PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

FACULTAD DE CIENCIAS E INGENIERÍA

ESTABLECIMIENTO, IMPLEMENTACIÓN, MANTENIMIENTO Y MEJORA DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, BASADO EN LA ISO/IEC 27001:2013, PARA UNA EMPRESA DE CONSULTORÍA DE SOFTWARE

Tesis para optar por el Título de Ingeniero Informático, que presenta el bachiller:

Santos Llanos, Daniel Elías

ASESOR: Luis Silva-Santisteban Sierra

Lima, Agosto del 2016

RESUMEN

Actualmente, las empresas de consultoría de desarrollo de software cuentan con muchos retos propios de este tipo de negocio. Entre estos, destacan los relacionados a la seguridad de información, pues, debido al constante intercambio de información entre la empresa y sus clientes, aparecen riesgos potenciales que pueden comprometer el éxito e incluso la subsistencia de la organización.

La solución planteada para este problema es un Sistema de Gestión de Seguridad de Información (SGSI), el cual cuenta con el estándar ISO 27001:2013 como marco formal de requisitos a cumplir. Este sistema permitirá que los directivos y demás involucrados gestionen y tomen decisiones adecuadas respecto a la seguridad de información de la organización, para asegurar que cuente con niveles adecuados respecto a la confidencialidad, integridad y disponibilidad de la información crítica que se maneja como parte de su operación.

En este informe se especifican las cuatro fases cíclicas del SGSI: el establecimiento, donde las bases del sistema se integran a los procesos del negocio; la implementación, que desarrolla los mecanismos para la adecuada administración de la seguridad; el mantenimiento, donde se detectan fallos que pueden existir en la organización o en el propio sistema; y la mejora, que finalmente permite cerrar el ciclo mediante la aplicación de todas las correcciones y optimizaciones significativas que han sido detectadas.

Este modelo permite que el sistema opere bajo un principio de mejora continua, que beneficia permanentemente a la organización, propiciando un manejo adecuado de la seguridad de su información.

DEDICATORIA

A mi padre, Rafael Santos Basurto.

Tu familia nunca te abandona.

AGRADECIMIENTOS

A todos aquellos que siempre dieron más de lo que uno puede pedir: familia, en particular mi padre, mis tías y primas por su apoyo incondicional, desde siempre; amigos, a L.S.S., S.G.S., C.L.S., M.C.V. y en especial a Zelenia, sin el sol en las mañanas sería difícil despertar.

Índice de Contenido

Índice de Figuras

Índice de Tablas

1. Generalidades

En este capítulo se plantean las generalidades del proyecto, las cuales comprenden: la definición del problema que se resolverá; el desarrollo del marco conceptual, consistente en todas las definiciones necesarias para su comprensión; el estado del arte, que desarrolla la revisión de soluciones disponibles relacionadas; el plan de proyecto, que despliega las tareas que se planificaron para completar el trabajo realizado; la descripción y sustentación de la solución propuesta y, finalmente, el modelo de trabajo que ha sido usado para estructurar la solución; esquema en base al cual son desarrollados los siguientes capítulos.

1.1. Definición del problema

Una empresa de consultoría de software apoya a otras organizaciones en implementar, mejorar y asegurar el adecuado funcionamiento de las soluciones informáticas que automatizan sus procesos, para lo cual realizan las siguientes actividades:

- **Desarrollo de software.** Creación de nuevos sistemas y aplicaciones para la automatización de los procesos del negocio.
- **Mantenimiento de software.** Actualización correctiva o de mejora para mantener la vigencia del sistema o aplicación en funcionamiento, usualmente sobre proyectos previos con el mismo cliente.
- **Control de calidad sobre el software.** Proceso interno de la consultora para la revisión y verificación de la adecuada operación funcional de los sistemas y aplicaciones desarrollados.

Bajo este esquema de trabajo, el cliente brinda a la empresa consultora sus requerimientos y, para poder atenderlos, la información de su lógica de negocio. Esto se realiza mediante reuniones de trabajo con su personal así como también la presentación de: diagramas, procedimientos, modelos de bases de datos e incluso muestras de la información contenida en estas. El proveedor ejecuta sus servicios en base a la información recibida, para obtener como resultado: código fuente, ejecutables, compilados, informes, diagramas, manuales, documentos técnicos, capacitaciones y otras fuentes de información, propias del servicio.

Para realizar estas actividades es inevitable el intercambio de información entre ambas organizaciones participantes. Esto implica la posibilidad de que, dentro de la información intercambiada, pueda encontrarse alguna de carácter sensible que esté expuesta a riesgos de seguridad de información, que impacten y comprometan a ambas partes, ya sea en el traslado, procesamiento, almacenamiento, creación, copia e incluso eliminación.

Al respecto, el entorno actual de riesgos respecto a la seguridad de información en las consultoras de software y sus clientes presenta un escenario retador: espionaje industrial, adulteración de documentos, colectivos de hackers, alteración ilícita de datos, bombas lógicas introducidas en sistemas, fuga de información, sabotaje informático, entre otros.

Por lo expuesto, los proveedores de consultoría de software necesitan garantizar que, tanto la información que reciben como la que producen como parte de su servicio, sea asegurada de la manera más adecuada y eficiente. No basta con tomar medidas relacionadas a la implementación de controles de seguridad de información, sino que estas deben ser manejadas eficientemente y probar ser efectivas, sin que esto implique encarecer los costos del servicio.

En conclusión, se requiere una solución para gestionar de manera eficiente y efectiva la seguridad de información de la consultora y, por extensión, de todas las partes interesadas con las que interactúa, especialmente sus clientes.

Nota sobre la confidencialidad de la fuente y los términos usados:

La tesis mostrada desarrolla contenido referido a una empresa consultora de software. Para asegurar la confidencialidad respecto a la misma, en adelante nos referiremos a ella como la “consultora”. Por otro lado, debido a la referencia recurrente a la ISO/IEC 27001:2013 [02], denominaremos a este marco como el “estándar 27001” o el “estándar”, a lo largo del texto.

1.2. Objetivo General

Desarrollar un Sistema de Gestión de Seguridad de Información (SGSI) para una empresa de consultoría en desarrollo y calidad de software, tomando como marco normativo el estándar ISO/IEC 27001:2013 [02].

1.3. Objetivos Específicos

- Crear los componentes requeridos para establecer el SGSI: Planes de operación – comunicaciones, marco documental, contexto de la organización, requisitos de los interesados, alcance, política de seguridad de información y roles del sistema.
- Crear los componentes requeridos para implementar el SGSI: Gestión de riesgos, objetivos de seguridad de información, concientización y operación del sistema.
- Crear los componentes requeridos para mantener el SGSI: Métricas de seguridad de información, auditoría interna y revisión por la dirección del sistema.
- Crear los componentes requeridos para mejorar el SGSI: Acciones correctivas y de mejora sobre el sistema.

1.4. Resultados Esperados

Como resultado de esta investigación se espera:

- Entender y modelar el contexto y requisitos de seguridad de información de una consultora de desarrollo de software.
- Obtener los componentes requeridos para la operación de un Sistema de Gestión de Seguridad de Información, para una consultora de desarrollo de software.
- Verificar que el diseño y aplicación práctica de los componentes elaborados para el SGSI cumplan con el estándar ISO/IEC 27001:20013.

1.5. Alcance y limitaciones del proyecto

El alcance del proyecto abarca a la creación de los componentes del Sistema de Gestión de Seguridad de Información (SGSI), para sus cuatro fases de operación: establecer, implementar, mantener y mejorar. Estos componentes se aplicarán en los procesos seleccionados en la consultora de desarrollo y calidad de software. Se limita la elaboración de los componentes del sistema a los indicados en el estándar ISO/IEC 27001:2013 [02] y otros marcos que este referencia.

1.6. Marco conceptual

Para la comprensión del trabajo presentado se deben tener en cuenta algunos conceptos importantes, los cuales son desarrollados, en los siguientes numerales:

1.6.1. Definiciones específicas para el SGSI

Todas las definiciones mostradas a continuación provienen de la ISO/IEC 27000:2014 [01], marco referencial para comprender los términos en los estándares de la familia 27000.

Sistema de Gestión de Seguridad de Información. Un Sistema de Gestión de Seguridad de la Información (SGSI) consiste en políticas, procedimientos, directrices, recursos asociados y actividades, gestionadas colectivamente por una organización, en la búsqueda de la protección de sus activos de información. Un SGSI es un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una organización para alcanzar los objetivos de negocio. Se basa en la evaluación del riesgo y los niveles de aceptación del riesgo de la organización, diseñada para tratar y gestionar los riesgos de manera efectiva. Analizar requisitos para la protección de los activos de información aplicar los controles adecuados para garantizar su protección, según sea necesario, contribuye a la implementación exitosa de un SGSI. (**ISO/IEC 27000: 2014 - 3.2.1**)

Información. La información es un activo que, al igual que otros activos de negocio importantes, es esencial para la misión de una organización y por lo tanto necesita ser protegida de forma adecuada. La información puede ser almacenada en muchas formas, incluyendo: forma digital (por ejemplo: archivos de datos

almacenados en medios electrónicos u ópticos), forma material (por ejemplo: en el papel), así como la información no estructurada en la forma de conocimiento de los empleados. La información puede ser transmitida por diversos medios, incluyendo: mensajería, comunicación electrónica o verbal. Cualquiera que sea la forma que adopte la información o el medio por el cual sea transmitida, siempre se necesita una protección adecuada.

En muchas organizaciones la información depende de la tecnología de la información y las comunicaciones. Esta tecnología es usualmente un elemento esencial en la organización y permite facilitar la creación, procesamiento, almacenamiento, transmisión, protección y destrucción de la información. (**ISO/IEC 27000: 2014 - 3.2.2**)

Seguridad de información. La seguridad de información incluye tres dimensiones principales: la confidencialidad, disponibilidad e integridad. Consiste en la aplicación y gestión de medidas de seguridad apropiadas, lo que implica la consideración de una amplia gama de amenazas, con el fin de garantizar el éxito y continuidad del negocio, de manera sostenida, y la minimización de los impactos de los incidentes de seguridad de la información.

Esto se logra mediante la implementación de un conjunto aplicable de controles, seleccionados a través del proceso de gestión de riesgos y administrados utilizando un SGSI; incluye las políticas, procesos, procedimientos, estructuras organizacionales, software y hardware para proteger los activos de información identificados. Estos controles deben ser especificados, implementados, monitoreados, revisados y mejorados cuando necesario, para asegurar que se cumplen los objetivos específicos de seguridad de información y del negocio son logrados. Se espera que los controles de seguridad de la información relevantes se integren a la perfección con los procesos de negocio de la organización. (**ISO/IEC 27000: 2014 - 3.2.3**)

Sistema de gestión. Un sistema de gestión utiliza un marco de recursos para lograr los objetivos de una organización. El sistema de gestión incluye la estructura organizativa, políticas, planificación de actividades, responsabilidades, prácticas, procedimientos, procesos y recursos. (**ISO/IEC 27000: 2014 - 3.2.5**)

Confidencialidad. Propiedad de la limitación o restricción de la información a individuos, entidades o procesos no autorizados. (**ISO/IEC 27000: 2014 - 2.61**)

Integridad. Propiedad de [la información de] exactitud y completitud. (**ISO/IEC 27000: 2014 - 2.40**)

Disponibilidad. Propiedad de [la información de] ser accesible o usable cuando sea demandada por una entidad autorizada. (**ISO/IEC 27000: 2014 - 2.9**)

Riesgo. Efecto que genera incertidumbre sobre [el logro de] los objetivos [de seguridad de información]. (**ISO/IEC 27000: 2014 - 2.68**)

Control. Medida que modifica la situación del riesgo. (**ISO/IEC 27000: 2014 - 2.68**)

Vulnerabilidad. Debilidad de un activo o control que puede ser explotada por una o más amenazas. (**ISO/IEC 27000: 2014 - 2.83**)

Amenaza. Causa potencial de un incidente inesperado, que podría resultar e daño a un sistema o a la organización. (**ISO/IEC 27000: 2014 - 2.83**)

Consecuencia. Resultado de un evento, que afecta a los objetivos. Un evento puede llevar a un rango de consecuencias. Una consecuencia puede ser certera o incierta y en el contexto de la seguridad de información es usualmente negativa. Las consecuencias pueden ser expresadas de modo cualitativo o cuantitativo. Las consecuencias iniciales pueden escalar a través de efectos derivados. (**ISO/IEC 27000: 2014 - 2.14**)

Propietario del Riesgo. Persona o entidad con la capacidad y autoridad para gestionar un riesgo. (**ISO/IEC 27000: 2014 - 2.68**)

Requisito. Necesidad o expectativa que está establecida, generalmente implícita u obligatoria. "Generalmente implícita" significa que es costumbre o práctica común para la organización y partes interesadas cuya necesidad o expectativa bajo consideración es implícita. Un requerimiento especificado es aquel que está establecido, por ejemplo, en información documentada. (**ISO/IEC 27000: 2014 - 2.63**)

1.6.2. Estándares involucrados

ISO/IEC 27001:2013 Tecnología de Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de Información. Requerimientos [02]

Es la última versión del estándar que establece los requisitos para los sistemas de gestión de seguridad de información. Define los requerimientos necesarios para el adecuado establecimiento, implementación, mantenimiento y mejora continua de un Sistema de Gestión de Seguridad de la Información (SGSI). Es un estándar certificable.

ISO/IEC 27000:2014 Tecnología de Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de Información. Descripción y vocabulario [01]

Contiene el glosario de términos y definiciones para la familia 27000. El contenido de este documento debe ser tomado en cuenta para el adecuado enfoque y entendimiento de las cláusulas y requisitos que exponen los estándares 27001, 27002, 27005, entre otros.

ISO/IEC 27002:2013 Tecnología de Información. Técnicas de Seguridad. Código de prácticas para controles de seguridad de información [03]

Desarrolla a un nivel más detallado los controles de seguridad de información listados en el anexo A de la ISO/IEC 27001: 2013. Especifica la forma en que deberían implementarse los controles gobernados mediante el SGSI.

ISO/IEC 27003:2010 Tecnología de Información. Técnicas de Seguridad. Directrices para la implementación de un sistema de gestión de seguridad de información [04]

Propone una guía de implementación para un SGSI, para lo cual indica etapas, documentos y roles que pueden permitir la adecuada atención de los requisitos establecidos en la ISO/IEC 27001: 2013. Sin embargo, los lineamientos indicados en este documento no son de cumplimiento obligatorio, ya que es una propuesta de implementación que no pretende reemplazar a los requisitos que establece la ISO/IEC 27001: 2013. Este estándar fue publicado el 2010, antes de la última versión de la ISO/IEC 27001: 2013, por lo que su desarrollo no está diseñado para atender todos los requisitos de este último.

ISO/IEC 27004:2009 Tecnología de Información. Técnicas de Seguridad. Gestión de Seguridad de Información. Medición [05]

Este estándar propone un marco para la definición y obtención objetiva de métricas, en el marco de un SGSI, las cuales deberán estar relacionadas a los requisitos, objetivos y controles de seguridad de información, de manera que se conviertan en indicadores de la efectividad del sistema.

ISO/IEC 27005:2008 Tecnología de Información. Técnicas de Seguridad. Gestión del Riesgo en Seguridad de Información [06]

Este estándar propone un marco para la gestión de riesgos de seguridad de la información, bajo un enfoque en cuatro etapas: inventario, análisis, evaluación y tratamiento de los riesgos de seguridad de información. Si bien constituye un esquema válido para la gestión de riesgos en seguridad de información, está más enfocado en la versión precedente del estándar 27001 (2005). Se debe tomar en cuenta que la nueva versión del estándar, selecciona como nuevo marco referencial de riesgos a la ISO 31000:2009 [07].

ISO 31000:2009 Gestión del Riesgo. Principios y Directrices [07]

Propone un marco para la gestión de riesgos y oportunidades, a partir de una evaluación del contexto de la organización. Este enfoque es referenciado por la ISO/IEC 27001:2013 [02], como fuente para establecer el contexto de la organización, además de identificar, evaluar y tratar los riesgos y oportunidades de seguridad de información.

IEC 31010:2009 Gestión de Riesgo. Técnicas de Apreciación del Riesgo [08]

Propone técnicas y estrategias para la identificación y evaluación de riesgos y oportunidades de seguridad de información de la organización, complementando las directrices establecidas en la ISO 31000:2009. Entre las estrategias propuestas se mencionan la técnica Delphi, la aplicación de Listas de Verificación, Análisis de Riesgos Preliminar (PHA), HAZOP, Análisis de peligros y puntos críticos de control (HACCP), Evaluación de Toxicidad, Técnica Estructurada "WHAT-IF" (SWIFT), Análisis de Escenarios, Análisis de Impacto en el Negocio (BIA), entre otros.

1.6.3. Otros referentes

NTP ISO/IEC 27001:2014 Tecnología de Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de Información. Requerimientos [09]

Norma técnica peruana de requisitos para implementar un SGSI. Es una traducción del estándar ISO/IEC 27001:2013 [02], razón por la cual cambia mucho respecto a la versión precedente (2008), actualmente se encuentra vigente y es de cumplimiento obligatorio para las entidades del estado peruano, por resolución aprobada por la Presidencia del Consejo de Ministros (PCM). Las entidades privadas pueden tomarlo como marco referencial.

NTP ISO/IEC 17799:2007 Tecnología de Información. Técnicas de Seguridad. Código de prácticas para controles de seguridad de información [10]

Norma técnica peruana de controles de seguridad de información. Es una traducción de la ISO/IEC 17799:2005. Si bien ya existe una nueva versión del estándar (ISO/IEC 27002:2013), aún no se ha realizado su traducción como norma técnica peruana, por lo que la presentación de los grupos de controles contenidos en esta norma técnica se puede considerar desfasado.

OCTAVE - Allegro [11]

Es el acrónimo de evaluación de las amenazas, activos y vulnerabilidades operacionalmente críticas (OCTAVE, por sus siglas en inglés). Contiene una metodología de análisis de riesgo desarrollada por Computer Emergency Response Team (CERT), enfocada en el estudio de riesgos para organizaciones pequeñas (versión Allegro). La evaluación parte de la identificación de activos relacionados con la información, para identificar amenazas y vulnerabilidades, a partir de los cuales se pueden determinar riesgos de seguridad de información. A partir de estos resultados se plantean estrategias y planes, para mitigar los riesgos identificados.

Marco MOR – Guía para la Gestión de Riesgos [12]

El marco Management of Risk (MOR) es una guía para la gestión de riesgos, desarrollada por el Office of Government Commerce (OGC) de Reino Unido. Está alineada a la ISO 31000 [07] y propone un ciclo de gestión de riesgos en 4 etapas: identificar (información, amenazas y oportunidades), evaluar (probabilidad e impacto), planificar (medidas de mitigación de riesgos y maximización de oportunidades) e implementar (concretar las medidas y medir su efectividad).

NIST SP 800 - 100 Manual de Seguridad de Información: Guía para gestores [13]

La SP 800-100 es la guía de gobierno de la seguridad de información del National Institute of Standards and Technology (NIST); incluye los roles de gobierno, el ciclo de vida para la gestión de la seguridad, la capacitación, gestión de recursos, indicadores, gestión de riesgos, manejo de incidentes, entre otros aspectos de la administración de la seguridad de información en organizaciones.

NIST SP 800 - 39 Gestionar Riesgos de Seguridad de Información [14]

La SP 800-39 es la guía para la gestión de riesgos de seguridad de información del National Institute of Standards and Technology (NIST); comprende: el Enmarcado del Riesgos, estableciendo un contexto; la Evaluación del Riesgo, identificando, priorizando y estimando el riesgo; la Respuesta al Riesgo, definiendo las opciones de curso de acción frente al riesgo; y el Monitoreo del Riesgo, para evaluar la situación final de los riesgos.

NIST SP 800 – 53 Controles de Seguridad y Privacidad para Sistemas de Información Federales y Organizaciones – Revisión 4 [15]

La SP 800-53 es un marco referencial de controles de seguridad de información del National Institute of Standards and Technology (NIST). El fin de esta propuesta de controles es servir de referente para la selección de aquellos que sean necesarios para la organización. Los presenta en grupos de controles organizados en 18 dominios. La versión vigente de este documento es la revisión 4 (2013).

MAGERIT VERSIÓN 3 [16]

Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, desarrollada por el gobierno español. Propone un esquema de gestión de riesgos basado en identificar activos, amenazas, impactos, controles (salvaguardas) y estado del riesgo; posteriormente, con esta información se realiza la evaluación del riesgo y la subsecuente aceptación / tratamiento del riesgo.

Directiva de Seguridad (Ley de Protección de Datos Personales 29733) [17]

Marco de recomendaciones en seguridad de información, relacionadas al adecuado tratamiento y custodia de la información de carácter personal. Documento emitido por la Autoridad Nacional de Datos Personales como marco complementario para la implementación de la Ley. En base a la categoría de los bancos de datos personales administrados por las organizaciones, esta directiva define niveles de requisitos a manejarse. A mayor volumen y complejidad de los datos, mayor el nivel de exigencia. En el nivel más alto se recomienda implementar un SGSI.

COBIT 5 – Para Seguridad de Información [18]

Es una guía profesional que parte del modelo, conceptos, artefactos y principios de COBIT 5. Se basa en el modelo BMIS (Modelo de Negocio para la Seguridad de Información) bajo un enfoque específico de seguridad de información sobre las tecnologías de información. Integra componentes y controles desarrollados por otros estándares, en un esquema único que permite que la organización interesada pueda seleccionar los más adecuados. Desarrolla un marco de: Políticas y principios, los cinco grupos de procesos de COBIT aplicados a la seguridad de información, el marco organizacional y cultural, los controles para el manejo de la información, los servicios, infraestructura y aplicaciones, personas, gobierno y riesgos. Para el desarrollo de un marco de gestión de riesgos que le permita operar, se apoya en la propuesta metodológica de RISK IT (Gestión de riesgo empresarial TI, de ISACA).

Marco Risk IT para la Gestión de TI Relacionada a Riesgos del Negocio [19]

Es el marco de gestión de riesgos TI de ISACA, relacionado a su vez al marco de riesgos empresariales que aplican sobre la organización. Cuenta con una serie de principios propios, similares a los de COBIT, a partir de los cuales despliega tres dominios para poner en práctica el marco: el Gobierno del Riesgo, donde se establece el enfoque de riesgos, la integración a los riesgos empresariales y la toma de decisiones; la Evaluación de Riesgos, donde se obtienen datos, se analiza y mantienen los riesgos; y la Respuesta a los Riesgos, donde se reacciona a los riesgos.

1.7. Estado del arte

Se presentan los diseños e implementaciones de sistemas de gestión de seguridad de información identificados, las tesis y otras investigaciones relacionadas al tema:

1.7.1. Implementaciones certificadas

A nivel mundial existen muchas organizaciones que cuentan con sistemas de gestión de seguridad de información implementados y operando, pero solo algunas de ellas cuentan con la certificación que acredita que su operación es adecuada y acorde al estándar 27001.

A continuación se muestran algunos de los casos más significativos de los sistemas nacionales e internacionales que han sido certificados exitosamente:

Ámbito	Organización Certificada
SGSI Internacionales	Microsoft Global Foundation Services (GFS), Google Apps, Amazon Web Services (AWS), IFX Networks Colombia, EQUIFAX Chile.
SGSI Nacionales Sector Público	Oficina de Normalización Previsional (ONP), Organismo Supervisor de la Inversión en Energía y Minería (OSINERGMIN), Organismo Supervisor de Inversión Privada en Telecomunicaciones (OSIPTEL), Banco Central de Reserva del Perú (BCRP), Instituto Nacional de Defensa de La Competencia y de La Protección de La Propiedad Intelectual (INDECOPI), Superintendencia de Mercado de Valores (SMV).
SGSI Nacionales Sector Privado	Bolsa de Valores de Lima (BVL), Grupo Graña y Montero (GMD), RIMAC Seguros, Hermes, Compañía Minera Hochscild, Terra (Media Network), Atento Perú, T-Gestiona, Telefónica Empresas, Telefónica del Perú, PMC Latam, Soluciones Orión.

Tabla 1. Muestra de organizaciones certificadas en la ISO 27001

Debido a que a la fecha no existe una fuente oficial donde se publiquen las entidades certificadas en el estándar 27001, la indagación respecto a las organizaciones listadas ha tenido que realizarse mediante consultas a especialistas en seguridad de información, a personal que pertenece a algunas de las organizaciones listadas y a otras fuentes, para verificarlo.

1.7.2. Investigaciones relacionadas

Las tesis más significativas relacionadas con Sistemas de Gestión de Seguridad de la Información (SGSI) son las siguientes:

Investigador	Fecha	Nombre de la Tesis
Justino Salinas, Zully Isabel	04/06/2015	PUCP. Diseño de un sistema de gestión de seguridad de información para una empresa inmobiliaria alineado a la norma ISO/IEC 27001:2013
Huamán Monzón, Fernando Miguel	12/09/2014	PUCP. Diseño de procedimientos de auditoría de cumplimiento de la norma NTP-ISO/IEC 17799:2007 como parte del proceso de implantación de la norma técnica NTP-ISO/IEC 27001:2008 en instituciones del estado peruano
Talavera Álvarez, Vasco Rodrigo	22/06/2015	PUCP. Diseño de un sistema de gestión de seguridad de la información para una entidad estatal de salud de acuerdo a la ISO/IEC 27001:2013
Espinoza Aguinaga, Hans Ryan	20/11/2013	PUCP. Análisis y diseño de un sistema de gestión de seguridad de información basado en la norma ISO/IEC 27001:2005 para una empresa de producción y comercialización de productos de consumo masivo
Aguirre Mollehuanca, David Arturo	30/10/2014	PUCP. Diseño de un sistema de gestión de seguridad de información para servicios postales del Perú S.A.
Montoya Pachas, Nelson Kal	03/12/2013	PUCP. Diseño de un sistema de gestión de seguridad de información para un centro cultural binacional
Ampuero Chang, Carlos Enrique	11/11/2011	PUCP. Diseño de un sistema de gestión de seguridad de información para una compañía de seguros
Aliaga Flores, Luis Carlos	02/09/2013	PUCP. Diseño de un sistema de gestión de seguridad de información para un instituto educativo
Villena Aguilar, Moisés Antonio	09/05/2011	PUCP. Sistema de gestión de seguridad de información para una institución financiera
Ríos Villafuerte, Josefina	02/09/2014	PUCP. Diseño de un sistema de gestión de seguridad de información para una central privada de información de riesgos
Barrantes Porras, Carlos Eduardo; Hugo Herrera, Javier Roberto	2012	USMP. Diseño e implementación de un sistema de gestión de seguridad de información en procesos tecnológicos.
Calderón Onofre, Diana; Estrella Ochoa, Martín; Flores Villamarín, Manuel	2011	ESPOL. Implementación de sistema de gestión de seguridad de la información aplicada al área de recursos humanos de la empresa DECEVALE S.A.

Tabla 2. Tesis relacionadas al tema

1.7.3. Software que automatiza la operación de un SGSI

Se han identificado las siguientes herramientas de software que automatizan parte de la operación de un SGSI:

ISO TOOLS

Es una herramienta web producida por ISO TOOLS Perú, que automatiza el cumplimiento de algunos requisitos del estándar 27001. Incorpora elementos de otros estándares como la ISO 9001 o de modelos BPM, los cuales no son necesariamente obligaciones del estándar de seguridad de información. No está estrictamente enfocado en el cumplimiento del estándar 27001.

E-GAM

Este software, producido por EGAMBPM, es un workflow de BPM genérico, adaptable a distintos estándares ISO; al igual que en el caso anterior, presenta una solución compleja, con una estructura más útil para organizaciones que cuentan con un sistema integrado de gestión.

INMUNO SUITE

Este sistema web, producido por M&T, cuenta con un módulo de gestión de riesgos complejo y un módulo de operación del SGSI, el cual ha sido modelado específicamente para el cumplimiento del estándar 27001, ya que guarda correlación con todos los requisitos, aunque no los llega a automatizar completamente.

E-PULPO

Es un sistema de escritorio producido por INGENIA, implementado con un enfoque de cumplimiento del estándar 27001 y que se integra al software EAR/PILAR del gobierno español, el cual usa para atender los requisitos de gestión de riesgos.

EAR PILAR

Es una herramienta de gestión de riesgos, desarrollada por el Centro Criptológico Nacional (CCN) de España, que implementa la metodología MAGERIT de análisis y gestión de riesgos, cuenta con licencias libres para organismos de la administración pública española.

1.8. Plan de proyecto

En esta sección se presenta la distribución de las tareas del proyecto y su planificación a lo largo del tiempo, en base a algunos artefactos del PMBOK [20].

1.8.1. Distribución de tareas

La Estructura de Distribución de Tareas (EDT) requerida para el desarrollo del presente proyecto se muestra en la siguiente imagen, bajo la forma de un diagrama en donde se destacan los grupos de tareas, que son:

	Etapa	Tareas
Implementación de un sistema de gestión de seguridad de la información para una empresa de consultoría de software	**Iniciación**	• Definición del problema • Marco conceptual • Estado del arte • Plan de proyecto • Descripción y sustentación de la solución • Esquema de organización de requisitos
	Establecer el SGSI	• Operación del sistema • Comunicaciones internas y externas • Gestión de la documentación • Contexto externo e interno de la organización • Necesidades y expectativas de las partes interesadas • Alcance del SGSI • Política de seguridad de información • Roles, responsabilidades y autoridades del sistema
	Implementar el SGSI	• Gestión de riesgos y oportunidades • Objetivos de seguridad de información • Concientización, capacitación y evaluación • Operación, planes, recursos y registros
	Mantener el SGSI	• Análisis y evaluación de las métricas • Auditoría interna • Revisión por la dirección
	Mejorar el SGSI	• Acciones correctivas • Acciones de mejora
	Verificación del cumplimiento del estándar y Cierre	• Mapa de requisitos • Análisis del cumplimiento de cada fase • Observaciones, recomendaciones y conclusiones

Tabla 3. Estructura de distribución de tareas

1.8.2. Planeamiento del proyecto en el tiempo

Se presenta el cronograma del proyecto, que detalla la ejecución de las tareas, una estimación de la duración de éstas y las fechas de finalización estimadas:

Nombre de tarea	Duración	Comienzo	Fin
Diseño de un SGSI para una consultora de software	**333 días**	vie 02/01/15	vie 29/04/16
1. Iniciación	**41 días**	vie 02/01/15	vie 27/02/15
Definición del problema	5 días	vie 02/01/15	jue 08/01/15
Marco conceptual	10 días	vie 09/01/15	jue 22/01/15
Estado del Arte	10 días	vie 23/01/15	jue 05/02/15
Plan de proyecto	5 días	vie 06/02/15	jue 12/02/15
Descripción y sustentación de la solución	5 días	vie 13/02/15	jue 19/02/15
Esquema de organización de requisitos	6 días	vie 20/02/15	vie 27/02/15
2. Etapa para Establecer el SGSI	**81 días**	lun 02/03/15	mar 30/06/15
Planificación del sistema	10 días	lun 02/03/15	vie 13/03/15
Esquema de comunicaciones internas y externas	10 días	lun 16/03/15	mar 31/03/15
Gestión de la documentación	10 días	mié 01/04/15	jue 16/04/15
Contexto externo e interno de la organización	15 días	vie 17/04/15	vie 08/05/15
Necesidades y expectativas de las partes interesadas	10 días	lun 11/05/15	vie 22/05/15
Alcance del SGSI	10 días	lun 25/05/15	vie 05/06/15
Política de seguridad de información	10 días	lun 08/06/15	vie 19/06/15
Roles, responsabilidades y autoridades del sistema	6 días	lun 22/06/15	mar 30/06/15
3. Etapa para Implementar el SGSI	**64 días**	mié 01/07/15	mié 30/09/15
Gestión de riesgos y oportunidades	40 días	mié 01/07/15	jue 27/08/15
Objetivos de seguridad de información	4 días	vie 28/08/15	mié 02/09/15
Concientización, capacitación y evaluación	10 días	jue 03/09/15	mié 16/09/15
Operación, planes, recursos y registros	10 días	jue 17/09/15	mié 30/09/15
4. Etapa para Mantener el SGSI	**42 días**	jue 01/10/15	lun 30/11/15
Análisis y evaluación de las métricas	17 días	jue 01/10/15	lun 26/10/15
Auditoría interna	20 días	mar 27/10/15	lun 23/11/15
Revisión por la dirección	5 días	mar 24/11/15	lun 30/11/15
5. Etapa para Mejorar el SGSI	**20 días**	mar 01/12/15	jue 31/12/15
Acciones correctivas	13 días	mar 01/12/15	vie 18/12/15
Acciones de mejora	7 días	lun 21/12/15	jue 31/12/15
6. Verificación del cumplimiento y cierre	**85 días**	lun 04/01/16	vie 29/04/16
Mapa de Requisitos	5 días	lun 04/01/16	vie 08/01/16
Análisis del Cumplimiento	10 días	lun 11/01/16	vie 22/01/16
Observaciones, recomendaciones y conclusiones	10 días	lun 25/01/16	vie 05/02/16
Revisión del documento Final	20 días	lun 08/02/16	vie 04/03/16
Revisión de los anexos	20 días	lun 07/03/16	vie 01/04/16
Presentación de la versión corregida	20 días	lun 04/04/16	vie 29/04/16

Tabla 4. Planeamiento del proyecto

1.9. Descripción y sustentación de la solución

Como se ha indicado, el problema se origina en los riesgos intrínsecos relacionados a la pérdida de confidencialidad, integridad y disponibilidad de la información, tanto en la operación de la consultora de software como en la interacción con sus clientes. Por ello, se han buscado alternativas que constituyan una herramienta para la administración de la seguridad de información, que atienda las necesidades de la organización de manera efectiva.

Tal como se ha mostrado en el estado del arte existen muchos marcos normativos relacionados a la seguridad de información. Sin embargo, algunos están limitados a contener solo definiciones, buenas prácticas, esquemas de controles o metodologías de gestión de riesgos, entre otros. Solamente tres de los marcos listados pueden constituirse en modelos para la operación y administración de la seguridad de información de una organización, y son:

- **ISO 27001:2013 Tecnología de Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de Información. Requerimientos [01]**
- **NIST SP 800-100 Manual de Seguridad de Información: Guía para gestores [13]**
- **Guía Profesional COBIT 5 para Seguridad de Información [18]**

Para estos, se ha optado por hacer una evaluación de los siguientes aspectos:

- Adaptabilidad. Compatibilidad entre la naturaleza de la organización y la propuesta del marco.
- Material y complementos disponibles. Publicaciones y alcance de las mismas que sea accesible para su uso en el proyecto.
- Especialistas disponibles. Expertos del medio que puedan apoyar y participar en el proyecto.
- Valor agregado. Mejoras o potenciales mejoras que, más allá de aspectos de la seguridad de información, puedan ser obtenidas por la organización.

Esquema de valoración: Si el aspecto es positivo recibe un valor de 3; si es neutro o representa aspectos favorables y desfavorables equivalentes, recibe el valor 2; finalmente, si representa principalmente dificultades, recibe un valor de 1:

Aspecto	ISO 27001:2013	Valor	NIST SP 800-100	Valor	GP COBIT 5 – SI	Valor
Adaptabilidad	La ISO 27001 puede ser implementada en organizaciones de cualquier tamaño.	3	La NIST está diseñada para organizaciones de tamaño y complejidad considerable (agencias federales de EE.UU).	1	COBIT5-SI es un modelo que segrega funciones y procesos, por lo que es más aprovechable por organizaciones grandes. Sin embargo, puede ser adaptada a la organización rediseñando el esquema.	2
Material y complementos disponibles	Cuenta con la familia de normas 27000 y la ISO 31000, directamente relacionadas a la seguridad de información y riesgos. Si bien la adquisición de los documentos ISO tiene un costo, existen versiones "libres" traducidas como normas técnicas.	2	Cuenta con otros documentos NIST para dominios específicos de control, relacionados a la seguridad de información. Este y otros documentos NIST son públicos.	3	Cuenta con otros elementos de COBIT: gobierno de TI, control y riesgos. La documentación de COBIT 5 y su Guía Profesional para Seguridad de Información están sujetas a pago. Pese a esto, existen publicaciones de especialistas en el tema que brindan información.	2
Especialistas disponibles	La organización cuenta con un coordinador de seguridad certificado como implementador líder 27001. Por el carácter obligatorio que tiene en el estado (NTP), se ha promovido la aparición de especialistas experimentados en la ISO: implementadores y auditores.	3	No se han identificado especialistas locales en este dominio, que puedan dar soporte a una implementación.	1	Existen especialistas locales de COBIT 5, pero muchos de ellos solo cuentan con el nivel "Fundamentos" y desconocen la "Guía Profesional COBIT 5 para la Seguridad de Información".	2
Valor agregado	Permite proyectar la implementación de un sistema integrado de gestión mediante la incorporación progresiva de otras ISOS de sistemas de gestión. Para las entidades del estado es una fuente de confianza, ya que se alinea la NTP 27001:2014.	3	No es un modelo escalable. Tampoco tiene un valor normativo local, pues es un estándar exclusivo de EE.UU.	1	Permite tener un primer acercamiento al modelo COBIT, para la implementación de sus otros componentes.	3
Resultado	**ISO 27001:2013**	**11**	**NIST SP 800-100**	**6**	**GP COBIT 5 – SI**	**9**

Tabla 5. Comparación de alternativas

En base al análisis realizado, se ha seleccionado la **ISO/IEC 27001:2013**, como base para la implementación. Por lo tanto, el producto para estructurar el gobierno, gestión y operación de la seguridad de información en la consultora de software, se denominará **Sistema de Gestión de Seguridad de la Información (SGSI)**, tal como lo establece ese estándar.

1.10. Esquema de organización de requisitos

Si bien la versión precedente del estándar 27001 (edición 2005) establecía el modelo **Planear – Hacer – Revisar – Actuar** para la operación del SGSI, en la actual (2013) este ha sido omitido y, en su lugar, el numeral 4.4 indica que:

"La organización debe establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de Información, en concordancia con los requerimientos de este estándar internacional" [02].

Por este motivo, se han organizado todos los requisitos vigentes bajo una propuesta de modelo propio, donde se ordenan y agrupan las cláusulas en las etapas: **Establecer**, **Implementar**, **Mantener** y **Mejorar**, según se muestra:

Etapa	Grupo de componentes del SGSI	Cláusulas
Establecer	Planificación del sistema	4.4
	Comunicaciones internas y externas	7.4
	Gestión de la documentación	7.5
	Contexto externo e interno de la organización	4.1
	Necesidades y expectativas de las partes interesadas	4.2
	Alcance del SGSI	4.3
	Política de seguridad de información	5.2
	Roles, responsabilidades y autoridades del sistema	5.1, 5.3
Implementar	Gestión de riesgos y oportunidades	6.1, 8.2, 8.3
	Objetivos de seguridad de información	6.2
	Concientización, capacitación y evaluación	7.2, 7.3
	Operación, planes, recursos y registros	8.1, 7.1
Mantener	Análisis y evaluación de las métricas	9.1
	Auditoría interna	9.2
	Revisión por la dirección	9.3
Mejorar	Acciones correctivas	10.1
	Acciones de mejora	10.2

Tabla 6. Clasificación de requisitos del estándar ISO 27001 por etapas

En cada capítulo, para cada uno de los requisitos atendidos, se han creado tablas de verificación del cumplimiento, que contienen lo siguiente:

- El numeral referencial de los requisitos del estándar 27001.
- La forma en que el sistema creado cumple con ellos.
- La referencia a los componentes que lo evidencian (los cuales se encuentran adjuntos como anexos a este documento).

Los componentes desarrollados no son creados como módulos aislados del sistema, sino que han sido estructurados tomando en cuenta las dependencias y secuencialidad que define el estándar. Para identificar adecuadamente estos elementos se ha desarrollado el siguiente esquema de requisitos y sus componentes, con las respectivas relaciones entre estos:

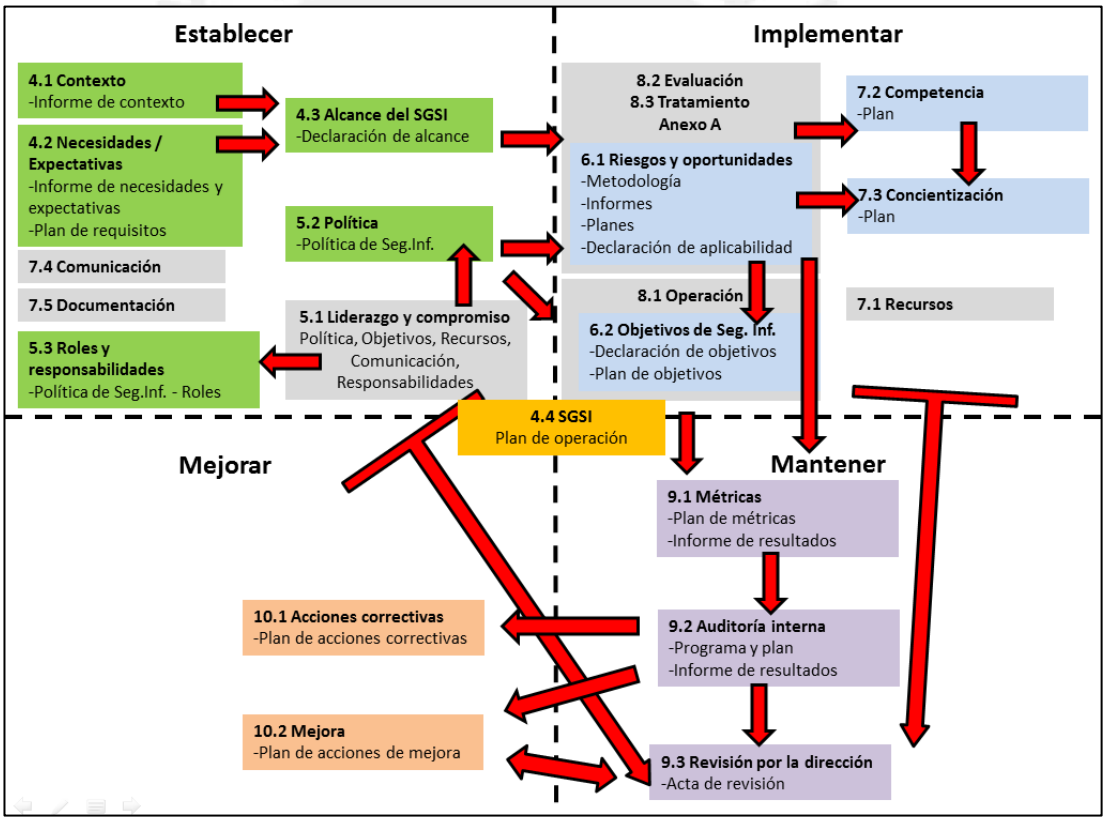

Figura 1. Modelo de requisitos y componentes del SGSI

[Fuente: Elaboración propia]

2. Componentes para establecer el SGSI

En este capítulo se presenta lo realizado para cumplir con los requisitos para establecer el sistema según lo que indica el estándar ISO/IEC 27001:2013. Para ello se exponen los lineamientos para su operación, la gestión de las comunicaciones internas y externas, el manejo de la documentación; la definición del contexto externo e interno de la organización; la identificación de las necesidades y expectativas de las partes interesadas; la definición del alcance del sistema; el establecimiento de la política de seguridad de información y, finalmente, la definición de los roles, responsabilidades y autoridades del sistema.

2.1. Planificación del sistema

Como se ha indicado en el esquema de organización de requisitos, el estándar 27001, en su numeral 4.4, dispone que el sistema cuente con las siguientes etapas:

- **Establecer.** Se preparan y aprueban los componentes necesarios para el funcionamiento del sistema.
- **Implementar.** Se realiza la gestión de los procesos, personas y controles de seguridad de información que se encuentran dentro del alcance del sistema.
- **Mantener.** Se obtienen y evalúan indicadores y resultados respecto a la operación del sistema y sus controles de seguridad de información.
- **Mejorar.** Se toma acción para mejorar o corregir los fallos identificados en las etapas anteriores sobre el sistema y sus controles de seguridad de información.

Para cada etapa, se han organizado las acciones que permiten cumplir, en conjunto, con todos los requisitos del estándar 27001.

Para planificar, ejecutar y monitorear cada componente del sistema, se ha elaborado un **Plan de operación y comunicaciones del SGSI (Anexo A)**, el cual contiene acciones de tipo "operación", las cuales se presentan tal como se indica a continuación:

ISO 27001	Cumplimiento del requisito	Evidencia
4.4	El **Plan de operación y comunicaciones del SGSI** está estructurado en acciones agrupadas en las fases: **Establecer** • Entender el contexto • Entender los requisitos de las partes interesadas • Establecer un plan para el logro de los requisitos • Ejecutar el plan para el logro de los requisitos • Determinar el alcance del SGSI • Validar la política de seguridad de información **Implementar** • Apreciar los riesgos de los procesos • Definir el tratamiento los riesgos identificados • Ejecutar el tratamiento los riesgos identificados • Validar los objetivos de seguridad de información • Establecer un plan para el logro de los objetivos • Ejecutar el plan para el logro de los objetivos • Mantener un plan de concientización, capacitación y evaluación • Ejecutar el plan de concientización, capacitación y evaluación **Mantener** • Definir métricas de Seguridad de Información • Analizar y evaluar las métricas • Ejecutar la auditoría interna del SGSI • Realizar la revisión por la dirección **Mejorar** • Establecer acciones correctivas y de mejora (auditoría interna) • Ejecutar el plan de acciones correctivas y de mejora (auditoría interna) • Establecer acciones correctivas y de mejora (revisión por la dirección) • Ejecutar el plan de acciones correctivas y de mejora (revisión por la dirección)	A. Plan de operación y comunicaciones del SGSI

Tabla 7. Requisitos de la operación del SGSI

2.2. Comunicaciones internas y externas

El numeral 7.4 exige determinar los parámetros que guiarán las comunicaciones relevantes que se dan para complementar la operación del sistema (qué, quién, a quién, cuándo, cómo).

Para lograr que estas comunicaciones se realicen de manera adecuada se ha creado un **Plan de operación y comunicaciones del SGSI (Anexo A)**, con acciones de tipo “comunicación”, respecto a cada uno de los siguientes hitos, enmarcados en las fases del sistema:

Establecer. Se comunican:

- El inicio de ciclo de operación del SGSI
- El plan para el logro de los requisitos
- La política de seguridad de información

Implementar. Se comunican:

- El inicio de la gestión de riesgos
- El fin de la gestión de riesgos
- El plan para el logro de los objetivos
- Las convocatorias del plan de concientización, capacitación y evaluación

Mantener. Se comunican:

- Los requerimientos para el monitoreo y medición de las métricas
- El inicio de la auditoría interna
- Resultados de la auditoría interna
- Las convocatorias a la revisión por la dirección

Mejorar. Se comunican:

- El plan de acciones correctivas y de mejora (auditoría interna)
- El plan de acciones correctivas y de mejora (revisión por la dirección)

Tal como lo dispone el estándar 27001, para cada una de las acciones de comunicación del plan se han definido algunos atributos que permiten que las comunicaciones logren su objetivo de manera efectiva y sin ambigüedades:

ISO 27001	Cumplimiento del requisito	Evidencia
7.4.a	**Mensaje (Qué)** Las acciones de comunicación del sistema establecen lo que se va a comunicar en la columna “Acción” del plan.	A. Plan de operación y comunicaciones del SGSI
7.4.b	**Momento (Cuándo)** Las acciones de comunicación del sistema establecen el causal de la comunicación en la columna “Condiciones” del plan.	
7.4.c	**Receptor (A quién)** Las acciones de comunicación del sistema establecen a quién se trasmitirá el mensaje, en la columna “Involucrados” del plan, donde se especifica quién asumirá el rol de receptor.	
7.4.d	**Emisor (Quién)** Las acciones de comunicación del sistema establecen a quién se trasmitirá el mensaje, en la columna “Involucrados” del plan, donde se especifica quién asumirá el rol de emisor.	
7.4.e	**Proceso de comunicación (Cómo)** Las acciones de comunicación del sistema establecen los pasos que involucra la comunicación, en la columna “Tareas” del plan, donde se indican los pasos a seguir para efectuar la comunicación.	

Tabla 8. Requisitos de las comunicaciones del sistema

Se debe tomar en cuenta que el plan diseñado corresponde a un ciclo inicial, por lo que si surgieran necesidades de comunicación futuras asociadas al sistema, estas deberían generar una versión actualizada del plan.

2.3. Gestión de la documentación

El numeral 7.5 del estándar 27001, dispone la gestión de documentos requeridos por el estándar y la que la organización dispone:

- En el primer caso, es la documentación según la cual el estándar, en distintos numerales, indica que *"debe estar disponible como información documentada"*:

ISO 27001	Cumplimiento del requisito	Evidencia
4.3	Alcance del sistema	D. Declaración de alcance del SGSI
5.2.e	Política de Seguridad de Información	E. Política de Seguridad de Información
6.1.2	Registros del proceso de apreciación de riesgos	H. Informe de gestión de riesgos
6.1.3	Registros del proceso de tratamiento de riesgos	H. Informe de gestión de riesgos I. Plan de tratamiento de riesgos K. Declaración de aplicabilidad de controles
6.2	Objetivos de seguridad de información	L. Declaración de objetivos de seguridad de información
7.2.d	Registros de evidencia de competencia	O. Plan de concientización, capacitación y evaluación
8.1	Registros del seguimiento a los procesos del SGSI	A. Plan de operación y comunicaciones del SGSI
8.2	Registros de resultados de la apreciación de riesgos	H. Informe de gestión de riesgos
8.3	Registros de resultados del tratamiento de riesgos	I. Plan de tratamiento de riesgos J. Informe de seguimiento de riesgos
9.1	Registros de monitoreo y medición de resultados	P. Plan de métricas de seguridad de información
9.2	Registros del planeamiento y resultados de auditorías	R. Programa de auditoría interna del SGSI S. Plan de auditoría interna del SGSI T. Informe de resultados de la auditoría interna
9.3	Registros de las revisiones por la dirección	U. Acta de revisión por la dirección
10.1	Registros de análisis de las no conformidades, las acciones tomadas y los resultados de estas	V. Plan de acciones correctivas W. Plan de acciones de mejora

Tabla 9. Documentos obligatorios por requisitos de la ISO 27001

- En el segundo caso, la documentación que la organización dispone para que el sistema sea efectivo, se refiere a las políticas específicas de seguridad, los procedimientos y otros controles documentales específicos, implementados por la organización y listados en la **Declaración de aplicabilidad de controles (Anexo K)**.

Finalmente, en cuanto a la gestión de ambos grupos de documentos, el estándar 27001 indica, en sus numerales 7.5.2 y 7.5.3, que aquellos gestionados, creados o actualizados deben cumplir con una serie de restricciones y obligaciones sobre el manejo de la documentación, las cuales han sido incluidas como numerales en las **Políticas específicas de seguridad de información (Anexo F) – Gestión de Documentos**, según se muestra:

ISO 27001	Cumplimiento del requisito	Evidencia
7.5.1	**General** Se han documentado los requisitos exigidos por el estándar 27001 y los controles que la organización ha determinado como necesarios.	Todos los documentos
7.5.2.a, c	**Atributos** El numeral 6.1 de la política dispone contar con registros de: nombre, descripción, medio (físico, digital), revisión y aprobación de documentos.	F. Políticas específicas de seguridad de información
7.5.2.b	**Formato** El numeral 6.2 de la política define el manejo de los formatos de los documentos (físico, digital).	
7.5.3.a-f	**Restricciones** El numeral 6.4 de la política da lineamientos para asegurar la confidencialidad, integridad y disponibilidad de la documentación, según corresponda.	
7.5.3	**Documentos externos** El numeral 6.5 de la política establece lineamientos para controlar y administrar los documentos de fuentes externas, si son usados por el sistema.	

Tabla 10. Requisitos de la gestión documental

2.4. Contexto externo e interno de la organización

El estándar 27001 en su numeral 4.1 indica que debe realizarse un entendimiento de la organización y su contexto, situación actual respecto a los distintos aspectos que pueden impactar en su operación.

Para el desarrollo de esta actividad el estándar referencia como marco de trabajo a la ISO 31000:2009 – numeral 5.3 [07], donde se describe el enfoque con el que se debe analizar el contexto interno y externo de la organización:

- **Generalidades.** Define la necesidad y el nivel al cual se debe documentar el contexto.
- **Establecimiento del contexto externo.** Propone lineamientos referenciales y una breve guía de lo que debería ser considerado dentro de los elementos de contexto externo.
- **Establecimiento del contexto interno.** Propone lineamientos referenciales y una breve guía de lo que debería ser considerado dentro de los elementos de contexto interno.
- **Establecimiento del contexto de gestión de riesgos.** Propone los elementos que deben definirse como margo general para la aplicación de la gestión de riesgos.
- **Definición de los criterios de riesgo.** Propone los parámetros específicos que deben ser definidos por la organización, para poder iniciar su gestión de riesgos.

Para documentar todos estos elementos se ha tomado en cuenta la naturaleza y características de la organización, por lo que se han seleccionado aquellos aspectos relevantes (externos, internos y de riesgos) para una consultora de software. Los componentes del sistema para el cumplimiento de esta cláusula, se han estructurado en el **Informe de contexto de la organización (Anexo B)**, documento que cuenta con las siguientes secciones:

- **Contexto externo.** Desarrolla los elementos de análisis de contexto externo del estándar ISO 31000:2009 [07].
    - Partes interesadas externas;
    - entorno político, legal, reglamentario y contractual;
    - entorno competitivo;
    - entorno social, cultural y natural;
    - entorno económico - financiero y
    - entorno tecnológico.

- **Contexto interno.** Desarrolla los elementos de análisis de contexto interno del estándar ISO 31000:2009 [07].
    - Partes interesadas internas;
    - misión y objetivos estratégicos;
    - procesos; organización y funciones;
    - recursos disponibles y
    - tecnología vigente.

- **Contexto del proceso de gestión del riesgo.** Contiene:
    - los objetivos de la gestión de riesgos,
    - la selección de procesos con información más crítica para el negocio (alcance preliminar) y
    - otros parámetros para la gestión de riesgos.

- **Criterios de riesgo.** Referencia a la **Metodología de gestión de riesgos (Anexo G)** que contiene:
    - los criterios de riesgos,
    - formulación del cálculo del riesgo (probabilidad y consecuencia),
    - la participación de las partes interesadas y
    - el nivel de tolerancia al riesgo.

- **Procesos críticos respecto a la seguridad de información.** A manera de conclusión del documento, se indican aquellos procesos que han sido determinado como críticos, tras tener un entendimiento completo del negocio.

El **Informe de contexto de la organización (Anexo B)** cumple con los requisitos del estándar 27001 y 31000 según se muestra a continuación:

ISO 27001	Cumplimiento del requisito	Evidencia
4.1	**Entendimiento del contexto** Se han definido el propósito, los resultados esperados en el **Informe de contexto de la organización**, donde se documentan también los aspectos internos y externos de la organización, tomando como referente los requisitos de la ISO 31000.	B. Informe de contexto de la organización G. Metodología de Gestión de Riesgos
Referencia: ISO31000 - 5.3.1	**Generalidades** Se ha documentado un **Informe de contexto de la organización** y una **Metodología de Gestión de Riesgos**, ambos bajo el enfoque del estándar ISO 31000.	
Referencia: ISO31000 - 5.3.2	**Contexto externo** En el informe se han especificado los siguientes elementos: • Partes interesadas externas • Entorno político, legal, reglamentario y contractual • Entorno competitivo • Entorno social, cultural y natural • Entorno económico y financiero • Entorno tecnológico	
Referencia: ISO31000 - 5.3.3	**Contexto interno** En el informe se han especificado los siguientes elementos: • Partes interesadas internas • Misión y objetivos estratégicos • Procesos de la organización • Organización y funciones • Recursos disponibles • Tecnología vigente	
Referencia: ISO31000 - 5.3.4	**Contexto del proceso de gestión del riesgo** En el informe se han especificado los siguientes elementos en el **Contexto y criterios del proceso de gestión de riesgo:** • **Objetivo.** De la gestión de riesgos • **Estrategia.** Aplicar la **Metodología de Gestión de Riesgos** • **Alcance.** Para la gestión de riesgos se referencian a los procesos de la **Declaración de alcance del SGSI**. • **Parámetros.** Comprende los procesos, recursos, responsabilidades, autoridades y metodología	
Referencia: ISO31000 - 5.3.5	**Criterios de riesgo** En **Contexto y criterios del proceso de gestión de riesgo - Criterios de riesgo**, la **Metodología de Gestión de Riesgos** es el marco para identificar, analizar, evaluar y tratar riesgos, con: • Niveles de consecuencias • Niveles de probabilidad • Cálculo del nivel de riesgo • Nivel de aceptación del riesgo • Criterios de aceptación de riesgos	

Tabla 11. Requisitos del entendimiento del contexto

2.5. Necesidades y expectativas de las partes interesadas

Las partes interesadas son aquellas entidades que tienen mayor importancia para la organización, por lo que sus requisitos de seguridad de información también deben ser tomados en cuenta para entender cuál debe ser el enfoque adecuado para implementar el sistema.

Se debe aclarar que estos requisitos de seguridad de información corresponden a dos grupos:

- **Necesidades.** Aquellos requisitos que tienen carácter obligatorio y comprenden el cumplimiento legal, contractual y reglamentario interno (directivas y políticas).
- **Expectativas.** Aquellos requisitos que surgen de los logros esperados respecto a los resultados de la operación de la organización.

Esto es requerido en el numeral 4.2 del estándar 27001, por lo que se ha documentado un **Informe de necesidades y expectativas de las partes interesadas (Anexo C)**. Este informe ha sido estructurado de la siguiente manera:

- **Generalidades.** Lista y especifica a las partes interesadas externas e internas que han sido identificadas. Las cuales son:
    - **Internas.**
        - Dirección (Socios y gerentes)
        - Gestor de proyecto (supervisor)
        - Operador (consultores)
        - Operador TIC (responsable de soporte)
        - Coordinador de seguridad de información
    - **Externas.**
        - Clientes (varios)
        - Proveedores (varios)
        - Competidores (varios)
        - Reguladores (Ministerio de Justicia, INDECOPI)

- **Requisitos de partes interesadas.** Detalla aquellos requisitos relacionados a la seguridad de la información, para cada interesado externo e interno, los cuales pueden ser:

    - **Necesidades**: Obligaciones contractuales, legales, directivas o normativas.
        - **Contractuales.** Comprende las especificaciones contractuales en aspectos de seguridad de información y acuerdos de confidencialidad, tanto con trabajadores como con proveedores.
        - **Legales.** Si bien se han identificado diversas leyes relacionadas al manejo de información (Protección de Datos Personales, Comercio Electrónico, General de Comunicaciones, Firma Electrónica, Propiedad Intelectual, Transparencia, Delitos Informáticos), solamente algunas aplican debido a las características de la organización:
            - Ley de Protección de Datos Personales – 29733 [21]
            - Ley sobre el Derecho de Autor – DL 822 [27]
            - Ley de Delitos Informáticos – 30096 [28]
        - **Directivas.** Lineamientos internos de la organización, de carácter obligatorio.

    - **Expectativas**: Resultados esperados de la operación de la organización, para lo cual se consideran.
        - Resultados económicos de la organización
        - Resultados en la imagen de la organización
        - Resultados en la forma en que opera la organización
        - Resultados sobre el personal de la organización
        - Resultados sobre la tecnología de la organización

A continuación se muestran, los resultados obtenidos del análisis de cada uno de los requisitos, considerando tanto necesidades (N) como expectativas (E):

Requisitos de Seguridad de Información	Tipo	Partes interesadas
Contratos y acuerdos con clientes (Confidencialidad, Integridad, Disponibilidad): Cumplir con las condiciones de seguridad de información asumidas con el cliente en el contrato y acuerdos relacionados a la seguridad de información.	**N**	**Externas:** Clientes. **Internas:** Dirección (Gerente de Operación), Gestor de proyecto
Contratos y acuerdos con el personal (Confidencialidad, Integridad, Disponibilidad): Asegurar el cumplimiento de las condiciones de seguridad de información asumidas por el personal en el contrato y acuerdos de confidencialidad y reconocimiento de las políticas de seguridad de información.	**N**	**Internas:** Dirección (Gerente de Operación, Gerente de Administración), Gestor de proyecto, Coordinador de seguridad de información
Contratos con proveedores de servicios TI (Disponibilidad): Asegurar el cumplimiento de los niveles de servicio respecto a los servicios tecnológicos que sirven de base para la elaboración de los productos.	**N**	**Externas:** Proveedores. **Internas:** Dirección (Gerente de Operación), Gestor de proyecto, Operadores (Consultores)
Ley de Protección de Datos Personales (Confidencialidad): Cumplir con la Ley y su Reglamento, aplicable solo a la información tratada de los trabajadores de la consultora (no existen proyectos con clientes que involucren información personal).	**N**	**Externas:** Reguladores (ANPDP). **Internas:** Dirección, Coordinador de seguridad de información
Ley sobre el Derecho de Autor (Integridad): Cumplir con la Ley, aplicable sobre la autenticidad del software usado en los procesos de consultoría de la organización.	**N**	**Externas:** Reguladores (INDECOPI). **Internas:** Dirección, Coordinador de seguridad de información
Ley de Delitos Informáticos (Confidencialidad, Integridad): Cumplir con la Ley, aplicable sobre la información facilitada y los productos (sistemas) entregados a clientes.	**N**	**Externas:** Reguladores (MINJUS). **Internas:** Dirección, Coordinador de seguridad de información
Entrega de productos a clientes (Integridad): Prevenir fallos en las entregas del producto (incompletas o mal versionadas).	**E**	**Externas:** Clientes. **Internas:** Dirección (Gerente de Operación), Gestor de proyecto

Tabla 12. Resultados de necesidades y expectativas

Los requisitos de seguridad de información son tomados en cuenta para la definición del alcance del SGSI, tal como se indica en el numeral 2.6 del presente informe. Sin embargo, la selección de los elementos incorporados al sistema corresponde a la dirección de la organización.

Además, como se verá más adelante, para lograr que estos sean cumplidos, se ha diseñado y ejecutado un **Plan de requisitos de seguridad de información (Anexo N)**.

Como se puede verificar, el informe preparado con estos requisitos permite cumplir con las disposiciones del estándar 27001:

ISO 27001	Cumplimiento del requisito	Evidencia
4.2.a	**Partes interesadas** En la sección **Generalidades** se especifica el detalle de quiénes son las partes interesadas, que fueron identificadas anteriormente, en el **Informe de contexto de la organización**.	C. Informe de necesidades y expectativas de las partes interesadas
4.2.b	**Requisitos de las partes interesadas** Estos requisitos de seguridad de información se han definido indagando en las necesidades (obligaciones contractuales, legales, directivas o normativas) y expectativas (respecto a los resultados de la organización) sobre las partes interesadas internas y externas.	

Tabla 13. Requisitos de necesidades y expectativas de partes interesadas

Estos requisitos deben ser reevaluados en cada ciclo de operación, ya que las necesidades de la organización, sus acuerdos o las leyes aplicables pueden cambiar durante ese periodo.

2.6. Alcance del SGSI

Para determinar el alcance del sistema se han realizado las siguientes actividades:

- Se ha revisado el **Informe de contexto de la organización (Anexo B)**:
  - **Contexto interno - Procesos de la organización**. Se definen y clasifican los procesos de la organización.
  - **Procesos críticos respecto a la seguridad de información**. Se definen los procesos que cuentan con información más sensible.
- Se ha revisado el **Informe de necesidades y expectativas de las partes interesadas (Anexo C)**, donde:
  - **Requisitos de partes interesadas**. Se identifica cada requisito relevante para la seguridad de información.
  - Los requisitos identificados incluyen aquellos que se originan en las dependencias con entidades internas y externas.

Producto de este análisis, la dirección de la organización ha definido los procesos y requisitos seleccionados, los cuales perfilan el alcance:

<table>
<tr><th colspan="4">Consultora de software</th></tr>
<tr><th colspan="4">Procesos estratégicos</th></tr>
<tr><td colspan="2">A1. Gestión de la dirección
(planificación y recursos)</td><td colspan="2">A2. Gestión comercial
(ventas y prospectiva de servicios)</td></tr>
<tr><th colspan="4">Procesos operacionales</th></tr>
<tr><td><u>B1. Gestión de proyectos de consultoría</u></td><td colspan="2"><u>B2. Ejecución de servicios de desarrollo y mantenimiento de software</u></td><td><u>B3. Aseguramiento de la calidad del software</u></td></tr>
<tr><th colspan="4">Procesos de apoyo</th></tr>
<tr><td>C1. Gestión de la contabilidad y finanzas</td><td>C2. Gestión de recursos humanos</td><td>C3. Gestión de tecnología e infraestructura</td><td>C4. Gestión de logística y patrimonio</td></tr>
</table>

Figura 2. Procesos seleccionados por la importancia de su información

Esta selección establece los procesos en los que es más importante gestionar la seguridad de información; sin embargo, su enumeración no basta para constituir un alcance del sistema; por lo que, en la **Declaración de alcance del SGSI (Anexo D)**, se especifican los siguientes aspectos de los procesos:

- Generalidades
- Procesos y áreas involucradas
- Información de los procesos
- Personal y organización
- Activos y servicios
- Ubicación
- Requisitos de seguridad de información gestionados por el sistema

Estos elementos componen los límites y aplicabilidad del sistema y se han desarrollado en base a las disposiciones del estándar 27001 respecto a su alcance:

ISO 27001	Cumplimiento del requisito	Evidencia
4.3	Se definen los límites y aplicabilidad del sistema sobre los procesos y sus componentes, para lo cual: • Se consideran el contexto interno y el externo para identificar los procesos críticos respecto a la seguridad de su información (**Informe de contexto de la organización**) • Se consideran los requisitos de seguridad de información para incorporarlos al alcance (**Informe de necesidades y expectativas de las partes interesadas**). • Para realizar la identificación de requisitos se toman en cuenta las partes interesadas (internas y externas), así como las dependencias respecto a ellas, por lo que este aspecto también ha influido en la definición del alcance. La versión completa del alcance está documentada en la **Declaración de alcance del SGSI**.	B. Informe de contexto de la organización C. Informe de necesidades y expectativas de las partes interesadas D. Declaración de alcance del SGSI

Tabla 14. Requisitos de la definición del alcance

Debido a la alta interrelación que existe entre los procesos seleccionados (**B1. Gestión de proyectos de consultoría, B2. Ejecución de servicios de desarrollo y mantenimiento de software, B3. Aseguramiento de la calidad del software**), se ha visto conveniente diagramar sus componentes y relaciones en un único esquema en la **Declaración de alcance del SGSI (Anexo D)**, el mismo que se muestra a continuación:

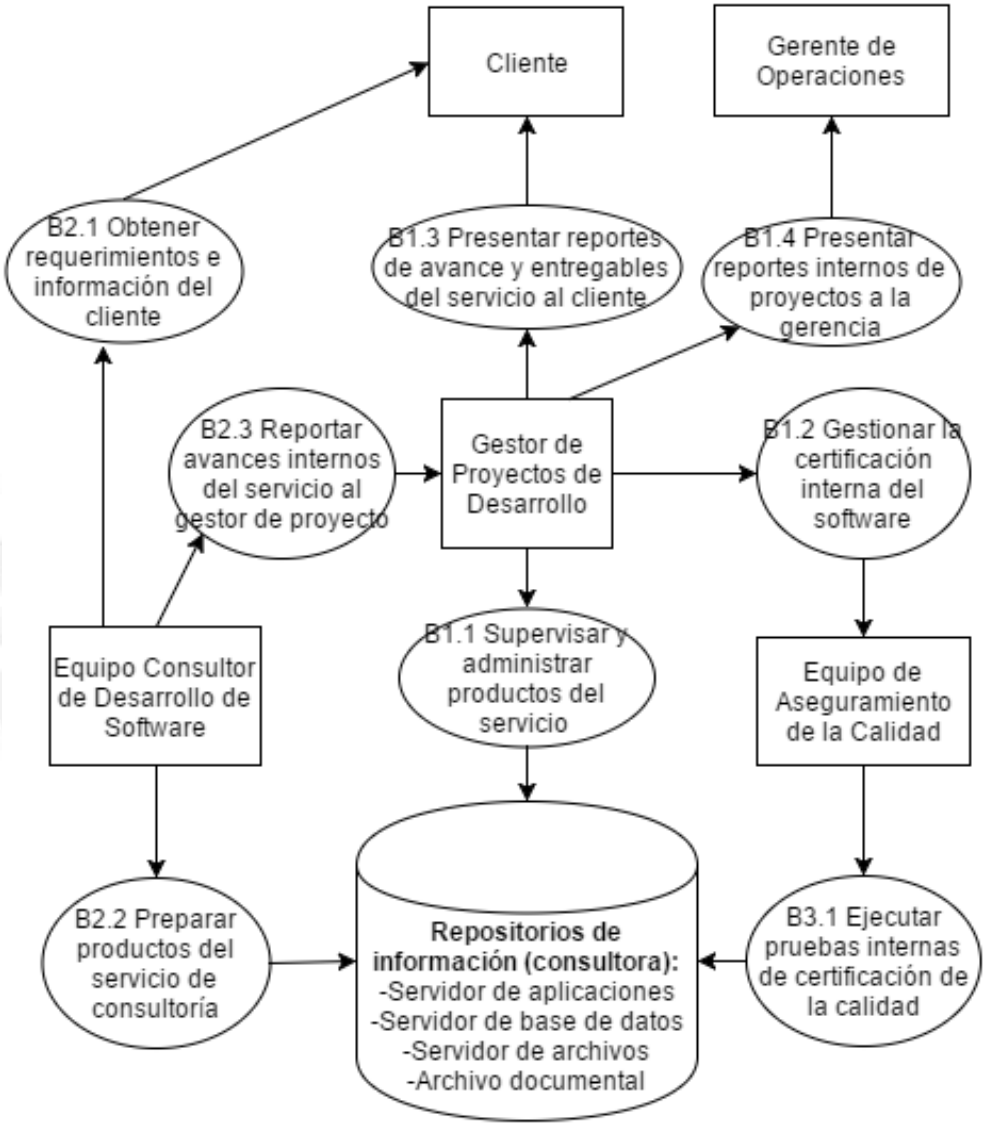

Figura 3. Diagrama de procesos en el alcance

[Fuente: Elaboración propia]

2.7. Política de seguridad de información

La política de seguridad de información representa el compromiso y enfoque de la organización, respecto a la seguridad de la información crítica de sus procesos; la cual debe ser definida y aceptada por la dirección.

Si bien el estándar la establece como requisito en su numeral 5.2, esta política trasciende al sistema, pues, ya sea que esté documentada o no, toda organización cuenta con una política intrínseca a la naturaleza del negocio, respecto a: la importancia que tiene la totalidad o un subconjunto de información crítica para sus procesos.

Para la consultora de software se ha aprobado una política, enfocada en sus particularidades y tomando en cuenta el entendimiento logrado durante la elaboración del **Informe de contexto de la organización (Anexo B)** y el **Informe de necesidades y expectativas de las partes interesadas (Anexo C)**:

- Se ha comprendido que la naturaleza del negocio implica el uso intensivo y central de información, sobre todo en medios electrónicos y digitales.
- Se ha identificado que la organización maneja información propia y de sus clientes.
- Se toma en consideración que esta información puede estar expuesta a riesgos del medio.
- Además, se reconoce que existe requisitos, algunos de los cuales no son optativos (leyes, contratos) y cuyo incumplimiento pueden afectar tanto a la imagen como a la economía de la organización

En base a los puntos anteriores se ha redactado y comunicado la **Política de seguridad de información (Anexo E)**, la cual cuenta con la aprobación de los representantes de la dirección, la cual la hace válida y de cumplimiento general en toda la organización.

Este documento cumple con los requisitos del estándar 27001, según se muestra a continuación:

ISO 27001	Cumplimiento del requisito	Evidencia
5.2	La **Política de seguridad de información** se establece bajo la aprobación del representante de la dirección (Gerente general).	E. Política de seguridad de información L. Declaración de objetivos de seguridad de información N. Plan de requisitos de seguridad de información
5.2.a	**Propósito de la organización** Párrafo 1. Explica la naturaleza del negocio y, en a partir de ello, reconoce la importancia que tiene su información y declara su compromiso de salvaguardarla, en beneficio de la consultora y sus clientes.	
5.2.b	**Referencia a Objetivos** Párrafo 2: Referencia a dónde (**Declaración de objetivos de seguridad de información**) y cómo (**Plan de Objetivos de Seguridad de Información**) se definirán y lograrán los objetivos de seguridad de información, alineados a los de la organización.	
5.2.c	**Compromiso sobre los requisitos** Párrafo 3: Compromete la atención de los requisitos de seguridad de información identificados de la organización, e indica cómo se logrará atenderlos (**Plan de Requisitos de Seguridad de Información**).	
5.2.d	**Compromiso de mejora continua** Párrafo 4: Establece la creación del **Sistema de Gestión de Seguridad de Información (SGSI)**, se compromete a su mejora continua en seguridad de información, así como también a la mejora de los procesos que forman parte de su alcance.	
5.2.e	**Documentación** Se encuentra documentada en la **Política de seguridad de información**.	
5.2.f – g	**Publicación y difusión** Párrafo 5: Dispone que sea publicada y comunicada entre los miembros de la organización y aquellos interesados que se vean afectados por ella en aspectos relacionados a la seguridad de información.	

Tabla 15. Requisitos de la política de seguridad de información

2.8. Roles, responsabilidades y autoridades del sistema

Los roles del sistema y los cargos que los están asumiendo en la organización han sido indicados en la **Declaración de alcance del SGSI (Anexo D) – Personal y Organización**. Además, las responsabilidades asociadas a cada uno de estos roles del sistema están detalladas en las **Políticas específicas de seguridad de información (Anexo F)**, sección de **Roles, responsabilidades y autoridades**.

En concordancia con esta distribución de personas y actividades, a continuación se indican, de manera general, los dominios del SGSI, donde los roles actúan como el principal responsable (A: autoridades) o como involucrados (P: participantes):

ISO 27001	Actividad	Rol					
		Comité de seguridad de información	Representante de la dirección	Representante de procesos / Propietario del riesgo	Participantes del proceso	Operador del SGSI	Auditor interno
4.4	Operación del sistema	A	A			P	
7.4	Comunicaciones internas y externas	A	A			P	
7.5	Gestión de la documentación		A			P	
4.1	Contexto externo e interno de la organización		A	P	P	P	
4.2	Necesidades y expectativas de las partes interesadas		A	P	P	P	
4.3	Alcance del SGSI	A	A	P		P	
5.2	Política de seguridad de información	A	A	P		P	
5.1, 5.3	Roles, responsabilidades y autoridades del sistema	A	A			P	
6.1, 8.2, 8.3	Gestión de riesgos y oportunidades			P	P	A	
6.2	Objetivos de seguridad de información		A	P		P	
7.2, 7.3	Concientización, capacitación y evaluación		P	P	P	A	
8.1, 7.1	Planes y recursos		A	P	P	P	P
9.1	Análisis y evaluación de las métricas			P		A	
9.2	Auditoría interna	P	P	P	P	P	A
9.3	Revisión por la dirección	A	A			P	
10.1	Acciones correctivas			P	P	A	
10.2	Acciones de mejora			P	P	A	

Tabla 16. Matriz de roles y actividades del SGSI

Nota: El rol de propietario del riesgo corresponde ser asumido por el representante de aquel proceso que cuente con la autoridad y recursos para asumir la responsabilidad de algún riesgo detectado. Es asignado como resultado de la gestión de riesgos.

Con el esquema de roles propuesto, se tiene cumplimiento del estándar 27001, tanto para el liderazgo como para los roles y responsabilidades:

ISO 27001	Cumplimiento del requisito	Evidencia
5.1	Existe un rol líder dentro del sistema, que es asumido por el Gerente general (Representante de la dirección) el cual, según lo definido en las **Políticas específicas de seguridad de información - Roles, responsabilidades y autoridades (numeral 1.2.b)**, realiza lo siguiente: a) Valida y aprueba la política de seguridad de información y los objetivos, alineados a la estrategia de la organización, para establecerlos. b) Integra las actividades del sistema en los procesos, mediante la aprobación y seguimiento del plan de operación y comunicaciones. c) Brinda los recursos planificados en el plan de operación y comunicaciones del sistema. d) Comunica la necesidad de operar adecuadamente el sistema, mediante: la publicación de la política de seguridad de información y las charlas. e) Valida el cumplimiento de las metas del sistema, durante la revisión por la dirección. f) Define la orientación de los roles y designa responsables para la capacitación y evaluación del personal que los asumirá. g) Promueve la mejora continua, mediante la revisión y toma de decisiones cíclica de respecto a la operación del sistema, durante la revisión por la dirección. h) Participa de otras actividades del sistema como líder, aprobador o facilitador.	F. Políticas específicas de seguridad de información E. Política de seguridad de información L. Declaración de objetivos de seguridad de información A. Plan de operación y comunicaciones del SGSI O. Plan de concientización, capacitación y evaluación U. Acta de revisión por la dirección
5.3	Las responsabilidades y autoridades definidas han sido oficializadas y comunicadas mediante la designación del personal para que las asuma.	F. Políticas específicas de seguridad de información
5.3.a	Entre los roles designados se encuentran los necesarios para atender los requisitos del estándar 27001, según se observa en la **Matriz de roles y actividades del SGSI**.	
5.3.b	El **Operador del SGSI** es el responsable de reportar al **Comité de seguridad de información**, presidido por el **Representante de la dirección**, respecto al desempeño del sistema, en las revisiones por la dirección.	

Tabla 17. Requisitos de liderazgo, roles y responsabilidades

3. Componentes para implementar el SGSI

En este capítulo se presenta lo realizado para cumplir con los requisitos para implementar el sistema según lo que indica el estándar ISO/IEC 27001:2013. Para ello se exponen los lineamientos para la gestión de riesgos y oportunidades de seguridad de información, la definición y planeamiento de los objetivos, la realización de actividades de concientización, capacitación y evaluación del personal involucrado en el sistema y la puesta en marcha de los planes, recursos y registros de operación involucrados.

3.1. Gestión de riesgos y oportunidades

El estándar 27001 define como obligatoria la gestión periódica de riesgos y oportunidades de seguridad de información (las oportunidades son riesgos de impacto positivo por lo que, en adelante, nos referiremos también a estas como riesgos). Los numerales 6.1.1, 6.1.2 y 6.1.3 especifican cómo se deben evaluar y tratar los riesgos, y los numerales 8.1, 8.2 y 8.3 disponen mantener los resultados de estas actividades.

Para atender estos requisitos se ha diseñado la **Metodología de gestión de riesgos (Anexo G)** alineada a los principios y guía del estándar ISO 31000:2009 [07], según el cual, la gestión de riesgos se desarrolla así:

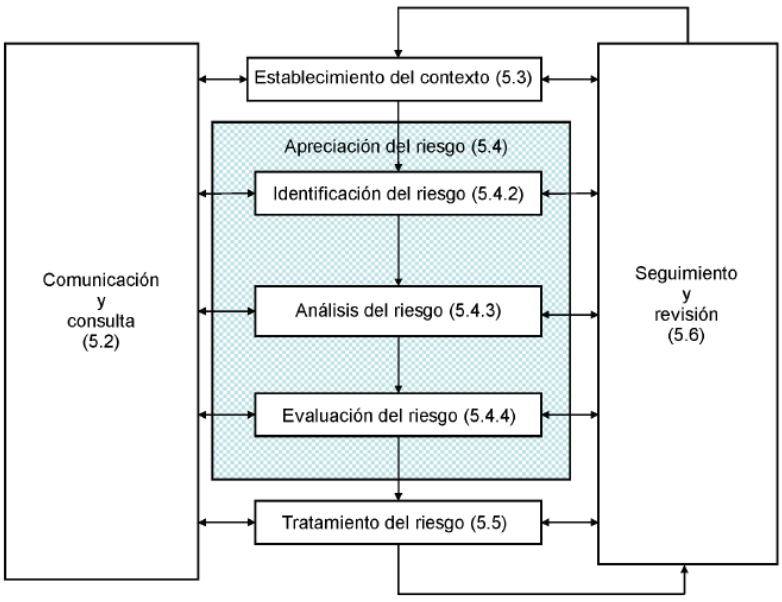

Figura 4. Modelo de Gestión de Riesgos bajo la ISO 31000:2009

Las etapas de la gestión de riesgos se describen a continuación:

Establecimiento del contexto. Se ha conocido el estado actual de la organización y se han definido los criterios para la gestión de riesgos:

- Se revisó el **Informe de contexto de la organización (Anexo B)**, el **Informe de necesidades y expectativas de las partes interesadas (Anexo C)** y la **Declaración del Alcance del SGSI (Anexo D)**.
- Se ha determinado que el marco y alcance de la gestión de riesgos no requieren cambiar pues son adecuados.
- Se ha documentado esta verificación en el **Informe de gestión de riesgos (Anexo H)**.

ISO 27001	Cumplimiento del requisito	Evidencia
6.1.1	**General** La actividad para identificar riesgos y oportunidades, gestión de riesgos de seguridad de información, usa como insumos en la fase de **Establecimiento del Contexto**: el **Informe de contexto de la organización** (requisito 4.1 del estándar) y el **Informe de necesidades y expectativas de las partes interesadas** (requisito 4.2 del estándar). Los riesgos y oportunidades se identifican para: • Propiciar que el sistema obtenga los resultados esperados, pues gestionando los riesgos (**Informe de gestión de riesgos**) fortalece la seguridad de información general. • Prevenir la materialización de efectos indeseables (riesgos), ya que son anticipados y tratados mediante el **Plan de Tratamiento de Riesgos**. • Promover la mejora continua, ya que los controles incluidos en el **Plan de Tratamiento de Riesgos** implican un mejoramiento del entorno de seguridad de la organización Por ello, se ha planificado ejecutar: • Un **Plan de tratamiento de riesgos** para los riesgos y oportunidades. • Como consecuencia, se genera un **Informe de seguimiento de riesgos** para verificar los controles y su integración a los proceso y evaluar su efectividad.	G. Metodología de Gestión de Riesgos I. Plan de tratamiento de riesgos J. Informe de seguimiento de riesgos

Tabla 18. Requisitos de la gestión de riesgos y oportunidades

Apreciación del riesgo. Se ha revisado la IEC 31010:2009 [08] como referente para crear la metodología que contempla la apreciación de riesgos, y define como realizar la identificación, análisis y evaluación:

Identificación del riesgo. Se siguen los siguientes pasos para la detectar riesgos sobre los procesos dentro del alcance:

- Tomar como referencia el diagrama de flujo de datos de la **Declaración del Alcance del SGSI (Anexo D)** para identificar en que instancias (activos) se encuentra la información de la actividad.
- Realizar un recorrido del proceso e identificar entrevistando en cada actividad del flujo al responsable para identificar los riesgos que puedan afectar a la información, usando el **Marco para la identificación de riesgos** que propone la metodología.
- Registrar esos riesgos en la **Matriz de Riesgos**, documentada en el **Informe de gestión de riesgos (Anexo H)**.

Como resultado de esta actividad se han identificado 36 riesgos y 1 oportunidad de seguridad de información a analizar.

Análisis del riesgo. Se han analizado los atributos que permiten determinar el nivel de riesgo en cada caso:

- Usando la **Matriz de riesgos** se define para cada riesgo:
  - El propietario del riesgo
  - Los controles que se le relacionan
- En base a esta información se determina:
  - El impacto de las consecuencias en su conjunto
  - La probabilidad de que el riesgo se materialice
- Con los datos obtenidos se obtiene el nivel de riesgo para cada caso, en base a la metodología (**Cálculo de nivel de riesgos**).
- El resultado del análisis realizado se documenta en la **Matriz de riesgos** dentro del **Informe de gestión de riesgos (Anexo H)**.

Al finalizar la fase se determina que 28 riesgos no son de nivel “Aceptable”.

Evaluación del riesgo. Se definieron los riesgos aceptables e inaceptables, por su nivel de riesgo y los criterios de aceptación de riesgos.

- Se identifican los riesgos aceptables / inaceptables con la **Matriz de riesgos**, y la matriz para calcular el nivel de aceptación de riesgos.
- A cada riesgo inaceptable, se le asigna una prioridad referencial.
- El resultado de la evaluación se documenta en la misma **Matriz de riesgos** dentro del **Informe de gestión de riesgos (Anexo H)**.

Al finalizar la fase se han evaluado y priorizado los 8 riesgos y la oportunidad de nivel “Inaceptable”.

ISO 27001	Cumplimiento del requisito	Evidencia
6.1.2	**Apreciación de Riesgos de Seguridad de Información** Para la apreciación de riesgos se ha establecido un marco de trabajo en la **Metodología de Gestión de Riesgos**.	G. Metodología de Gestión de Riesgos
6.1.2.a, b	**Criterios de riesgos de seguridad de información** La metodología define estos parámetros: • Criterios de aceptación de riesgos: nivel de riesgo y criterios de aceptación. • Criterios para apreciación del riesgo: matriz para valorar los riesgos. Debido al diseño bajo un enfoque objetivo de apreciación de riesgos (criterios, niveles y otros parámetros), la metodología garantiza resultados válidos, consistentes y comparables.	
6.1.2.c	**Identificación de riesgos de seguridad de información** La metodología indica la forma de identificar riesgos de seguridad de información, siguiendo el flujo de información en los procesos del alcance, y asignándoles un propietario.	G. Metodología de Gestión de Riesgos H. Informe de gestión de riesgos
6.1.2.d	**Análisis de riesgos de seguridad de información** Los riesgos se analizan para determinar los niveles de probabilidad y consecuencias que implican para determinar el nivel de riesgo.	
6.1.2.e	**Evaluación de riesgos de seguridad de información** En base al nivel de riesgo y los criterios de aceptación, se define si el riesgo será o no tratado y bajo qué prioridad. Las actividades indicadas se documentan en el **Informe de gestión de riesgos**.	
8.2	**Resultados de la apreciación de riesgos** La metodología dispone ejecuciones cíclicas o al ocurrir un cambio significativo. Los resultados se documentan en el **Informe de gestión de riesgos**.	

Tabla 19. Requisitos de la apreciación de riesgos

Tratamiento del riesgo. Tras terminar con las etapas de apreciación del riesgo, se inició el tratamiento para los riesgos definidos como inaceptables. Se documentaron los planes para implementarlos y los registros requeridos:

- Con los riesgos priorizados en la **Matriz de riesgos** se definen las estrategias de tratamiento: aceptar, reducir o aumentar, en la matriz de riesgos.
    - Si se "Acepta" un riesgo "inaceptable", debe indicarse y explicarse qué **criterio de aceptación** se usó.
    - Si se opta por "Reducir" o "Aumentar", se debe indicar: los controles, la acción relacionada a estos y la referencia al numeral relacionado en la lista de controles Anexo A del estándar, estimando el riesgo residual que se obtendrá.
- Para cada estrategia que no sea "Aceptar", se documenta un plan:
    - Los controles originados en "Reducir" y "Aumentar", se documentan en el en el **Plan de tratamiento de riesgos (Anexo I)**.
- En el caso de ambos planes se especifican los responsables, recursos y fechas de ejecución (inicio y fin).
- Se documenta la definición de los tratamientos en el **Informe de gestión de riesgos (Anexo H)**.
- Finalmente la lista de controles usados en la gestión de riesgos se incluyen en la **Declaración de aplicabilidad de controles (Anexo K)**, especificando los motivos que generan su inclusión o exclusión.

Al finalizar la fase se ha planificado el tratamiento de los riesgos y oportunidad seleccionados, a través los 9 controles determinados.

Una vez aprobado el **Plan de tratamiento de riesgos (Anexo I)**, se inicia el seguimiento periódico sobre los controles comprometidos en el plan. Esta actividad de seguimiento queda documentada en el **Informe de seguimiento de riesgos (Anexo J)**.

ISO 27001	Cumplimiento del requisito	Evidencia
6.1.3	**Tratamiento de riesgos de seguridad de información** El proceso de tratamiento de riesgos se desarrolla según la **Metodología de Gestión de Riesgos**.	G. Metodología de Gestión de Riesgos
6.1.3.a	**Opciones de tratamiento** En base a la lista de riesgos inaceptables identificados durante la apreciación, se opta por alguna de las siguientes opciones de tratamiento: **aceptar**, solo en base a criterios de aceptación de riesgos; **reducir**, mediante la implementación de actividades que implementen o mejoren los controles; y **aumentar**, alternativa similar a la de reducir, solo que es empleada para oportunidades.	G. Metodología de Gestión de Riesgos H. Informe de gestión de riesgos I. Plan de tratamiento de riesgos K. Declaración de aplicabilidad de controles
6.1.3.b	**Controles requeridos** Para las opciones reducir o aumentar, se seleccionan controles que permitan tratar el riesgo / oportunidad.	
6.1.3.c	**Validación de controles** La referencia principal para determinar los controles requeridos es el anexo A del estándar 27001, por lo que la estos no son omitidos.	
6.1.3.d	**Declaración de aplicabilidad** Se elabora una **Declaración de aplicabilidad de controles**, sobre los requeridos para que la organización cuente con un entorno de seguridad de información razonable (ya sea estén implementados o no). En la matriz de esta declaración se justifica la exclusión e inclusión de los mismos.	
6.1.3.e	**Plan de tratamiento de riesgos** El resultado final de los controles seleccionados para el tratamiento de riesgos es documentado en el **Plan de tratamientos de riesgos de seguridad de información**.	
6.1.3.f	**Aprobaciones** Los propietarios del riesgo aprueban finalmente: • **Informe de Gestión de Riesgos**. Contiene los riesgos aceptados (mantienen su nivel de riesgo) y no aceptados (con su nivel de riesgo residual estimado). • **Plan de Tratamiento de Riesgos**. Que los compromete a involucrarse en el tratamiento de los riesgos no aceptados.	
8.3	**Resultados del tratamiento de riesgos de seguridad de información** El **Plan de Tratamiento de Riesgos** se implementa de acuerdo a los plazos y responsables determinados en el mismo plan. Los resultados de esta implementación se reportan mediante el seguimiento realizado en el **Informe de seguimiento de riesgos**.	

Tabla 20. Requisitos del tratamiento de riesgos

A continuación se muestran los resultados del contexto, apreciación y tratamiento de riesgos, realizado en base a la **Metodología de gestión de riesgos (Anexo G)**:

- En el contexto establecido se tomaron los procesos que formaron parte del alcance del sistema.
- Se realizaron reuniones de trabajo con los involucrados en los procesos, para aplicar la metodología.
- Resultado de la apreciación y tratamiento de riesgos se obtuvo para cada fase de la metodología:

Fases	Resultado
Contexto	Se mantienen los 3 procesos con la información consignada en los informes de contexto y el alcance.
Identificación	Se han identificado 36 riesgos y 1 oportunidad en los procesos seleccionados
Análisis	Se han seleccionados 8 riesgos y 1 oportunidad como significativos (nivel: inaceptable)
Evaluación	Los 8 riesgos y la oportunidad inaceptables han sido priorizados (en corto-1, mediano-2 y largo-3 plazo).
Tratamiento	Para los 8 riesgos y la oportunidad se han propuesto 9 controles a implementar o mejorar. Con este resultado se elabora el **Plan de tratamiento de riesgos** y la **Declaración de aplicabilidad de controles**.
Seguimiento	Se planifican y ejecutan seguimientos trimestrales: 4 **Informes de Seguimiento de Riesgos** hasta la próxima gestión de riesgos.

Tabla 21. Resultados de la gestión de riesgos y oportunidades

Los productos obtenidos como resultado de esta gestión de riesgos son:

- **Informe de gestión de riesgos (Anexo H)**
- **Plan de tratamiento de riesgos (Anexo I)**
- **Declaración de aplicabilidad de controles (Anexo K)**
- **Informe de seguimiento de riesgos (Anexo J)**

El principal resultado de la gestión de riesgos es el conjunto de riesgos (y oportunidades) significativos y los controles que los tratan:

Riesgo	Descripción	Tratamiento
GR15-R01	Robo de laptop de consultoría que contiene información del cliente durante la visita o en tránsito desde el cliente	**Reducir** **8.3.3 Encriptamiento de unidades de disco duro destinadas fuera de la empresa** Implementar el encriptamiento a nivel de BIOS para el disco duro de las laptops de consultoría.
GR15-R02	Copia no autorizada de información mediante dispositivo USB desde la laptop de consultoría	**Reducir** **11.2.8 Bloqueo automático de equipos por inactividad** Reducir a 3 minutos el tiempo de bloqueo por inactividad en el equipo de consultoría
GR15-O01	Conocimiento limitado del personal del cliente respecto a las condiciones contractuales de seguridad de información	**Aumentar** **7.2.2 Charlas explicativas de las condiciones de seguridad de información para los clientes** Establecer la presentación detallada de los limites y responsabilidades establecidas en el contrato con los clientes para evitar reclamos sin sustento y propiciar la retroalimentación de mejoras
GR15-R07	Copia no autorizada de registros por los consultores, desde el servidor de archivos con información del proyecto	**Reducir** **8.3.1 Bloqueo de puertos USB en los equipos - consultores** Implementar el bloqueo de puertos USB en los equipos de los consultores
GR15-R08	Copia no autorizada de registros por el administrador de plataformas, desde el servidor de archivos con información del proyecto	**Reducir** **7.2.2 Charla de sensibilización - administrador de plataformas** Realizar charlas sobre seguridad de información específicas para el administrador de plataformas y sus funciones
GR15-R11	Eliminación o modificación intencional para sabotear productos, por personal descontento	**Reducir** **7.2.3 Penalización por sabotajes o daños intencionales** Incluir en el contrato el reconocimiento de que en caso se reciban penalidades a la empresa, originadas en un intento de daño intencional por el empleado, este asumirá la totalidad del monto de pérdida.
GR15-R13	Conflictos de versionado en los productos del servicio, por uso inadecuado del mecanismo versionador	**Reducir** **12.1.1 Protocolo de desarrollo de software y productos del servicio** Actualizar el protocolo de desarrollo de software, de manera que especifique en un anexo los lineamientos técnicos para manejar un conflicto de versiones o duplicidad de componentes.
GR15-R24	Copia no autorizada de registros por los analistas de calidad, desde el servidor de archivos con información del proyecto	**Reducir** **8.3.1 Bloqueo de puertos USB en los equipos - analistas de calidad** Implementar el bloqueo de puertos USB en los equipos de los analistas de calidad
GR15-R34	Pérdida del CD que contiene los componentes presentados en el entregable, en tránsito al cliente	**Reducir** **9.4.1 Protección por contraseña del acceso a discos compactos (CD/DVD)** Establecer la obligación para el consultor de realizar todas las grabaciones de discos para clientes usando una capa de autenticación

Tabla 22. Controles para tratar riesgos y oportunidades

3.2. Objetivos de seguridad de información

Las organizaciones deben establecer objetivos de seguridad de información, de manera que cuenten con una visión del estado al que quieren llegar respecto a aspectos particulares de la confidencialidad, integridad o disponibilidad de su información.

Los objetivos de seguridad de información se documentan en la **Declaración de objetivos de seguridad de información (Anexo L)** y, tal como lo indica la **Política de seguridad de información (Anexo E)**, se generan a partir de los objetivos estratégicos de la organización, considerando aquellos aspectos en los que esta puede mejorar (resultados del logro de requisitos, resultados de la gestión de riesgos).

El siguiente gráfico muestra la relación directa entre los objetivos estratégicos de la consultora y los objetivos de seguridad de información:

Objetivos estratégicos		Objetivos de Seguridad de Información
Fomentar la excelencia del personal que brinda los servicios de consultoría	⟶	**OSI1:** Fomentar la difusión del cumplimiento de la **confidencialidad** en el manejo de la información de los proyectos
Mejorar la satisfacción de los clientes respecto a los servicios recibidos	⟶	**OSI2:** Mejorar la **integridad** de los productos de consultoría en cuanto a versiones exactas y completitud
Incrementar la efectividad y productividad de los proyectos de consultoría	⟶	**OSI3:** Incrementar la **disponibilidad** de la información y servicios requeridos para realizar las actividades de consultoría

Figura 5. Relación entre objetivos de seguridad de información y estratégicos

Para planificar y lograr estos objetivos se ha desarrollado un **Plan de objetivos de seguridad de información (Anexo M)**, en el cual, para cada objetivo, se definen actividades, responsables y recursos para lograrlos.

La realización de todas las actividades mencionadas forma parte de la operación del sistema y han sido establecidas en cumplimiento de los lineamientos del estándar 27001:

ISO 27001	Cumplimiento del requisito	Evidencia
6.2.a-e	**Establecimiento de los objetivos de seguridad de información** La dirección del sistema ha establecido objetivos de seguridad de información, bajo las siguientes características: • Son congruentes con las disposiciones de la Política de Seguridad de Información respecto a su creación (alineamiento a los objetivos estratégicos). • Están asociadas a métricas, como puede verificarse en el **Plan de Métricas de Seguridad de Información**. • Consideran para su definición si alguno de los requisitos de seguridad de información no estar siendo atendido de manera satisfactoria. • Consideran para su definición los resultados de la gestión de riesgos, para entender las necesidades de la organización. • Han sido incluidos en los temas dictados en el **Plan de concientización, capacitación y evaluación**, para ser difundidos. • Son revisados en cada ciclo de operación, según se indica en el **Plan de operación y comunicaciones del SGSI**, para evaluar si ameritan ser actualizados.	L. Declaración de objetivos de seguridad de información O. Plan de concientización, capacitación y evaluación P. Plan de métricas de seguridad de información
6.2.f-j	**Planificación de los objetivos de seguridad de información** Los objetivos de seguridad de información se encuentran documentados en la **Declaración de objetivos de seguridad de información**. Para su planificación se ha creado un **Plan de objetivos de seguridad de información**, donde a partir de los objetivos se han planificado acciones que buscan su cumplimiento, especificando en las columnas: • Acciones. Lo que se hará. • Recursos. Lo que se usará. • Involucrados. Los responsables. • Inicio / Cierre. Cuándo se completará • Efectividad. Cómo se evaluarán sus resultados	L. Declaración de objetivos de seguridad de información M. Plan de objetivos de seguridad de información

Tabla 23. Requisitos de los objetivos de seguridad de información

3.3. Concientización, capacitación y evaluación

Existen requisitos de los numerales 7.2 y 7.3 relacionados a los tópicos de competencia (capacitación y evaluación) en los roles y responsabilidades que cumple cada persona que participa en el sistema, además de la concientización y difusión en seguridad de información del personal de la organización, y otras partes interesadas.

Para contar con un esquema efectivo para manejar estos aspectos de la seguridad de información se ha definido un **Plan de concientización, capacitación y evaluación (Anexo O)**, a partir del cual se han creado las siguientes actividades y recursos:

- **Charlas de Concientización.** Las actividades de concientización son periódicas y se planifican al menos una vez por periodo, para recordar la política y buenas prácticas en seguridad de información, así como también para informar de sucesos o cambios importantes relacionados a este tema. Se usan los siguientes recursos:
  - Temario de tópicos de las charlas de concientización
  - Diapositivas de concientización (general)
- **Capacitaciones para roles específicos.** La capacitación se aplica a personal que muestra deficiencias o que es nuevo asumiendo un rol dentro del sistema. Para ello, se usan los siguientes recursos:
  - Matriz de personal y roles del SGSI
  - Diapositivas de capacitación (para cada rol)
- **Evaluar la competencia del personal.** Finalmente, la evaluación permite corroborar si el personal designado puede cumplir de manera satisfactoria con su rol o, en caso contrario, se realice una nueva capacitación o se busque a un reemplazo. En estos casos el material usado es:
  - Evaluaciones para cada rol dentro del sistema

Todas las actividades indicadas son aplicadas conforme lo dispone el plan, para atender de manera adecuada los requisitos del estándar:

ISO 27001	Cumplimiento del requisito	Evidencia
7.2.a	**Competencia** El marco para la competencia del personal que cuenta con roles en el sistema son las **Políticas específicas de seguridad de información** en su numeral de roles y responsabilidades.	F. Políticas específicas de seguridad de información
7.2.b	**Evaluación** Para asegurar que estas responsabilidades son atendidas de manera satisfactoria, dentro del **Plan de concientización, capacitación y evaluación** se han incluido actividades de evaluación, donde se toma la **Matriz de personal y roles del SGSI** y para cada persona se toma una evaluación, específica para el rol que le corresponde.	O. Plan de concientización, capacitación y evaluación
7.2.c	**Capacitación** En caso se identifique que algún rol se encuentre vacante o no cuenta con personal con un nivel de competencia adecuado, se le brinda una charla respecto a su rol y se le toma una nueva evaluación, para corroborar la mejora. Para el personal nuevo que se incorpora con un rol en el sistema también aplica esta actividad de capacitación.	
7.2.d	**Registros** Se mantienen registros de la asistencia a las charlas, cursos y resultados de evaluaciones del personal que participa en el sistema.	
7.3	**Concientización** En las fechas dispuestas en el **Plan de concientización, capacitación y evaluación**, se ejecutan las charlas. Para ello, se define un temario de tópicos, los cuales contienen por lo menos: • La política de seguridad de información. • Los objetivos de seguridad de información. • La participación del personal respecto al aseguramiento y mejora de la seguridad. • La importancia de la prevención de no conformidades sobre el sistema.	O. Plan de concientización, capacitación y evaluación

Tabla 24. Requisitos de la capacitación y concientización

3.4. Operación, planes, recursos y registros

El numeral 7.1 exige que se brinden los recursos para el establecimiento, implementación, mantenimiento y mejora del sistema (modelo de operación especificado en el numeral 2.1 del presente informe).

Las actividades y recursos se especifican para cada una de las acciones de tipo “operación”, definidas en el **Plan de operación y comunicaciones del SGSI (Anexo A)**, y corresponden a:

- Personas (horas hombre del personal involucrado)
- Documentos (investigaciones, normativa, planes)
- Tecnología (servicios tecnológicos, adquisiciones)
- Otras facilidades (capacitaciones, servicios generales)

De entre estas actividades, el numeral 8.1 del estándar 27001 destaca las aquellas centradas en planear, implementar y controlar los requisitos, objetivos y tratamiento de riesgos de seguridad de información, mediante sus respectivos planes, respectivamente:

- **Riesgos y oportunidades:**
  - **Plan de tratamiento de riesgos (Anexo I)**
- **Objetivos de seguridad de información**
  - **Plan de objetivos de seguridad de información (Anexo M)**
- **Requisitos de seguridad de información**
  - **Plan de requisitos de seguridad de información (Anexo N)**

Este mismo numeral, indica que se debe controlar la documentación, control de cambios y trato con proveedores, lo cual se establece mediante las **Políticas específicas de seguridad de información (Anexo F) - Gestión de Documentos / Actividades del negocio / Gestión de Terceros**, que en sus distintos numerales regulan estas actividades como obligatorias.

Mediante la ejecución del **Plan de operación y comunicaciones del SGSI (Anexo A)** y de los planes a los que referencia, se tiene cumplimiento de los numerales de operación y recursos, del estándar 27001:

ISO 27001	Cumplimiento del requisito	Evidencia
8.1	**Operación del SGSI** La organización ha establecido los siguientes planes: • **Plan de requisitos de seguridad de información**. Para atender los requisitos identificados. • **Plan de tratamiento de riesgos**. Para asegurar el tratamiento de los riesgos y oportunidades. • **Plan de objetivos de seguridad de información**. Para lograr sus objetivos de seguridad de información. En general, los procesos requeridos por el SGSI están desarrollados en otros planes, que son referenciados en el **Plan de operación y comunicaciones del SGSI**. Por otro lado, las **Políticas específicas de seguridad de información** cuentan con disposiciones relacionadas a: • Gestionar los registros dejados como resultado de la operación del SGSI (Gestión de Documentos). • Gestionar los cambios planificados y controlar los inesperados (Actividades del negocio). • Definir y gestionar los procesos externalizados con terceros (Gestión de Terceros).	N. Plan de requisitos de seguridad de información I. Plan de tratamiento de riesgos M. Plan de objetivos de seguridad de información A. Plan de operación y comunicaciones del SGSI F. Políticas específicas de seguridad de información
7.1	**Recursos** La dirección de la organización provee los recursos necesarios para todas las etapas de operación del sistema, lo cual se evidencia en el **Plan de operación y comunicaciones del SGSI**, así como en el resto de planes desplegados para el sistema.	

Tabla 25. Requisitos de los recursos y planes de operación

4. Componentes para mantener el SGSI

En este capítulo se presenta lo realizado para cumplir con los requisitos para mantener el sistema según lo que indica el estándar ISO/IEC 27001:2013. Para ello se exponen los lineamientos para la ejecución de las métricas, la planificación y ejecución de la auditoría interna del sistema, y la revisión por la dirección.

4.1. Análisis y evaluación de las métricas

En el numeral 9.1, el estándar establece que el **sistema debe medir su desempeño** (procesos del sistema de gestión) y la **efectividad de la seguridad de la organización** (efectividad de los controles) y, según el requisito 6.2.b, también **los objetivos de seguridad de información**.

Por lo tanto, se han analizado y evaluado estos tres grupos en el **Plan de métricas de seguridad de información (Anexo P)**: operación del sistema; grupos de controles; y objetivos de seguridad de información. Cada métrica especifica lo que se medirá, la forma en que se hará, el momento y responsable de obtener las mediciones y analizarlas. Finalmente se documentan los resultados en el **Informe de métricas de seguridad de información (Anexo Q)**, como se especifica a continuación:

ISO 27001	Cumplimiento del requisito	Evidencia
9.1	**Análisis y evaluación del desempeño** Se han definido métricas que evalúan el desempeño de los controles más representativos de la organización, así como también métricas para la efectividad de los componentes del sistema en el **Plan de métricas de seguridad de información**, para cada una de las métricas del plan se tiene las columnas: • **Acción.** Lo que se va a medir. • **Tareas.** El método de medición y evaluación. • **Condiciones.** Cuándo se medirá y cuándo se analizará • **Involucrados.** Quién monitoreará-medirá los factores y quién analizará-evaluará los resultados Los resultados de estas actividades son documentados en el **Informe de Métricas de Seguridad de Información**.	P. Plan de métricas de seguridad de información Q. Informe de Métricas de Seguridad de Información.

Tabla 26. Requisitos del análisis y evaluación de métricas

Las métricas para el sistema se muestran conjuntamente con el referente que las originó y para desarrollarlas se ha revisado el estándar ISO/IEC 27004:2009 [05], como referente técnico para su redacción:

Operación del SGSI		Métricas asociadas
Implementación de Controles	→	Avance en la implementación de controles del Plan de Tratamiento de Riesgos
Concientización del Personal	→	Cobertura respecto a la adecuada concientización del personal
Cumplimiento de Requisitos	→	Avance en el cumplimiento del plan de requisitos
Implementación de acciones correctivas	→	Avance en la implementación de acciones correctivas
Implementación de acciones de mejora	→	Avance en la implementación de acciones de mejora
Grupos de Controles		**Métricas asociadas**
Control de accesos a plataformas de trabajo donde se aloja información	→	Porcentaje de cuentas activas en los servidores de archivos, desarrollo y base de datos, justificadas y autorizadas
Acuerdos de Confidencialidad en personal interno	→	Porcentaje de personal que ha firmado los acuerdos de confidencialidad
Adecuada cobertura antimalware en equipos de usuarios	→	Porcentaje de equipos de usuario que cuentan con el antivirus activo y actualizado
Personal que cumple con las prácticas de escritorio limpio y bloqueo de pantallas	→	Porcentaje de personal que cumple con la práctica de escritorio limpio y el bloqueo de pantalla en ausencia
Equipos de usuarios con software autorizado instalado	→	Porcentaje de equipos de usuario que cuentan solo con software autorizado y licenciado
Objetivos de Seguridad de Información		**Métricas asociadas**
Fomentar la difusión del cumplimiento de la confidencialidad en el manejo de la información de los proyectos	→	Porcentaje de personal de los equipos de consultoría, concientizado en la seguridad y confidencialidad de la información usada en los proyectos
Mejorar la integridad de los productos de consultoría en cuanto a versiones exactas y completitud	→	Porcentaje de operaciones de actualización regulares respecto a su integridad, en los repositorios de versionado
Incrementar la disponibilidad de la información y servicios requeridos para realizar las actividades de consultoría	→	Porcentaje de disponibilidad de servicios tecnológicos y equipos usados para los proyectos, respecto al horario laboral

Figura 6. Relación entre métricas y sus referentes

4.2. Auditoría interna

El estándar, en su numeral 9.2, dispone la realización de auditorías internas periódicas del sistema para verificar el cumplimiento que la organización tiene del estándar 27001 y de las directivas internas propias de seguridad de información (políticas y procedimientos).

Para la planificación de las auditorías internas del sistema se han creado dos documentos que plantean sus especificaciones:

- **Programa de auditoría interna del SGSI (Anexo R)**. Contiene secciones donde se definen los parámetros de las auditorías: alcance, objetivos, criterios de auditoría, frecuencia, métodos y responsabilidades de planificación y ejecución.
- **Plan de auditoría interna del SGSI (Anexo S)**. Especifica los participantes, fecha y hora de las actividades del ciclo de auditoría establecido en el programa: entrevistas, inspecciones de áreas, revisión de información, pruebas de controles, entre otras.

Las auditorías internas del sistema son realizadas de la siguiente forma:

- El auditor elabora un **Programa de auditoría interna del SGSI (Anexo R)** considerando los procesos involucrados y los resultados de auditorías previas.
- La dirección valida y aprueba el programa para el periodo.
- Para cada ciclo de auditoría incluido en el programa, el auditor diseña un **Plan de auditoría interna del SGSI (Anexo S)**.
- Se valida el plan respecto a la disponibilidad de los involucrados y se ejecuta el plan actualizado.
- Los resultados obtenidos son validados con el personal entrevistado, para obtener descargos o corroborar los hallazgos.
- Finalmente los resultados son documentados en el **Informe de resultados de la auditoría interna (Anexo T)**.
- Este informe es comunicado al representante de la dirección y a todos los participantes de la auditoría.

Las **Políticas específicas de seguridad de información (Anexo F)** disponen las responsabilidades y requisitos para los auditores internos y demás participantes del proceso. Además, en este mismo documento se especifica la categorización que tendrán los hallazgos de auditoría:

- **No conformidades.** Incumplimientos de los requisitos de la norma o lineamientos internos de la organización.
- **Observaciones.** Hechos que pueden conllevar a una futura no conformidad.
- **Oportunidades de Mejora.** Recomendaciones que, sin estar asociadas a incumplimientos, pueden aportar mejoras al sistema.

Las auditorías realizadas cumplen con los lineamientos del estándar:

ISO 27001	Cumplimiento del requisito	Evidencia
9.2.a-b	**Auditoría Interna** Se planifican las auditorías internas en el **Programa de Auditoría Interna del SGSI** del periodo. En este documento se especifican los criterios de auditoría que corresponden a: • **Los requisitos establecidos por la norma ISO 27001:2013** • **Las disposiciones en seguridad de información asumidas por la organización.** Los resultados de la auditoría brindan un diagnóstico sobre si el sistema está implementado y manteniéndose de manera efectiva.	F. Políticas específicas de seguridad de información R. Programa de auditoría interna del SGSI S. Plan de auditoría interna del SGSI T. Informe de resultados de la auditoría interna
9.2.c - d	En el **Programa de Auditoría Interna del SGSI** se definen los parámetros: alcance, objetivos, criterios de auditoría, frecuencia, métodos y responsabilidades de planificación y ejecución. Para su elaboración el auditor interno considera la naturaleza de los procesos auditados o los resultados de auditorías anteriores, de manera que las actividades a planear se enfoquen en aquellos aspectos más preocupantes o vulnerables de la organización.	
9.2.e	Las **Políticas Específicas de Seguridad de Información** disponen que los auditores seleccionados sean independientes de los procesos auditados y contar, por lo menos, con un curso de auditoría sobre la ISO 27001.	
9.2.f	El **Informe de resultados de la auditoría interna** es comunicado al representante de la dirección, como paso final de la auditoría y reiterado durante la revisión por la dirección.	
9.2.g	La planificación y ejecución del proceso de auditoria queda documentada en los siguientes documentos: **Programa de auditoría interna del SGSI**, **Plan de auditoría interna del SGSI** e **Informe de resultados de la auditoría interna**	

Tabla 27. Requisitos de la auditoría interna del SGSI

La auditoría realizada en cumplimiento a lo planificado en el **Plan de auditoría interna del SGSI (Anexo S)** ha comprendido las siguientes actividades:

- Reunión de inicio de auditoría
- Auditoría al Representante de la Dirección
- Auditoría al Responsable de la Seguridad de Información
- Auditoría a los representantes de los procesos
- Auditoría a participantes de los procesos
- Auditoría al responsable de seguridad física
- Auditoría al responsable de recursos humanos
- Auditoría al responsable de logística y patrimonio
- Auditoría al responsable de tecnología y soporte
- Inspección a ambientes de trabajo de los procesos
- Inspección al centro de datos
- Reunión de fin de auditoría

Como resultado se han obtenido dos hallazgos (1 no conformidad y 1 observación) y una recomendación (oportunidad de mejora):

Hallazgo / Recomendación	Evidencia	Categoría
7.2 Competencia **AI15-001:** Si bien existen registros de las capacitaciones dadas al personal, y el personal conoce cuáles son sus funciones en el sistema, algunos de ellos conocen parcialmente la metodología de gestión de riesgos, pese a ser parte del equipo responsable de realizarla.	Entrevista al personal, registros de la evaluación de riesgos	No conformidad
A.9.2.5 Revisión de acceso a los usuarios **AI15-002:** Si bien se tiene el control de altas y bajas del personal en repositorio de consultoría, en algunos casos, el formato no cuenta con las firmas requeridas, por lo que se evidencia falta de revisiones de control.	Registros de altas y bajas en servicios TI	Observación
9.3.d Retroalimentación de partes interesadas **AI15-003:** Implementar y difundir un buzón de recomendaciones de seguridad de información, a fin de que las partes interesadas internas y externas puedan comunicar sugerencias para retroalimentar el sistema	Entrevista al personal	Oportunidad de Mejora

Tabla 28. Resultados de la auditoría interna del SGSI

En cumplimiento del estándar 27001 estos generarán acciones correctivas y de mejora, como se verá más adelante.

4.3. Revisión por la dirección

La dirección del sistema está representada por el Gerente general, quien es presidente del comité de seguridad de la información, y es acompañado por el resto de gerentes, como miembros. Para cumplir con el numeral 9.3 del estándar, las **Políticas específicas de seguridad de información (Anexo F)** disponen que el comité realice al menos una revisión por la dirección, por cada ciclo de operación del sistema.

Para la realización de esta sesión el **Operador del SGSI** debe preparar una presentación que sintetice la siguiente información:

- **Política de seguridad de información (Anexo E)** – para revisión.
- **Acta de revisión por la dirección (Anexo U)** – de la sesión anterior, si la hay.
- **Informe de contexto de la organización (Anexo B)** – cambios importantes en la organización, si los hay.
- **Plan de acciones correctivas (Anexo V)**
- **Plan de objetivos de seguridad de información (Anexo M)**
- **Informe de métricas de seguridad de información (Anexo Q)** – incluye las métricas de objetivos.
- **Informe de resultados de la auditoría interna (Anexo T)**
- **Plan de tratamiento de riesgos (Anexo I)**
- **Informe de seguimiento de riesgos (Anexo J)**
- **Plan de acciones de mejora (Anexo W)** – incluye las iniciativas o recomendaciones de las partes interesadas.

Esta síntesis de resultados es expuesta al comité para que tome decisiones y acuerdos, las cuales son documentadas en una nueva **Acta de revisión por la dirección (Anexo U)**. A partir de las decisiones documentadas en esta acta se generan nuevas acciones de mejora.

Si bien la sesión de revisión por la dirección suele ser una por periodo, eso no impide que el comité pueda reunirse para tomar decisiones cuando se considere conveniente, frente a cambios o incidentes significativos.

El esquema de revisión por la dirección ha sido elaborado en cumplimiento de las disposiciones del estándar 27001 al respecto:

ISO 27001	Cumplimiento del requisito	Evidencia
9.3	**Revisión por la dirección** Según lo dispuesto en las **Políticas específicas de seguridad de información**, el **Comité de Seguridad de Información** realiza una revisión periódica del sistema, para evaluarlo. El encargado de preparar el resumen y realizar la presentación (diapositivas) es el **Operador del SGSI**, en cuyo contenido incluye: • Política de seguridad de información • Acta de revisión por la dirección • Informe de contexto de la organización • Plan de acciones correctivas • Plan de objetivos de seguridad de información • Informe de métricas de seguridad de información • Informe de resultados de la auditoría interna • Plan de tratamiento de riesgos • Informe de seguimiento de riesgos • Plan de acciones de mejora Las decisiones tomadas por el comité respecto a lo expuesto son documentadas en el **Acta de revisión por la dirección (Anexo U)**, la cual dará lugar a posibles acciones de adicionales, las cuales se incorporarán en el **Plan de acciones de mejora** y el **Plan de acciones correctivas**, según corresponda.	B. Informe de contexto de la organización E. Política de Seguridad de Información F. Políticas específicas de seguridad de información I. Plan de tratamiento de riesgos J. Informe de seguimiento de riesgos M. Plan de objetivos de seguridad de información Q. Informe de Métricas de Seguridad de Información T. Informe de resultados de la auditoría interna U. Acta de revisión por la dirección V. Plan de acciones correctivas W. Plan de acciones de mejora

Tabla 29. Requisitos de la revisión por la dirección

Al finalizar la sesión, tal como indica el **Acta de revisión por la dirección (Anexo U)**, se tomaron dos acuerdos, que generarán acciones de mejora:

- **RD15-001:** Mejoras en la capacitación: Se dispone la preparación de un curso e-learning consistente en un video y cuestionario en línea, como material de inducción obligatorio para todo personal y proveedores nuevos.
- **RD15-002:** Superación de la métrica de software autorizado: Se dispone la revisión y depuración de software no autorizado en los equipos de la organización, así como la nueva medición de la métrica asociada para verificar que esta alcance un nivel razonable.

5. Componentes para mejorar el SGSI

En este capítulo se presenta lo realizado para cumplir con los requisitos para mejorar el sistema según lo que indica el estándar ISO/IEC 27001:2013. Para ello se exponen los lineamientos para la gestión de las acciones correctivas y de mejora respecto al sistema.

5.1. Acciones correctivas

El numeral 10.1 del estándar indica que toda no conformidad identificada sobre el sistema debe ser manejada mediante una acción correctiva, bajo ciertas especificaciones.

En el caso de la consultora, cada vez que se identifique una no conformidad, ya sea que se origine en una auditoría interna, incidente de seguridad de información, revisión por la dirección o por alguna otra fuente, esta es manejada en un **Plan de acciones correctivas (Anexo V)** de la siguiente forma:

- La no conformidad reportada es validada y evaluada por el **Operador del SGSI**, quien determina si realmente es una no conformidad.
- Si corresponde, se genera un registro de acción correctiva en el plan, donde en la sección de tareas se incluyen tres grupos de tareas:
    - **Reacción**: Acción inmediata realizada para atender la no conformidad.
    - **Causas:** Análisis sobre el origen de la acción.
    - **Eliminación:** Acciones complementarias en caso la acción necesite ser atendida en su origen para prevenir repeticiones.
- Posteriormente a la realización de la acción se verifica que los resultados obtenidos hayan sido efectivos, según los criterios especificados en la sección **Efectividad**.
- Finalmente se da por cerrada la acción, indicando el resultado final que se ha obtenido de ella.

La aplicación de tareas de análisis de causas y eliminación de las no conformidades no siempre serán necesarias, solo en aquellas acciones correctivas que por su complejidad requieran resolverse en su origen y que no hayan podido atenderse completamente mediante la reacción inicial.

El esquema de trabajo con el que se planifican, desarrollan y resuelven las acciones correctivas cumple con el estándar 27001 según se muestra:

ISO 27001	Cumplimiento del requisito	Evidencia
10.1.a-e	**Acciones correctivas** Las acciones correctivas sobre el sistema se realizan a partir de la identificación de no conformidades y se desarrollan en el **Plan de acciones correctivas**, para lo cual: • Se aplican tareas inmediatas para reaccionar a la no conformidad y cualquier posible consecuencia (sección **Tareas - Reacción** del plan). • Si la acción anterior solo ha atendido las consecuencias de la no conformidad y no la ha solucionado, se realiza una tarea de análisis de **Causas** para identificar el origen y se planifican tareas para su **eliminación**. • Todas las tareas de las acciones correctivas del plan se implementan. • Se revisan los resultados finales de las tareas realizadas con los criterios de la sección **Efectividad**. • Las acciones realizadas en algunos casos implicarán cambios sobre los controles de seguridad de información, pero en otros sobre el propio sistema.	V. Plan de acciones correctivas
10.1.f-g	**Registros de acciones correctivas** Todas las actividades relacionadas a las acciones correctivas quedan registradas en el **Plan de acciones correctivas**, principalmente en las secciones de **Tareas** (desarrollo) y **Resultados** (conclusión).	

Tabla 30. Requisitos de las acciones correctivas

Como resultado, el **Plan de acciones correctivas (Anexo V)** lista dos acciones:

- **ACO01:** Aplicar la acción correctiva al hallazgo AI15-001 (no conformidad)
- **ACO02:** Aplicar la acción correctiva al hallazgo AI15-002 (observación)

5.2. Acciones de mejora

El numeral 10.2 del estándar indica que deben aplicarse acciones para mejorar la idoneidad, adecuación y eficacia del sistema. Estas se han denominado acciones de mejora y se planifican, desarrollan y resuelven mediante el **Plan de acciones de mejora (Anexo W)**. A diferencia de las acciones correctivas que se originan en no conformidades, las acciones de mejora se pueden originar en distintas fuentes; las más frecuentes son:

- **Oportunidades de mejora**. Obtenidas como recomendaciones durante las auditorías internas.
- **Decisiones de la revisión por la dirección**. Documentadas en el acta de la reunión, donde se aplican las decisiones del comité para la mejora del sistema y sus controles.

Cualquiera sea su fuente, las acciones de mejora generan alguna mejora del sistema y sus controles respecto a su:

- **Conveniencia**. Aprovechamiento en beneficio de la organización.
- **Adecuación**. Mayor adaptación e integración con la organización.
- **Eficacia**. Mejor aprovechamiento de los recursos.

ISO 27001	Cumplimiento del requisito	Evidencia
10.2	**Mejora continua** Se han establecido acciones de mejora en el **Plan de acciones de mejora** que permiten hacer que el sistema y sus controles sean más provechosos, estén mejor adaptados y sean más eficientes en la organización.	W. Plan de acciones de mejora

Tabla 31. Requisitos de las acciones de mejora

Como resultado, el **Plan de acciones de mejora (Anexo W)** lista tres:

- **AME01:** Aplicar la acción de mejora al hallazgo AI15-003
- **AME02:** Aplicar la acción de mejora para atender el acuerdo RD15-001
- **AME03:** Aplicar la acción de mejora para atender el acuerdo RD15-002

6. Observaciones, conclusiones y recomendaciones

En esta sección se refieren las observaciones identificadas a partir de la experiencia obtenida durante la realización del presente proyecto. Además, se señalan y discuten las conclusiones que se han obtenido a partir de los resultados del proyecto. Finalmente, se señalan las recomendaciones que se desprenden de esta experiencia y se proponen algunos trabajos futuros, tomando como punto de partida lo desarrollado en esta investigación.

6.1. Observaciones

Durante la realización del presente proyecto, se identificaron algunos hechos y aspectos relevantes que se desean destacar:

Observación 1: Tendencias de los modelos de sistemas de gestión

Durante la indagación sobre los estándares relacionados a los requisitos de sistemas de gestión, que produce y publica la Organización Internacional de Normalización (ISO) se ha identificado que se manejan estructuras documentales uniformes. Es decir, la ISO 27001 (seguridad de información), la ISO 22301 (continuidad de negocio), la ISO 9001 (calidad), la ISO 14001 (ambiental) y la futura ISO 45001 (seguridad y salud en el trabajo) cuentan con las mismas secciones y numerales para su estructura documental:

- 0. Introducción;
- 1. Alcance;
- 2. Referencias normativas;
- 3. Términos y definiciones;
- 4. Contexto de la organización;
- 5. Liderazgo;
- 6. Planificación;
- 7. Soporte;
- 8. Operación;
- 9. Evaluación del desempeño;
- 10. Mejora.

Como parte de la misma tendencia a la integración y normalización de los estándares la ISO 31000 está siendo asumida como un referente general para la gestión de riesgos. Actualmente, este marco de riesgos es referenciado por el estándar 27001, pero también por la “ISO 14001:2015 Sistema de Gestión Ambiental – Requisitos” y la “ISO 9001:2015 Sistema de Gestión Ambiental – Requisitos”.

Se observa que la tendencia de uniformizar los estándares de los sistemas de gestión facilitará futuros esfuerzos de integración de distintos sistemas en un único Sistema Integrado de Gestión en las organizaciones.

Observación 2: Fallos en el manejo de los términos en versiones traducidas del estándar 27001

Uno de los elementos más importantes para implementar un estándar es comprenderlo en su sentido original. Las versiones en español del estándar 27001 por entidades ajenas a la ISO suelen presentar fallos debido a las traducciones literales o erradas de los términos. Por ejemplo, la norma chilena NCH ISO 27001:2013 [26] traduce en el numeral 4.3.c el término "interfaces" como "interferencias"; mientras que, en el caso peruano la NTP ISO/IEC 27001:2014 [09] el término "assesment" es traducido a veces como "valoración" y otras como "evaluación".

Para evitar confusiones, esta investigación ha usado la fuente original de la ISO 27001 en inglés. Como resultado, por ejemplo, se ha interpretado "assesment" como "apreciación" y "evaluation" como "evaluación". Si bien puede parecer trivial, esta diferenciación es importante, ya que en el numeral 6.1.2, el proceso de riesgos se denomina "Information security risk assesment", mientras que el numeral 6.1.2.e, corresponde a la actividad de "evaluates the Information security risk", un subconjunto de la anterior.

Se observa que existe un riesgo originado en una inadecuada interpretación de los estándares, originado en los precedentes de traducciones inadecuadas de la norma por entidades que no son la ISO.

Observación 3: El requisito de la Ley de Protección de Datos Personales y su alcance

En la actualidad, cualquier organización peruana, ya sea pública o privada, debe considerar a la Ley de Protección de Datos Personales [21] dentro del marco de los requisitos de seguridad de información que se originan en el cumplimiento legal. Si bien la organización debe considerarlo como parte de su plan de implementación de requisitos, no debe precipitarse a considerar dentro del alcance del SGSI a todo el marco que la acompaña:

Se identificó que existe una Directiva de Seguridad [17] que acompaña a la Ley de Protección de Datos Personales [21] y a su reglamento [22]. Esta puede ser entendida como obligatoria, ya que la Ley indica, en su artículo 16 "Seguridad del tratamiento de datos personales", lo siguiente:

"Para fines del tratamiento de datos personales, el titular del banco de datos personales debe adoptar medidas técnicas, organizativas y legales que garanticen su seguridad y eviten su alteración, pérdida, tratamiento o acceso no autorizado. Los requisitos y condiciones que deben reunir los bancos de datos personales en materia de seguridad son establecidos por la Autoridad Nacional de Protección de Datos Personales […]."

Sin embargo, el oficio N° 471-2015-JUS/DGPDP [23] de la **Autoridad de Protección de Datos Personales** aclara este punto, indicando:

"La finalidad de esta directiva es entregar una herramienta útil para quien requiera consultarla. En su presentación se dejó constancia que dicho documento era un instrumento facilitador, que constituye una indicación de cómo pueden hacerse las cosas, toda vez que la obligación de los administrados es adecuarse o cumplir con la LPDP y el reglamento, no la Directiva. […]."

Se observa que, si bien la Directiva de Seguridad que acompaña a la Ley puede ser tomada como un referente, no constituye en sí misma un requisito de seguridad de información, y no tiene aplicación obligatoria.

6.2. Conclusiones

Como resultado del desarrollo de la investigación, se pueden concluir algunas afirmaciones relacionadas al logro de los objetivos del proyecto, los productos obtenidos y el proceso seguido:

Conclusión 1: Marcos periféricos a considerar para el desarrollo de componentes del sistema

El estándar 27001 se complementa con otros estándares de la ISO que explican a mayor detalle cómo se puede cumplir con sus requisitos:

- La única referencia directa es la de la ISO 31000:2009 [07], que es referenciada como marco para el contexto y la gestión de riesgos (en la versión anterior de la norma era la ISO ISO/IEC 27005:2008 [06]).
- Para el tratamiento de riesgos, aunque no es referenciada, la ISO/IEC 27002:2013 [03] se debe considerar, ya que es una versión mucho más detallada del anexo A del estándar 27001 y puede permitir un mejor entendimiento para el diseño de los controles.
- Sobre las auditorías, la ISO 27001 indica algunos requisitos puntuales. Sin embargo, no detallan o dan lineamientos específicos para realizar esta acción. Para estos casos, se debe tomar en cuenta la "ISO 27007:2011 Guía para auditorías de SGSI" [24], que a su vez referencia a la "ISO 19011:2011 Directrices para la auditoría de Sistemas de Gestión" [25], las cuales cuentan con lineamientos para más específicos para auditorías internas.
- Respecto a las métricas, el estándar ISO/IEC 27004:2009 [05] brinda lineamientos y nociones necesarias para la adecuada elaboración, análisis y evaluación de las mediciones sobre el sistema y sus controles.

Se concluye que para elaborar adecuadamente los componentes que permitan cumplir los requisitos del estándar 27001 deben considerarse aquellos estándares que, aunque no son referenciados, forman parte del dominio de algunos de los requisitos del SGSI.

Conclusión 2: Innovaciones originadas en el tipo de organización

La principal característica de una consultora de software, que la diferencia de otras industrias, es que su principal insumo y producto es la información, motivo por el cual cuenta con especialistas en modelarla, modificarla y realizar propuestas respecto a su mejor uso o explotación. Por ello, al iniciar la implementación de un sistema, su creador se enfrenta al reto de responder a las exigencias de un público que, sin conocimientos profundos de seguridad de información, conoce mucho sobre lo que debe ser un sistema y tiene expectativas respecto a que sea funcional y, sobre todo, útil.

A partir de esta situación, se han presentado cuestionamientos, ideas y recomendaciones, que dieron origen a las siguientes innovaciones, las cuales fueron aplicadas para la elaboración de los componentes del SGSI:

- **Metodología de gestión de riesgos.** En lugar del enfoque teórico de un taller y de convocar al personal a una sala para identificar activos y riesgos en base a una abstracción, se aplicó uno práctico, mediante el recorrido in situ de los procesos, a partir de un diagrama de flujo, para identificar, analizar y evaluar los riesgos.
- **Normalización de planes.** Con miras a una posible automatización del sistema como software, se incidió en la necesidad de normalizar los registros o “tablas del sistema”, por lo que se elaboró una estructura de atributos uniforme para los distintos planes del SGSI.
- **Verificación del cumplimiento.** Un requerimiento final de la organización ha sido verificar que los componentes creados cumplan efectivamente con los requisitos del estándar, a partir de ello se ha incorporado una tabla de verificación de cada componente, en el presente informe.

Se concluye que, como resultado de las exigencias del proyecto y sus interesados, se han podido elaborar propuestas innovadoras asociadas a: la metodología de gestión de riesgos, la normalización de los planes del sistema y realizar la verificación integral de cumplimiento de los componentes requeridos como requisitos por la ISO/IEC 27001:2013.

6.3. Recomendaciones

Finalmente, a partir de la experiencia y resultados de este proyecto, se han determinado algunas recomendaciones sobre aspectos a tomar en cuenta para investigaciones futuras relacionadas al estándar 27001. Además, se proponen algunos temas que sería interesante desarrollar, relacionados a la presente investigación:

Recomendación 1: El alcance inicial del SGSI

La operación del SGSI beneficia a toda la organización, ya que muchas de las actividades y controles que gestiona tienen alcance general; sin embargo, muchos otros, de carácter más exhaustivo (gestión de riesgos, auditorías internas, revisión por la dirección, entre otros), están limitados estrictamente a un sub conjunto de los procesos de la organización: aquellos que han sido declarados dentro del alcance del SGSI.

Bajo esta premisa, el ideal de toda organización sería incluir dentro del alcance de su sistema a todos aquellos procesos críticos o sensibles respecto a la información que manejan. Sin embargo, la realidad muestra que en las organizaciones no siempre se cuenta con recursos para hacerlo. Se debe tomar en cuenta que la inclusión de cada proceso en el alcance implica para cada uno de ellos un esfuerzo adicional: horas de trabajo de su personal, recursos para la implementación de controles y para otras actividades del sistema.

Se recomienda que el alcance inicial del SGSI (primer ciclo de operación) sea asumido en base a la disponibilidad de recursos de la organización, entendiendo que es válido definir que el sistema inicie con solo algunos de los procesos críticos y planifique la incorporación de los faltantes en los siguientes ciclos de operación del sistema, apelando al principio de mejora continua. Esta decisión deberá ser tomada por la dirección de la organización, en el momento en que se apruebe el alcance del sistema.

Recomendación 2: Lograr el apoyo de la dirección – Beneficios del SGSI

Uno de los requisitos más difíciles de cumplir es el relacionado al liderazgo, ya que ello implica obtener el compromiso efectivo de la dirección respecto a recursos y participación en el sistema. Debido a que esta función corresponde a personal de nivel gerencial, corresponde obtener su apoyo mediante argumentos objetivos que evidencien la rentabilidad que representa el SGSI para la organización. En el caso de la consultora esta sustentación se ha realizado exitosamente, en base a lo siguiente:

- Permite gestionar eficientemente los recursos para controles. Ya que su implementación es realizada para que atienda los riesgos más significativos de la organización.
- Potencia la mejora del personal y las áreas involucradas, mediante las charlas e implementación de actividades que regulan el manejo adecuado de su información.
- Proporciona una mejora en la visibilidad de la organización y la consecuente toma de decisiones. A partir de las métricas del sistema y los controles de seguridad de información aplicables.
- Desarrolla una gestión de riesgos, no conformidades e incidentes. Permite aminorar eventos de impacto negativo en seguridad de información e incluso prevenirlos.
- Propicia el cumplimiento de las leyes y regulación aplicable. En aquellas cláusulas relacionadas a la seguridad de información, ya que las identifica como requisitos y planifica su atención.
- Posibilita, como valor agregado, certificar el SGSI y hacerlo un factor comercial diferencial. Generando mayor confianza del entorno (clientes) respecto al manejo de la información intercambiada.

Se recomienda tomar argumentos de rentabilidad como un referente para proponer a la dirección de una organización las bondades de un SGSI y los beneficios que puede generarle. De manera que se pueda obtener su apoyo y recursos para la operación del sistema.

Recomendación 3: Trabajo Futuro - Diseño de una metodología ágil aplicada a la creación de un SGSI

En base a la experiencia realizada, se ha identificado que los ciclos completos de operación de un SGSI tienen una duración considerable (usualmente 1 año), siendo el hito principal de cierre la revisión por la dirección. Sin embargo, se ha identificado que sería posible segmentar este gran ciclo de operación en periodos más pequeños, de manera que, por ejemplo, algunas actividades del sistema (gestiones de riesgos, auditorías, ejecución de métricas, entre otras) se realicen de manera distribuida y progresiva a lo largo del periodo, y dejen de ser hitos anuales.

Se recomienda considerar como tema para futuras investigaciones una metodología ágil para la creación y operación progresiva de un SGSI, que planifique las actividades en pequeños ciclos de operación, de manera que se pueda contar con un SGSI activo respecto a la mayoría de requisitos del estándar, desde los primeros meses de su creación.

Recomendación 4: Trabajo Futuro - Implementación de un Sistema Integrado de Gestión que integre la ISO 27001 y estándares afines

Como se ha indicado anteriormente, los estándares de los sistemas de gestión cuentan actualmente con una estructura idéntica respecto a sus numerales. Además, la presente investigación ha desarrollado todos los componentes del sistema de gestión del estándar 27001, que son requeridos para su implementación, muchos de los cuales pueden ser adaptados o extendidos para atender los requisitos de otras ISO, como la 9001 o 14001.

Se recomienda como tema futuro la creación de un sistema integrado de gestión que integre el estándar 27001 y el de algún otro sistema de gestión distinto, tomando como referente los componentes diseñados en la presente investigación. De esta manera será posible identificar qué componentes de un sistema de gestión de seguridad de información son adaptables o reutilizables respecto a otros estándares.

Recomendación 5: Trabajo Futuro - Software para la guía y automatización de la operación de un SGSI

Durante la documentación del estado de arte se ha determinado que no existe un software que implemente en su totalidad la completa automatización de un SGSI. Profundizando esta crítica, muchos de estos productos cuentan con una lógica poco intuitiva e incluso se limitan a servir de repositorio de documentos y registros, sin explotar el valor agregado que debería aportar un sistema de software:

- Automatización de los flujos de información. Con la consiguiente reducción de la posibilidad de error por parte del usuario mediante el encauzamiento de su trabajo en campos de ingreso de datos controlados.
- Explotación de los datos almacenados. De manera que la información que está en la base de datos del sistema pueda ser analizada en reportes automatizados, y propicien una mejor toma de decisiones por la dirección.
- Educación del usuario. Mediante funcionalidades que indiquen a través de alertas, mensajes de error, funcionalidades de ayuda o tutoriales.

Se recomienda, para futuros trabajos, la implementación de un software que automatice la operación de un SGSI. Como valor distintivo, además de la cobertura integral de los requisitos se debería contemplar un diseño que: defina roles segregados, cuenten con funcionalidades que eviten ingresos erróneos, cuente con un esquema de alerta de tareas pendientes, y permita que un usuario inexperto pueda, con una breve capacitación, asumir su rol dentro del SGSI.

Bibliografía

Referencias documentales consultadas para la elaboración del presente trabajo de investigación:

[01] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION
2014 ISO/IEC 27000:2014 Tecnología de Información - Técnicas de Seguridad - Sistemas de Gestión de Seguridad de Información - Descripción y vocabulario. Suiza, 2014.

[02] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION
2013 ISO/IEC 27001:2013 Tecnología de Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de Información. Requerimientos. Suiza, 2013.

[03] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION
2013 ISO/IEC 27002:2013 Tecnología de Información. Técnicas de Seguridad. Código de prácticas para controles de seguridad de información. Suiza, 2013.

[04] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION
2010 ISO/IEC 27003:2010 Tecnología de Información. Técnicas de Seguridad. Directrices para la implementación de un sistema de gestión de seguridad de información. Suiza, 2010.

[05] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION
2009 ISO/IEC 27004:2009 Tecnología de Información. Técnicas de Seguridad. Gestión de Seguridad de Información. Medición. Suiza, 2009.

[06] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION
2008 ISO/IEC 27005:2008 Tecnología de Información. Técnicas de Seguridad. Gestión del Riesgo en Seguridad de Información. Suiza, 2008.

[07] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION
2009 ISO 31000:2009 Gestión del Riesgo. Principios y Directrices. Suiza, 2009.

[08] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION
2009 IEC 31010:2009 Gestión de Riesgo. Técnicas de Apreciación del Riesgo. Suiza, 2009.

[09] INDECOPI
2014 NTP ISO/IEC 27001:2014 Tecnología de Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de Información. Requerimientos. Lima, 2014.

[10] INDECOPI
2007 NTP ISO/IEC 17799:2007 Tecnología de Información. Técnicas de Seguridad. Código de prácticas para controles de seguridad de información. Lima, 2007.

[11] SOFTWARE INGINEERING INSTITUTE
2007 Introduciendo OCTAVE Allegro: Mejorando el proceso de evaluación de riesgos de seguridad de información. Pittsburgh, 2007.

[12] OFFICE OF GOVERNMENT COMMERCE
2010 Gobierno Corporativo y Gestión de Riesgos (M_o_R). Londres, 2010.

[13] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
2006 NIST SP 800 - 100 Manual de Seguridad de Información: Guía para gestores. Gaithersburg, 2006.

[14] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
2011 NIST SP 800 - 39 Gestionar Riesgos de Seguridad de Información. Gaithersburg, 2011.

[15] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
2013 NIST SP 800 – 53 Controles de Seguridad y Privacidad para Sistemas de Información Federales y Organizaciones – Revisión 4. Gaithersburg, 2013.

[16] MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS
2012 MAGERIT - versión 3.0 Metodología de análisis y gestión de riesgos de los sistemas de información. Madrid, 2012.

[17] MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS
2013 Directiva de Seguridad (Ley de Protección de Datos Personales 29733). Lima, 2013.

[18] INFORMATION SYSTEM AUDIT AND CONTROL ASSOCIATION
2012 COBIT 5 – Para Seguridad de Información. Illinois, 2012.

[19] INFORMATION SYSTEM AUDIT AND CONTROL ASSOCIATION
2009 Marco Risk IT para la Gestión de TI Relacionada a Riesgos del Negocio. Illinois, 2009.

[20] PROJECT MANAGEMENT INSTITUTE
2013 Guía de los fundamentos para la dirección de proyectos (guía del PMBOK) - 5ta. ed. Pensilvania, 2013.

[21] CONGRESO DE LA REPÚBLICA
2011 Ley N° 29733, Ley de Protección de Datos Personales. Lima, 2011.

[22] PRESIDENCIA DE LA REPÚBLICA
2013 Decreto Supremo N°003-2013-JUS Reglamento de la Ley N° 29733, Ley de Protección de Datos Personales. Lima, 2015.

[23] MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS
2015 Oficio N° 471-2015-JUS/DGPDP. Lima, 2015.

[24] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION
2011 ISO/IEC 27007:2011 Tecnología de Información - Técnicas de Seguridad - Guía para auditorías de Sistemas de Gestión de Seguridad de Información. Suiza, 2011.

[25] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION
2011 ISO 19011:2011 Directrices para la auditoría de sistemas de gestión. Suiza, 2011.

[26] INSTITUTO NACIONAL DE NORMALIZACIÓN
2013 NCh-ISO 27001 Tecnología de la Información - Técnicas de Seguridad - Sistemas de gestión de seguridad de la información - Requisitos. Santiago de Chile, 2013.

[27] CONGRESO DE LA REPÚBLICA
1996 Decreto Legislativo 822, Ley sobre el Derecho de Autor. Lima, 1996.

[28] CONGRESO DE LA REPÚBLICA
2011 Ley N° 30096, Ley de Delitos Informáticos. Lima, 2013.