METODOLOGÍA PARA ALINEAR LA ISO 27001 AL MODELO OPERATIVO DE UNA ENTIDAD ASEGURADORA: caso de estudio

METHODOLOGY FOR ISO 27001 ALIGN TO FORM AN INSURANCE COMPANY OPERATING: case study

Carlos Javier Vargas García
Ingeniero Industrial
Universidad Militar Nueva Granada, Bogotá, Colombia,
cajavivargas@gmail.com.co

RESUMEN

Partiendo de la base que una metodología pretende plantear un camino o ruta a seguir en búsqueda de alcanzar un objetivo en particular, en este artículo, se toma como base el actual modelo operativo del área de tecnología de una entidad aseguradora y se plantea una alternativa que permite alinearlo con la Norma ISO 27001 particularmente en el numeral 4 (Sistema de gestión de seguridad de la información).

Inicialmente se efectuó un diagnóstico de la situación actual frente al numeral 4 de la norma ISO 27001:2006, al igual que frente a lo reglamentado en la circular externa No. 022 del 2010 de la Superintendencia financiera de Colombia para las entidades pertenecientes al sector financiero, posteriormente se hace una descripción del modelo operativo del área de tecnología, donde se plantean las diferentes políticas relacionadas entre otros, con el monitoreo de la infraestructura y la plataforma tecnológica, como también las relacionadas con los roles y responsabilidades en las diferentes áreas de la entidad.

Se plantea una propuesta de tratamiento a los incumplimientos detectados en el numeral 4 de la Norma en el diagnóstico y una metodología de integración entre la Norma ISO 27001:2006 y el modelo operativo del área de tecnología de la entidad aseguradora, que permite mantener y controlar la operación de esta, involucrando a todas las partes interesadas mediante una serie de fases que involucran desde la cuantificación de hallazgos o falencias detectadas frente a la Norma , pasando por el diseño de un plan estratégico de tecnología, hasta la fase de mejoramiento continuo.

Palabras clave: Metodología, ISO27001, modelo, operativo.

ABSTRACT

Assuming that a methodology aims at presenting a route or path to follow searching of achieving a particular objective, in this article, the basis is the current operating model technology area an insurer and an alternative is to can align with ISO 27001 particularly in paragraph 4 (safety Management System information).

Initially made a diagnosis of the current situation facing the numeral 4 of ISO 27001:2006, as compared to the External Circular Letter regulated in 2010, No. 022 of the Financial Superintendence of Colombia for financial sector entities, then provides a description of the operational model of the area of technology, where different policies arise related among others, monitoring of infrastructure and technology platform, as well as those related to the roles and responsibilities in different areas of the company .

It raises a treatment proposal to the breaches detected in Section 4 of the Standard for the diagnosis and methodology integration between ISO 27001:2006 and operating model technology area of the insurance company, which keeps operation and control of this, involving all stakeholders through a series of stages involving the quantification of findings from or detected failures under the standard, including the design of a strategic technology plan, to the continuous improvement phase.

Keywords: Methodology, ISO27001:2006, model, operative.

1. INTRODUCCIÓN

En primer lugar definimos el término “seguridad” que según la Real Academia de la Lengua Española se refiere como “Libre y exento de todo peligro, daño o riesgo” lo cual se evidencia a lo largo de la historia como un factor importante en la evolución del hombre, pues en un comienzo se basaba exclusivamente en salvaguardarse de los peligros que ofrecía la naturaleza, lo que con el paso de los años fue cambiando y no solo contemplaba este factor sino también la protección contra sus propios congéneres. Esto nos lleva a pensar que la seguridad informática se basa en la capacidad con que cuentan los sistemas informáticos para salvaguardarse de todo daño o peligro.

1.1 CONTEXTO DE LA EMPRESA

En 1956 nace UCONAL, Unión Cooperativa Nacional, fundada por Francisco Javier Mejía. Esta entidad de carácter cooperativo e integrador, busca tener su propia compañía de seguros para cubrir las necesidades que las cooperativas manifestaban en materia de seguros. Es así cuando le propone a Cuna Mutual trabajar en equipo para adquirir experiencia y entrenamiento suficiente para abarcar el mercado de los seguros. Para esta alianza era indispensable contar con un espacio físico adecuado, por tal razón se adelantaron todas las gestiones para la construcción de un edificio situado en Avenida Ciudad de Lima (Avenida 19) con carrera 13A que sirviera de sede para las dos instituciones. Se acordó entre las dos entidades, que Cuna Mutual, financiaría el proyecto y cedería a UCONAL el 50 % del costo con un plazo de 20 años para pagarlo.

En 1964 Cuna Mutual, la multinacional de seguro cooperativo que tiene asiento en 52 países del mundo, se establece en Colombia con autorización y reconocimiento de Dancoop, Departamento Administrativo de Cooperativas hoy en día la Superintendencia de Economía Solidaria. Cuna Mutual inicia ofreciendo servicios de seguros de vida sobre ahorros y protegiendo préstamos posteriormente, Vida Grupo y Fianza para Cooperativas.

Para 1975, en el mes de octubre se llevó a cabo el acto de inauguración, donde asistieron dirigentes del cooperativismo nacional e internacional, del gobierno y de la iglesia. El presidente de Cuna Mutual Robert Curry, expresó: “Dedicamos este edificio a los ideales del cooperativismo, al principio de hermandad del cooperativismo de ahorro y crédito que une a las gentes sin barreras sociales, religiosas, políticas o geográficas, en una organización que aspira a fomentar la dignidad entre los hombres y lograr paz en el mundo”.

Gracias al entrenamiento y cumplimiento de metas que se logró con Cuna Mutual, UCONAL decidió crear una nueva entidad en el ámbito de seguros a la cual fue invitado Coopdesarrollo para que se hiciera participe en esta gran creación. El 16 de diciembre de 1983 se llevó a cabo la asamblea de constitución de SEGUROS UCONAL, cuyo objetivo principal era proporcionar a los grupos pre-cooperativos, cooperativas de primer grado, instituciones auxiliares del cooperativismo, fondos de

empleados, fondos mutuos, fundaciones y demás entidades sin ánimo de lucro al igual que sus asociados y empleados, servicio de seguro de vida y generales para cumplir su objetivo.

El primero de julio de 1985 SEGUROS UCONAL inicia operaciones con cartera de seguros cedida por CUNA MUTUAL, como parte de su compromiso y política con las cooperativas de la región, contando con oficinas en Medellín, Barranquilla, Bucaramanga, Barrancabermeja, Cartagena, Pereira e Ibagué. Más tarde se vincularon empresas como Cupocrédito, Coopsibaté, Solidarios, Donmatías, Coopserfun y Cajacoop que contribuyeron con el capital.

Para 1993, seguros Uconal sufre cambios debido a la reforma financiera que se llevaba a cabo por esta época, motivo por el cual la Asamblea General de Seguros Uconal decide cambiar la razón social por Aseguradora Solidaria de Colombia Símbolo de unión cooperativa.

Aseguradora Solidaria de Colombia, institución auxiliar del cooperativismo especializada en la actividad aseguradora, constituida bajo los parámetros de la ley 18 de 1988 para el funcionamiento de las cooperativas, fondos de empleados y sociedades mutualistas, que en conjunto construyen la base de la economía solidaria en Colombia.

En comienzos del nuevo milenio, mediante notables esfuerzos se logra mantener y posicionar la Compañía en el mercado de seguros como una de las Aseguradoras de reconocida gestión en el país gozando de enorme credibilidad y satisfacción entre sus clientes y usuarios. Los excelentes resultados que arroja la Compañía la colocan en el primer puesto en rentabilidad patrimonial en el sector de seguros generales confirmando así la solidez evolución y crecimiento de Aseguradora Solidaria de Colombia.

Entre los años 2004 y 2005, la compañía de servicios exequiales Los Olivos, representada en Coopserfun, Serfuncoop, Corfuncoop, Serfullanos, Cartafun, Vivir, Coofuneraria, Serfunorte y Emcofun se convirtieron en los asociados de

Aseguradora Solidaria de Colombia después de que Megabanco cediera su participación.

Aseguradora Solidaria de Colombia lanza nueva estrategia de comunicación de marca con la frase “Solidaria es… tu familia, la mano que te abriga, quien te apoya, una mejor Colombia”. La campaña publicitaria muestra el espíritu de la compañía: La Solidaridad.

A partir del mes de septiembre de 2004 la Compañía fue abanderada en el tema de inversión social en su programa de ayuda a las comunidades menos favorecidas, donando más de 40 millones de pesos a seis fundaciones sociales de Bogotá, Medellín, Buga y Manzanares (Caldas).

Aseguradora Solidaria de Colombia traslada su sede de la dirección general al edificio inteligente 100 street ubicado en la calle 100 9A-45 mejorando así su infraestructura y ubicación para ofrecer una mejor calidad de servicio a sus clientes.

Se crea 'Solidaria es tu futuro', convenio educativo firmado por la compañía y el Icetex, el 10 de agosto de 2005, proyecto bandera para generar educación.

2. MATERIALES Y MÉTODOS

2.1 MATERIALES

En términos de seguridad de la información, la protección de los datos contra su pérdida o modificación no autorizada, garantiza la confidencialidad y disponibilidad. Cabe destacar que en Colombia para regular este tema se ha generado varias leyes y normas relacionadas con el tema como son entre otras:

LEY ESTATUTARIA 1266 DEL 31 DE DICIEMBRE DE 2008: Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones

LEY 1341 DEL 30 DE JULIO DE 2009: Por la cual se definen los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías

de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.
CE- 042 de 2010 - SUPERINTENDENCIA FINANCIERA DE COLOMBIA: Por medio de la cual se incorporan algunas modificaciones al Capítulo Décimo Segundo del Título Primero de la Circular Básica Jurídica, en materia de requerimientos mínimos de seguridad y calidad para la realización de operaciones
A nivel internacional:
NORMA ISO 27001:2006 "Sistema de gestión de Seguridad de la información"
ISO/IEC 17799:2005 Information technology - Security techniques - Code of practice for information security management.

2.2 MÉTODO

El método adoptado fue explorativo documental cuya fuente de formación fueron las leyes, decretos, resoluciones y personal vinculado a los procesos. Las etapas del método desarrollado fueron cuatro. Evaluación de los requerimientos de la norma ISO 27001:2006, comparación de los requisitos con el modelo operativo, estrategias para la integración y generación de políticas de seguridad informática para el área de tecnología de la empresa objeto de estudio.

2.2.1 Requerimientos de la Norma ISO27001

ISO/IEC 27001 es la única norma internacional auditable que define los requisitos para un sistema de gestión de la seguridad de la información (SGSI). La norma se ha concebido para garantizar la selección de controles de seguridad adecuados y proporcionales. La norma ISO/IEC 27001 especifica los requisitos para establecer, implantar, documentar y evaluar un Sistema de Gestión de la Seguridad de la Información (SGSI).

2.2.2 Modelo operativo

El modelo operativo de una entidad aseguradora donde sus agencias, convenios y socios estratégicos cargan la información relacionada con su producción en el sistema CORE del negocio.

2.2.3 Políticas de seguridad

La generación de políticas útiles para responsabilizar y comprometer a todos los funcionarios en la seguridad de la información.

2.2.4 Análisis de cumplimiento de requerimientos

Cumplimiento al numeral 4 “Sistema de Gestión de la Seguridad de la Información” de la Norma ISO 27001:2006 por parte del Área de Tecnología de la entidad Aseguradora.

2.2.5 Metodología de integración

Diseñada por fases.

3. RESULTADOS Y ANÁLISIS

A continuación se presentan los resultados obtenidos y la metodología propuesta.

3.1 ANALISIS DE REQUERIMIENTOS DE LA NORMA ISO27001

Mediante la siguiente Tabla 1, se explican los requerimientos de la norma ISO27001:2006 y su relación con los requerimientos de la Superintendencia Financiera.

ITEM	NORMA ISO 27001:2006	SUPER INTENDENCIA FINANCIERA CE No.022 del 2010	OBSERVACIONES
4.1 requerimientos Generarles	La organización debe establecer, implementar, operar, hacer seguimiento , revisar, mantener y mejorar un SGSI documentando, en el contexto de las actividades globales del negocio de la organización y de los riesgos que enfrenta	***Numeral 3.1.2*** Gestionar la seguridad de la información, para lo cual podrán tener como referencia el estándar ISO 27000, o el que lo sustituya.	No existe una política definida en la compañía

4.2.2 Implementación y operación del SGSI	La organización debe formular e implementar un plan para el tratamiento de riesgos relacionados con seguridad de la información a través de controles que permitan lograr los objetivos planteados para tal fin	***Numeral 3.1.12:*** Establecer procedimientos para el bloqueo de canales o de instrumentos para la realización de operaciones, cuando existan situaciones o hechos que lo ameriten o después de un número de intentos de accesos fallidos por parte de un cliente, así como las medidas operativas y de seguridad para la reactivación de los mismos.	***Manual de políticas de tecnología, numeral 5.1.1. "propietarios de los activos de información"*** Solicitar a la Gerencia de Procesos y Calidad y a la Coordinación de Plataforma que se esblezcan los controles requeridos y se administren los perfiles definidos en los activos de información
4.2.3 Monitorear y revisar el SGSI	La organización debe ejecutar procedimeientos que permitan identificar errores de procedimiento y que faciliten a la dirección definir si las actividades de seguridad necesarias mediante tecnologías de la información son las esperadas , asi como emprender revisiones periodicas de la eficacia del SGSI que permitan determinar la actualización de los planes de seguridad.	***Numeral 3.1.15*** Definir los procedimientos y medidas que se deberán ejecutar cuando se encuentre evidencia de la alteración de los dispositivos usados en los canales de distribución de servicios financieros.	***Manual de políticas de tecnología, numeral 5.1.1. "propietarios de los activos de información"*** Reportar al Help Desk los incidentes ocurridos con relación a Seguridad de la información que tienen bajos su responsabilidad con el fin de que se realicen las investigaciones necesarias
4.2.4 mantenimiento y mejora del SGSI	La organización debe regularmente implementar mejoras identificadas en el SGSI, asi como emprender acciones correctivas y preventivas adecuadas y comunicarlas a las partes interesadas para asegurar que estas cumplan con los objetivos previos	***Numeral 3.1.1*** Disponer de hardware, software y equipos de telecomunicaciones, así como de los procedimientos y controles necesarios, que permitan prestar los servicios y manejar la información en condiciones de seguridad y calidad.	***Manual de políticas de tecnología, numeral 5.2.1. "Administración de las instalaciones al centro de computo "*** Con el objeto de proporcionar un ambiente físico conveniente que proteja los equipos y el personal de Aseguradora Solidaria de Colombia contra peligros naturales como fallas humanas, se deben instalar controles físicos y ambientales adecuados que sean revisados regularmente para garantizar su buen funcionamiento
4.3.1 Generalidades	La organización debe demostrar la relación desde los controles seleccionados y de regreso a los resultados del proceso de evaluación del riesgo y tratamiento del riesgo y subsecuentemente, de regreso a la política y objetivos del SGSI	No se encuentra un numeral definido	No existe una política definida en la compañía

4.3.2 Control de documentos	Los documentos exigidos por el SGSI se deben proteger y controlar, se **DEBE** establecer un procedimiento documentado para definir las acciones de gestión necesarias para aprobar, revisar y actualizar los documentos además de garantizar que los cambios y el estado de actualización de los documentos estén identificados	***Numeral 3.3.2*** Velar por que los órganos de control, incluyan en sus informes la evaluación acerca del cumplimiento de los procedimientos, controles y seguridades, establecidos por la entidad y las normas vigentes, para la prestación de los servicios a los clientes y usuarios, a través de los diferentes canales de distribución.	***Manual de políticas de tecnología, numeral 4.1. "Definición de procesos de tecnología y comunicaciones "*** La Gerencia de Tecnología debe documentar todos los procedimientos relacionados con el proceso de gestión de tecnología y comunicaciones que apoya los procesos misionales de la Compañía. los procedimientos operativos se deben mantener actualizados y deben llevar un control de sus versiones
4.3.3. Control de registros	Se **DEBEN** establecer y mantener registros para brindar evidencia de la conformidad con los requisitos y la operación eficaz del SGSI. Los registros **DEBEN** estar protegidos y controlados. El SGSI **DEBE** tener en cuenta cualquier requisito legal o reglamentario y las obligaciones contractuales pertinentes. Los registros deben permanecer legibles, fácilmente identificables y recuperables. Los controles necesarios para la identificación, almacenamiento, protección, recuperación, tiempo de retención y disposición se **DEBEN** documentar e implementar.	***Numeral 3.2.2.*** Incluir en los contratos que se celebren con terceros o en aquellos que se prorroguen a partir de la entrada en vigencia del presente Capitulo, por lo menos, los siguientes aspectos: a) Niveles de servicio y operación. b) Acuerdos de confidencialidad sobre la información manejada y sobre las actividades desarrolladas. c) Propiedad de la información. d) Restricciones sobre el software empleado. e) Normas de seguridad informática y física a ser aplicadas. f) Procedimientos a seguir cuando se encuentre evidencia de alteración o manipulación de dispositivos o información. g) Procedimientos y controles para la entrega de la información manejada y la destrucción de la misma por parte del tercero una vez finalizado el servicio.	***Manual de políticas de tecnología, numeral 6.1.2. "Protección de la información"*** Toda la información de Aseguradora Solidaria de Colombia debe tener un periodo de almacenamiento asignado que puede ser dictaminado por requerimientos legales o del negocio. Este periodo debe estar definido en la tabla de retención documental. cuando expire el periodo de almacenamiento, todas las copias de los documentos o medios de almacenamiento deben ser adecuadamente destruidos, de acuerdo con lo establecido en la misma tabla.

3.2 MODELO OPERATIVO DEL AREA DE TECNOLOGIA

El modelo operativo de la Aseguradora donde sus, agencias, convenios y socios estratégicos cargan la información relacionada con su producción en el sistema core del negocio, mediante el cual dicha información viaja a la Web donde se almacena y procesa para que nuevamente mediante el sistema core en la Dirección general se puedan generar reportes requeridos para la toma de decisiones como también para soporte en los requerimientos de los diferentes organismos de control. La Figura 1 muestra el modelo operativo de la empresa objeto de estudio.

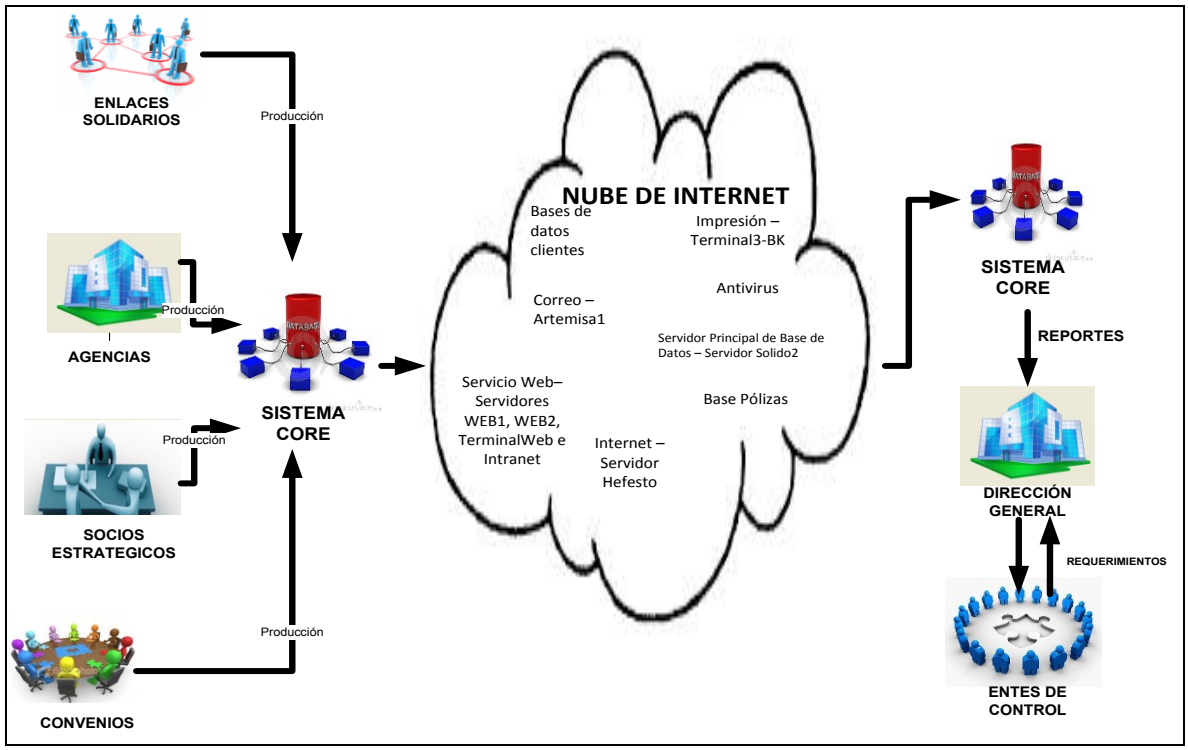

Figura 1. Modelo operativo

3.2.1 Políticas operativas del área de tecnología

- **Monitoreo de la infraestructura**

La Coordinación de Plataforma y el equipo de Mesa de ayuda deben implementar el uso de herramientas para realizar monitoreo en línea del estado de los canales de comunicación de las Agencias y socios estratégicos, fallas en el software instalado, en el hardware, en los puertos y en la conectividad. Estas herramientas deben enviar alarmas al Ingeniero de Soporte de Redes y Accesos para que se tomen las acciones del caso.

El proveedor de comunicaciones debe poner a disposición de la Aseguradora, herramientas de software para monitorear los canales 7 X 24 y en caso de falla de los mismos permitir al Ingeniero de Soporte de Redes y Accesos o al Coordinador de Plataforma tomar las acciones del caso.

La Coordinación de Plataforma debe contar con una herramienta que monitoree en línea el estado de los switches del centro de cableado y principales servidores del CAD en la Dirección General y del CCP. Esta herramienta debe enviar alarmas a los Ingenieros de Soporte de Redes y Accesos e Ingeniero de Soporte de Servidores.

- **Monitoreo y auditoria de la plataforma tecnológica**

El Área de Tecnología a través de la Coordinación de Plataforma debe realizar monitoreo permanente del uso que dan los funcionarios a la plataforma tecnológica de la compañía, así como mantener la custodia y revisión periódica de los archivos de auditoria con el fin de controlar actividades que afecten la seguridad de la información y facilitar investigaciones futuras.

Se debe contar con archivos de bitácora (logs) y los registros de auditoría (audit trails) que graban los eventos relevantes sobre la seguridad de los recursos de procesamiento y sistemas de información. Estos archivos se deben almacenar durante el período establecido por la compañía de acuerdo a las guías de clasificación de la información y se deben proteger para que nadie los pueda alterar y sólo puedan ser accedidos por las personas autorizadas.

Los archivos de auditoría de los recursos de procesamiento y sistemas de información (logs y audit trails) deben ser revisados periódicamente por el Ingeniero

de seguridad Informática. Dichos archivos son importantes para la detección de intrusos, brechas en la seguridad, investigaciones y otras actividades de auditoría.

La Coordinación de Plataformas debe habilitar sistemas de monitoreo que permitan detectar incumplimientos de la política de control de acceso, registrar eventos que proporcionen evidencia en caso de ocurrir incidentes de seguridad y verificar el uso adecuado de los recursos de procesamiento y sistemas de información.

3.3 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

El Área de Tecnología debe garantizar que los funcionarios y proveedores de bienes o servicios relacionados con la prestación de servicios de tecnología y comunicaciones conozcan y apliquen los lineamientos establecidos en estas políticas para mantener la seguridad de la información, así como revisar y ajustar de manera periódica su vigencia.

Para asegurar la confidencialidad, integridad y disponibilidad de la información, cada vez que se realice una modificación (automática o manual) en los sistemas de información de la compañía, el responsable de la misma debe informar previamente a todos los usuarios involucrados en el proceso, mediante los mecanismos establecidos de comunicación al interior de la entidad aseguradora.

La política global de seguridad de la información de la Aseguradora está soportada por políticas, normas y procedimientos específicos los cuales orientan sobre el manejo adecuado de la información de la compañía.

3.3.1 Roles y responsabilidades

A continuación se describen las áreas involucradas en la definición, mantenimiento y seguimiento de las políticas de seguridad de la información. Las responsabilidades de cada cargo involucrado, deben estar incluidas dentro de los manuales de funciones de la compañía.

- Vicepresidencia de Operaciones y Tecnología
- Gerencia de Tecnología
- Gerencia de Procesos y Calidad
- Área de Servicios Administrativos
- Dirección de Riesgo y Gobierno Corporativo
- Contraloría Interna.

Un grupo especial de usuarios, es el de propietarios de los activos de información. A continuación se definen sus roles y responsabilidades.

3.3.2 Propietarios de los activos de información

Los propietarios de activos de información se asignaron por módulo en el sistema core del negocio y por sistema de información para otros aplicativos, y se describen a continuación:

Tabla 1. Core del negocio y responsables

MÓDULO EN SISTEMA CORE DEL NEGOCIO	RESPONSABLE
Banca Seguros	Gerencia de Negocios Corporativos
Cartera	Gerencia de Crédito y Cartera
Contabilidad	Gerencia de Contabilidad
Autos	Gerencia de Automóviles
Personas	Gerencia de Personas
Generales	Gerencia Seguros Generales
Patrimoniales	Gerencia de Seguros Patrimoniales
Informática	Gerencia de Tecnología
Pagos	Gerencia de Contabilidad
Reaseguros	Gerencia de Reaseguros
Recaudos	Gerencia de Crédito y Cartera

Siniestros Autos	Gerencia Siniestros Automóviles
Siniestros Generales / Personas /Patrimoniales	Gerencia Nacional de Siniestros
Vida Y Exequias	Gerencia Negocios Cooperativos y Solidarios
Comercial / Administración De Personas	Gerencia de Tecnología
Socios estratégicos	Gerencia de Seguros Patrimoniales

- Velar por la información que genera o administra su área, la cual debe ser clasificada de acuerdo con las Guías de Clasificación de la Información.
- Participar en la definición de los niveles de acceso que se otorgarán a los usuarios sobre sus activos de información, demostrando una adecuada segregación de funciones.
- Solicitar al Área de Procesos y Calidad y a la Coordinación de Plataforma que se establezcan los controles requeridos y se administren los perfiles definidos en los activos de información.
- Reportar a la Mesa de Ayuda los incidentes ocurridos con relación a Seguridad de la información que tienen bajo su responsabilidad, con el fin que se realicen las investigaciones necesarias.
- Asegurar que los controles definidos para los activos de información a su cargo sean probados periódicamente.
- Autorizar la creación, modificación y eliminación de accesos a sus activos de información.
- Revisar periódicamente los niveles de acceso otorgados sobre sus activos de información.

3.3.3 Seguridad Física y del entorno

Administración de las instalaciones al centro de cómputo

- La empresa objeto de estudio cuenta con dos centros de cómputo:
  - Centro de Cómputo Principal – CCP - que se encuentra ubicado en el data center de Global Crossing S.A llamado Colombia XV.
  - Centro Alterno de Datos - CAD que se encuentra ubicado en las instalaciones de la Aseguradora.

- Tanto el CCP como el CAD deben cumplir con las condiciones físicas establecidas.
- Con el objeto de proporcionar un ambiente físico conveniente que proteja los equipos y el personal de la entidad Aseguradora contra peligros naturales o fallas humanas, se deben instalar controles físicos y ambientales adecuados que sean revisados regularmente para garantizar su buen funcionamiento teniendo en cuenta, entre otros, los siguientes aspectos:
  - Acceso a las instalaciones.
  - Identificación clara del sitio.
  - Controles de seguridad física. (Aire acondicionado, control de temperatura, humedad, humo, estándares internacionales para el CCP y el CAD).
  - Definición de políticas de inspección y escalamiento de problemas.
  - Planeamiento de continuidad del negocio y administración de crisis.
  - Salud y seguridad del personal. Copaso / Reglamento de higiene y seguridad industrial.
  - Políticas de mantenimiento preventivo.
  - Protección contra amenazas ambientales.
- La entidad Aseguradora debe proveer las condiciones medioambientales adecuadas para la operación de los recursos informáticos y de procesamiento de información.

Control de acceso a los centros de cómputo y al centro de cableado en la Dirección General

- El Gerente de Tecnología es el responsable del CCP y CAD y del Centro de Cableado de la Dirección General.
- Los únicos cargos autorizados para permitir el ingreso al CCP, CAD y Centro de Cableado son el Gerente de Tecnología y el Coordinador de Plataforma con el acompañamiento del funcionario designado por el Gerente de Tecnología.

Centro de Cómputo Principal

- Para el acceso al CCP se han establecido los siguientes controles:
  - Acceso puntual: El Coordinador de Plataforma es el responsable de enviar correo electrónico al proveedor, cuando se otorgue acceso a personal autorizado por un día determinado, en un horario de trabajo acordado, con 24 horas de anticipación durante los días hábiles (lunes a viernes). Para labores a realizar el fin de semana (sábados, domingos y festivos), solamente se puede ingresar por solicitudes de carácter urgente, donde

se tiene que relacionar: Nombre completo del funcionario, Documento de identidad, Nombre de la compañía, razón de la visita, fecha y hora de acceso y duración de la visita. El correo electrónico debe ir dirigido al coordinador de operaciones del data center y al grupo de ingenieros de operación del data center.

- Acceso permanente: El Coordinador de Plataforma es el único autorizado para realizar altas y bajas y/o modificaciones del personal autorizado para el acceso en forma no limitada a horarios ni días en particular. Para tal fin se informa mediante carta en papel membreteado de la compañía, dirigida al coordinador de operaciones de data center, en donde se relaciona nombre y número de documento de identidad del personal autorizado. Igualmente se envía a través de correo una foto reciente y fotocopia del documento de identidad (físico y en medio magnético).
- El CCP cuenta con todos los estándares y certificaciones de seguridad.

- Centro Cómputo Alterno y Centro de Cableado
  - El ingreso al CAD está permitido únicamente al Gerente de Tecnología, Coordinador de plataforma, Ingeniero de Seguridad informática, Ingeniero de soporte de redes y acceso, Ingeniero de soporte de servidores, Administrador de la Base de datos del Área de Tecnología, Gerente de Servicios administrativos. Para el caso del centro de cómputo alterno los vigilantes tienen acceso.
  - Todo ingreso y salida de funcionarios distintos a los autorizados o de terceros debe registrarse en el formulario "Bitácora de acceso al Centro de Computo y Centro de Cableado". Esta actividad debe ser supervisada por el funcionario del Área de Tecnología encargado del acompañamiento, para el caso de la Dirección General. En las Agencias esta actividad debe ser realizada por el funcionario designado por el Gerente o el Director Administrativo.
  - El ingreso al CAD se debe realizar a través de una tarjeta de acceso provista por el Gerente de Servicios Administrativos previa solicitud del Gerente de Tecnología. El Software que controla el ingreso a través de la tarjeta es administrado por el Ingeniero de Seguridad Informática del Área de Tecnología. La tarjeta de acceso solo debe ser asignada a los cargos autorizados en este manual; es personal e intransferible.
  - Es responsabilidad del Ingeniero de Seguridad Informática efectuar la activación y desactivación de las tarjetas de acceso al CAD previa autorización de la Gerencia de Gestión humana (para el caso de funcionarios) o la Área de Servicios Administrativos cuando se trate de un outsourcing (Vigilantes).

- La solicitud de ingreso al CAD y Centro de Cableado por proveedores externos debe ser tramitada por el Gerente de Servicios Administrativos a través de la intranet de la compañía y debe contener la información de la actividad que se va a realizar en forma detallada, motivo del ingreso y tiempo de duración, datos del proveedor (Número de documento de identificación, nombre) con el propósito de establecer las medidas de acompañamiento y seguimiento.
- La Mesa de Ayuda debe asignar el caso al Coordinador de Plataforma o al Ingeniero de soporte de redes y accesos para su correspondiente seguimiento.
- El ingreso al Centro de Cableado, está permitido únicamente al Ingeniero de Soporte de Redes y Acceso y al Coordinador de Plataforma del área de Tecnología y al Gerente de Servicios Administrativos.
- Todos los terceros al finalizar su trabajo, el mismo día que lo ejecuta, deben elaborar y entregar un informe de la actividad realizada y entregarlo a la Gerencia de Tecnología o Área de Servicios Administrativos, según el caso.
- Los motivos para el ingreso de funcionarios o terceros al CAD y cableado son:
  - Mantenimiento preventivo y correctivo de aire acondicionado del CAD y Centro de Cableado.
  - Mantenimiento preventivo y correctivo a servidores y hardware instalado en el CAD y Centro de Cableado.
  - Mantenimiento preventivo y correctivo de instalaciones y redes eléctricas localizadas en el CAD y Centro de Cableado.
  - Mantenimiento preventivo y correctivo del Software, si es necesario estar en el centro de cómputo, de lo contrario se utilizan estaciones de trabajo localizadas fuera del CAD y Centro de Cableado y se trabaja por acceso remoto.
  - Mantenimiento preventivo y correctivo de Instalaciones locativas.
  - Mantenimiento preventivo al sistema de extinción de incendios.
  - Mantenimiento preventivo y correctivo a equipos de comunicación.
  - Mantenimiento preventivo y correctivo del cableado estructurado de voz y datos.
- Los ingresos al CAD y centro de cableado, siempre deben ser monitoreados por video para identificar accesos no autorizados y para confirmar que los controles de acceso son efectivos. Este monitoreo es realizado por las Recepcionistas y/o los vigilantes.
- La asignación de espacio, ubicación, movimiento y demás requerimientos físicos para los recursos informáticos del CAD, deben ser autorizados por el Vicepresidente de Operaciones y Tecnología.

- Las puertas de acceso al CAD y Centro de Cableado deben permanecer siempre cerradas y aseguradas. De igual manera, todos los gabinetes y puertas de los equipos que se encuentran allí deben permanecer cerrados.
- El CAD y Centro de Cableado, al igual que el cuarto de las UPS, deben estar libres de elementos ajenos a los mismos.
- Los funcionarios del Área de Servicios Administrativos en coordinación con los funcionarios del Área de Tecnología y los Directores Administrativos de las Agencias (Si aplica), deben llevar control de la programación de los mantenimientos preventivos y pruebas de funcionalidad de los sistemas que se mencionan a continuación y verificar su realización, conforme a las condiciones establecidas.

    - Sistema de UPS y verificar su realización.
    - Sistema de aire acondicionado y verificar su realización.
    - Sistema de detección y extinción de incendios del Centro de Cómputo y verificar su realización.
- El mantenimiento de la red telefónica es responsabilidad de la Área de Servicios Administrativos.
- De ser posible los mantenimientos se deben programar los fines de semana o después de terminada la jornada laboral.

3.4 CUMPLIMIENTO DE REQUERIMIENTOS ISO 27001:2006 NUMERAL 4

A continuación se describen el cumplimiento al numeral 4 “Sistema de Gestión de la Seguridad de la Información” de la Norma ISO 27001 por parte del Área de Tecnología de la entidad Aseguradora.

NUMERAL	CONCEPTO	CUMPLE / NO CUMPLE	OBSERVACIONES
4.1	Requisitos generales	No cumple	No existe una política definida en la compañía
4.2	**Establecimiento y gestión del S.G.S.I**		
4.2.1	Establecimiento del SGSI	Cumple	Se cuenta con políticas definidas
4.2.2	Implementación y operación del SGSI	Cumple	Se cuenta con políticas definidas
4.2.3	Seguimiento y revisión del SGSI	Cumple	Se cuenta con políticas definidas
4.2.4	Mantenimiento y mejora del SGSI	Cumple	Se cuenta con políticas definidas
4.3	**Requisitos de documentación**		
4.3.1	Generalidades	No cumple	No existe una política definida en la compañía
4.3.2	Control de documentos	Cumple	Se cuenta con políticas definidas
4.3.3	Control de registros	Cumple	Se cuenta con políticas definidas

Tabla 2. Cumplimiento numeral 4

3.4.1 Tratamiento de incumplimientos al numeral 4 de la Norma ISO 27001:2006.

ITEM: 4.1 Requisitos generales

Se sugiere que los procesos relacionados con manejo de información contemplen en sus actividades controles que permitan hacer seguimiento en su operación y a su vez ayuden a detectar los riesgos a que se pueda estar expuesto.

ITEM: 4.3.1 Generalidades

Se recomienda que todos los procesos diseñados para la aseguradora, relacionadas con el SGSI contengan:

- Política documentada
- Objetivos del SGSI
- Alcance del SGSI
- Controles que apoyen al SGSI
- Una matriz de riesgos que incluya:

- Efecto de la materialización de los riesgos
- Riesgo a que se está expuesto
- Posibles causas
- La probabilidad de que suceda
- Impacto
- Exposición
- Controles existentes en la entidad aseguradora para mitigar el riesgo

Se sugiere implementar un software mediante el cual se administren los riesgos en los procesos relacionados con el SGSI, donde se pueda efectuar el seguimiento en las etapas de identificación, medición, control y monitoreo sistemático de los riesgos.

3.5 METODOLOGÍA DE INTEGRACIÓN ENTRE NORMA ISO 27001:2006 Y EL MÓDELO OPERATIVO DEL ÁREA DE TECNOLOGÍA

Se propone una metodología por fases.

Fase 1. Diagnóstico de la situación actual del sistema de SGSI

En esta fase se evalúa la operación actual del Área de Tecnología, frente a los requisitos establecidos en el numeral 4 de la Norma ISO 27001:2006.

Fase 1.1 Cuantificación de hallazgos del diagnóstico

Efectuar la cuantificación de las falencias que tiene el área de Tecnología frente a los requisitos establecidos en la Norma ISO 27001:2006, relacionados con procesos de control, infraestructura necesaria, documentación, capacitación entre otras que incidan en el SGSI.

Fase 2. Diseño de Plan estratégico de Tecnología

Diseñar un plan estratégico que involucre:

- La creación de procesos que soporten el plan de continuidad del negocio de la plataforma tecnológica.

- Evaluación y actualización de la plataforma física
- Identificación de posibles riesgos que afecten la seguridad de la información de la compañía.
- Evaluación de la capacidad de respuesta ante un evento de riesgo por parte de los proveedores donde reposan los servidores.
- Capacitación a los dueños de procesos críticos ante eventos de riesgo
- Capacitación al personal de tecnología en cuanto a soporte y administración de recursos informáticos.
- Actualización de las políticas de seguridad de la información donde se involucren procesos de análisis y solución de incidentes.
- Generar un programa relacionado con gente y cultura que permita concientizar a los funcionarios de la compañía en la aplicación de las buenas prácticas del manejo de recursos tecnológicos y cuidados en el manejo de información.

Fase 3. Implementación del Plan estratégico de Tecnología

Para la puesta en marcha se recomienda la creación de un cronograma donde se definan, los roles, perfiles de cada uno de los responsables en la implementación de cada una de las fases, así como los tiempos y recursos estimados en su ejecución.

Fase 4. Mejoramiento continúo

Es necesaria la definición de indicadores que permitan evaluar la eficacia de la implementación del plan estratégico y la generación de planes a de acción a que haya lugar para de esta manera garantizar su control y mantenimiento.

Resultados

A continuación se describe un ejemplo del manejo y administración de la información en la Gerencia de Procesos y Calidad de la entidad aseguradora.

La Gerencia de procesos y Calidad es la encargada de gestionar la organización por procesos, cuyo objetivo es incrementar la eficiencia organizacional, asesorando y apoyando a todas las áreas de la aseguradora en el logro de sus metas, a través

de una constante optimización y modernización de los procesos, normatividad, sistemas de información y estructura orgánica.

Tipo de información: Documentos en Word, Excel, Visio y PDF resultantes de la Gestión realizada para el diseño y mejoramiento de todos los procesos que se encuentren identificados para la compañía; como son:

- Caracterizaciones, (Word, Pdf)
- Diagramas de flujo (Visio, Pdf)
- Manuales (Word, Pdf)
- Formatos(Word, Excel, Pdf)
- Instructivos (Word, Pdf)
- Documentos soporte (Word, Excel, Pdf)

Custodia: Base de datos de Procesos y calidad

Aplicación de la Norma:

La Gerencia de Procesos y Calidad de la aseguradora, producto de un requerimiento de una de las áreas misionales, realiza el diseño de un proceso el cual incluyo el desarrollo de una caracterización, diagrama de flujo y dos formatos.

El proceso diseñado y aprobado reposa en la Base de datos de la Gerencia de Procesos y Calidad ubicada en un servidor cuyo acceso se encuentra restringido a las demás áreas de la compañía.

Como política del SGSI de la aseguradora, a toda la información relacionada con los diferentes requerimientos solicitados y que reposa en los equipos de los Ingenieros de procesos de esta Gerencia se deben encontrar debidamente identificados, semanalmente se debe realizar un Backup, el cual debe reposar en la Base de datos de la Gerencia de Procesos y Calidad ubicada en el servidor establecido para tal fin, se debe ubicar en las carpetas correspondientes, teniendo en cuenta:

- El Proceso
- La versión correspondiente
- El tipo de información (Procesos, diagramas, formatos, manuales, instructivos, etc)
- Documentos en construcción

- Documentos finales
- Documentos aprobados
- Documentos obsoletos

Una vez se ha culminado el diseño y desarrollo del proceso y se encuentra con todas sus aprobaciones, se procede a incluirlo en la carpeta correspondiente a los documentos aprobados de acuerdo a su codificación en la base de datos de procesos y calidad ubicada en el servidor; adicionalmente se carga en la página de Procesos y Calidad para su consulta. Se informa a todos los funcionarios de la compañía a través de un mensaje emergente que el proceso diseñado se encuentra publicado en la página de Procesos y Calidad ubicada en la intranet de la aseguradora, donde puede ser consultada en el mapa de procesos de acuerdo a su codificación, cabe destacar que este documento se encuentra bloqueado para impresión, con el fin de mantener como versión oficial para su uso, la última que se encuentra publicada en dicha página.

En el caso de actualizaciones de procesos, antes de ser publicados se procede a pasar la versión a reemplazar a la carpeta de los documentos obsoletos en la base de datos de la Gerencia de Procesos y calidad en el servidor establecido para tal fin. Posteriormente se reemplaza en la Página de Procesos y Calidad y se procede a su publicación.

Todos los documentos publicados o declarados como obsoletos deben ser registrados en el control de documentos correspondientes de acuerdo a lo establecido en las políticas establecidas en el SGSI de la entidad aseguradora.

4. CONCLUSIONES

- La metodología propuesta permite contar con controles que alineados con los requisitos de la Norma ISO 27001:2006 identifica las falencias que se puedan llegar a tener relacionadas con el SGSI de la entidad aseguradora y la toma de acciones de mejora pertinentes.

- La entidad aseguradora al contar con una metodología que alinee su modelo operativo con los requisitos de la Norma ISO 27001:2006, facilita el cumplimiento a las exigencias establecidas por la Superintendencia Financiera de Colombia en temas relacionados con seguridad de la información.

- La Norma ISO27001:2006 brinda los parámetros necesarios para que la Aseguradora cuente con un SGSI que le permita controlar y minimizar los riesgos a que están expuestas todas las compañías del sector financiero.

REFERENCIAS

[1]Sistemas de Gestión de la Calidad. Requisitos (NTC - ISO -9001). Consultada el 13 de Abril de 2013, disponible en: http://farmacia.unmsm.edu.pe/noticias/2012/documentos/ISO-9001.pdf

[2]Directrices para la documentación del sistema de gestión de la calidad (GTC-ISO/TR 10013).Consultada el 13 de Abril de 2013, disponible en:http://es.scribd.com/doc/52299369/GTC-ISO-TR10013

[3]Sistemas de gestión de la calidad. Fundamentos y vocabulario (NTC-ISO 9000). Consultada el 13 de Abril de 2013, disponible en:http://ujtl11.utadeo.edu.co/documentos/calidad/norma_tecnica_colombiana_NTC-ISO_9000.pdf

[4]LEY 100 DE 1993 (Diciembre 23) “Por la cual se crea el sistema de seguridad social integral y se dictan otras disposiciones”. Consultada el 13 de Abril de 2013, disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley/1993/ley_0100_1993.html

[5]DECRETO 1011 DE 2006 (Abril 3) “Por el cual se establece el Sistema Obligatorio de Garantía de Calidad de la Atención de Salud del Sistema General de Seguridad Social en Salud”. Consultada el 13 de Abril de 2013, disponible en:http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=19975

[6]RESOLUCIÓN 1043 DE 2006 (Abril 3) “Por la cual se establecen las condiciones que deben cumplir los Prestadores de Servicios de Salud para habilitar sus servicios e implementar el componente de auditoría para el mejoramiento de la calidad de la atención y se dictan otras disposiciones”. Consultada el 13 de Abril de 2013, disponible en:http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=20268

[7]RESOLUCIÓN 2680 DE 2007 (agosto 3)“por la cual se modifica parcialmente la Resolución 1043 de 2006 y se dictan otras disposiciones”. Consultada el 13 de Abril de 2013, disponible en:
http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=26257

[8]RESOLUCIÓN 3763 DE 2007 (agosto 3) “Por la cual se modifican parcialmente las Resoluciones 1043 y 1448 de 2006 y la Resolución 2680 de 2007 y se dictan otras disposiciones”. Consultada el 13 de Abril de 2013, disponible en:http://www.avancejuridico.com/actualidad/documentosoficiales/2007/46717/r_mps_2680_2007.html