. [En línea]. Available: http://www.canalasegurador.es/influencia-del-marketing-movil-en-el-sector-asegurador/#.WSxmH2iGPb0

[13] Encar Ferreiro, Canal Asegurador Marketing, Influencia del Marketing Móvil en el Sector Asegurador, 2014. [En línea]. Available: http://searchdatacenter.techtarget.com/es/cronica/Beneficios-del-computo-en-la-nube-para-la-industria-de-seguros

[14] Lizzette B. Pérez Arbesú, Beneficios del cómputo en la nube para la industria de seguros, abril 2013. [En línea]. Available: http://searchdatacenter.techtarget.com/es/cronica/Beneficios-del-computo-en-la-nube-para-la-industria-de-seguros

[15] Lucy Hook, ¿Cómo afectará la Inteligencia Artificial a los seguros?, 03 de noviembre 2016. [En línea]. Available: http://legaliboopro.com/afectara-la-inteligencia-artificial-los-seguros/

[16] Yael Córdovaene, Aseguradoras perfilan prioridades para el Internet de las Cosas, enero 2017. [En línea]. Available: http://eleconomista.com.mx/sistema-financiero/2017/01/12/aseguradoras-perfilan-prioridades-internet-las-cosas.

[17] Pablo Fuentes Sodupe, La gamificación en el sector asegurador, una tendencia en alza, septiembre 2015. [En línea]. Available: https://revistalafundacion.com/septiembre2015/seguro/

[18] Abrahami Jaramillo, Redes sociales son una oportunidad para los vendedores de seguros, mayo 2017. [En línea]. Available: https://www.merca20.com/redes-sociales-son-una-oportunidad-para-los-vendedores-de-seguros/

[19] Ernst & Young Global Limited (EYG), XIV Encuesta Global de Seguridad de la Información, 2017. [En línea]. Available: http://www.ey.com/mx/es/services/advisory/xiv-encuesta-global-de-seguridad-de-la-informacion---entrar-a-la-nube-salir-de-la-niebla.

[20] Yael Cordova, Seguros se blindan ante ataques cibernéticos, mayo 2017. [En línea]. Available: http://eleconomista.com.mx/sistema-financiero/2017/05/22/seguros-se-blindan-ante-ataques-ciberneticos.

[21] Jaime Sandoval, La Casa Blanca señala la tecnología Bitcoin como el futuro de las finanzas, junio 2016. [En línea]. Available:

https://criptonoticias.com/sucesos/casa-blanca-senala-tecnologia-bitcoin-futuro-finanzas/#axzz4iUtPSMN6

[22] MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE. Informe Diseño del Plan Estratégico de tecnologías de información y comunicaciones y la estrategia de información (PETIC), diciembre 2012. [En línea]. Available: http://www.minambiente.gov.co/images/tecnologias-de-la-informacion-y-comunicacion/pdf/Petic_mads_2013.pdf

8. ANEXOS

ANEXO 8.1. CONOCIMIENTO DE LA ORGANIZACIÓN

La Compañía aseguradora establece la importancia de desarrollar un Plan Estratégico de Seguridad de la Información PESI, alineado con el Plan Estratégico Corporativo con el fin de cumplir con los pilares de seguridad de la información, para preservar y garantizar la confidencialidad, integridad y disponibilidad de la información y de los sistemas de información que la procesan.

Actualmente la compañía tiene definidas cuatro (4) perspectivas que agrupan sus objetivos del plan Estratégico corporativo, los cuales son: resultados, atractividad, eficiencia y alma.

A continuación, se enuncian la presentación de la matriz de objetivos estratégicos:

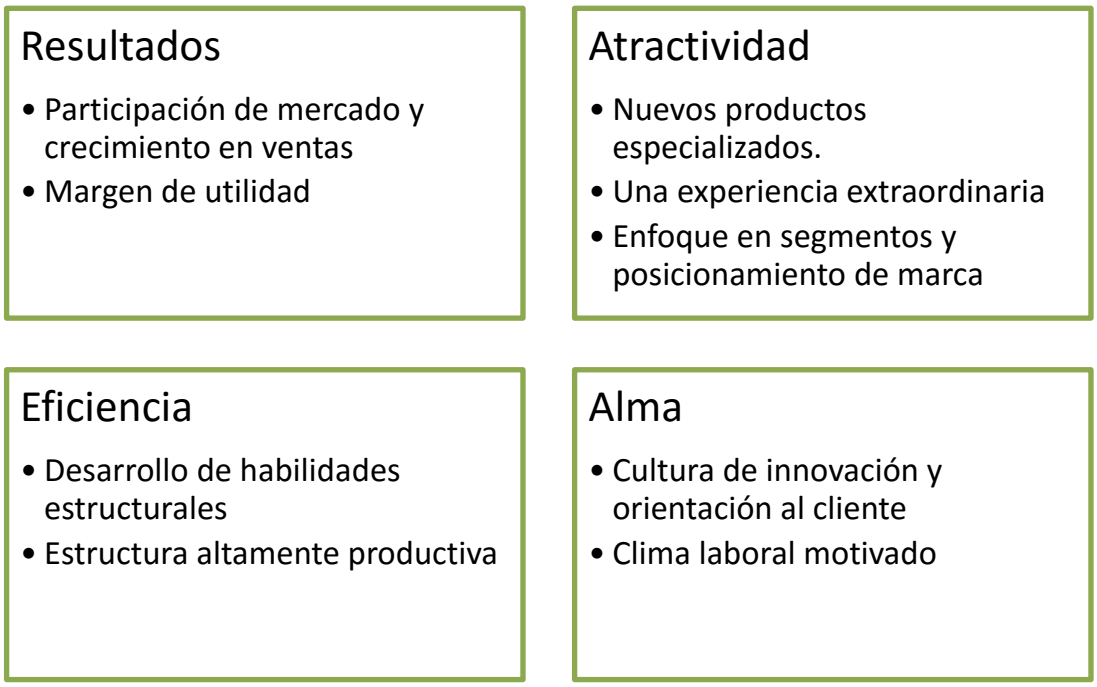

Ilustración 5. Matriz objetivos estratégicos corporativos

Ahora bien, estos objetivos del plan estratégico corporativo puedes se apalancados con la aplicación, uso y apropiación de las siguientes tecnologías:

- **Analítica Big Data**: Extraer datos útiles para mejorar la toma de decisiones en tres áreas: Una mejor experiencia del cliente; innovación; seguros y reclamos, aprovechando la sabiduría de los datos.[11]
- **Móviles:** Los dispositivos móviles como canales prioritarios en diferentes momentos del proceso de compra del cliente actual, como consulta, compra, contratación, u otra acción similar, en Internet dentro de sus hábitos de consumo.[12]
- **Computación en la nube**: Mantener una austera, pero ágil y eficiente organización de TI que pueda proveer servicios TI bajo demanda[13].
- **Aprendizaje automático (Inteligencia artificial)**: Permite evaluar el riesgo de manera más precisa, debido a la gran cantidad de datos de los que dispone y los algoritmos de aprendizaje cada vez más sofisticados que ayudan a analizarlos como: Estimar las pérdidas de una aseguradora a nivel mundial; activar el análisis

[11] http://www.dinero.com/empresas/articulo/aplicacion-del-big-data-y-analitica-en-el-sector-asegurador/240722
[12] http://www.canalasegurador.es/influencia-del-marketing-movil-en-el-sector-asegurador/#.WSxmH2iGPb0
[13] http://searchdatacenter.techtarget.com/es/cronica/Beneficios-del-computo-en-la-nube-para-la-industria-de-seguros

predictivo avanzado ante la posibilidad de un acontecimiento; ayudar a las aseguradoras contra el fraude.[14]

- **Internet de las Cosas**: El Internet de las Cosas ya no es más una predicción de futuro sino una realidad en el sector asegurador, por lo que no solamente tiene el potencial de cumplir con la personalización del producto de seguros a gran escala, sino también de pasar de tener un foco exclusivamente en la indemnización hacia un producto orientado a la prevención, y ser una fuente real de innovación en términos de servicio y modelos de negocio.[15]
- **Cursos masivos On line (Gamificación)**: La *gamificación* es una forma innovadora de gestionar, que consiste en usar el formato de juegos en procesos internos o externos de las organizaciones, siempre en busca de objetivos y resultados, sirve para analizar el comportamiento de los asegurados, diseñar productos que satisfagan sus necesidades y gestionar el riesgo de forma más eficaz.[16]
- **Redes Sociales**: Las redes sociales como Facebook, Twitter o Instagram representan una oportunidad para vender seguros a escala debido a que estas plataformas digitales tienen una huella muy importante en la mente de la gente, en su tiempo y en sus dispositivos móviles.[17]
- **Modelo de negocios Digitales**: El cambio de lo físico a lo digital. La digitalización está teniendo un efecto profundo sobre los modelos de negocio, en donde las industrias tradicionales son dominadas o completamente reemplazadas por modelos que se basan esencialmente solo en software.[18]
- **Ciberseguridad**: El incremento y variabilidad del riesgo de ciber ataques constituye un reto para el sector asegurador en el que se recogen, almacenan y procesan muchos tipos de datos. Es un tema muy importante para el sector debido a que depende de la información, la calidad, la robustez y de los sistemas donde está alojada.[19]
- **Moneda Digital (Criptomonedas):** Realizar transacciones financieras de forma rápida y segura con tan solo utilizar una aplicación en el teléfono móvil.[20]

A continuación, se presenta el resultado consolidado de la encuesta aplicada a la Alta Dirección, Gerentes, directores, empleados e intermediarios de la Compañía, sobre la aplicación, uso y apropiación de la nueva tecnología en la aseguradora:

---

[14] http://legaliboopro.com/afectara-la-inteligencia-artificial-los-seguros/
[15] http://eleconomista.com.mx/sistema-financiero/2017/01/12/aseguradoras-perfilan-prioridades-internet-las-cosas
[16] https://revistalafundacion.com/septiembre2015/seguro/
[17] https://www.merca20.com/redes-sociales-son-una-oportunidad-para-los-vendedores-de-seguros/
[18] http://www.ey.com/mx/es/services/advisory/xiv-encuesta-global-de-seguridad-de-la-informacion---entrar-a-la-nube-salir-de-la-niebla
[19] http://eleconomista.com.mx/sistema-financiero/2017/05/22/seguros-se-blindan-ante-ataques-ciberneticos
[20] https://criptonoticias.com/sucesos/casa-blanca-senala-tecnologia-bitcoin-futuro-finanzas/#axzz4iUtPSMN6

RANKING APLICACIÓN, USO Y APROPIACION DE LAS NUEVAS TECNOLOGÍAS										
Entrevistados	**Analítica Big Data**	**Móviles**	**Computación en la nube**	**Aprendizaje automático (Inteligencia artificial)**	**Internet de las Cosas**	**Cursos masivos On line (Gamificación)**	**Redes Sociales**	**Modelo de negocios Digitales**	**Ciberseguridad**	**Moneda Digital (Criptomonedas)**
Presidente	7	6	10	8	9	4	5	3	2	1
Gerencia Ejecutivo	10	9	8	6	7	5	4	3	2	1
Gerencia de Riesgos	7	6	8	9	5	2	4	3	10	1
Gerencia de Tecnología y operaciones	8	5	10	7	6	1	4	3	9	2
Gerencia Comercial	3	10	4	2	9	8	7	5	6	1
Gerencia de productos Generales	8	7	6	5	10	4	3	9	2	1
Gerencia de productos de Vida	9	8	7	6	6	4	3	10	2	1
Empleados	8	10	9	1	2	3	4	6	7	5
Intermediarios	8	7	10	9	6	4	5	3	2	1
TOTAL	**68**	**68**	**72**	**53**	**60**	**35**	**39**	**45**	**42**	**14**

La calificación es de 1 a 10, siendo (10) la tecnología más requerida por la aseguradora y (1) la menos requerida.

Tabla 4. Resultado encuestas sobre la aplicación, uso y apropiación nuevas tecnologías

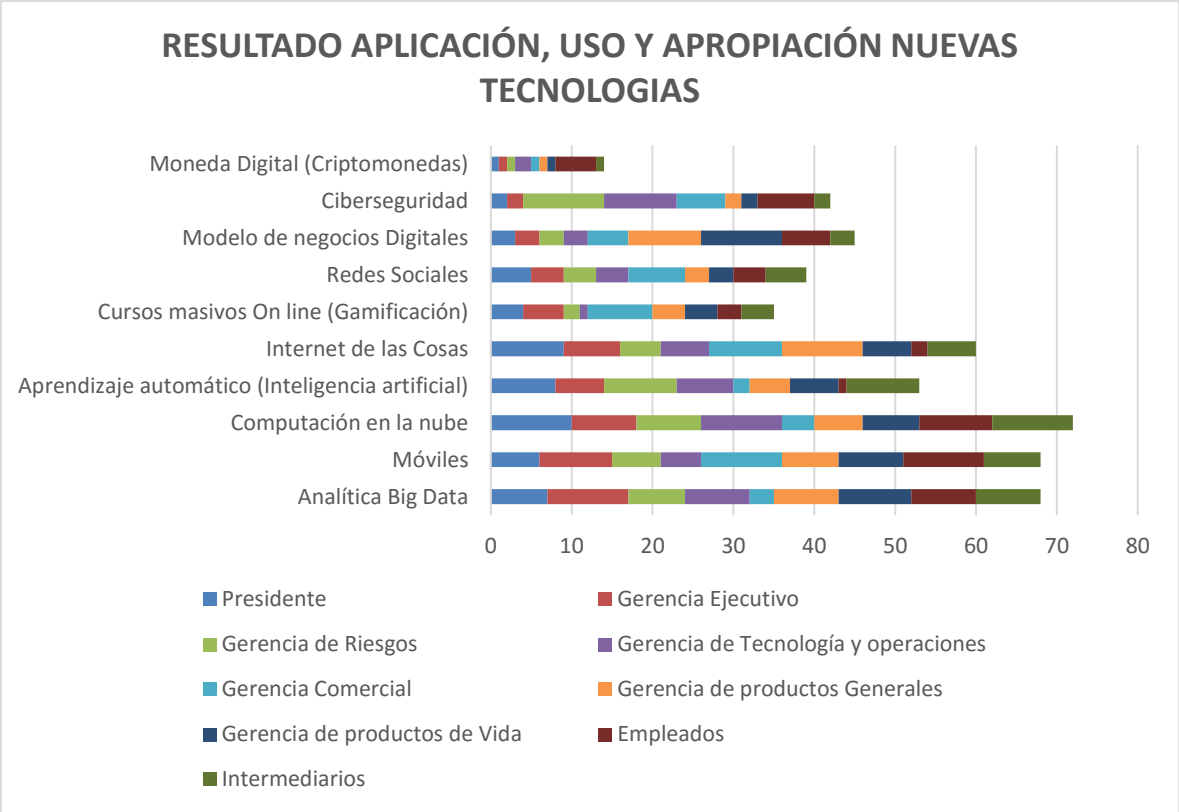

Ilustración 6. Resultado aplicación, uso y apropiación nuevas tecnologías

De otra parte, se realizó una pregunta adicional a cada uno de los entrevistados con respecto a cómo percibe la seguridad de la información en la Compañía, obteniendo los siguientes resultados:

Entrevistado	¿Cómo percibe la seguridad de la información en la Compañía?
Presidente	Altos costos en inversiones de seguridad de la información y seguridad informática. Bajo retorno sobre la inversión en Seguridad (ROSI).
Gerencia Ejecutivo	Falta adoptar y apropiar la cultura de seguridad de la información a nivel de toda la compañía. Buscar aliados de seguridad en los empleados de la Compañía. Asegurar el cumplimiento de la normatividad existente.
Gerencia de Riesgos	Falta una cultura de gestión de riesgos integrados. Falta apoyo de la alta dirección en el accionar y postura de la seguridad de la información frente a nuevas iniciativas del negocio. No existe en la organización un plan estratégico de seguridad de la información (PESI) que apalanque los objetivos estratégicos de la Organización y sea avalado por la alta dirección y socializado a toda la organización. Por lo que las iniciativas de seguridad de la información son dispersas, por lo que se requiere definir el portafolio de proyectos del plan estratégico

Gerencia de Tecnología y operaciones	Desorden y falta de priorización debido a las múltiples iniciativas a nivel del negocio que no están alineadas con las buenas prácticas de seguridad de la información y continuidad del negocio.
Gerencia Comercial	Perciben la seguridad como un obstáculo en el cumplimiento de sus objetivos estratégicos. El cliente percibe afectación de los servicios por indisponibilidad de las plataformas que lo operan. No son conscientes de sus responsabilidades frente al uso de los aplicativos tecnológicos a los que tienen acceso. En cuanto a los proveedores se observa inexistente o bajo nivel de madurez en sus sistemas de gestión de seguridad de la información y continuidad del negocio.
Gerencias de productos	No se les provee de herramientas tecnológicas eficientes para poder posicionar sus productos en el mercado, incursionar en posicionar nuevas tecnologías como: aplicaciones web para venta directa a clientes, pagos electrónicos, app para móviles, análisis de datos para ventas cruzadas, perfilamiento de los clientes, entre otros. La Compañía es una organización altamente tercerizada, especialmente en los procesos comerciales (intermediarios), procesos misionales, y tecnologías, esto infiere que las personas involucradas en los procesos no están directamente bajo el gobierno de la Aseguradora. Desconocimiento en la normatividad aplicable en temas de seguridad y privacidad de información. Desconocimiento de las amenazas de seguridad de la información a la cual está expuesta la organización.
Empleados	Perciben la seguridad de la información como una carga adicional a su trabajo de día a día. Desconocimiento de las políticas, procedimientos y estándares de seguridad de la información. Bajo conocimiento de temas de seguridad de la información. Falta de sensibilización, capacitación y entrenamiento por roles y perfiles. Desconocimiento de las amenazas de seguridad de la información a la cual está expuesta la organización.
Intermediarios	Perciben la seguridad como un obstáculo en su proceso de comercialización. Desconocimiento de las políticas, procedimientos y estándares de seguridad de la información. Desconocimiento de las amenazas de seguridad de la información a la cual está expuesta la organización. Desconocimiento en la normatividad existente en temas de seguridad y privacidad de datos personales

Tabla 5. Resultado entrevista posicionamiento de la seguridad de la información

Del resultado de las entrevistas se establecen los objetivos de Seguridad de la información y se realiza la alineación con los Objetivos Estratégicos corporativos, como se detalla a continuación:

Perspectivas	Objetivos estratégicos de corporativos	Aplicación de nuevas tecnologías	Objetivos de seguridad de la Información
Resultados	Participación de mercado y crecimiento en ventas	Analítica Big Data	• Monitorear el retorno de inversión en Seguridad de la Información a través del cálculo económico de la mitigación de los incidentes de seguridad versus la inversión en seguridad de la información. • Cuantificar el impacto de los incidentes de Seguridad y privacidad de la información, reconocer su necesidad de inversión para garantizar la seguridad de la información.
	Margen de utilidad	Moneda Digital (Criptomonedas)	• Asegurar el mejoramiento continuo del Sistema de Gestión de seguridad de la información para responder a los cambios futuros. • Prevenir el fraude electrónico que puede afectar el estado de resultados y el buen nombre de la compañía.
Atractividad	Nuevos productos especializados.	Modelo de negocios Digitales Internet de las Cosas Móviles	• Gestionar los riesgos de seguridad de la información, para que sean conocidos y según su impacto sean asumidos, transferidos, minimizados y/o eliminados de una forma documentada, repetible y eficiente. • Evaluar los cambios que se produzcan en la empresa, el entorno y las tecnologías con el fin de establecer lineamientos de seguridad de la información durante su implementación.
	Una experiencia extraordinaria	Computación en la nube	• Proteger la información de nuestros clientes y la tecnología utilizada para su procesamiento, asegurando el cumplimiento de los principios de confidencialidad, integridad y disponibilidad de la información. • Aseguramiento en el uso y apropiación de los servicios durante el proceso de transición hacia esas nuevas tecnologías.
	Enfoque en segmentos y posicionamiento de marca	Redes Sociales	• Monitorear la marca y controlar la divulgación de contenidos.
.Eficiencia	Desarrollo de habilidades estructurales	Ciberseguridad	• Optimizar la gestión de incidentes de seguridad de la información y protección de datos personales. • Implementar acciones correctivas y de mejora para el Sistema de Gestión de Seguridad de la Información y el

Perspectivas	Objetivos estratégicos de corporativos	Aplicación de nuevas tecnologías	Objetivos de seguridad de la Información
			Modelo de Seguridad y Privacidad de la Información. • Realizar la correcta gestión de las acciones preventivas y correctivas que se deriven del reporte de eventos e incidentes de seguridad de la información. • Monitorear el cumplimiento de los requisitos de seguridad de la información, mediante el uso de herramientas de diagnóstico y auditorías internas. • Ampliar la visibilidad de Riesgos y Amenazas. • Monitorear los indicadores de gestión de seguridad de la información y continuidad del negocio.
	Estructura altamente productiva	Aprendizaje automático (Inteligencia artificial)	• Aseguramiento de los datos.
Alma	Cultura de innovación y orientación al cliente	Cursos masivos On line (Gamificación)	• Desarrollar cultura de Seguridad de la información en la compañía para fomentar en los empleados, intermediarios, proveedores y aun clientes, las buenas prácticas y comportamientos seguros en el manejo de información. • Sensibilizar los riesgos de seguridad de la información y protección de datos personales ya que el uso de la tecnología conlleva una serie de riesgos, tanto tecnológicos como de cumplimiento legal, regulatorio y normativo que todos los empleados, intermediarios y clientes deben conocer, para tener una postura de seguridad de la información adecuada al momento de usar dicha tecnología y en consecuencia evitar que se materialicen los riesgos asociados. • Capacitar a los funcionarios, colaboradores y contratistas acerca del Sistema de Gestión de Seguridad de la Información y Privacidad de la Información fortaleciendo el nivel de conciencia de los mismos en cuanto a la necesidad de salvaguardar la información de la compañía, de los empleados, proveedores y clientes.
	Clima laboral motivado		

Tabla 6. Resultado Objetivos estratégicos Corporativos vr. Objetivos de Seguridad

Por último, se muestra gráficamente la distribución de los objetivos de seguridad de la información y su asociación con perspectivas del Plan estratégico corporativo.

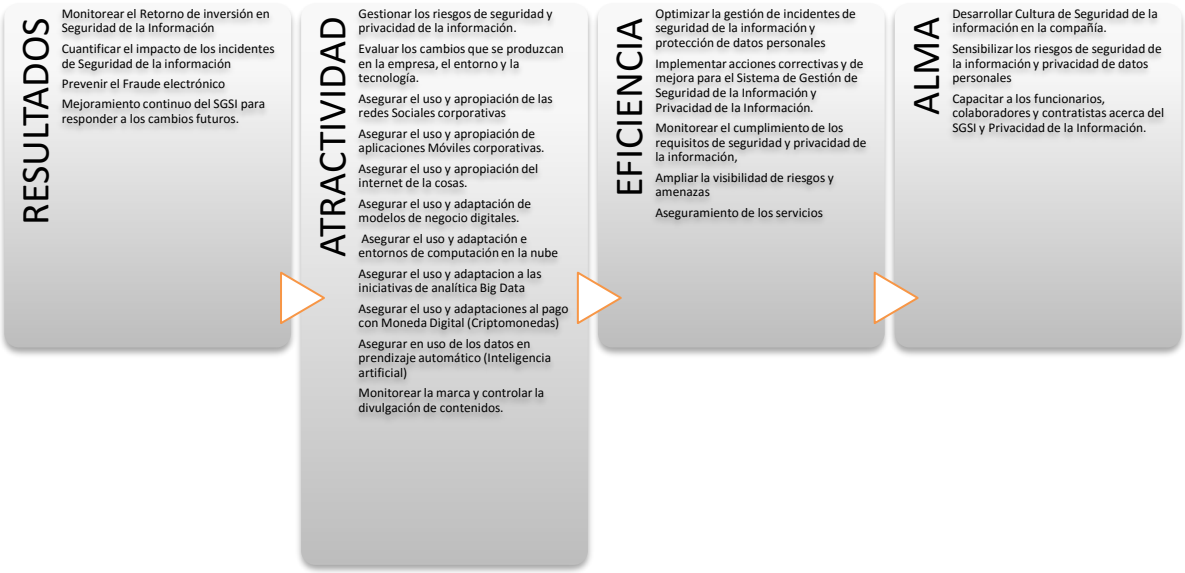

Ilustración 7. Perspectivas del Plan Estratégico Corporativo versus los Objetivos de Seguridad de la Información

ANEXO 8.2. DIAGNÓSTICO DE LA SITUACIÓN ACTUAL DE SEGURIDAD DE LA INFORMACIÓN.

8.2.1 Nivel de cumplimiento detallado – ISO 27001:2013

Se realiza el levantamiento de información a través de entrevistas a los líderes de los procesos, a continuación, se presenta el detalle del resultado de la encuesta realizada para determinar el grado de cumplimiento con respecto a la norma internacional ISO 27001:2013. Se evalúa cada uno de los requerimientos de los dominios de la norma y se asigna un 0% si no cumple y un 100% si cumple.

LISTA DE CHEQUEO ANALISIS GAP ISO 27001:2013				
Código ISO	**Nombre ISO**	**Pregunta**	**Estado Actual del objetivo de control y control**	**Cumplimiento**
4. Contexto de la organización				**25%**

LISTA DE CHEQUEO ANALISIS GAP ISO 27001:2013				
Código ISO	**Nombre ISO**	**Pregunta**	**Estado Actual del objetivo de control y control**	**Cumplimiento**
4.1	Conocimiento de la organización y de su contexto	Se han determinado las cuestiones externas e internas y que afectan la capacidad para lograr los resultados previstos del SGSI?	Se encuentra identificado el contexto de la Organización (Misión, visión, misión, visión, objetivos estratégicos, estructura organizacional, productos, servicios prestados, otros)	100%
4.2	Comprensión de las necesidades y expectativas de las partes interesadas	Se han determinado las partes interesadas del SGSI y los requisitos de estas partes interesadas	No se han establecido las necesidades y expectativas de las partes interesadas	0
4.3	Determinación del alcance del sistema de Seguridad de la información	Se ha definido el alcance del SGSI?	Como parte del alcance del proyecto de implementación del Sistema de Gestión de Seguridad de la Información, se ha definido el alcance para los procesos estratégicos, misionales y de apoyo de la aseguradora.	0
4.4	Sistema de gestión de seguridad de la información	Se ha establecido, implementado, mantenido y mejorado el SGSI?	Se encontró que no se ha establecido, implementado, mantenido y mejorado el SGSI	0
5. Liderazgo				**100%**
5.1	Liderazgo y compromiso	La alta dirección ha demostrado liderazgo y compromiso con respecto al SGSI, estableciendo la política, objetivos, recursos para el SGSI, comunicando la importancia de un SGSI, logro de los resultados, promoviendo la mejora continua?	La alta dirección ha establecido la política y los objetivos del SGSI. Ha promovido el levantamiento de los activos de información por cada proceso y la realización de su valoración en términos de su confidencialidad, integridad y disponibilidad. Ha promovido el análisis de Riesgos Así como campañas de divulgación.	100%
5.2	Política	Se ha documentado la política del SGSI	Se encontró definida la política de seguridad de la información?	100%

LISTA DE CHEQUEO ANALISIS GAP ISO 27001:2013				
Código ISO	**Nombre ISO**	**Pregunta**	**Estado Actual del objetivo de control y control**	**Cumplimiento**
5.3	Roles, responsabilidades y autoridades en la organización	Se han asignado y comunicado los roles y responsabilidades para el SGSI?	Se han definido roles y responsabilidades para los responsables de los procesos así como para el personal del área de tecnología	100%
6. Planificación				**17%**
6.1	Acciones para tratar los riesgos y oportunidades			33%
6.1.1	Generalidades	Al planificar el SGSI se ha tenido en cuenta el contexto de la organización las partes interesadas y sus requisitos?	En el sistema de administración de riesgos (Operativos y LAFT), el cual es utilizado para el análisis y tratamiento de riesgos en toda la Organización se ha tenido en cuenta el contexto de la organización y sus partes interesadas	0
6.1.2	Valoración de los riesgos de seguridad de la información	Se conserva información documentada acerca del proceso de valoración de riesgos del SGSI?	Actualmente se cuenta con un sistema de administración de riesgos (Operativos y LAFT), el cual es utilizado para el análisis de riesgos en toda la Organización. Sin embargo, dentro de las actividades descritas, no se puede establecer los pasos a seguir en el proceso de análisis de riesgos de seguridad de la información, debido a que las actividades se encuentran en diferentes documentos y no hay un enlace entre las mismas: Manual del sistema de administración de riesgos – SAR Metodología Riesgos No Financieros	100%
6.1.3	Tratamiento de riesgos de seguridad de la información	Se conserva información documentada acerca del proceso de tratamiento de riesgos	Actualmente se cuenta con un sistema de administración de riesgos (Operativos y LAFT), el cual es utilizado para el	0

LISTA DE CHEQUEO ANALISIS GAP ISO 27001:2013				
Código ISO	**Nombre ISO**	**Pregunta**	**Estado Actual del objetivo de control y control**	**Cumplimiento**
		del SGSI y de la declaración de aplicabilidad?	tratamiento de riesgos en toda la Organización. Sin embargo, dentro de las actividades descritas, no se puede establecer los pasos a seguir en el proceso de tratamiento de riesgos de seguridad de la información, debido a que las actividades se encuentran en diferentes documentos y no hay un enlace entre las mismas: Manual del sistema de administración de riesgos – SAR Metodología Riesgos No Financieros La norma establece la necesidad de documentar los objetivos de control y controles que se van a implementar en la Organización, así como la justificación de aquellos controles que no van a ser implementados. Para conseguir este listado, se requiere de la identificación de los riesgos de seguridad de la información. Actualmente, no se cuenta con éste documento (Declaración de Aplicabilidad).	
6.2	Objetivos de seguridad de la información y planes para lograrlos	Se conserva información documentada sobre los objetivos del SGSI?	Aunque se encuentran establecidos los objetivos de Seguridad de la Información, no se han definido las actividades y responsables para lograrlos	0
7. Apoyo				**63%**

LISTA DE CHEQUEO ANALISIS GAP ISO 27001:2013				
Código ISO	**Nombre ISO**	**Pregunta**	**Estado Actual del objetivo de control y control**	**Cumplimiento**
7.1	Recursos	Se han proporcionado recursos para el establecimiento, implementación, mantenimiento y mejora continua del SGSI?	Se evidencia la asignación de recursos para el SGSI.	100%
7.2	Competencia	Se ha determinado la competencia del personal que afecta el desempeño de la seguridad de la información?	Se encuentran definidas las competencias en el manual de perfiles del personal que interviene en el SGSI	100%
7.3	Toma de Conciencia	Se ha proporcionado concientización a las personas que afectan el desempeño del SGSI?	Se encontró que se ha realizado la divulgación de la política de seguridad informática a todo el personal por Intranet, pero no se han realizado charlas de sensibilización de la seguridad de la información.	0
7.4	Comunicación	Se ha determinado la necesidad de comunicaciones internas y externas para el SGSI?	Se cuenta con área de comunicación para divulgación de comunicaciones intenas del SGSI, además se cuenta con la herramienta Isodoc para consulta de documentos del SGSI	100%
7.5	Información documentada			67%
7.5.1	Generalidades	Cuenta con información documentada solicitada por la norma ISO/IEC 27001:2013 y la necesaria para demostrar eficacia del SGSI?	Se encuentra en elaboración y aprobación documentos solicitados por la norma ISO/IEC 27001:2013, se encontró documentación de operación de tecnología importante para evidenciar cumplimiento de controles del SGSI	0
7.5.2	Creación y actualización	Se cuenta con un procedimiento para identificación y descripción de la documentación y para revisión y aprobación?	La aseguradora cuenta con un procedimiento para identificación y descripción de la documentación y para revisión y aprobación.	100%

LISTA DE CHEQUEO ANALISIS GAP ISO 27001:2013				
Código ISO	**Nombre ISO**	**Pregunta**	**Estado Actual del objetivo de control y control**	**Cumplimiento**
7.5.3	Control de la información documentada	La información documentada se encuentra disponible, protegida adecuadamente, protegida contra el control de cambios y se tienen controles de distribución, acceso, recuperación y uso?	Se encontró que la información documentada como políticas, procedimientos, instructivos, y formatos se encuentra disponible en la herramienta Isodoc, protegida contra la pérdida de confidencialidad, uso inadecuado, y contra la pérdida de integridad ya que los documentos se encuentran en pdf o con control de edición. Así mismo se encuentra protegida contra el control de cambios, almacenamiento y preservación.	100%
8. Operación				**33%**
8.1	Planificación y control operacional	Se han planificado, implementado y controlado los procesos necesarios para cumplir los requisitos del SGSI así como para implementar las acciones de tratamiento de riesgos? Se han implementado planes para lograr los objetivos de seguridad?	La Organización estableció un plan para implementar el SGSI, el cual fue ejecutado conforme a lo establecido.	0
8.2	Valoración de los riesgos de seguridad de la información	Se conserva información documentada de los resultados de las valoraciones de riesgos?	La evaluación de riesgos se realiza semestralmente y los resultados son presentados a la Junta Directiva.	100%
8.3	Tratamiento de riesgos de seguridad de la información	Se conserva información documentada de los resultados de tratamientos de riesgos?	Actualmente se está iniciando con la definición de los planes de tratamiento de riesgos.	0
9.Evaluación del desempeño				**33%**

LISTA DE CHEQUEO ANALISIS GAP ISO 27001:2013				
Código ISO	**Nombre ISO**	**Pregunta**	**Estado Actual del objetivo de control y control**	**Cumplimiento**
9.1	Seguimiento, medición, análisis y evaluación	Se ha determinado a qué procesos y controles de seguridad de la información hacer seguimiento y medir?	Se estableció la forma de medir el desempeño del SGSI, pero no se ha llevado a cabo el análisis y evaluación del mismo.	0
9.2	Auditoría interna	Se conserva información documentada de la implementación del programa de auditorías y de sus resultados?	Se realizan auditorías internas a intervalos planificados de acuerdo con los procedimientos establecidos. Se evidencia programa, plan, listas de verificación e informe de auditoría.	100%
9.3	Revisión por la dirección	Se conserva información documentada como evidencia de la revisión por la dirección?	Se realiza revisión por la dirección del Sistema de Gestión de Seguridad de la Información, sin embargo, ésta no cumple con los requisitos definidos en la norma.	0
10. Mejoramiento				0
10.1	No conformidad y acciones correctivas	Se conserva información documentada de la naturaleza de las no conformidades, de cualquier acción posterior y de resultados de acción correctiva?	Se identifican las no conformidades (hallazgos) de acuerdo con los procedimientos establecidos, resultados estos del proceso de auditoría. Sin embargo, el seguimiento depende de la criticidad de los mismos.	0
10.2	Mejora continua	Se ha realizado la mejora continua al SGSI?	Se cuenta con un proceso de mejora continua pero aún no se ha realizado esta mejora continua al SGSI	0

Tabla 7. Resultado evaluación detallada de cumplimiento de la norma ISO 27001:2013

8.2.2 Nivel de cumplimiento general – ISO 27001:2013

Con base en los resultados obtenidos a continuación, se presentan los resultados generales de cumplimiento de la norma ISO 27001:2013.

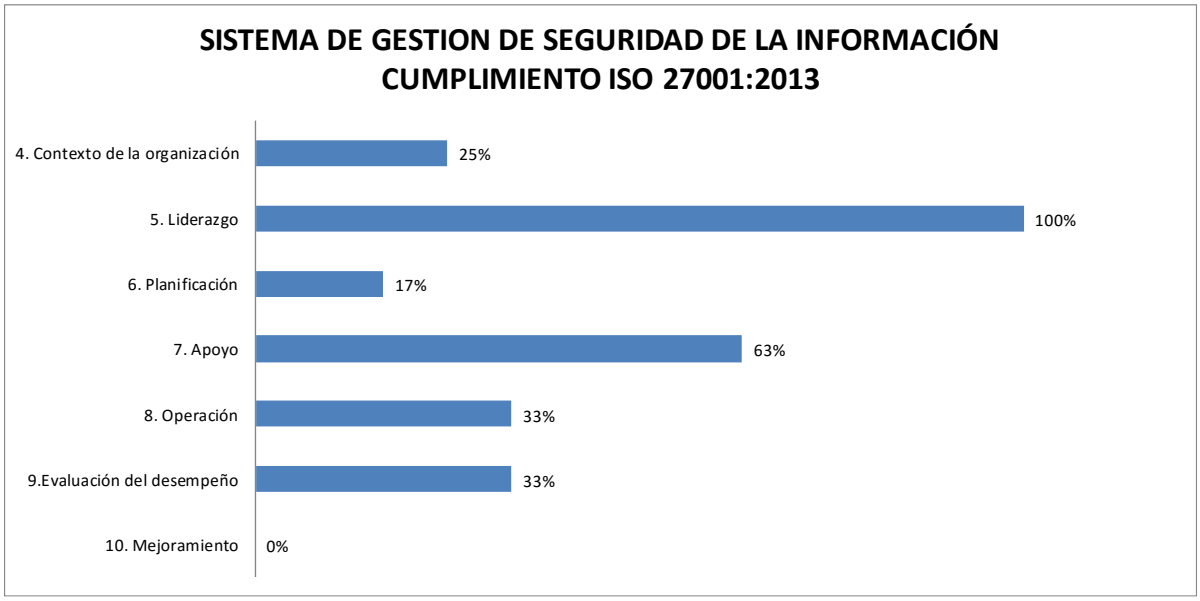

Ilustración 8. Resultado grafico del cumplimiento ISO 27001:2013

Dominio	Puntaje
4. Contexto de la organización	25%
5. Liderazgo	100%
6. Planificación	17%
7. Apoyo	63%
8. Operación	33%
9.Evaluación del desempeño	33%
10. Mejoramiento	0%
PROMEDIO	***39%***

**Los valores son redondeados.*

Tabla 8. Nivel de cumplimiento ISO 27001:2013

8.2.3 Nivel de cumplimiento – ISO 27002:2013

Se aplica para la evaluación de los controles de seguridad de la información la norma internacional ISO/IEC 27002:2013, obteniendo los siguientes resultados:

Ilustración 9. Resultado grafico del cumplimiento ISO 27001:2013

El puntaje obtenido para cada uno de los dominios se presenta a continuación:

PUNTAJE - DOMINIO	
DOMINIO	**Puntaje**
5. Políticas de seguridad de la información	100%
6. Organización de la seguridad de la información	20%
7. Seguridad de los recursos humanos	61%
8. Gestión de Activos	17%
9. Control de acceso	33%
10. Controles criptográficos	0
11. Seguridad física y del entorno	56%
12. Seguridad en las operaciones	50%
13. Seguridad en las comunicaciones	50%
14. Adquisición, desarrollo y mantenimiento de sistemas de información	70%
15. Relación con proveedores	0
16. Gestión de los incidentes de la seguridad de la información	0
17. Aspectos de seguridad Información en la gestión de continuidad del negocio	45%
18. Cumplimiento	53%
PROMEDIO	**40%**

Tabla 9. Nivel de cumplimiento ISO 27002:2013

Se puede concluir que se observan importante oportunidad de mejora, con respecto a la norma internacional ISO/IEC 27001:2013 se obtuvo un puntaje de cumplimiento del 39%, y para la 27002:2013 que mide el nivel de cumplimientos de controles de

seguridad se obtuvo un 40%. Por lo anterior, es perentorio que el portafolio de proyectos de seguridad de la información debe incluir un proyecto que permita el fortalecimiento y mejoramiento del sistema de gestión de seguridad de la información para la aseguradora.

8.2.4 Nivel de Madurez del Modelo de seguridad de la información

Una vez analizada la información anterior, se procede a determinar el nivel de madurez del modelo de seguridad de la información tomando como referencia el modelo de madurez establecido por el Framework Cobit 4.1.[21]

NIVEL DE MADUREZ MODELO DE SEGURIDAD DE LA INFORMACION	
Dominio	**Nivel de Madurez**
4. Contexto de la organización	1
5. Liderazgo	2
6. Planificación	2
7. Apoyo	3
8. Operación	2
9.Evaluación del desempeño	2
10. Mejoramiento	2
Nivel de Madurez ISO 27001:2013	**2**
5. Políticas de seguridad de la información	2
6. Organización de la seguridad de la información	2
7. Seguridad de los recursos humanos	3
8. Gestión de Activos	2
9. Control de acceso	2
10. Controles criptográficos	1
11. Seguridad física y del entorno	2
12. Seguridad en las operaciones	2
13. Seguridad en las comunicaciones	2
14. Adquisición, desarrollo y mantenimiento de sistemas de información	3
15. Relación con proveedores	2
16. Gestión de los incidentes de la seguridad de la información	2
17. Aspectos de seguridad Información en la gestión de continuidad del negocio	3
18. Cumplimiento	3
Nivel de Madurez ISO 27002:2013	**2**

Tabla 10. Nivel de madurez ISO 27001:2013 e ISO 27002:2013

Teniendo en cuenta lo anterior, el nivel de madurez del modelo de seguridad de la información, obtiene una calificación de dos (2), lo que significa que la Compañía

[21] http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/COBIT-4-1.aspx

que los procesos y los controles siguen un patrón regular, donde los procesos se han desarrollado hasta el punto en que diferentes procedimientos son seguidos por diferentes personas, aun no existe formación ni comunicación formal sobre los procedimientos y estándares de seguridad de la información. Se evidencia un alto grado de confianza en los conocimientos de cada persona, por eso hay probabilidad de que se comentan errores.

El nivel de madurez es considerado bajo para el nivel requerido que en promedio del sector es del 3,5, por lo que se hace necesario abordar iniciativas que permitan mejorar esta puntuación.

ANEXO 8.3 ANÁLISIS Y PRIORIZACIÓN DE INICIATIVAS.

Teniendo en cuenta el resultado anterior, se identifican las iniciativas de seguridad de la información, los cuales deben están alineadas con el plan estratégico corporativo, y a las necesidades que se identificaron en los procesos del negocio, conforme al resultado de las entrevistas y del diagnóstico realizado con respecto al cumplimento y nivel de madurez del modelo de seguridad de la información.

Las iniciativas estén enmarcadas dentro de los controles sugeridos para garantizar una adecuada arquitectura de seguridad de la información y un esquema de defensa a profundidad utilizando soluciones de tecnología y las nuevas tendencias de seguridad de la información.

INICIATIVA	DESCRIPCIÓN INICIATIVA	Estrategia Seguridad de la Información Objetivos de seguridad			
		Gobierno o Modelo de seguridad de información	Gestión de riesgos de Seguridad	Desarrollo y gestión del programa de seguridad de la in formación.	Gestión de incidentes de seguridad de la información.
I.00	Elaborar el plan estratégico de seguridad de la información	X			
I.01	Monitorear y evaluar los cambios que se produzcan en la empresa, el entorno y la tecnología.	X			
I.02	Diseñar y documentar un programa anual de capacitación y sensibilización en seguridad de la información para empleados, proveedores e intermediarios de la aseguradora.	X			
I.03	Implementar el programa anual de capacitación y sensibilización en seguridad de la información para empleados, proveedores e intermediarios de la aseguradora.	X			

INICIATIVA	DESCRIPCIÓN INICIATIVA	Estrategia Seguridad de la Información Objetivos de seguridad			
		Gobierno o Modelo de seguridad de información	Gestión de riesgos de Seguridad	Desarrollo y gestión del programa de seguridad de la in formación.	Gestión de incidentes de seguridad de la información.
I.04	Diseñar y documentar el programa de ejercicios al plan de recuperación ante desastres, ante escenarios de fallas de las tecnologías, garantizando que se mantengan los controles de seguridad.	X			
I.05	Ejecutar el programa de ejercicios al plan de recuperación ante desastres, ante escenarios de fallas de las tecnologías, garantizando que se mantengan los controles de seguridad.	X			
I.06	Implementar los servicios de seguridad administrada a través de un Centro de operaciones de seguridad de la información (SOC), que permita tener capacidades suficientes para operar la seguridad de la información	X			
I.07	Diseñar y documentar un programa anual de auditoría informática periódico a los sistemas de información internos como de los servicios que proveen los terceros.	X			
I.08	Implementar el programa de auditoría informática anual periódico a los sistemas de información internos como de los servicios que proveen los terceros.				
I.09	Implementar una herramienta que permita la administración del sistema de gestión de seguridad de la información, la administración de los activos de información, la gestión del riesgo, el control documental y las revisiones de auditoría.	X			
I.10	Diseñar indicadores que permitan evaluar la eficacia de la gestión de la seguridad de la información.	X			
I.11	Implementar indicadores que permitan evaluar la eficacia de la gestión de los controles de seguridad de la información	X			
I.12	Definir y establecer una política y un procedimiento formal y sistemático para reportar y escalar los eventos e incidentes de seguridad.				X

INICIATIVA	DESCRIPCIÓN INICIATIVA	Estrategia Seguridad de la Información Objetivos de seguridad			
		Gobierno o Modelo de seguridad de información	Gestión de riesgos de Seguridad	Desarrollo y gestión del programa de seguridad de la in formación.	Gestión de incidentes de seguridad de la información.
I.13	Definir y establecer un procedimiento formal para el tratamiento de información de producción en ambientes de desarrollo y prueba, en el cual se establezcan controles para proteger la confidencialidad de la información.			X	
I.14	Definir y establecer la metodología de desarrollo seguro			X	
I.15	Definir y establecer las políticas y procedimientos relacionados con la gestión de usuarios privilegiados que administren las plataformas tecnológicas (servidores, elementos de red, bases de datos), así como a las funciones de negocio que requieren el uso de privilegios.			X	
I.16	Establecer e implementar la Gestión de cambios, proceso que debe incluir el análisis de riesgos de seguridad.			X	
I.17	Implementar y celebrar Cláusulas de confidencialidad, integridad y seguridad de la información en contratos con empleados y proveedores que prestan servicios a la Compañía			X	
I.18	Definir e implementar una política sobre el uso de controles criptográficos para la protección de la información en la organización.			X	
I.19	Establecer e implementar una política de copias de respaldo para salvaguardar la información crítica para la aseguradora.			X	
I.20	Actualizar los activos de información y realizar su valoración según la criticidad para la compañía, igualmente identificar los riesgos de seguridad de la información asociados		X		
I.21	Establecer e implementar una metodología para la gestión de riesgos de seguridad de la información.		X		
I.22	Identificar los riesgos de seguridad de la información para cada uno de los procesos		X		

INICIATIVA	DESCRIPCIÓN INICIATIVA	Estrategia Seguridad de la Información Objetivos de seguridad			
		Gobierno o Modelo de seguridad de información	Gestión de riesgos de Seguridad	Desarrollo y gestión del programa de seguridad de la in formación.	Gestión de incidentes de seguridad de la información.
I.23	Definir y establecer un proceso sistemático de gestión de riesgos de seguridad de la información.		X		
I.24	Monitorear a los terceros periódicamente para verificar que los controles de seguridad, los acuerdos de servicio definidos y demás requerimientos de seguridad que se contrataron están siendo implementados, operados y mantenidos.				X
I.25	Monitorear la adecuada gestión de usuarios privilegiados			X	
I.26	Monitorear el cumplimiento del ciclo de vida de gestión de usuarios (creación, modificación, activación, desactivación, eliminación, entre otros) verificando que se cumple para todas las aplicaciones.			X	
I.27	Implementar la gestión centraliza de usuarios para todos los aplicativos del negocio			X	
I.28	Implementar una solución de gestión de identidades para usuarios privilegiados			X	
I.29	Implementar una solución como servicio de borrado seguro de información			X	
I.30	Implementar como servicio una solución de anti malware avanzado para la protección contra amenazas avanzadas persistentes (APT).			X	
I.31	Establecer e implementar pruebas, análisis y gestión de vulnerabilidades a los elementos de mayor criticidad tanto a nivel de infraestructura como a nivel de aplicaciones web.			X	
I.32	Establecer e implementar pruebas de Hacking Ético sobre los aplicativos críticos a nivel de aplicaciones web.			X	
I.33	Implementar como servicio las pruebas de desarrollo seguro que combinan análisis de seguridad de código estático y de código dinámico, para revisar las aplicaciones Web y de dispositivos			X	

INICIATIVA	DESCRIPCIÓN INICIATIVA	Estrategia Seguridad de la Información Objetivos de seguridad			
		Gobierno o Modelo de seguridad de información	Gestión de riesgos de Seguridad	Desarrollo y gestión del programa de seguridad de la in formación.	Gestión de incidentes de seguridad de la información.
	móviles, e identificar vulnerabilidades y brechas de seguridad.				
I.34	Establecer y fortalecer las políticas de firewall y reglas de enrutamiento para prevenir accesos no autorizados a la gestión de equipos, aplicaciones y/o dispositivos de red.			X	
I.35	Implementar los mecanismos de cifrado sobre las web Services (intercambio de información seguros).			X	
I.36	Implementar los mecanismos de cifrado sobre el servicio de correo electrónico.			X	
I.37	Implementar una solución que permite la transferencia segura de archivos, mediante protocolos de cifrado			X	
I.38	Implementar una solución para la generación de copias de seguridad para respaldar la información crítica del negocio y/o archivos vitales.			X	
I.39	Implementar esquemas de contingencia en los sistemas de información para cumplir con la disponibilidad requerida por los procesos.			X	
I.40	Implementar una solución de DLP (Data Loss Prevention), con el fin de controlar y monitorear el intercambio de información confidencial y/o sensible.			X	
I.41	Definición de fuentes a monitorear con un objetivo de prevención de fuga de información.			X	
I.42	Implementar capacidades en un Centro de operaciones de seguridad (SOC por sus siglas en inglés), para la identificación y gestión de los incidentes de seguridad.			X	
I.43	Potencializar las capacidades del SOC, integrando fuentes relacionadas con procesos y activos que están expuestos al riesgo de pérdida de la confidencialidad e integridad resultado del análisis de riesgos y valoración del activo de información.	X			

INICIATIVA	DESCRIPCIÓN INICIATIVA	Estrategia Seguridad de la Información Objetivos de seguridad			
		Gobierno o Modelo de seguridad de información	Gestión de riesgos de Seguridad	Desarrollo y gestión del programa de seguridad de la in formación.	Gestión de incidentes de seguridad de la información.
I.44	Implementar una solución como servicio de un Firewall de base de datos para la protección y monitoreo.			X	
I.45	Implementar una solución como servicio de Firewall de aplicaciones Web para la protección de aplicaciones Web			X	
I.46	Implementar soluciones de seguridad que permiten tener total auditoría y control sobre la infraestructura contratada en la nube			X	
I.47	Monitoreo de los servicios de la Nube IaaS			X	
I.48	Implementar el servicio de enmascaramiento en ambientes de desarrollo y pruebas sobre los servicios que se prestan en computación en la nube.			X	
I.49	Implementar un correlacionador de eventos (SIEM) como servicios para monitorear el comportamiento de activos de información críticos.			X	
I.50	Implementar la solución de Enterprise Mobility Management (EMS) que integre estos componentes: Monitoreo de aplicaciones para validar la seguridad en las App instaladas, Seguridad en contenido y prevención de fuga de información			X	
I.51	Implementar como servicio el monitoreo de marca			X	
I.52	Operar y mantener el Sistema de Gestión de Continuidad del Negocio, incluyendo todos los procesos de la compañía.			X	
I.53	Desarrollar el programa de ejercicios y pruebas de continuidad con proveedores que prestan servicios críticos.			X	
I.54	Operar y mantener el sistema de gestión de seguridad de la información SGSI, incluyendo todos los procesos de la compañía.			X	
I.55	Capacitación especializada en seguridad de la información y seguridad	X			

INICIATIVA	DESCRIPCIÓN INICIATIVA	Estrategia Seguridad de la Información Objetivos de seguridad			
		Gobierno o Modelo de seguridad de información	Gestión de riesgos de Seguridad	Desarrollo y gestión del programa de seguridad de la in formación.	Gestión de incidentes de seguridad de la información.
	informática para los responsables del SGSI.				
I.56	Asegurar el mejoramiento continuo del Sistema de Gestión de seguridad de la información para responder a los cambios futuros.			X	
I.57	Asegurar el uso y apropiación de las redes Sociales corporativas			X	
I.58	Asegurar el uso y apropiación de aplicaciones móviles corporativas.			X	
I.59	Asegurar el uso y apropiación del internet de las cosas.			X	
I.60	Asegurar el uso y adaptación de modelos de negocio digitales.			X	
I.61	Asegurar el uso y adaptación e entornos de computación en la nube			X	
I.62	Asegurar el uso y adaptación a las iniciativas de analítica Big Data			X	
I.63	Asegurar el uso y adaptaciones al pago con Moneda Digital (Criptomonedas)			X	
I.64	Asegurar en uso de los datos en aprendizaje automático (Inteligencia artificial)			X	
I.65	Implementar indicadores del sistema de gestión de seguridad de la información	X			
I.66	Sensibilización y capacitación en continuidad del negocio	X			
I.67	Entrenamiento a los equipos de recuperación de los procesos críticos del negocio	X			

Tabla 11. Iniciativas de seguridad de la información versus objetivos estrategicos de SI

ANEXO 8.4 DEFINICIÓN DEL PORTAFOLIO DE PROYECTOS DE SEGURIDAD DE LA INFORMACIÓN

A continuación, se presentan las iniciativas de seguridad agrupadas por proyectos:

PROYECTO	DESCRIPCIÓN PROYECTO	INICIATIVA	DESCRIPCIÓN INICIATIVA
P0	Gestión del Programa	I.00	Elaborar el plan estratégico de seguridad de la información
P0	Gestión del Programa	I.01	Monitorear y evaluar los cambios que se produzcan en la empresa, el entorno y la tecnología.
P0	Gestión del Programa	I.04	Diseñar y documentar el programa de ejercicios al plan de recuperación ante desastres, ante escenarios de fallas de las tecnologías, garantizando que se mantengan los controles de seguridad.
P0	Gestión del Programa	I.06	Implementar los servicios de seguridad administrada a través de un Centro de operaciones de seguridad de la información (SOC), que permita tener capacidades suficientes para operar la seguridad de la información
P0	Gestión del Programa	I.07	Diseñar y documentar un programa anual de auditoría informática periódico a los sistemas de información internos como de los servicios que proveen los terceros.
P0	Gestión del Programa	I.09	Implementar una herramienta que permita la administración del sistema de gestión de seguridad de la información, la administración de los activos de información, la gestión del riesgo, el control documental y las revisiones de auditoría.
P0	Gestión del Programa	I.10	Diseñar indicadores que permitan evaluar la eficacia de la gestión de la seguridad de la información.
P0	Gestión del Programa	I.56	Asegurar el mejoramiento continuo del Sistema de Gestión de seguridad de la información para responder a los cambios futuros.
P1	Operación y mantenimiento del Sistema de Gestión de Seguridad de la información	I.08	Implementar el programa de auditoría informática anual periódico a los sistemas de información internos como de los servicios que proveen los terceros.
P1	Operación y mantenimiento del Sistema de Gestión de Seguridad de la información	I.11	Implementar indicadores que permitan evaluar la eficacia de la gestión de los controles de seguridad de la información
P1	Operación y mantenimiento del Sistema de Gestión de Seguridad de la información	I.12	Definir y establecer una política y un procedimiento formal y sistemático para reportar y escalar los eventos e incidentes de seguridad.
P1	Operación y mantenimiento del Sistema de Gestión de Seguridad de la información	I.13	Definir y establecer un procedimiento formal para el tratamiento de información de producción en

PROYECTO	DESCRIPCIÓN PROYECTO	INICIATIVA	DESCRIPCIÓN INICIATIVA
			ambientes de desarrollo y prueba, en el cual se establezcan controles para proteger la confidencialidad de la información.
P1	Operación y mantenimiento del Sistema de Gestión de Seguridad de la información	I.14	Definir y establecer la metodología de desarrollo seguro
P1	Operación y mantenimiento del Sistema de Gestión de Seguridad de la información	I.15	Definir y establecer las políticas y procedimientos relacionados con la gestión de usuarios privilegiados que administren las plataformas tecnológicas (servidores, elementos de red, bases de datos), así como a las funciones de negocio que requieren el uso de privilegios.
P1	Operación y mantenimiento del Sistema de Gestión de Seguridad de la información	I.16	Establecer e implementar la Gestión de cambios, proceso que debe incluir el análisis de riesgos de seguridad.
P1	Operación y mantenimiento del Sistema de Gestión de Seguridad de la información	I.17	Implementar y celebrar Cláusulas de confidencialidad, integridad y seguridad de la información en contratos con empleados y proveedores que prestan servicios a la Compañía
P1	Operación y mantenimiento del Sistema de Gestión de Seguridad de la información	I.18	Definir e implementar una política sobre el uso de controles criptográficos para la protección de la información en la organización.
P1	Operación y mantenimiento del Sistema de Gestión de Seguridad de la información	I.19	Establecer e implementar una política de copias de respaldo para salvaguardar la información crítica para la aseguradora.
P1	Operación y mantenimiento del Sistema de Gestión de Seguridad de la información	I.54	Operar y mantener el sistema de gestión de seguridad de la información SGSI, incluyendo todos los procesos de la compañía.
P1	Gestión del Programa	I.65	Implementar indicadores del sistema de gestión de seguridad de la información
P2	Gestión de Riesgos de Seguridad de la información	I.20	Actualizar los activos de información y realizar su valoración según la criticidad para la compañía, igualmente identificar los riesgos de seguridad de la información asociados
P2	Gestión de Riesgos de Seguridad de la información	I.21	Establecer e implementar una metodología para la gestión de riesgos de seguridad de la información.
P2	Gestión de Riesgos de Seguridad de la información	I.22	Identificar los riesgos de seguridad de la información para cada uno de los procesos

PROYECTO	DESCRIPCIÓN PROYECTO	INICIATIVA	DESCRIPCIÓN INICIATIVA
P2	Gestión de Riesgos de Seguridad de la información	I.23	Definir y establecer un proceso sistemático de gestión de riesgos de seguridad de la información.
P3	Defensa en profundidad	I.29	Implementar una solución como servicio de borrado seguro de información
P3	Defensa en profundidad	I.30	Implementar como servicio una solución de anti malware avanzado para la protección contra amenazas avanzadas persistentes (APT).
P3	Defensa en profundidad	I.31	Establecer e implementar pruebas, análisis y gestión de vulnerabilidades a los elementos de mayor criticidad tanto a nivel de infraestructura como a nivel de aplicaciones web.
P3	Defensa en profundidad	I.32	Establecer e implementar pruebas de Hacking Ético sobre los aplicativos críticos a nivel de aplicaciones web.
P3	Defensa en profundidad	I.33	Implementar como servicio las pruebas de desarrollo seguro que combinan análisis de seguridad de código estático y de código dinámico, para revisar las aplicaciones Web y de dispositivos móviles, e identificar vulnerabilidades y brechas de seguridad.
P3	Defensa en profundidad	I.34	Establecer y fortalecer las políticas de firewall y reglas de enrutamiento para prevenir accesos no autorizados a la gestión de equipos, aplicaciones y/o dispositivos de red.
P3	Defensa en profundidad	I.37	Implementar una solución que permite la transferencia segura de archivos, mediante protocolos de cifrado
P3	Defensa en profundidad	I.38	Implementar una solución para la generación de copias de seguridad para respaldar la información crítica del negocio y/o archivos vitales.
P3	Defensa en profundidad	I.40	Implementar una solución de DLP (Data Loss Prevention), con el fin de controlar y monitorear el intercambio de información confidencial y/o sensible.
P3	Defensa en profundidad	I.44	Implementar una solución como servicio de un Firewall de base de datos para la protección y monitoreo.
P3	Defensa en profundidad	I.46	Implementar soluciones de seguridad que permiten tener total auditoría y control sobre la infraestructura contratada en la nube

PROYECTO	DESCRIPCIÓN PROYECTO	INICIATIVA	DESCRIPCIÓN INICIATIVA
P3	Defensa en profundidad	I.48	Implementar el servicio de enmascaramiento en ambientes de desarrollo y pruebas sobre los servicios que se prestan en computación en la nube.
P3	Defensa en profundidad	I.49	Implementar un correlacionador de eventos (SIEM) como servicios para monitorear el comportamiento de activos de información críticos.
P3	Defensa en profundidad	I.50	Implementar la solución de Enterprise Mobility Management (EMS) que integre estos componentes: Monitoreo de aplicaciones para validar la seguridad en las App instaladas, Seguridad en contenido y prevención de fuga de información
P4	Seguridad en aplicaciones	I.35	Implementar los mecanismos de cifrado sobre los web services (intercambio de información seguros).
P4	Seguridad en aplicaciones	I.36	Implementar los mecanismos de cifrado sobre el servicio de correo electrónico.
P4	Seguridad en aplicaciones	I.45	Implementar una solución como servicio de Firewall de aplicaciones Web para la protección de aplicaciones Web
P5	Gestión de accesos y privilegios	I.25	Monitorear la adecuada gestión de usuarios privilegiados
P5	Gestión de accesos y privilegios	I.26	Monitorear el cumplimiento del ciclo de vida de gestión de usuarios (creación, modificación, activación, desactivación, eliminación, entre otros) verificando que se cumple para todas las aplicaciones.
P5	Gestión de accesos y privilegios	I.27	Implementar la gestión centraliza de usuarios para todos los aplicativos del negocio
P5	Gestión de accesos y privilegios	I.28	Implementar una solución de gestión de identidades para usuarios privilegiados
P6	Desarrollar cultura y competencias en seguridad de la información	I.02	Diseñar y documentar un programa anual de capacitación y sensibilización en seguridad de la información para empleados, proveedores e intermediarios de la aseguradora.
P6	Desarrollar cultura y competencias en seguridad de la información	I.03	Implementar el programa anual de capacitación y sensibilización en seguridad de la información para empleados, proveedores e intermediarios de la aseguradora.

PROYECTO	DESCRIPCIÓN PROYECTO	INICIATIVA	DESCRIPCIÓN INICIATIVA
P6	Desarrollar cultura y competencias en seguridad de la información	I.55	Capacitación especializada en seguridad de la información y seguridad informática para los responsables del SGSI.
P6	Desarrollar cultura y competencias en seguridad de la información	I.66	Sensibilización y capacitación en continuidad del negocio
P6	Desarrollar cultura y competencias en seguridad de la información	I.67	Entrenamiento a los equipos de recuperación de los procesos críticos del negocio
P7	Gestión de proveedores (aseguramiento servicios)	I.24	Monitorear a los terceros periódicamente para verificar que los controles de seguridad, los acuerdos de servicio definidos y demás requerimientos de seguridad que se contrataron están siendo implementados, operados y mantenidos.
P8	Monitoreo Inteligente	I.41	Definición de fuentes a monitorear con un objetivo de prevención de fuga de información.
P8	Monitoreo Inteligente	I.42	Implementar capacidades en un Centro de operaciones de seguridad (SOC por sus siglas en inglés), para la identificación y gestión de los incidentes de seguridad.
P8	Monitoreo Inteligente	I.43	Potencializar las capacidades del SOC, integrando fuentes relacionadas con procesos y activos que están expuestos al riesgo de pérdida de la confidencialidad e integridad resultado del análisis de riesgos y valoración del activo de información.
P8	Monitoreo Inteligente	I.47	Monitoreo de los servicios de la Nube IaaS
P8	Monitoreo Inteligente	I.51	Implementar como servicio el monitoreo de marca
P9	Desarrollo y Gestión del programa de continuidad del Negocio	I.05	Ejecutar el programa de ejercicios al plan de recuperación ante desastres, ante escenarios de fallas de las tecnologías, garantizando que se mantengan los controles de seguridad.
P9	Desarrollo y Gestión del programa de continuidad del Negocio	I.39	Implementar esquemas de contingencia en los sistemas de información para cumplir con la disponibilidad requerida por los procesos.
P9	Desarrollo y Gestión del programa de continuidad del Negocio	I.52	Operar y mantener el Sistema de Gestión de Continuidad del Negocio, incluyendo todos los procesos de la compañía.

PROYECTO	DESCRIPCIÓN PROYECTO	INICIATIVA	DESCRIPCIÓN INICIATIVA
P9	Desarrollo y Gestión del programa de continuidad del Negocio	I.53	Desarrollar el programa de ejercicios y pruebas de continuidad con proveedores que prestan servicios críticos.
P10	Tendencias futuras de cumplimiento	I.57	Asegurar el uso y apropiación de las redes Sociales corporativas
P10	Tendencias futuras de cumplimiento	I.58	Asegurar el uso y apropiación de aplicaciones móviles corporativas.
P10	Tendencias futuras de cumplimiento	I.59	Asegurar el uso y apropiación del internet de las cosas.
P10	Tendencias futuras de cumplimiento	I.60	Asegurar el uso y adaptación de modelos de negocio digitales.
P10	Tendencias futuras de cumplimiento	I.61	Asegurar el uso y adaptación e entornos de computación en la nube
P10	Tendencias futuras de cumplimiento	I.62	Asegurar el uso y adaptación a las iniciativas de analítica Big Data
P10	Tendencias futuras de cumplimiento	I.63	Asegurar el uso y adaptaciones al pago con Moneda Digital (Criptomonedas)
P10	Tendencias futuras de cumplimiento	I.64	Asegurar en uso de los datos en aprendizaje automático (Inteligencia artificial)

Tabla 12. Portafolio de proyectos de seguridad de la información

A continuación, se presenta la priorización de los proyectos

PROYECTO	NOMBRE DE PROYECTO	Proyectos Priorizados				
		Prioridad 0 - PESI (Año 0)	Prioridad 1 - Estrategia de la Dirección de seguridad de la información (Año 1)	Prioridad 2 - Riesgos Operacionales (Año 2)	Prioridad 3 - Misional (Año 3)	Prioridad 4 - Desempeño
P0.0	Elaborar el plan estratégico de seguridad de la información	X				
P0	Gestión del Programa		X			
P1	Operación y mantenimiento del Sistema de Gestión de Seguridad de la información		X			
P2	Gestión de Riesgos de Seguridad de la información		X			
P3	Defensa en profundidad		X	X		

PROYECTO	NOMBRE DE PROYECTO	Proyectos Priorizados				
		Prioridad 0 - PESI (Año 0)	Prioridad 1 - Estrategia de la Dirección de seguridad de la información (Año 1)	Prioridad 2 - Riesgos Operacionales (Año 2)	Prioridad 3 - Misional (Año 3)	Prioridad 4 - Desempeño
P4	Seguridad en aplicaciones		X			
P5	Gestión de accesos y privilegios			X		
P6	Desarrollar cultura y competencias en seguridad de la información		X			
P7	Gestión de proveedores (aseguramiento servicios)		X			
P8	Monitoreo Inteligente			X		
P9	Desarrollo y Gestión del programa de continuidad del Negocio		X			
P10	Tendencias futuras de cumplimiento				X	

Tabla 13. Priorización Portafolio de proyectos de seguridad de la información

ANEXO 8.5 PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN

El plan estratégico corresponde a la ejecución de los proyectos definidos en el portafolio de proyectos de seguridad de la información que aportan al cumplimiento de los objetivos de seguridad de la información y al plan estratégico corporativo.

Ilustración 10. Plan estratégico de seguridad de la información