UNIVERSIDAD DE CHILE
FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS
DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA SUBSECRETARIA DE ECONOMÍA Y EMPRESAS DE MENOR TAMAÑO

TESIS PARA OPTAR AL GRADO DE MAGISTER EN TECNOLOGÍAS DE LA INFORMACIÓN

NELSON ALEJANDRO YAÑEZ CACERES

PROFESOR GUÍA:
MARÍA CECILIA BASTARRICA PIÑEYRO

MIEMBROS DE LA COMISION:
ALEJANDRO HEVIA ANGULO
PATRICIO INOSTROZA FAJARDIN
PATRICIO GALDÁMEZ SEPULVEDA

SANTIAGO DE CHILE
2017

RESUMEN

La presente tesis detalla la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) en la Subsecretaría de Economía y Empresas de Menor Tamaño utilizando herramientas open source y modelos de desarrollo de mejora continua para dar cumplimiento a un subconjunto de 44 objetivos de control del anexo normativo de la norma ISO27001:2013.

La presente tesis no cubre la implementación de los 114 objetivos de control de la norma ISO27001, pero cierra las principales brechas de seguridad de la información existentes en la organización al cubrir en forma completa el primer ciclo PDCA del SGSI, escogiendo un subconjunto de 44 objetivos de control priorizados por una análisis de brechas, incorporando las recomendaciones de DIPRES y cuya selección se realizó por un comité de seguridad de la Información constituido en el presente trabajo

Las políticas y procedimientos son mantenidos en régimen mediante los seis sistemas que forman el SGSI y cuyo objetivo es administrar, monitorear, documentar y mejorar en forma continua la seguridad de la información

La metodología que se utiliza esta tesis, se centra en ciclos de aprobación que permitan establecer consensos y conciliar visiones en torno a un fuerte sentimiento de trabajo en equipo para facilitar la implementación de las políticas y procedimientos de seguridad de la información.

Esta tesis propone que la metodología de implementación de SGSI se apoye en la gestión de riesgos, utilizando las guías y buenas prácticas de la norma ISO31000. Con ello los procesos estratégicos de la subsecretaría son clasificados por prioridad según su exposición a los riesgos y su impacto. De este modo se optimiza la asignación de recursos a los proyectos de seguridad de la información, se favorece el aprendizaje y la creación de equipos de trabajo orientados a los objetivos prioritarios, sin que ellos perdieran la visión de conjunto y objetivo final.

Como evaluación de la implementación del SGSI y de las políticas y procedimientos de seguridad de la información se realizaron dos auditorías, una interna y otra realizada por una empresa externa. Ambas auditorias fueron totalmente independientes al equipo que diseñó e implementó tanto el SGSI como las políticas y procedimientos de seguridad de la información. Ambas auditorias llegaron a la conclusión que el estado actual de seguridad de la información está en un nivel medio. Esto es un avance sustancial pues al inicio de la presente tesis no había un SGSI ni políticas y procedimientos efectivos para proteger la seguridad de la información. La principal recomendación entregada por las auditorías fue profundizar la difusión de las políticas y procedimientos de seguridad de la información, continuar con la implementación de los restantes 70 objetivos de control de la norma ISO27001:2013 y realizar una nueva evaluación durante el 2017 del funcionamiento del SGSI, es decir se han implementado los restante objetivos de control y evaluar el grado de institucionalización de las políticas y procedimientos de seguridad de la información.

DEDICATORIA

Con inmenso amor dedico esta tesis a mi hijo Adolfo, es el quien con su infinita sonrisa y su bondad, lleno de alegría todos mis momentos de dudas y que pese a sus cortos cuatro años parece entender mucho de la vida y de los verdaderos ideales que nos deben conducir. Es así como realice esta tesis, pensando en mi hijo y en el legado de mi padre en forma de una frase: “no importa caer, pero caer luchando”

AGRADECIMIENTOS.

Son muchas a las personas que debo tiempo y consejos, sería imposible nombrarlos a todos, pero a través de las siguientes personas hago un reconocimiento a todos quienes me ayudaron.

A mi esposa, a quien no solo debo tiempo y comprensión, sino que además siempre estuvo para mí, para apoyarme.

A mis padres que con su ejemplo de vida me han dado las fuerzas para siempre hacer lo correcto, aun cuando sea el camino más difícil.

A mi Estimada Profesora Guía Cecilia Bastarrica, durante todos mis años de estudio en la Universidad de Chile una apoyo fundamental, fuente inagotable de consejos.

A Todos los profesores con los cuales tuve el honor de aprender, por su amabilidad y su compromiso por la labor que desempeñan, de una manera que realza la docencia.

A los profesores me mi comisión, por su dedicación y lo ameno y acertado de sus comentarios y correcciones.

A Teresa Huenunguir y Yordy Arévalo, por su infinita paciencia amabilidad y ayuda.

A Angélica Aguirre por guiarme tan amablemente en todos los trámites referentes a mi tesis.

A Mario Lemus, Perito Judicial, Experto en seguridad de la Información, pero sobre todas las cosas un amigo entrañable.

A mi querida Universidad de Chile, a todas las personas maravillosas con las cuales compartí, en todos estos años siempre vi gente feliz motivada y orgullosa de su labor, siempre dispuestas a dar lo mejor de sí.

TABLA DE CONTENIDO

1 INTRODUCCIÓN

1.1 CONTEXTO

La Subsecretaria de Economía y Empresas de Menor Tamaño del Ministerio de Economía es responsable de formular e implementar políticas de fomento productivo para las empresas de menor tamaño (EMT) de Chile. Las políticas están especialmente orientadas a aumentar la productividad de estas empresas. Para ello, la Subsecretaria diseña y evalúa planes y políticas públicas, coordina con diferentes entidades públicas y privadas y mantiene diversas instancias de consulta e información, entre otras acciones.

La actual política de fomento a las EMT tiene su foco en el aumento de la productividad de las micro, pequeñas y medianas empresas del país. Esto les permite crecer, innovar e internacionalizarse y en consecuencia, generar mayores ingresos, mejores empleos y más oportunidades para los chilenos.

La estrategia para fomentar la eficiencia y la productividad de las EMT se concentra en tres ejes de acción:

Financiamiento. El objetivo estratégico es mejorar el acceso y las condiciones de financiamiento para micro, mediana y pequeña empresa (MIPYME). Para ello, se busca ampliar los instrumentos y potencial crediticio, lograr mayor cobertura y menores tasas de interés.

Gestión. Tiene como finalidad mejorar y aumentar las competencias y habilidades de gestión empresarial de las MIPYME. Para alcanzar este objetivo, se pretende ampliar los servicios de capacitación y asistencia técnica; promover la innovación empresarial y la difusión tecnológica; disminuir los costos de transacción para las empresas y mejorar su interacción con el Estado y con el sector privado.

Mercados. Su tarea es fortalecer la competencia y mejorar el acceso de las MIPYME a los mercados. Para esto, se busca promover la libre competencia y proteger los derechos de las MIPYME frente a prácticas anticompetitivas y competencia desleal, facilitar el acceso a mercados existentes, promover la apertura de nuevos mercados, perfeccionar y mejorar la calidad de las regulaciones, y facilitar el emprendimiento.

La efectiva implementación de la política y estrategia de fomento requiere de un trabajo público privado coordinado que promueva la interacción estrecha entre las capacidades del Gobierno y de las empresas. Para ello, se generan y coordinan diversas instancias de participación, como el Consejo Nacional Consultivo de la EMT y sus Mesas de trabajo MIPYME, el Consejo PYME de CORFO y Consejos Regionales. Además, se participa activamente en otras instancias de diálogo relacionadas como el Consejo Consultivo de Desarrollo Cooperativo y Economía Social y el Consejo de Desarrollo Digital y otros.

1.2 **LA PROBLEMÁTICA A ABORDAR**

La Subsecretaria de Economía no contaba con medidas efectivas para proteger la integridad, confidencialidad y disponibilidad de su información crítica. La seguridad de la información no era un eje de preocupación fundamentalmente porque no se comprendía su relación con el cumplimiento de los objetivos estratégicos de la organización. La seguridad de la información no se había tratado en forma sistémica pues no era responsabilidad de una unidad específica y menos un tema para la organización como un todo.

Informes de la División de Tecnología y Desarrollo habían revelado que los procesos claves de la organización, aquellos que inciden directamente en los objetivos estratégicos, presentaban problemas de eficacia y eficiencia producidos por diversos incidentes informáticos. Algunos de ellos eran: interrupción de servicios en sistemas y redes, información inconsistente y divulgación de información sensible.

Adicionalmente, la Dirección de Presupuesto de la Nación (DIPRES), como impulsor de la modernidad y eficiencia del Estado, instruyó a la Subsecretaria de Economía, el deber de establecer un Sistema de Gestión de Seguridad de la Información (SGSI) bajo la Norma ISO27001:2013 (Norma relativa a las buenas prácticas para resguardar la integridad, confidencialidad y disponibilidad de la información) que actúa de una manera preventiva frente a riesgos de seguridad de la información que puedan afectar la calidad del servicio entregado por la Subsecretaría de Economía, en especial “la efectiva implementación de las políticas y estrategias de fomento”.

El problema se resumió en responder las siguientes interrogantes:

- *¿Cómo proteger convenientemente a un costo razonable la información y los procesos que la recolectan, procesan, almacenan y distribuyen, frente riesgos de pérdida, divulgación, indisponibilidad o alteración?*

- *¿Cómo evidenciar que los riesgos que ponen en peligro a la propia información afectan los niveles de servicio, rentabilidad social y conformidad legal, necesarios para alcanzar los objetivos institucionales?*

- *¿Cómo implementar un sistema que gestione la seguridad de la información de forma económica, de manera que la Subsecretaria de Economía implemente los controles exigidos por la norma ISO27001:2013 y que, a su vez, institucionalice la mejora continua del SGSI y de los procesos, políticas y procedimientos de seguridad de la Información?*

1.3 OBJETIVOS

El objetivo general de la Tesis, es definir e implementar un conjunto de sistemas basados en software open source para crear un SGSI de costo asequible, que cumpla con la normativa indicada en la ISO27001:2013, bajo una estrategia de mejora continua de procesos en una institución pública.

Este SGSI debe lograr niveles adecuados de integridad, confidencialidad y disponibilidad de la información institucional de manera tal que se asegure la continuidad operacional de los procesos institucionales.

Los objetivos específicos que se desprenden del objetivo general son los siguientes:

- *Contar con un conjunto de sistemas implementados mediante software open source que conformen el SGSI al menor costo posible, pero que permitan la gestión de la seguridad de la Información.*

- *Implementar un conjunto de políticas y procedimientos de seguridad de la información en cumplimiento con los objetivos de control de la norma ISO27001:2013.*

- *Contar con un proceso de evaluación de riesgos de seguridad de la información que produzca resultados consistentes y comparables entre las evaluaciones de riesgos realizadas año a año.*

- *Contar con un conjunto de indicadores que permitan evaluar la disminución de la ocurrencia y gravedad de los incidentes de seguridad de la información, como son: las pérdidas de información, ingresos no autorizados y la indisponibilidad de la información.*

1.4 SOLUCIÓN

Para abordar la seguridad de la información de la Subsecretaria de Economía, propuse la implementación un SGSI bajo la norma ISO27001:2013 con software open source para reducir costos. Y además se acotar el alcance, tanto de las políticas y procedimientos de seguridad de la información a implementar como de los procesos estratégicos a cubrir para optimizar el uso de los recursos económicos disponibles. El SGSI implementado se compone de cinco sistemas, implementados en el siguiente orden:

1- Sistema de Toma de Decisiones.

2- Sistema de Gestión de Riesgos.

3- Sistema de Monitoreo.

4- Sistema de Gestión de Proyectos.

5- Sistema de Gestión Documental.

El orden de implementación lo propuse para facilitar la puesta en marcha del SGSI, ya que cada uno de ellos sentó las condiciones para proceder con el siguiente sistema, para finalmente proceder con la Implantación de políticas y procedimientos de seguridad de la información. Estos cinco sistemas, que en conjunto forman el SGSI, aseguran que los ciclos de mejora continua se realicen, pues existe monitoreo de los controles implementados, gestión de los riesgos, toma de decisiones informada y toda la documentación está debidamente protegida para que exista consistencia en los proyectos de mejora.

El SGSI implementado se centra en:

1. *Disponer de indicadores que permitirán una toma de decisiones basada en hechos, brindando el fundamento para la mejora continua del SGSI y las políticas y procedimientos de seguridad de la información.*

2. *Disponer de un proceso de gestión de riesgos centrado en los activos de información de la organización, para controlar las amenazas al cumplimiento de los objetivos estratégicos Institucionales y medir la eficiencia de las políticas y procesos de seguridad de la información para mitigar los riesgos.*

3. *Institucionalizar de la mejora continua del propio SGSI y las políticas y procedimientos de seguridad de la información, como respuesta de la organización a un nivel de riesgo dado.*

2 METODOLOGÍA PARA IMPLANTACIÓN DEL SGSI Y DE LAS POLÍTICAS Y LOS PROCESOS DE SEGURIDAD DE LA INFORMACIÓN

El método que seleccione para este trabajo de tesis tiene 4 etapas cíclicas (ver Figura 1): (1) Diagnóstico situación actual de la seguridad de la información, (2) Implementación del SGSI, (3) Implementación políticas y procedimientos de seguridad de la información y (4) Evaluación del SGSI, Políticas y procedimientos de seguridad de la información.

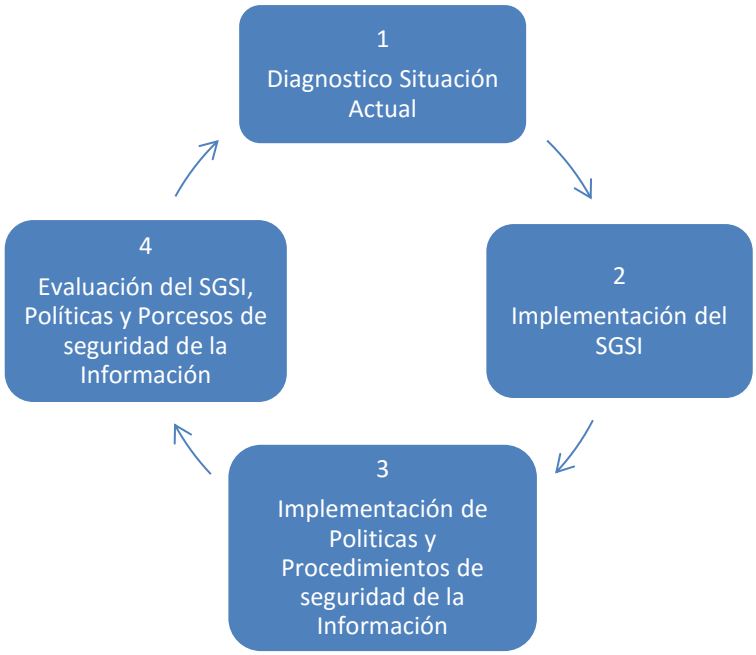


Figura 1 Etapas Mejora Continua

2.1 DIAGNÓSTICO DE LA SITUACIÓN ACTUAL DE LA SEGURIDAD DE LA INFORMACIÓN

El objetivo de esta etapa es develar el contexto organizacional, evaluar la percepción general de la seguridad de la información por parte del personal e identificar las expectativas de las partes interesadas (directivos, funcionario, profesionales del área TI y en general todos quienes laboran en la institución).

2.2 IMPLEMENTACIÓN DEL SGSI

Durante esta etapa se implementa la infraestructura de gobernanza de seguridad de la información tomando en cuenta los hechos constatados en el diagnóstico de la situación actual, esto asegura que las decisiones tomadas permitirán implementar, monitorear, evaluar e institucionalizar las políticas y procesos de seguridad de la información de la manera más ajustada a las necesidades de la Institución.

2.3 IMPLEMENTACIÓN DE POLÍTICAS Y PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN

Según la metodología propuesta, la decisión de qué políticas y procesos implementar en cada ciclo debe ser tomada por el comité de seguridad de la información (CSI). Para ello el comité revisa la información entregada por los sistemas de gestión de riesgos, monitoreo y el diagnóstico de la situación actual. Las políticas y procedimientos seleccionados se registran en el sistema de gestión de proyecto. La culminación de un proyecto de implementación de políticas y procedimientos tiene como resultado la aprobación de las mismas por el CSI y pasan a ser documentos oficiales de seguridad de la información quedando a disposición del personal en el sistema de gestión documental, información que es difundida por el departamento de RRHH y charlas realizadas por el equipo a cargo del SGSI.

2.4 EVALUACIÓN DEL SGSI Y DE LAS POLÍTICAS Y LOS PROCESOS DE SEGURIDAD DE LA INFORMACIÓN

Para realizar la verificación del trabajo hecho en esta tesis se realizaron dos auditorías, una interna y otra externa. Ambas fueron solicitadas por área de gestión de seguridad de la información, pero realizadas en forma independiente del área de gestión de seguridad de la información, lo que garantiza la imparcialidad de sus resultados.

Auditoria Interna de Control de acceso.

Esta auditoria evaluó el cumplimiento de las Políticas y procedimientos de seguridad de la información implementada, para verificar el estado de avance del programa de mejora de gobierno (PMG) de seguridad de la información antes de la evaluación del cumplimiento a realizar por la Dirección de Presupuesto (DIPRES). Esta auditoria tiene como objetivo ver la situación actual y si está en buen pie para cumplir las metas.

Auditoria Externa

Esta autoría fue realizada por la empresa Neosecure[1]. Esta evaluó la seguridad general de los servicios y plataformas de TI de la Subsecretaria de Economía y Empresas de Menor Tamaño, entregando una opinión respecto del nivel general de seguridad. Esta auditoría externa fue ordenada por la administración anterior y su coincidencia con esta tesis fue en principio accidental y luego reprogramada para coincidir con el final del primer ciclo de implementación del SGSI.

[1] Empresa de servicios de seguridad de la información www.neosecure.com

3 MARCO TEÓRICO

En este capítulo se hace una pequeña inducción a los estándares sobre los cuales se sustenta esta tesis. En el sección 3.1 se exponen conceptos generales de seguridad de la información y la familia de normas ISO27000, con énfasis de la norma ISO27001:2013 sobre la cual se implementó el Sistema de Gestión de seguridad de la información. En el Anexo B se exponen los conceptos de Gestión de riesgo, en la visión de la norma ISO31001 recogidos en el documento técnico N°70 del Consejo de Auditoria General de Gobierno (CAIGG).

3.1 NORMAS ISO/IEC 27000.

ISO/IEC 27000 es un conjunto de estándares desarrollados por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

ISO/IEC 27000 se basa en el tratamiento de los riesgos que amenazan la seguridad de la Información y es consistente con las demás normas ISO. Según el estándar ISO un riesgo se define como:

Riesgo es el efecto de la incertidumbre en los objetivos. Un efecto es una desviación sobre lo esperado y puede ser positivo o negativo. Los objetivos pueden ser de diferentes índoles, tales como metas ambientales, financiera, de salud y bienestar, de seguridad de la información. Pueden también referirse a distintos niveles, a toda la organización, estratégicos, a un proyecto, a un producto o simplemente a un proceso.

Los riesgos de seguridad de la Información se asocian con el potencial que amenazas exploten las vulnerabilidades de un Activo de Información o grupo de Activos de información y por lo tanto causar daño a una organización.

La información de riesgos de seguridad de la información se expresa en términos de una combinación de las consecuencias de un evento de seguridad de la información y la probabilidad asociada de ocurrencia[2].

Las normas ISO/IEC 27000 plantean que, para la adecuada protección de la información, es necesario implantar un sistema que gestione la seguridad de la información de una manera metódica, documentada y basada en la evaluación sistemática de los riesgos a los que está expuesta la información de la organización. Indican que todas las organizaciones al recolectan, procesar, almacenar y trasmitir información, la exponen a riesgos que podrían materializarse, afectando la disponibilidad, integridad o confidencialidad de la información. Esta materialización de riesgos puede afectar la cadena de valor de la organización y, dependiendo del impacto y

[2] ISO/IEC 27000 segunda edición 2012

severidad de los incidentes de seguridad de la información, puede llegar a afectar a sus objetivos estratégicos.

3.2 NORMAS ISO27000 CONSULTADAS EN ESTA TESIS

A continuación se exponen las Normas ISO27000 consultadas en la presente Tesis. En el Anexo A se presenta un esquema con la relación completa de las Normas que componen el conjunto de Normas ISO2700.

3.2.1 ISO27000 Visión General y Vocabulario

ISO27000 es una especificación técnica que ofrece una visión general de los sistemas de gestión de seguridad de la información, gestión de riesgos y definiciones de la terminología utilizada. Esta norma da homogeneidad en el lenguaje a toda la familia de normas ISO/IEC de seguridad de la Información, para facilitar la comunicación y evitar ambigüedades.

3.2.2 ISO27001 Tecnología de la Información – Técnicas de Seguridad - Sistemas de Gestión de la Seguridad de la Información –Requisitos

La norma ISO27001 define los requerimientos para establecer, implementar, mantener y mejorar de manera continua un Sistema de Gestión de la Seguridad de la Información, dentro del contexto de la organización. Se compone de dos tipos de cláusulas con objetivos bien definidos. Por un lado, cláusulas que apuntan al establecimiento del SGSI como un ente propulsor, regulador y garante de la seguridad de la información. Y cláusulas de control de seguridad de la información, contenidas en el Anexo A de la Norma y que indican los objetivos de control a cumplir mediante la implementación de las políticas y procedimientos de seguridad de la información, para lograr una protección razonable de la integridad, confidencialidad y disponibilidad de la información.

La norma ISO27001, define un Sistema de Gestión de Seguridad de Información (SGSI):

"Un sistema formado por políticas, procedimientos, directrices, actividades y sus recursos asociados, gestionados colectivamente por una organización, en la búsqueda de la protección de sus activos de información. 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 una evaluación de riesgos y aceptación de niveles riesgo de la organización, diseñados para tratar y gestionar los riesgos con eficacia[3]".

[3] ISO27001 segunda edición 2013.

Cláusulas para el establecimiento del SGSI

Las cláusulas 4 a la 10 de la norma ISO27001 hacen referencia a la necesidad de conocer el contexto organizacional, lograr apoyo, recursos y planificar las actividades de seguridad de la información e implantar la mejorar continua. Ellas conforman la gobernanza del SGSI. A continuación, se hace una breve reseña de cada una de las cláusulas:

Cláusula 4 Contexto de la organización

"La organización debe determinar los asuntos externos e internos que son importantes para su objetivo y que afecte su capacidad para lograr el(los) resultado(s) esperado(s) de su sistema de gestión de la seguridad de la información".

Cláusula 5 Liderazgo

"La alta dirección debe demostrar liderazgo y compromiso con respecto al sistema de gestión de la seguridad de la información".

Cláusula 6 Planificación

"Al planificar el sistema de gestión de la seguridad de la información, la organización debe considerar los asuntos referentes a comprender la organización, su contexto y comprender las necesidades y expectativas de las partes interesadas, además de determinar los riesgos y oportunidades que necesitan ser cubiertos."

Cláusula 7 Apoyo

"La organización debe determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión de la seguridad de la información."

Cláusula 8 Operación

"La organización debe planificar, implementar y controlar los procesos necesarios para cumplir con los requisitos de seguridad de la información y para implementar las acciones definidas durante la etapa de planificación del SGSI. La organización además debe implementar los planes para lograr los objetivos de seguridad de la información."

Cláusula 9 Evaluación de desempeño.

"La organización debe evaluar el desempeño de la seguridad de la información y la efectividad del sistema de gestión de la seguridad de la información."

Cláusula 10 Mejora

"La organización debe mejorar de manera continua la conveniencia, suficiencia y efectividad del sistema de gestión de la seguridad de la información, las políticas y procedimientos de seguridad de la información."

Cláusulas de Control de Seguridad de la Información

Las cláusula de control de seguridad de la información, hacen referencia a objetivos de control que deben cumplir las políticas y procedimientos de seguridad de la información y que deben ser implementados, para la protección de la información.

Para efectos de certificación en la norma ISO27001, se deben cumplir a cabalidad 114 objetivos de control establecidos en las 14 cláusulas del Anexo A de la norma ISO27001. Es bastante común la confusión entre objetivos de control y el control mismo; esto se ve en la aseveración frecuente de encargados de seguridad de la información al decir que la norma ISO27001 implica el diseño, implementación y aplicación de 114 controles. Lo que la norma exige es que se cumplan los objetivos de control (protección de activos de información) y como resultado un objetivo de control puede tener asociado una, o más políticas y procedimientos de seguridad de la información dependiendo ello de lo crítico que sea el Activo de Información.

A continuación se indican las cláusulas de control de seguridad de la información según su numeración en el Anexo A de la norma ISO 27001:2013.

A.5 Políticas de seguridad de la información

A.6 Organización de la seguridad de la información

A.7 Seguridad ligada a los recursos humanos

A.8 Administración de activos

A.9 Control de acceso

A.10 Criptografía

A.11 Seguridad física y del ambiente

A.12 Seguridad de las operaciones

A.13 Seguridad de las comunicaciones

A.14 Adquisición, desarrollo y mantenimiento del sistema

A.15 Relaciones con el proveedor

A.16 Gestión de incidentes de seguridad de la información

A.17 Aspectos de seguridad de la información en la gestión de la continuidad del negocio

A.18 Cumplimiento

3.2.3 ISO27002 Tecnologías de la Información - Técnicas de Seguridad - Código de Prácticas para los Controles de Seguridad de la Información

La Norma ISO27002 contiene un conjunto de buenas prácticas y directrices para la implementación de los Objetivos de Control Indicados en el Anexo A de la norma ISO27001. Es una Norma complementaria, no certificable, es decir no da lugar a una certificación y por lo tanto, la organización tiene la libertad de cumplir los objetivos de control requeridos utilizando otras fuentes de guía, en la medida que las políticas y procedimientos de seguridad de la información implementados cumplan con los Objetivos de control indicados por la Norma ISO27001.

Veamos como ejemplo la cláusula A.11 Seguridad física y del ambiente

Objetivo de control: Evitar el acceso físico no autorizado, los daños e interferencia a la información de la organización y las instalaciones de procesamiento de la Información.

Una buena práctica referida en la norma ISO27002 con respecto a esta cláusula A.11 de la norma ISO27001, es: “Se debería contar con un área de recepción atendida por una persona u otros medios para controlar el acceso físico al sitio o al edificio; el acceso a los sitios y al edificio se debería restringir solo al personal autorizado”.

El implementador facultado para seguir o no estas buenas prácticas o implementar otras en la medida que el objetivo de control se cumpla.

3.2.4 ISO27003 Guía de Implementación del SGSI

ISO / IEC 27003 proporciona una guía para ayudar en la implementación de la norma ISO27001, en lo referente al SGSI. Esta guía indica como iniciar un proyecto de implementación de SGSI, describe el proceso de especificación y diseño del SGSI desde su creación hasta la producción de los planes de proyecto y su ejecución. En general abarca las actividades de preparación y planificación antes de la implementación real. El Instituto de Nacional de Normalización (INN) no tiene homologada esta norma y su actual versión en inglés no cubre la Norma ISO27001:2013 que es la versión de la Norma utilizada en esta Tesis. Sin embargo, los temas clave de esta norma que se exponen a continuación si fueron aplicados al desarrollo de la presente Tesis.

Aprobación de la administración:

La autorización final para proceder con el proyecto de implementación de un SGSI corresponde a la alta administración de la organización y su apoyo es fundamental para el éxito del SGSI.

Definición del alcance y los límites que abarcara el SGSI:

El SGSI puede abarcar toda la organización o unos cuantos procesos organizacionales, tecnologías de la información o dependencias físicas.

Evaluación de los riesgos de seguridad de la información:

El SGSI se centra en la planificación del tratamiento apropiado de riesgos. Si no existiesen los riesgos no sería necesario definir los requisitos de control de seguridad de la información.

3.2.5 ISO27004 Métricas de Seguridad de la Información

Uno de los conceptos principales detrás del establecimiento de un SGSI es la mejora continua, tanto de las políticas y procedimientos que buscan proteger los activos de información como los procesos que definen el SGSI. La norma ISO27004 está destinada a dar lineamientos para que las organizaciones puedan definir un esquema de mediciones para definir elementos de toma de decisiones y mejorar sistemáticamente la eficacia del SGSI y de las políticas y procedimientos de seguridad de la Información.

3.2.6 ISO27005 Gestión de Riesgos de Seguridad de la Información

Las Normas ISO27000 están deliberadamente alineadas con la gestión de riesgos. Las organizaciones idealmente deben evaluar sus riesgos antes de tomar medidas y actuar según el alcance e impacto de la materialización de un riesgo en las operaciones de la organización. La Norma ISO27005 proporciona directrices para la gestión de riesgos de seguridad de la información y es compatible con los conceptos generales especificados en la norma ISO27001 y está diseñado para ayudar a la aplicación satisfactoria de seguridad de la información basado en un enfoque de Gestión de Riesgos.

3.2.7 ISO31000 Gestión de Riesgos - Principios y Directrices

El Consejo de Auditoria Interna General de Gobierno (CAIGG), define una guía para la *implantación, mantención y actualización del proceso de Gestión de Riesgos en el sector público (documento técnico Nº70),* que tiene como principal objetivo facilitar a las organizaciones gubernamentales, la implementación y cumplimiento del proceso de gestión de riesgos, así como su mantención y mejora continua. Este enfoque técnico está basado principalmente en la Norma Chilena NCh-ISO31000:2012, Gestión del Riesgo - Principios y Orientaciones. Además, es el sistema de gestión de riesgos que utiliza Auditoria Interna y la Unidad de Control de Gestión de la Subsecretaria de Economía y Empresas de Menor Tamaño. Por lo anterior propuse al CSI utilizar en conjunto con la Norma ISO27005, la guía del CAIGG para estar alineados con las Unidades de Auditoria Interna y Control de Gestión.

La metodología de gestión de riesgos del Documento Técnico Nº70 del CAIGG, se basa en el paradigma de mejora continua de procesos PDCA[4]. Esto hace que la gestión de riesgos quede completamente integrada con el sistema de gestión de seguridad de la información el cual también está basado en una propuesta de mejora continua con PDCA.

---

[4] Modelo de mejora continua de procesos definido por Edwards Deming

Si revisamos la introducción al anexo A de la norma ISO27001:2013 tenemos el siguiente texto:

Los objetivos de control y los controles enumerados en Tabla A.1 se obtuvieron directamente y están alineados con aquellos enumerados en ISO/IEC 27002:2013, cláusulas 5 a 18 y deben ser utilizados con cláusula 6.1.3.

Si vemos lo que indica la cláusula 6.1.3 ella dice: La organización debe definir y aplicar un proceso de tratamiento de riesgo de la Seguridad de la Información[5]*.*

La interpretación de este extracto no es otra que indicar que toda política o procedimiento de seguridad de la información que se implemente para proteger un activo de información debe ser realizado teniendo en consideración una adecuada gestión de riesgos. En el Anexo B se explican las etapas del proceso de gestión de riesgos definidos por el Documento Técnico Nº70 del CAIGG que se utilizaron para hacer el análisis de riesgos de activos de la información de esta Tesis.

[5] NCH-ISO 27001:2013 cláusula 6.1.3 Tratamiento de riesgos de seguridad de la información

4 IMPLEMENTACIÓN DEL SGSI, POLÍTICAS Y PROCESOS DE SEGURIDAD DE LA INFORMACIÓN

Esta sección muestra la ejecución de la primera implementación y primer ciclo del SGSI. Este parte con un diagnóstico de la situación actual y termina con una evaluación del estado general del Sistema de gestión de seguridad de la información y de las políticas y procedimientos de seguridad de la información implementados en el ciclo actual.

4.1 DIAGNOSTICO SITUACIÓN ACTUAL DE LA SEGURIDAD DE LA INFORMACIÓN

El diagnóstico de la situación actual se centró en identificar expectativas de las partes interesadas, la revisión de la implementación del SGSI del año 2012, el análisis de riesgos sobre los activos de información y concluyó con un informe de brechas.

4.1.1 Expectativas de las partes interesadas.

A partir de las entrevistas realizadas al área en estudio FIC y al área de Tecnologías de Información, se determinó que la creencia arraigada en el personal era que solo se debían implementar Políticas y Procesos de seguridad de la Información, que este no era un esfuerzo que involucraba a la organización como un todo, sino solo un problema de informática y redes. Fue necesario un cambio de visión, el que realizamos mediante charlas, presentaciones que explicaban las implicancias de las cláusulas 4 a 10 de gobernanza y las clausulas normativas contenidas en el Anexo A de la norma ISO27001:2013.

4.1.2 Revisión Implementación SGSI 2012

La Subsecretaria de Economía ya había implementado el año 2012 un conjunto de políticas y procedimiento de seguridad de la información para cumplir con los objetivos de control de la norma ISO27001:2005, versión de la norma anterior a la que se está utilizando para esta tesis. De la implementación del SGSI-2012 se buscó todo lo que se pudiera reutilizar, dada la restricción presupuestaria existente. Se consideraron dos actividades:

La primera actividad fue determinar la correspondencia entre la norma ISO27001:2005 y la Norma ISO27001:2013. Para esta tarea se empleó una la panilla Excel “Matriz de Riesgos FIC SGSI” basada en el documento ISO27001-mapping-guide-UK de BSI[6]. Esta actividad es la base para de diagnóstico de la implementación de seguridad implementada el año 2012. Sirviendo de antecedentes de la primera reunión de trabajo del Comité de seguridad de la Información. El objetivo fue optimizar recursos identificando procesos y políticas establecidas el año 2012 con estándar ISO27001:2005 las pudieran cumplir con los requisitos del nuevo SGSI basado en ISO27001:2013.

[6] British Standards Institution

La Segunda actividad fue Identificar el grado real de implementación de los procesos y políticas del SGSI-2012. Ello implicó verificar si las políticas y procesos de seguridad de la información estaban realmente implementados, es decir, eran conocidos por el personal, sus indicaciones eran seguidas y respetadas. Los resultados de esta actividad se registraron en la misma planilla de trabajo Excel “Matriz de Riesgos FIC SGSI”, la cual sería utilizada durante el desarrollo del PMG y la presente tesis como guía central de información.

Como resultado de estas dos actividades tipifique el cumplimiento de los objetivos de control de la norma ISO27001:2005 según su correspondencia a los siguientes estados:

1. *No hay política o procedimiento que cumpla el objetivo de control.*
2. *Existe una política o procedimiento, pero no existe cumplimiento del objetivo de control.*
3. *Objetivo de control cumplido (existe una política o procedimiento, formalmente escrito, comunicado, aplicado y monitoreado).*

Concluí finalmente, que la implementación ISO27001:2005 realizada el 2012 en su correspondencia a los 114 controles exigidos por la norma ISO27001:2013 presentaba lo siguiente:

- *70% de los objetivos de controles está en estado 1.*
- *30% de los objetivos de control está en estado 2.*
- *No hay controles implementados completamente, estado 3*

Adicionalmente la revisión de la implementación me permitió concluir que no hubo un sistema de gobernanza de la Seguridad de la información y tampoco se aplicó un Sistema de Gestión de Riesgos. Se escribieron las políticas y procedimientos de seguridad de la Información, pero no hubo implementación de procesos de monitoreo, seguimiento y difusión que brindaran la posibilidad de evaluar y mejorar los Procesos y Políticas de seguridad de la Información, pues no se creó la estructura del SGSI (cláusulas 4 a 10), específicamente no se designó personal que recolectara información que permitiera una evaluación del trabajo realizado para producir la mejora ciclo a ciclo.

4.1.3 Identificación de Activos de información y Análisis de Riesgos

Conocer cuáles son los activos de información, a qué riesgos están expuestos y en qué medida, es fundamental para establecer la prioridad de implementación de los procedimientos y políticas para asegurar la integridad, confidencialidad y disponibilidad de los activos de información relevantes para la Subsecretaría. Para identificar los activos realice un levantamiento de proceso con el fin de identificar la información procesada por la unidad FIC y posteriormente realice un análisis de los riesgos a los cuales está expuesta dicha información.

Identificación de Activos de información

El modelamiento inicial de procesos FIC se realizó con notación BPMN, dada la experiencia en proyectos con BPMN informada por personal directivo de la División de Tecnologías y Desarrollo, que es el responsable de la entrega de recursos para el cumplimiento del presente PMG-SSI, PMG que tiene como proceso bajo estudio la asignación del FIC y por ello proceso en estudio para esta tesis.

FIC se modelo en BPMN identificando la información utilizada, producida y almacenada, lo cual es básico para identificar los activos de información y conducir posteriormente el análisis de riesgos de seguridad de la información. Al poco andar con la notación BPMN, constate que la experiencia con BPMN en FIC se limitaba a desarrollos externos y que la familiaridad con la notación no era tal. Como el objetivo era identificar la información manipulada y con ello realizar el Inventario de Activos de información y no producir un modelamiento detallado de los procesos, busque una notación con una simbología más cómoda para el personal del área en estudio. Para tal efecto propuse IDEF07, que es una notación diseñada para modelar decisiones, acciones y actividades de una organización o sistema. Esta notación presenta un lenguaje gráfico bien establecido y sencillo, que nos permitió organizar el análisis de los procesos y tener una buena comunicación con el personal del área en estudio.

Según la Figura 2 cada proceso es representado por un cuadrado, que identifica la información de entrada, la información de control y la información de salida. Este modelo fue efectivo para representar la interacción de la información entre procesos. Posteriormente realice un estudio top-down para identificar todas las TI involucradas en la comunicación, producción y almacenamiento de información. Es importante indicar que no era objetivo de mi estudio dar un pronunciamiento sobre la eficiencia de los procesos de negocio o proponer una mejora a los mismos, no en este momento.

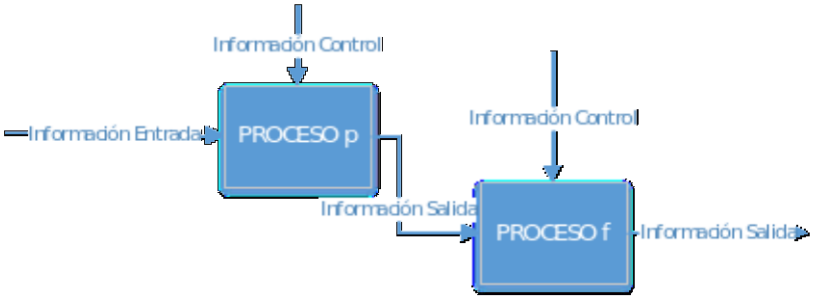


Figura 2 Modelo IDEF0

[7] Integration Definition for Function Modeling

Con la notación IDEF0 realice el estudio de los 4 subprocesos que componen FIC: (1) seguimiento y control de convenios, (2) elaboración de la política nacional de innovación, (3) monitoreo de indicadores y (4) confección encuesta de I+D e innovación ver Anexo C.

La información de entrada y salida de los procesos la definí como activos de información primarios o información primaria, por ser directamente identificados por los usuarios. Posteriormente la identificación de Activos de información continua de una manera descendente identificando los activos de información a los que llame “secundarios” al ser Activos de información de apoyo, pues permiten asegurar la disponibilidad, confidencialidad e integridad del activo de información primario. Luego cada activo de información secundario lo trate como si fuese un activo primario, identificado por capas todos los elementos tecnológicos que permiten la existencia y disponibilidad del activo. Con este modelo top-down se obtiene una jerarquía que empieza en los documentos (activos primarios), continua en los sistemas de información, sistemas operativos, bases de datos, servidores, hasta llegar a la identificación de los componentes de redes, instalaciones y personal. Cada activo de información lo registre en una planilla Excel, donde cada línea correspondía a la descripción un activo de información.

Análisis de Riesgos

Posteriormente a la identificación de los activos de información y su registro en la planilla, procedí a realizar el análisis de riesgos para cada activo de información. Este consistió en la identificación de vulnerabilidades y su estudio para determinar qué riesgos se podían materializar a través de ellas. Luego en conjunto con personal idóneo del departamento de informática y mediante juicio experto procedimos a asignar probabilidades de ocurrencia a cada riesgo. Este trabajo lo registre en las columnas “Descripción del Riesgo”, “Probabilidad de Ocurrencia”, “Impacto” y “Nivel de Severidad” todo ello en concordancia con la metodología de Gestión de Riesgos del CAIGG explicada en el Anexo B.

Ejemplo de Identificación de Activo y Análisis de Riesgos

Como ejemplo del trabajo realizado, veamos el Activo de Información Primario “Documento de Propuesta de Convenio" del subproceso de “Gestión y Administración de Convenios”. Es un documento Excel y para poder producirlo, gestionarlo y almacenarlo es necesaria la concurrencia de otros Activos de Información. Así en cadena tenemos que la información "Propuesta de Convenio" es recopilada en un documento Excel, que está en un recurso compartido de red, del cual existe una copia en el notebook del jefe de unidad y en un disco duro externo que administra la secretaria del área.

Proceso	Subproceso	Etapa	Nombre Activo
FIC	Gestión y Administración de Convenios	Formulación de convenio de acuerdo a la ley de Presupuesto	Propuesta Convenio
			Notebook
			Excel
			Disco duro Externo
			Carpeta de red
			Servitor de Archivos

Figura 3 Matriz de Riesgos SGSI FIC

El activo "Propuesta de Convenio", se registró en la planilla MatrizRiesgosSGSI_FIC_controlesISO como se aprecia en la Figura 3, junto con todos sus Activos de información secundarios obtenidos, ubicados inmediatamente en las celdas inferiores de la columna Nombre Activo.

Nombre Activo	Descripción del Riesgo	Probabilidad de Ocurrencia	Impacto	Severidad
Propuesta Convenio	El acceso no autorizado a información en estado de borrador, puede distorsionar la opinión pública al contrastar esta información con la documentación final.	Probable (4)	Moderado (3)	Alto (12)

Figura 4 Evaluación de Riesgos

La Figura 4 muestra el resultado del análisis de riesgos realizado para el activo de información "Propuesta de Convenio". El análisis realizado por la opinión experta de los usuarios del área FIC y el personal de la Unidad de seguridad de la información llegó a la conclusión que la severidad de materializarse el riesgo era Alta. Ello en base a experiencias anteriores, con lo cual se identificó la probabilidad de ocurrencia y el impacto. Muy importante resultó en el análisis expresar con claridad la descripción del riesgo al momento de cuantificar el impacto.

En el Anexo B Etapas Gestión de Riesgos Documento Técnico Nº 70 CAIGG encontrara los conceptos que componen la gestión de riesgos, sin embargo es necesario explicar brevemente, probabilidad, impacto y severidad del riesgo.

Probabilidad de ocurrencia: E*s la posibilidad de que ocurra un evento, que puede afectar el logro de los objetivos o planes establecidos de un proceso.*

Impacto*: Se refiere a las consecuencias de la ocurrencia de un evento, esta consecuencia puede ser negativa o positiva. El impacto según la metodología CAIGG va de efectos insignificantes hasta catastróficos*

Severidad: es la multiplicación de los valores nominales de la probabilidad de ocurrencia que va de 1 a 5 y del impacto cuyos valores nominales van también de 1 a 5. Entonces la severidad va de 1 severidad baja a 25 severidad extrema

4.1.4 Informe de Brechas PMG-SGSI

Las actividades que realice durante el Diagnóstico de la Situación Actual, dieron origen a un informe de brechas el cual entregue a departamento de informática y al representante de la subsecretaria de economía, cuyos principales hallazgos son los siguientes:

1. *Del sistema de seguridad de la información que se implementó el 2012 bajo la norma ISO27001:2005, se encuentran escritos, pero no vigentes 34 procedimientos y 5 políticas,*
2. *Los documentos originales se perdieron.*
3. *Solo existen copias en formato imagen.*
4. *Los documentos no son de conocimiento del personal al cual están dirigidos.*
5. *No existen registros de revisiones ni actualizaciones desde el año 2012.*
6. *No existe certeza si son las versiones finales de los documentos.*
7. *Los procesos actuales no se rigen por lo establecido en estas políticas y procedimientos*
8. *Algunos documentos no se encuentran firmados por la autoridad*
9. *Los procedimientos de control no se adecúan a los procesos operacionales actuales*

Por estas razones recomendé utilizar estos documentos solo como referencia de ayuda para la implementación de las nuevas políticas y procedimientos para cumplir con los objetivos de control indicados por la norma ISO27001:2013.

Con respecto a la gobernanza de la Seguridad de la información, las brechas detectadas son aún mayores, pues evidencia la inexistencia de la Administración de la Seguridad de la información. Así tenemos que la iniciativa de SGSI del 2012 no brinda:

- *Una hoja de ruta coherente para implementar la estructura administrativa y el conjunto de procesos y controles que constituyen el SGSI definido en la Norma ISO27001:2013 para proteger convenientemente la información y procesos que la recolectan, procesan, almacenan y distribuyen, frente a amenazas.*

- *Conciencia que los riesgos que ponen en peligro a la propia información, afectan la continuidad de los niveles de servicio, rentabilidad social y conformidad legal, necesarios para alcanzar los objetivos institucionales.*

- *Las estructuras funcionales que permitan implementar un sistema que gestione la seguridad de la información de manera que la subsecretaría cumpla con la normativa ISO 27001:2013 y que a su vez, institucionalice la mejora continua de los procesos que componen el SGSI en apoyo a los procesos operacionales y estratégicos de la organización.*

Para mayor detalle el documento de Análisis de Brechas y la lista de controles analizados ISO27001:2005 y su correspondencia a controles ISO27001:2013 vea en el Anexo D Informe de brechas PMG-SSI 2015.

Implementación de SGSI

Mi propuesta de la composición del SGSI estaba constituida por cinco sistemas en un esquema de capas, para las cuales dispuse un orden de implementación que facilitara la puesta en marcha del SGSI. Así la implementación del SGSI quedó constituido por el siguiente orden de implementación de sistemas:

- Sistema Toma de Decisiones
- Sistema Gestión de Riesgos
- Sistema Monitoreo
- Sistema Gestión de Proyectos
- Sistema Gestión Documental

En la figura 4, se ilustra como primero implementamos el sistema para toma de decisiones, gestión de riesgos y luego seguimos implementando los sistemas hasta llegar al sistema de gestión documental. La figura además incluye en su parte más exterior la implementación de políticas y procedimientos de seguridad de la información. Esta inclusión muestra que todas las capas que están por debajo, tienen como objetivo la implementación y mantención de las políticas y procedimiento de seguridad de la información.

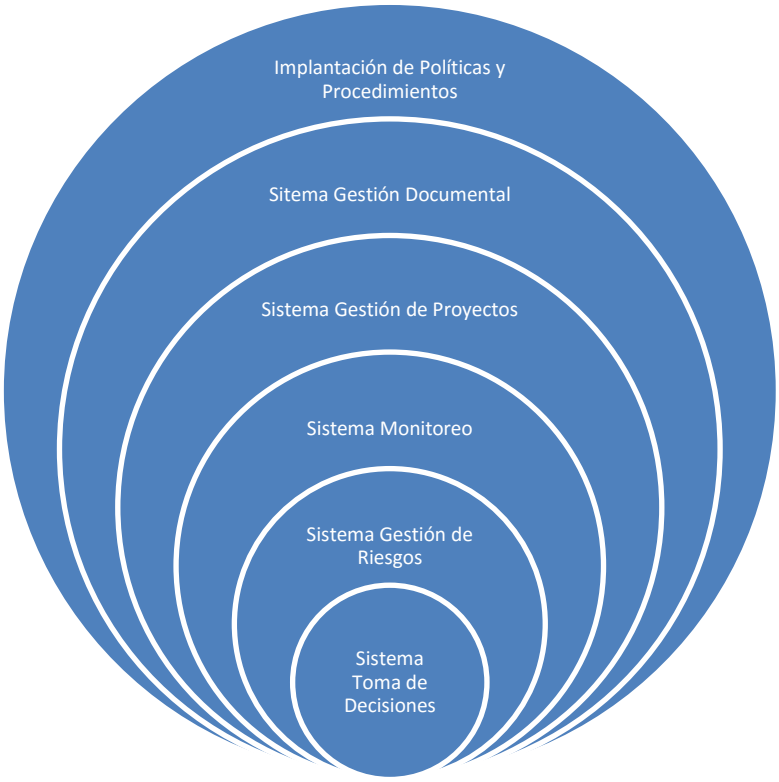


Figura 5 Capas del SGSI

4.1.5 Implementación del Sistema de Toma de Decisiones

Para la toma de decisiones se creó el Comité de Seguridad de la Información (CSI) presidido por un Oficial de Seguridad de la Información (OSI), secundado por el jefe del proyecto de implementación del SGSI cargo que detente por dos años incluido el periodo de realización de la actual tesis. El CSI asumió las siguientes responsabilidades:

1- *Aprobar la implementación de procedimientos y estándares que se desprenden de las políticas de seguridad de la información.*

2- *Aprobar las estrategias y soluciones específicas para la implantación de las políticas y procedimientos de Seguridad de la información establecidos frente a las situaciones de riesgo detectadas sugeridas por el jefe del proyecto de implementación del SGSI.*

3- *Arbitrar conflictos en materia de Seguridad de la información y los riesgos asociados, evaluar soluciones, coordinarse con los comités de calidad y de riesgos de la institución, para mantener estrategias comunes de gestión.*
4- *Reportar a la alta dirección.*

5- *Aprobar procesos de mejora en el SGSI.*

6- *Aprobar la implantación de políticas y procedimientos de seguridad de la información.*

El CSI fue integrado por los siguientes roles:

a) *Encargado de Seguridad de la Información (ESI), como presidente*
b) *Subsecretaria de Economía.*
c) *Jefe Control de Gestión.*
d) *Jefe de TI.*
e) *Ingeniero jefe proyecto Sistema de Gestión de Seguridad de la Información (Nelson Yañez).*

En el año 2012, el CSI se componía de 10 personas, con mayoría del área de TI, lo que inclinaba las decisiones a la visión de TI. Este número además demostró ser excesivo dado que el comité nunca podía sesionar en pleno o se suspendían las reuniones por falta de quórum. Por ello sugerí una composición más equilibrada entre miembros de TI y directivos de otras áreas. El reducir el número de integrantes facilito la coordinación de reuniones permitiendo una mejor toma de decisiones.

El objetivo del sistema de gestión de riesgos es facilitar el proceso de identificación y evaluación de los riesgos de los activos de información y consta dos etapas: la primera orientada a la identificación y registro de los activos de información y la segunda etapa orientada a facilitar la evaluación del riesgo al que están expuestos los activos de Información. Ambas etapas son llevadas actualmente en la planilla Excel MatrizRiesgosSGSI_FIC_controlesISO, la cual es una ampliación de la matriz de riesgos que utiliza Control de Gestión. La cual sugerí para permitir la integración de los riesgos de seguridad de la información con los riesgos operacionales de la subsecretaría.

La Matriz de Riesgos al ser una planilla Excel presenta todas las ventajas de una planilla de cálculo, ideal para el análisis de riesgos, pero tiene algunos inconvenientes como es repetir las entradas por cada Activo de Información al abrir la jerarquía de Activos de Información. Esto crea un problema de actualización y mantención de la planilla en la medida que se agregan Activos de información y se procede al correspondiente Análisis de Riesgos.

En virtud de lo anterior busque una herramienta que remplaza o complementa a la planilla Excel, permitiendo realizar lo siguiente:

- *Gestionar el inventario de activos de información*
    - *La identificación de activos de información por red*
    - *El registro de activos de información que no son detectables por red*
- *El cálculo de exposición al riesgo y riesgo residual*
- *La administración de base de datos de activos de información*

Sin embargo por motivos de tiempo y presupuesto durante la ejecución de la actual tesis no fue posible la selección e implementación de un software que satisficiera las necesidades identificadas

Gestión de Inventario de Activos de Información

Para cumplir con la primera etapa de Gestión de Riesgos, que es la identificación y registro de los activos de información, instalamos OCS-inventory[8]. Este software de código libre aporto el descubrimiento de los dispositivos de red y todos los dispositivos conectados a la red, como son las impresoras, notebook, computadores, servidores etc. La instalación en producción de esta herramienta nos permitió rápidamente levantar un nuevo inventario de activos complementario al inventario realizado durante la etapa de diagnóstico.

Evaluación de Riesgo de Activos de Información

Para cumplir el segundo objetivo, facilitar la evaluación del riesgo, solicite la instalación de Eramba[9] para evaluarlo. Eramba es una aplicación de código abierto dirigida a la Gobernanza y Análisis de Riesgos de Tecnologías de Información (TI). Si bien encontré que puede ser una herramienta interesante, que permite describir una organización mediante el registro de sus áreas funcionales y registrar los requisitos legales relacionados con las políticas y procedimientos para la protección de activos de la Información, presenta el gran inconveniente que el Análisis de Riesgos que realiza, es limitado manejando sólo el concepto de riesgo residual[10] según su propia definición y escala fija. Este riesgo residual no es calculado por el sistema, sino que debe calculado en forma manual y luego se agrega como un dato más a Eramba. Además de ello no maneja ningún concepto de gestión de riesgo, escalas o definiciones, limitándose a ser solo un registro de activos. Finalmente dados estos antecedentes no fue atractivo mantener Eramba, tomándose la decisión de continuar con plantilla Excel, agregando Macros y Programación para que el ingreso de datos fuese por medio de listas predefinidas, evitando la introducción de términos que estén fuera de las convenciones establecidas en el documento Técnico N70 del CAIGG. Lo mismo hicimos con los cálculos de exposición al riesgo

8 http://www.ocsinventory-ng.org/en/

9 http://www.eramba.org/

10 Riesgo remanente luego de aplicar mecanismos de mitigación de riesgos

para facilitar el análisis de riesgos sobre el inventario de activos, manteniendo una coherencia durante todo el proceso de análisis de riesgos.

4.1.6 Implementación Sistema de Monitoreo.

El objetivo de este sistema es la alerta temprana frente a la concreción de incidentes de seguridad de la información y la recolección de métricas que son fundamentales para la gestión de seguridad de la información. Las métricas provenientes del monitoreo complementan la evaluación de los procesos y políticas de seguridad de la información brindando información relevante para realizar la gestión de riesgos, lo que a la vez permite argumentar frente comité de seguridad de la información qué políticas o controles se deben reformular o reforzar.

Un objetivo secundario, pero importante de mencionar, es aumentar la confianza de la organización en los resultados de la aplicación de las políticas y procedimientos de seguridad de la información mediante la retroalimentación constante que brinda el sistema de monitoreo. Finalmente, la confianza ganada, ayuda a la obtención de recursos para los ciclos de mejora continua.

Para la implementación del sistema de monitoreo y mediciones, seleccione el siguiente grupo de herramientas de software: Nagios, Cacti, Zabbix, Snort y OSSIM [11]. Ello nos permite:

- *Implementar y operar un sistema de mediciones de seguridad de la información.*
- *Recolectar y analizar los datos.*
- *Mostrar gráficamente los resultados de las mediciones.*
- *Comunicar los resultados de las mediciones desarrolladas a las principales partes interesadas.*
- *Utilizar los resultados de las mediciones como apoyo a la toma de decisiones relacionadas a la seguridad de la información.*
- *Utilizar los resultados de las mediciones para identificar necesidades de mejorar el SGSI, incluyendo su alcance, políticas, objetivos, controles, procesos y procedimientos, facilitando la Mejora Continua de la seguridad de la información.*

La implementación de este sistema de monitoreo está compuesto por tres elementos centrales: la instalación y configuración de programas de monitoreo de plataforma, la implementación de un software para administración de registro de incidentes reportados por los usuarios y la definición del conjunto de reportes que contendrían las métricas para informar a los niveles directivos el estado de salud de la seguridad de la información.

11 https://www.nagios.org/ http://www.cacti.net/ http://www.zabbix.com/ https://www.snort.org https://www.alienvault.com/products/ossim

Programas de Monitoreo de plataforma

Dada la importancia de la implementación del sistema de monitoreo para los estamentos directivos, propuse que esta se llevara con una formalidad diferente a la implementación de los demás sistemas, al tratarse de actividades de revisión sobre equipos de comunicaciones, servidores y la red con todos sus dispositivos conectados, incluidos las estaciones de trabajo. El tema era muy sensible y por ello se trató como un proyecto dentro del proyecto de implementación de SGSI. En el Anexo E se puede ver el acta de constitución, donde se abordan los aspectos técnicos del mismo.

La implementación del proyecto de sistema de monitoreo, mirado en retrospectiva fue el punto más delicado de todo el proyecto de tesis. La inesperada complejidad de la implantación del monitoreo vino de aspectos culturales, los cuales no fueron vislumbre en la fase de diagnóstico de la situación actual y quedaron recién al descubierto al momento de la implementación.

El primer aplicativo de monitoreo que instalamos fue Nagios, toda una novedad en la subsecretaría, ya que no existía un sistema de monitoreo de redes y no se emitían informes de ataque a dispositivos y redes, además no se conocían las vulnerabilidades. El cambio de pasar de un mundo con una aparente quietud y seguridad sin cuestionamientos, a uno nuevo, lleno de la “sorpresas” producida por la develación de las vulnerabilidades existentes en la plataforma tecnológica de la información y comunicaciones, evidenciadas por las herramientas de monitoreo, creó un quiebre en la coordinación de los equipos de continuidad operativa y el nuevo personal encargado del monitoreo.

Si bien se definieron los objetivos y los factores críticos de éxito del Sistema de Monitoreo, las actividades de difusión hacia el área de tecnologías de la información claramente fueron insuficientes, pues no logramos que el personal comprendiera el objetivo positivo del monitoreo al detectar incidentes antes que estos causen daño. Continuidad operativa se sintió cuestionada por las evidencias entregadas por Nagios, Catti y OSIM sobre las vulnerabilidades de la red y las comunicaciones.

Para poder continuar con el proyecto e incorporar más servicios y máquinas al monitoreo impulse una visión más didáctica con la unidad de continuidad operativa. Les otorgue acceso guiado a la información y coordine nuevas reuniones de evaluación de riesgos promoviendo la implementación de las iniciativas emanadas de estas reuniones por sobre la planificación inicial de Políticas y procedimientos de seguridad de la Información. Lo primero que produjo esta mayor interacción fue un esquema actualizado de la topología de la red ver Anexo F.

Finalmente, con la cooperación del área de continuidad operativa, el sistema de monitoreo se instauró permanente y se evidenció el valor de tener alertas tempranas. El personal de continuidad operativa vio la posibilidad de actuar antes de que un evento de seguridad se transformara en un incidente, lo que terminó por convencer al área de la conveniencia de contar con el monitoreo del mayor número posible de equipos.

Registro de incidentes

Otra fuente importante de información de eventos de seguridad es la aportada por los propios usuarios al informar de hechos que están afectando su trabajo. Para registrar esta información se instaló GLPI[12] que es un aplicativo para el registro y seguimiento de atención de tickets, el cual aporta información complementaria al sistema de monitoreo, al registrar los incidentes se seguridad de la información reportados por los usuarios. Las herramientas de monitoreo como Nagios, Cacti, Zabbix, Snort y OSSim no detectan, por ejemplo, inconsistencia de datos en un aplicativo, pues está fuera de sus objetivos, pero el software de atención de tickets GLPI sí permite registrar las inconsistencias informadas por los usuarios. La información recopilada por medio de GLPI, también es tabulada y utilizada como métricas para evidenciar la efectividad de la aplicación de políticas y procedimiento de seguridad de la información o establecer la necesidad de incluir mejorara a los procesos actuales e invertir en el desarrollo de nuevos procedimientos.

Para registrar los tickets de atención a usuarios, éstos son ingresados por personal de informática desde el correo genérico soporte@ destinado al envió de solicitudes de atención e informe de incidentes. Originalmente pensé en un correo para soporte y otro para incidentes, pero constante que al usuario común le significaba una sobrecarga el decidir si lo que reportaba correspondía a una solicitud de soporte o un incidente de seguridad. Una vez ingresado el ticket este era atendido por el equipo de soporte. La presente tesis no contemplo el estudio de los protocolos de atención, pues no estaban dentro de los 44 objetivos de control priorizados para el PMG-SSI del año 2015.

Para los efectos de esta tesis este sistema, no alcanzó a estar operativo un tiempo significativo como para poder extraer datos para contrastarlos con las políticas y procedimientos de seguridad de la información implementados. Además, no existían registros de eventos anteriores a la implementación de GLPI, por lo cual no existía una línea base con la cual pudiese efectuar comparaciones entre los tickets pre y post implementación de políticas y procedimientos.

Pese a no existir registro de ticket con anterioridad a la implementación de GLPI, tenemos la firme convicción de la gran importancia en la operación futura del SGSI como fuente de información referente a efecto de medidas de control y mitigación de riesgos a través de las métricas de índices de fallas e incidentes de seguridad reportados.

Informes de seguridad

Si bien todas las herramientas de monitoreo que estamos usando tienen en mayor o menor medida implementados Dashboard con métricas resumidas del estado de la red, servidores y equipos de comunicaciones, en el Anexo G se puede ver capturas de pantalla de ellos indicando ataques, debilidades etc. Dichos tableros de resúmenes de mediciones no están diseñadas para un nivel directivo, sino para el personal de redes y plataforma. Por ello se definí tres informes base para reportar el estado general de seguridad de la

12 http://glpi-project.org/

información al comité de seguridad de la información. A continuación se da un resumen de los objetivos de dichos informes:

- *Informe de incidente significativo de seguridad*

El objetivo es documentar en forma detallada un incidente de seguridad de la información, informar si se trató de una concreción de riesgo por hecho fortuito sobre una debilidad o si se trató de un ataque. Se acompañan también las políticas o procesos de seguridad de la información que mitigaban el riesgo. Según la gravedad del incidente de seguridad de la información corresponderá discrecionalmente al OSI la convocatoria del CSI.

- *Informe Mensual de eventos/incidentes de seguridad de la información.*

El objetivo es mantener informadas al área de Control de Gestión y auditoria interna del comportamiento general de los sistemas de procesamiento y comunicaciones. Contiene un resumen de los eventos más significativos con las correspondientes glosas explicativas de cada evento.

- *Informe Trimestral de seguridad de la información*

Corresponde a un resumen ejecutivo de los informes anteriores y se prepara para las reuniones trimestrales del comité de seguridad de la información, que es la ocasión en la que se toman decisiones de implementación de nuevos procesos o mejora a los existentes.

4.1.7 Implementación Sistema de Gestión de Proyectos.

El objetivo de este sistema es que los proyectos de seguridad de la información, y en general los proyectos TIC, tengan una línea base en las etapas del ciclo de proyecto que facilite la estandarización de las actividades y la determinación de carga de trabajo, expresada en horas hombre. Todo esto permite balancear la carga de los jefes de proyecto y analistas. Para ello propuse buscar una herramienta de control de proyecto que a lo menos cumpliera con:

- *Informe de actividades*
- *Informe de avance*
- *Perfiles de usuario*
- *Control de acceso*
- *Asignación de tareas.*

Estudio de alternativas

Para cumplir con los objetivos propuestos para el sistema de gestión de proyectos, evalué dos alternativas: web2project y RedMine[13], las cuales fueron instaladas en servidores virtuales para proceder a probarlas. Junto con ello se investigue en la web, buscando referencias en torno a las características como son:

- *Facilidad de uso.*
- *Tamaño de la Comunidad.*
- *Calidad de la Documentación.*
- *Seguridad.*

Opción Implementada

De las dos alternativas se recomendé Redmine por permitir la visualización en dispositivos móviles, lo cual resulto muy atractivo para los niveles directivos. Además, soporta API, tiene autenticación LDAP y obtuvo una experiencia de uso más fluida.

Inmediatamente se instaló en producción para tener centralizada y controlada toda la planificación de proyectos relacionados al área de seguridad de la información, esto es, los proyectos de implementación de los demás sistemas del SGSI y la implementación de Políticas y procedimientos de seguridad de la información de la norma ISO27001:2013. Posteriormente, se capacite a los jefes de proyecto en el uso de Redmine, para que pudiesen subir las planificaciones de sus proyectos.

4.1.8 Implementación Sistema de Gestión Documental.

El objetivo de contar con un sistema de gestión documental va más allá de tener un repositorio ordenado y versionado de políticas, procedimientos, normativas y resoluciones, buscamos además mayor inclusión del personal al poner a su alcance y comprensión las políticas y los procedimientos de seguridad. Por ello el sistema de gestión documental e inclusión del personal está orientado a la sensibilización del personal en lo referente a la Seguridad de la información y busca que las personas sean parte de la red de seguridad de la información y sepan qué deben hacer en caso de incidentes de seguridad de la información en el ámbito de su trabajo.

13 http://web2project.net/ http://www.redmine.org/

Estudio de alternativas.

Hice una pre selección con tres software con los cuales el equipo tenía experiencia y que, y según mi opinión luego de revisar foros en la web, eran los tres gestores de documentos open-source con mayor uso: Joomla, Drupal y Alfresco ([14]). El análisis se realizó buscando referencias en la web en torno a las características como son:

- *Facilidad de uso.*
- *Tamaño de la Comunidad.*
- *Calidad de la Documentación.*
- *Seguridad.*

En general todo el material registrado daba calificaciones similares a los tres gestores de documentos, no observándose diferencias significativas.

Se hizo instalación de los tres, pero no se probó en forma exhaustiva ninguno de ellos.

Con la instalación se probó:

- *Facilidad de instalación.*
- *Experiencia general de uso.*

No se encontraron mayores dificultades en la instalación de los distintos gestores de documentos; además existe gran cantidad de información en la web de cómo proceder.

Con respecto a la facilidad general de uso, no se apreciaron opiniones objetivas que nos hicieran pensar que una alternativa estaba por sobre la otra.

Opción Implementada

Se instaló Alfresco como gestor de contenidos. La decisión se tomó por la llegada de dos profesionales al área de TI que tenían amplia experiencia en uso de Alfresco.

Inmediatamente se creó el sitio de seguridad de la información, según un diseño base que realice en Sharepoint[15] que había realizado en un trabajo anterior y se subió el material de trabajo compuesto por normas y documentos de seguridad de la información y las políticas y procedimientos de seguridad de la información en desarrollo y terminadas. Todo debidamente rotulado y separado. De esta manera tuvimos inmediato

14 https://www.joomla.org/ https://www.drupal.org/ https://www.alfresco.com/es

15 Gestor de contenidos web y administrador de portales web de Microsoft

control de las versiones de los documentos y se garantizó que todo el personal tuviera acceso a las versiones finales y vigentes de políticas y procedimientos.

Para el funcionamiento básico propuse la creación de tres perfiles: un perfil de administrador reservado para los encargados de mantener en funcionamiento Alfresco y crear sitios, un perfil de gestor de contenidos, reservado al personal encargado de administrar el contenido y la estructura de carpetas, y un tercer rol de lectura asignado al personal para consultar los documentos que componen la implementación de las políticas y controles de la Seguridad de la información de la Norma ISO27001:2013.

En el Anexo H se puede ver el sitio de Seguridad de la Información.

4.2 Implementación de Políticas y Procedimientos de Seguridad de la Información

Dado que no era factible por presupuesto y equipo de trabajo realizar en el 2015 la implementación completa de los 114 controles que define la norma, propuse la estrategia de seleccionar un subconjunto de cláusulas normativas definidas en el Anexo A de la norma ISO27001:2013. La etapa de Diagnóstico de la Situación Actual de Seguridad, había entregado todos los elementos para la selección de las políticas y procesos de seguridad de la información para cumplir con el subconjunto de controles de la norma a los cuales se daría cumplimiento durante el año 2015. De esta manera propuse al comité de seguridad de la información presidido por el OSI y teniendo en cuenta el análisis los resultados del contexto organizacional, el presupuesto, las expectativas de las partes interesadas, la revisión de la implementación 2012 y el análisis de riesgos realizado al inventario de activos. La implementación de un conjunto de 44 controles normativos a implementar en forma de políticas y procedimientos de seguridad de la información ver Anexo J.

4.2.1 Planificación Implementación de los 44 Controles Normativos.

Identificados los 44 objetivos de control, redacte el acta de constitución del proyecto de implementación de políticas y procedimientos de seguridad de la Información, describiendo el proyecto e identificando a los patrocinadores y personal asignado para la ejecución del proyecto. Posteriormente realice el cronograma de actividades. Finalmente, presente el acta de constitución del proyecto y el cronograma de actividades al comité de seguridad de la información para su aprobación y autorización para comenzar el proyecto de implementación.

Las políticas y procedimientos de seguridad de la información fueron desarrollados en conjunto entre la unidad de Seguridad de la información y las unidades de TI según correspondiera para evitar conflictos de intereses. Todos los documentos finales pasaron por revisión del comité de Seguridad de la información antes de ser entregados a la subsecretaría para su firma y puesta en vigencia. Cada política y procedimiento siguió el ciclo de desarrollo que detalla la figura 6: Codificación, Revisión Área Seguridad de la

información (ASI), Revisión Jefatura de área, Aprobación del CSI, Firma Subsecretaría e Implantación.

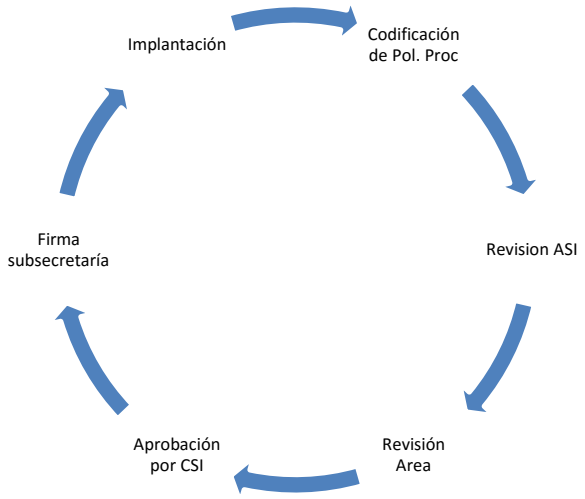


Figura 6 Ciclo Implementación Políticas y Procedimientos de Seguridad de la Información

4.2.2 Ciclo de Implementación. De Los 44 Controles

Para llevar el control de ciclo de implementación de cláusulas normativas ISO27001:2013, se cree un tablero kanban para que fuese visible para todas las áreas que se verían influenciadas con la implementación de las políticas y procedimientos de seguridad de la Información.

Cód.	CONTROL NORMATIVO COMPROMETIDO	Codif.	Rev. SSI	Rev. U. Dueña	Aprobado CSI	Sancionada	Implementado
A.05.01.01	POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN						✓
A.05.01.02	REVISIÓN DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN						✓
A.06.01.01	ROLES Y RESPONSABILIDADES DE LA SEGURIDAD DE LA INFORMACIÓN			↑			
A.06.01.02	SEGREGACIÓN DE FUNCIONES			↑			
A.06.01.03	CONTACTO CON AUTORIDADES						✓
A.07.01.01	SELECCIÓN			↑			
A.08.01.01	INVENTARIO DE ACTIVOS	◆					
A.08.01.04	DEVOLUCIÓN DE ACTIVOS				↑		
A.09.01.01	POLÍTICA DE CONTROL DEL ACCESO				↑		
A.09.02.03	GESTIÓN DE DERECHOS DE ACCESO PRIVILEGIADOS			↑			
A.09.04.02	PROCEDIMIENTO DE INICIO DE SESIÓN SEGURO			↑			
A.09.04.03	SISTEMA DE GESTIÓN DE CONTRASEÑAS			↑			
A.11.01.01	PERÍMETRO DE SEGURIDAD FÍSICA		↑				
A.11.02.01	UBICACIÓN Y PROTECCIÓN DEL EQUIPAMIENTO	◆					
A.11.02.04	MANTENIMIENTO DEL EQUIPAMIENTO	◆					
A.11.02.07	SEGURIDAD EN LA SOBREUTILIZACIÓN O DESCARTE DE EQUIPOS		↑				
A.11.02.08	EQUIPO DEL USUARIO DESATENDIDO		↑				
A.11.02.09	POLÍTICA DE ESCRITORIO Y PANTALLA LIMPIOS			↑			
A.12.01.01	PROCEDIMIENTOS DE OPERACIÓN DOCUMENTADOS	◆					

F*igura 7 Tablero Kanban para el segui miento de implementación de Políticas y Procedimientos*

A continuación se detallan las estepas del ciclo de implementación de las 44 políticas y procedimientos que dan cumplimiento a los 44 objetivos de control de la norma ISO27001:2013 que aborda la presente tesis.

Codificación de Políticas y Procedimientos

Corresponde a la primera etapa de elaboración de las políticas y procedimientos de seguridad de la información el nombre en la columna Kamban es Codif, en consecuencia al inicio de proyecto todos los objetivos de control estaban marcados en esta etapa. Le llame codificación de políticas y procedimientos y no escritura de políticas y procedimientos por sugerencia del CSI que buscaba un nombre que hiciera referencia a un código de conducta.

El esquema de trabajo con los equipos de redes, desarrollo, PMO y RRHH comenzó con reuniones iniciales introductorias para comunicar los objetivos de control según ISO27001:2013. En esta reunión les informe que yo sería el jefe de cada proyecto y que elaboraríamos en conjunto según correspondiera, las políticas y procedimientos de seguridad de la información, que documentaríamos a un alto nivel de abstracción la forma actual de hacer su trabajo y las restricciones u obligaciones que tenían para efectuarlo. Esta etapa duró un mes y produjo la primera versión de las políticas y procedimientos de seguridad de la información para cubrir los 44 objetivos de control seleccionados

Revisión Área Seguridad de la Información

La revisión del Área de Seguridad de la información (ASI) columna Rev. SSI, tiene como objetivo principal asegurar que todas las políticas y procedimientos escritos en la etapa anterior, cumplan con elementos de forma, control de versiones, visualización y en general la estética que los distingue como documentos de seguridad de la información. Además, el ASI se pronuncia en temas de fondo cuando estos contradicen a otras políticas o a la legalidad vigente o plantean exigencias que no son técnica o económicamente factibles de implementar.

Dado que al momento de realizar la presente tesis, el área de seguridad de la información solo contaba estaba constituida por mí en dedicación exclusiva más un integrante de la entidad acreditadora en forma parcial la revisión consistió en reunirme con miembros del área legal para analizar documento por documentos su legalidad y con los jefes de cada unidad para revisar aspectos técnicos de las políticas y procedimientos.

Revisión de área Funcional

Corresponde a las políticas y procedimientos que están en la columna kanban Rev. U. Dueña. Si bien las jefaturas de área son parte del proceso de gestación de las políticas y procesos de seguridad de la información, esta última revisión sobre el documento final contribuye como filtro de calidad detectando cualquier detalle que pudo ser omitido, tanto

de forma como de fondo. Además, afianza el compromiso de la jefatura con el equipo que desarrolló la política o procedimiento de la cual el área funcional será la responsable de su aplicación y cumplimiento.

En esta etapa mi función era facilitar y procurar que la revisión efectivamente se realizara dentro del plazo establecido por lo cual debí reunirme con cada jefe de unidad para conducir la reunión de revisión de las políticas y procedimientos y aclarar dudas y redactar nuevamente donde fuese requerido.

Aprobación del CSI

Corresponde a las políticas y procedimientos que están en la columna kanban Aprobación CSI. Este es el último escrutinio que recibe la política o procedimiento de seguridad de la información antes de ser despachado para su aprobación mediante una resolución exenta por parte de la máxima autoridad de la subsecretaria de Economía y empresas de Menor Tamaño.

Para esta etapa fueron necesarias planifique cuatro reuniones de aprobación, con una semana de intervalo entre ellas, previo a esto despache vía memo internos las políticas y procedimientos de seguridad de la información a todos los miembros de CSI. En las reuniones se realizaron aclaraciones y modifique los documentos que presentaron observaciones, las cuales fueron de forma y no de contenido. Los documentos que fueron inmediatamente aprobados por el CSI

Firma Subsecretaría

Corresponde a las políticas y procedimientos que están en la columna kanban Sancionada. Para que una política o procedimiento de seguridad de la información pueda ser difundida y aplicada, esta debe contar con la formalidad de la firma de la subsecretaría. Este trámite debería ser una formalidad administrativa, dado que en las etapas anteriores de formulación del documento ya se han discutido los aspectos técnicos y legales. Por lo tanto en esta etapa se debe ser celoso en cuanto a la forma y el documento que llega a firma debe contar con todas las solemnidades para evitar su rechazo.

En el Anexo K se muestra la Política General de Seguridad de la Información. Esta, al igual que todas las demás Políticas y procedimientos durante la presente tesis, se implementó siguiendo el ciclo definido en la Figura 6. De todas las políticas y procedimientos, la Política General de Seguridad de la Información es la más importante pues todas las otras políticas y procedimientos de seguridad de la información deben estar subordinadas a ella, no pudiendo contradecir sus lineamientos en ningún aspecto.

5 EVALUACIÓN DEL SGSI Y LAS POLÍTICAS Y PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN

La validación de los controles implementados se realizó por medio de dos auditorías: una auditoría interna al control de acceso (auditoría de cumplimiento) basada en el decreto supremo N°83 y los lineamientos de la DIPRES referidos a la implementación de la Norma ISO27001:2013 y una auditoría externa encargada a Neosecure para revelar brechas de seguridad de la información. En ambas auditorias mi rol como líder del proyecto de implementación del SGSI y el desarrollo de los 44 objetivos de control de la norma ISO seleccionados para implementar en este primer ciclo, fue el de proporcionar todas las evidencias de auditoria requeridas por los equipos auditores, actuando como coordinador para facilitar el trabajo de auditoria.

5.1 AUDITORÍA INTERNA

5.1.1 Equipo Auditor

El equipo que realizó esta auditoría corresponde a personal de auditoria ministerial y auditoría interna de la Subsecretaría de Economía y tiene total independencia de la unidad de seguridad de la información encargada de la implementación de SGSI, mi participación en esta Auditoria fue referida a la entrega de información y entrega de evidencia de auditoria, mostrar los diferentes sistemas y resultados de monitoreo.

5.1.2 Objetivo

Verificar la existencia de políticas y procedimientos de control de acceso físico, lógico, redes y sistemas, que limiten y controlen el acceso a los recursos físicos, sistemas y datos, para brindar protección contra la entrada o el uso no autorizado.

5.1.3 Metodología

La auditoría se realizó en base a reuniones de trabajo con los encargados de diseñar las políticas y procedimientos y con el personal que día a día en sus labores debe trabajar cumpliendo dichas políticas y procedimientos, para posteriormente validar su aplicación. Además se recorrieron las instalaciones de la subsecretaría para corroborar el control físico.

5.1.4 Hallazgos

Como resultado de la revisión practicada, se evidenció debilidades en la implementación procesos de control de acceso físico y entrega de contraseñas para acceso a sistemas. Las observaciones se centran específicamente en la divulgación de procedimientos internos destinados a controlar el acceso.

5.1.6 Recomendación de la Auditoría.

Si bien la mayoría de los Procedimientos y Políticas de seguridad de la información se encuentra aprobados mediante actos administrativos, se debe profundizar las actividades de difusión y sensibilización de estos e implementarlos en aquellas áreas o sistemas que aún están pendientes a la fecha de la realización de esta auditoría.

Se programa una auditoria de seguimiento para el 2017 destinada a ver el estado de avance una vez implementado el programa de mejora de gobierno de seguridad de la información 2015-2016.

5.2 AUDITORIA EXTERNA NEOSECURE.

NeoSecure es una empresa que brinda Soluciones de seguridad de la información cuenta con un Centro de Investigación de Malware (CIM) y un Security Operation Center (SOC), el segundo a nivel mundial en certificarse bajo la norma ISO 27001. Posee un equipo de ingenieros certificados en regulaciones internacionales: CISSP (ICS2), ISO 27001, CISM (ISACA), CERT entre otras y fue fundada en el año 1999.

5.2.1 Equipo Auditor

El equipo editor estuvo íntegramente conformado por personal externo el cual gozó de total autonomía para realizar su trabajo, corriendo aplicativos de escaneo de redes de desarrollo propio y otros bajo licencia. Asimismo solicitó toda la información de políticas y procedimientos de seguridad de la información sancionados a la fecha de la auditoría y se entrevistó con el personal para certificar el grado de conocimiento y cumplimiento de las políticas y procedimientos de seguridad de la información realizados bajo la norma ISO27001:2013 y el SGSI implementado.

5.2.2 Objetivo

Evaluar la seguridad general de los servicios y plataformas de TI de la Subsecretaría de Economía y Empresas de Menor Tamaño, entregando una opinión respecto del nivel general de seguridad que resulta del análisis de la evaluación efectuada.

5.2.3 Metodología.

La auditoría se realizó en base a reuniones de trabajo con el personal encargado de dar cumplimiento y seguimiento a las políticas y procedimientos de seguridad de la información para verificar su conocimiento y aplicación. Además se realizaron pruebas con software de monitoreo.

La auditoría consto de cuatro etapas:

- *Recopilación: Se realizó revisión de procesos y políticas de seguridad de la información sobre la plataforma y las operación de TI con el objetivo de recolectar evidencia de auditoría*
- *Evaluación: Se realizó, con la información obtenida, una evaluación global de brechas de seguridad de la información con base en ISO27001:2013.*

- *Evaluación con la oficina de seguridad de la información: Se realizó una segunda evaluación de brechas, riesgos y recomendaciones con el personal de seguridad de la información de la subsecretaría de Economía y empresas de Menor Tamaño, por el rol auditor que tiene la unidad de seguridad de la información sobre la Unidad de TI.*

- *Formulación de recomendaciones: Se generaron recomendaciones para mitigar el riesgo asociado a las brechas de seguridad.*

5.2.4 Conclusión General de la Auditoria Externa de Neosecure

A partir del análisis cualitativo y cuantitativo, se concluye que la Subsecretaria de Economía y Empresas de Menor Tamaño presenta un nivel de seguridad de la información medio, pues si bien se han configurado alternativas en caso de no disponibilidad de sistemas, se aplica configuración segura de equipos y servicios, y se evalúa periódicamente las vulnerabilidades, dichas buenas practicas están en proceso de implementación.

Se observa que la institución lleva a efecto mejoras y cambios a los sistemas de seguridad, basado en el monitoreo y la medición del avance en términos de mitigación de riesgos.

Se recomienda repetir la evaluación de riesgos una vez implementado el Programa de Mejora de Gobierno de seguridad de la información 2016-2017

6 CONCLUSIONES Y TRABAJO FUTURO.

6.1 CONCLUSIONES

La elaboración de este proyecto de implementación de un SGSI que detalla la presente tesis, logró un cambio del enfoque de lo que la unidad de sistemas entendía como seguridad de la información, desde una mirada solo de seguridad informática a un concepto más amplio y de carácter estratégico para la organización: la necesidad de proteger la información como el activo valioso. Este nuevo enfoque permitió la implementación de nuevas políticas y procesos de control, que sientan las bases para la creación de sistemas que monitorean y aseguran la mejora continua de las políticas y procedimientos definidos.

De este modo se puede concluir que se logró cumplir con el objetivo principal y los objetivos específicos perseguidos con la implementación del SGSI:

- *Se implementó un SGSI compuesto por 5 sistemas basados en software open source, destinados a asegurar la implementación de controles y la mejora continua de procesos de seguridad de la información.*

- *Se diseñaron 44 políticas y procedimientos de seguridad de la información para cumplir con los 44 controles de la norma ISO27001:2013 seleccionados para cubrir las brechas de seguridad de la información identificadas como prioridad por la evaluación de riesgos.*

La metodología de implementación del SGSI resultó ser práctica e inclusiva para favorecer el aprendizaje y la creación de equipos de trabajo orientados a tareas específicas sin que ellos perdieran la visión de conjunto y el objetivo final. El que las políticas y procedimientos pasaran por ciclos de aprobación, permitió establecer consensos, conciliar visiones y sobre todo lograr un sentimiento de trabajo en equipo.

La separación del SGSI en diferentes sistemas, cada uno con un objetivo claro y con una selección de herramientas de software como apoyo, fue fundamental para lograr orden y coherencia entre todas las políticas y procedimientos de seguridad de la información. Al ver el SGSI en forma gráfica y tangible, todos los diferentes equipos de trabajo entendían el objetivo final de la suma de todos los proyectos. Esto también les permitía ver cómo retrasos en su trabajo afectaban el trabajo de otros equipos. Lo anterior fue aprovechado por la unidad de Control de Gestión, encargada de la supervisión de todos los programas de mejora de gobierno, para monitorear directamente el avance en los planes y programas e informar directamente a DIPRES, sin necesidad de solicitar como en años anteriores un informe a la unidad de seguridad de la Información.

La utilización de software open source, permitió aliviar la carga económica de los proyectos, pudiendo dedicar más recursos a la implementación de políticas y procedimientos para cubrir una mayor área organizacional.

La mayor parte del software que se usó tiene versiones comerciales que incorporan opciones avanzadas de monitoreo y control. Para una organización que se está iniciando en seguridad de la información, consideramos altamente recomendable la utilización y prueba de las herramientas en sus versiones open source, tal como se hizo en esta tesis. Así se logra flexibilidad y la posibilidad de cruzar información entre las herramientas para descartar falsos positivos sin incurrir en gastos que para una pequeña o mediana empresa pueden ser difíciles de solventar.

El apoyo directivo para seguridad de la información es y será siempre un factor crítico de éxito. Muchas veces a primera vista los objetivos de seguridad de la información parecen contraponerse a los de proyectos de desarrollo de software o plataforma, pues los directivos ven como una traba consideraciones de seguridad y formalismos que impone la seguridad de la información. Sin embargo a la larga el no considerar aspectos de seguridad de la información puede invalidar meses de trabajo en desarrollo de software o implementación de plataforma al surgir la necesidad de escribir módulos o cambiar la configuración de plataforma debido a la necesidad de incorporar en forma tardía a los proyectos aspectos de seguridad de la información.

Para el caso de entidades públicas el tema del apoyo de las autoridades es aún más crítico dado que las iniciativas de seguridad de la información provienen de instancias superiores de gobierno externas a las instituciones. Se crean entonces, como en el caso de esta tesis, escenarios donde los proyectos de seguridad de la información pueden imponer restricciones a la implementación de otros programas de mejora de gobierno que tienen asignado un mayor peso global en las metas de la institución. En este trabajo, esta situación se mitigó con la utilización de herramientas de código abierto. Sin embargo el hecho que los proyectos de seguridad de la información no sean impulsados por las autoridades directoras del servicio, le quita peso a las iniciativas y complica el desarrollo de proyectos como el de la presente tesis.

Lo que observe en un principio fue una actitud aparentemente temeraria frente a los distintos tipos de riesgo tanto de seguridad de la información como de proyectos de desarrollo de software y plataforma. También una visión de conformismo expresada en resignación y dejando al azar lo que pudiera ocurrir. Al presentar una metodología de gestión de riesgos este enfoque rápidamente fue cambiando: el personal aceptaba la existencia de los riesgos y la posibilidad cierta de mitigarlos. Al asignar probabilidades de ocurrencia, niveles de impacto y determinar el riesgo residual, se pudo establecer estrategias, políticas y procedimientos de seguridad de la información al respecto. Además, como los riesgos fueron identificados y caracterizados en conjunto con el propio personal expuesto a los riesgos, hubo consenso en cuanto a las medidas a implementar.

La forma de trabajo, definida en torno a la creación de equipos constituidos por los propios dueños o encargados de los procesos organizacionales, tuvo un alto impacto positivo en la formulación e implantación de políticas y procedimientos de seguridad de la información. De esta manera ninguna política o procedimiento fue implantada sin lograr antes un consenso vertical y horizontal en la organización. Esta medida permitió además una importante disminución en los costos de desarrollo e implementación y no fue

necesario contratar talento externo a la organización, permitiendo que el personal se identificara con los resultados del SGSI.

Un aspecto relevante a destacar es la facilidad y fluidez que permitió la metodología de trabajo propuesta en esta tesis para implementar el SGSI dado que, a diferencia de intentos anteriores por implantar un SGSI, la visibilidad dada a las distintas etapas del proceso de implementación mediante el sistema de gestión documental y gestión de proyecto permitió en todo momento mantener una visión de conjunto por todos los involucrados, manteniendo la incertidumbre en un bajo nivel, lo que descomprimió el ambiente y evitó que el personal se sintiera amenazado al desconocer los alcances del cambio. Cambio que el propio personal pudo implementar dada la metodología participativa que utilizamos para crear las políticas y procedimientos y la visibilidad y simplicidad aportada por Kanban.

PMG de Seguridad de la Información.

La presente tesis estaba enmarcada en un programa de mejora de gobierno, ello implico entregar los antecedentes de todo el trabajo realizado a DIPRES para la evaluación del PMG de seguridad de la información. El sistema de evaluación de DIPRES es binario, se aprueba con todos sus requisitos o es rechazado aun cuando solo uno de sus requisitos no se cumpla. DIPRES aprobó el PMG de seguridad de la información correspondiente a la presente Tesis

6.2 TRABAJO FUTURO

Dado que esta tesis se desarrolló en conformidad con un programa de mejora de gobierno, en forma gradual y en base a la disponibilidad de presupuesto del servicio, se cumplieron los 44 objetivos de control que priorizo el análisis de riesgos realizado. Sin embargo la meta final al 2019 es la implementación completa de los 114 objetivos de control indicados en la norma ISO27001:2013, para ello es fundamental el papel que cumple el SGSI diseñado y puesto en marcha durante la presente tesis, al dar gobernanza a la seguridad de la información y permitir la mejora continua en base a una evaluación de riesgos consistente ciclo a ciclo.

Para el siguiente ciclo de mejora continua del SGSI existe un grupo de objetivos de control prioritarios, que por presupuesto y tiempo no pudieron ser implementados en el actual ciclo, Estas objetivos de control normativo son:

- ✓ *A.8.3 Manejo de los soportes de almacenamiento.*
  - *8.3.1 Gestión de soportes extraíbles.*
  - *8.3.2 Eliminación de soportes.*
  - *8.3.3 Soportes físicos en tránsito.*
- ✓ *A.16 Gestión de incidentes de seguridad de la información.*
  - *16.1.3 Notificación de puntos débiles de la seguridad.*

- *16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.*
- *16.1.5 Respuesta a los incidentes de seguridad.*
- *16.1.6 Aprendizaje de los incidentes de seguridad de la información.*
- *16.1.7 Recopilación de evidencias.*

✓ *A.10.1 Controles criptográficos.*

- *10.1.1 Política de uso de los controles criptográficos.*
- *10.1.2 Gestión de claves.*

✓ *A17.1 Continuidad de la seguridad de la información.*

- *17.1.1 Planificación de la continuidad de la seguridad de la información.*
- *17.1.2 Implantación de la continuidad de la seguridad de la información.*
- *17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad*
- *de la información.*

✓ *A17.2 Redundancias.*

- *17.2.1 Disponibilidad de instalaciones para el procesamiento de la*
- *información.*

No obstante la existencia de estos controles prioritarios, no exime a la metodología implementada de realizar una análisis de riesgos para seleccionar cuales controles implementar, mejorar o complementar.

Baja o Disposición de la Información

Otro punto importante que debe ser abordado es la evaluación de los procedimientos de tratamiento de la información que es dada de baja. Al momento de realizar esta tesis, una empresa externa realizaba estudios paralelos al programa de mejora de gobierno de seguridad de la información, centrados en la creación de procedimientos orientados a la destrucción de información. Por esta razón y a petición de estamentos superiores de la Subsecretaría, el SGSI propuesto en esta tesis no tocó ningún punto referente a la disposición o baja de la información, con el objetivo que en el año 2016, cuando los procesos de disposición de la información estuvieran implementados por la empresa externa, el SGSI los incorporara a su siclo de mejora continua, aplicando los criterios de la cláusula normativa A.8.3 Manejo de los soportes de almacenamiento.

Desarrollo de sistemas de apoyo a la gestión

Para afinar nuestras capacidades para identificar y cuantificar riesgos y así diseñar planes de mitigación más eficientes, identificamos dos desarrollos prioritarios, un sistema de información de riesgos y un datawarehouse

El desarrollo de un sistema de información de riesgos, basado en el documento técnico N70 de CAIGG, nos permita administrar los riesgos asociados a los activos de información para sustituir la panilla Excel que se utilizó en el desarrollo de esta tesis, la cual presenta inconvenientes de actualización y no tiene todas las características de facilidad de consulta que son requeridas. Por ejemplo si desea cambiar el responsable o propietario de un activo de información, la búsqueda y la modificación en todas las entradas de la planilla lo torna engorroso.

La construcción de un Datawarehouse con la información de la base de datos GLPI permitirá realizar análisis de multidimensionales, alimentar indicadores de incidentes, tiempos de respuesta, dar apoyo específico a la cláusula: A.16.1.5 Respuesta a los incidentes de seguridad y construir un modelo de minería de datos.

Sensibilización

Ambas auditorias hicieron hincapié en la necesidad de difundir los procedimientos y políticas de seguridad de la información a toda la organización. Al respecto, la institucionalización de la seguridad de la información sigue siendo el gran pendiente del SGSI que se ha implementado en la subsecretaria de economía. Si bien hicimos videos explicativos y se utilizaron plataformas de auto aprendizaje, lamentablemente la enseñanza presencial solo fue utilizada para dar a conocer los objetivos y temas centrales de la seguridad de la información a las partes directamente involucradas y no a toda la organización como había sido recomendado. Esto se dio así por un tema presupuestario. Dado que si bien DIPRES exige la implementación de un SGSI bajo la norma ISO27001:2013 no asigna presupuesto y no lo considera dentro de los procesos transversales de la organización, lo que además se agrava por su bajo peso de los proyectos de seguridad de la información en el cumplimiento de los programas de mejora de gobierno.

Cambio cultural de autoridades

Es el punto pendiente más delicado, en toda mejora de procesos siempre se hace referencia a lo vital que es tener el apoyo del más alto nivel jerárquico posible. En las experiencias de proyectos de seguridad de la información en que he participado en la empresa privada, dada la necesidad de recursos, un proyecto de este tipo solo es posible emprenderlo si se tiene el apoyo de la gerencia expresado asignación de presupuesto, en palabras simples si no hay fondos no hay proyecto. En las empresas públicas este tipo de proyectos que viene designados desde la presidencia, no cuentan con la comprensión de los directores del servicio pues "no tienen tiempo" y los proyectos de seguridad de la información terminan haciéndose sin un presupuesto asignado y tampoco son considerados como parte de la cartera de proyectos. Esto acaciana que muchas

reuniones se posterguen, que los equipos y software necesarios no estén a tiempo. Lamentablemente este cambio cultural solo se da cuando ocurren catástrofes con la información como ocurrió en MINSAL con la filtración de fichas clínicas o en el Ministerio de Relaciones Exteriores cuando se modificó la página de inicio institucional.

Estudiar él porque de esta cultura de corto plazo que solo responde a eventos, escapa de los alcances de esta tesis, pero si la seguridad de la información ha de cumplir sus objetivos, es fundamental que estudiemos formas que realmente aseguren la concurrencia necesaria de nuestras autoridades, con la creación de un ente público que coordines las iniciativas de SGSI de manera transversal a todos los organismos públicos a diferencia como ocurre hoy en día, que dos funcionarios públicos están encargados de coordinar los SGSI de todos los servicios públicos. Ello ocasiona por ejemplo que si un servicio solicita una reunión de coordinación esta puede tardar meses en concretarse, las consultas vía correo electrónico también toman meses. A lo anterior debemos señalar que no existe una política de gobiernos en torno a la seguridad de la información más allá de instruir a los organismos públicos que deben implementar la norma ISO27001.

GLOSARIO

CAIGG: Consejo de Auditoria General de Gobierno.

CORFO: Corporación de Fomento de la Producción.

CSI: Comité de Seguridad de la Información.

DIPRES: Dirección de Presupuesto Ministerio de Hacienda.

EMT: Empresas de Menor Tamaño.

MIPYME: Micro, Mediana y Pequeña Empresa.

OSI: Oficial de Seguridad de la Información.

PMG: Programa de Mejora de Gobierno.

PYME: Pequeña y Mediana Empresa.

SGSI: Sistema de Gestión de Seguridad de la información

BIBLIOGRAFÍA

1) *Alexander, Alberto G., Diseño de un Sistema de Gestión de Seguridad de Información, Bogotá, Colombia, Marcombo.*
2) *Andrés Molina. "Definición y validación de un proceso de gestión de seguridad de la información para la empresa Amisoft". Tesis de Magister en Tecnologías de la Información, Departamento de Ciencias de la Computación, Universidad de Chile. Septiembre, 2015.*
3) *Jakob Freund, Bernd Rucker, Bernhard Hipass, BPMN2.0 Manual de referencia y guía práctica, Depto. Informática Universidad Técnica Federico Santa María Edición hispana, cuarta edición Santiago de chile 2014, Gestión de Procesos Orientada a los Resultados, Primera Edición Brasilia 2013.*
4) *Bruno Plavarini, Claudia Quezado.*

Estándares

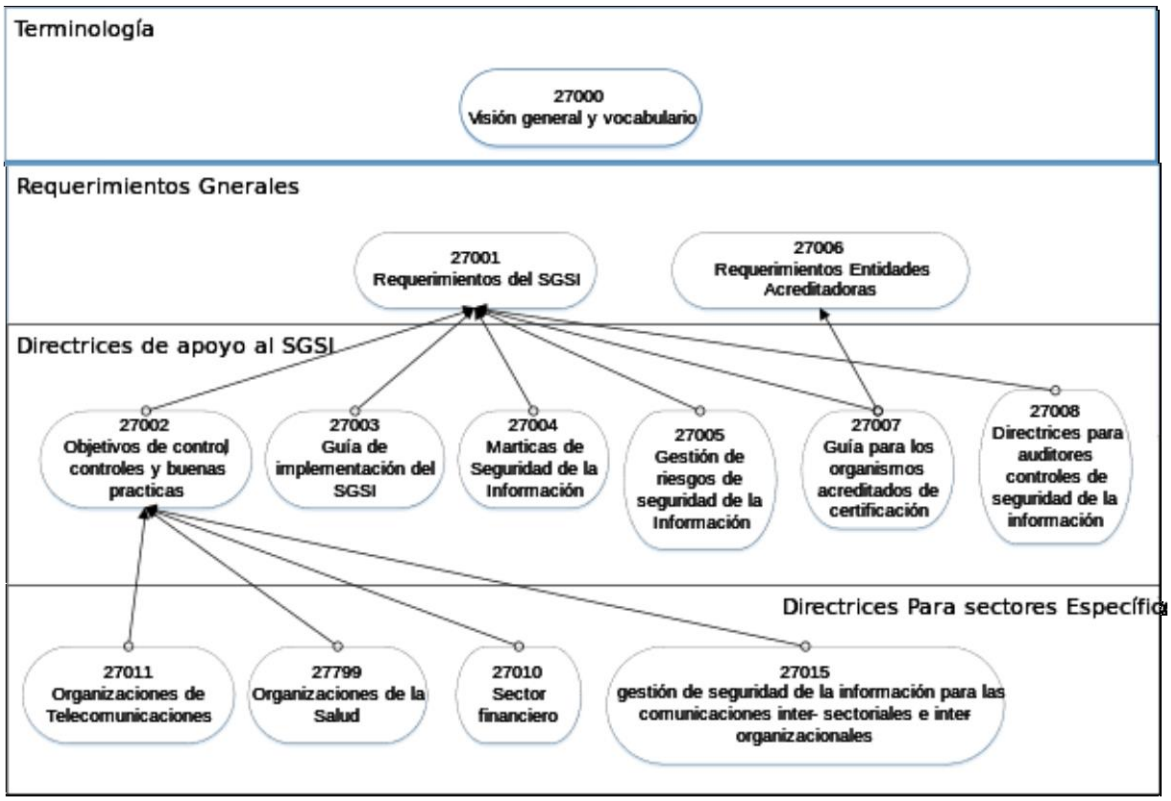
1) Project Management Institute, PMBOK*, Pensilvania, EE.UU.y, Project Management Institute, Inc.*
2) CAIGG*, Implantación, Mantención y Actualización del Proceso de Gestión de Riesgos en el Sector Público, Santiago, Chile, MINISTERIO SECRETARÍA GENERAL DE LA PRESIDENCIA.*
3) IRAM ISO/IEC*, Gestión de la seguridad de la información-Medición ISO27002, Buenos Aires, Argentina*
4) INN ISO/IEC*, Tecnología de la información – Técnicas de seguridad - Sistemas de gestión de la seguridad de la información Requisitos,Chile*
5) BSI ISO/IEC*, Information technology - Security techniques - Code of practice for information security controls ISO27003, Second edition 2013-10-01, UK*
6) BSI ISO/IEC*, Information Technology – Security Techniques Information Security Risk Management, First Edition 2008-06-15, UK.*
7) NTC ISO/IEC*, Gestión del Riesgo Principios y Directrices ISO3100, Editada 2014-12-19, Colombia*
8) BSI ISO/IEC, *Information technology — Security techniques — Information security management systems Overview and vocabulary, Third edition 2014-01-15, UK*

ANEXOS

La siguiente sección contiene documentación y referencias que explican de manera detallada los elementos de la metodología que se utilizó para el diseño e implementación del SGSI. Se muestran pantallas de los componentes del SGSI y se expone en forma íntegra la Política general de seguridad de la información, por ser este documento el más importante pues toda política y procedimientos actual o futuro debe necesariamente estar subordinado a ella.

Por razones de seguridad se ocultan nombres de servidores, elementos de red, sistemas de seguridad y no se muestra una lista de vulnerabilidades detectadas durante la gestión de riesgos, tanto de plataforma como de perímetro de seguridad

ANEXO A CONJUNTO DE NORMAS ISO27000



En el esquema se aprecia la relación entre las normas que componen las Normas ISO/IEC 27000.

Establecimiento Del Contexto

Esta fase es genérica a muchas normas ISO y concuerda con los objetivos de la fase de establecimiento del contexto organizacional de la ISO27001 y su objetivo es conocer la organización.

Identificación de Riesgos

En esta etapa corresponde al levantamiento de los riesgos que pueden afectar a los activos de la información, ello presume que con anterioridad o en paralelo se han identificado los activos de información, de este modo para cada activo de información se identifican las amenazas a las que está expuesto, sus vulnerabilidades

Análisis de Riesgos

La Guía técnica N°70 indica: "*Las Organizaciones Gubernamentales después de desarrollar la identificación de riesgos operativos, deben analizarlos, examinando los riesgos en relación a su probabilidad y consecuencias. A su vez, los controles deben ser analizados en términos de efectividad, para finalmente identificar el nivel de exposición al riesgo por proceso, subproceso, etapa y riesgo específico*"

Esta etapa corresponde a la valoración experta (juicio de los expertos de cada área) de la probabilidad de ocurrencia (ver cuadro 1) de un riesgo y el impacto (ver Cuadro 2) que este tendría sobre la disponibilidad, confidencialidad o integridad de un activo de información.

Categoría	Valor	Descripción
Casi certeza	5	Riesgo cuya probabilidad de ocurrencia es muy alta, es decir, se tiene un alto grado de seguridad que éste se presente en el año en curso. (90% a 100%).
Probable	4	Riesgo cuya probabilidad de ocurrencia es alta, es decir, se tiene entre 66% a 89% de seguridad que éste se presente en el año en curso.
Moderado	3	Riesgo cuya probabilidad de ocurrencia es media, es decir, se tiene entre 31% a 65% de seguridad que éste se presente en el año en curso.
Improbable	2	Riesgo cuya probabilidad de ocurrencia es baja, es decir, se tiene entre 11% a 30% de seguridad que éste se presente en el año en curso.
Muy improbable	1	Riesgo cuya probabilidad de ocurrencia es muy baja, es decir, se tiene entre 1% a 10% de seguridad que éste se presente en el año en curso.

Cuadro 1 Cuadro de Probabilidad de ocurrencia de Riesgos (fuente CAIGG N°70)

La escala cualitativa va desde la casi certeza hasta muy improbable y se le asignan valores numéricos para poder realizar los cálculos necesarios para el análisis de riesgos.

Categoría	Valor	Descripción
Catastróficas	5	Riesgo cuya materialización puede generar pérdidas financieras ($) que tendrán un impacto catastrófico en el presupuesto y/o comprometen totalmente la imagen pública de la organización y del Gobierno. Su materialización dañaría gravemente el desarrollo del proceso y el cumplimiento de los objetivos, impidiendo finalmente que estos se logren en el año en curso.
Mayores	4	Riesgo cuya materialización puede generar pérdidas financieras ($) que tendrán un impacto importante en el presupuesto y/o comprometen fuertemente la imagen pública de la organización y del Gobierno. Su materialización dañaría significativamente el desarrollo del proceso y el cumplimiento de los objetivos, impidiendo que se desarrollen total o parcialmente en forma normal en el año en curso.
Moderadas	3	Riesgo cuya materialización puede generar pérdidas financieras ($) que tendrán un impacto moderado en el presupuesto y/o comprometen moderadamente la imagen pública de la organización y del Gobierno. Su materialización causaría un deterioro en el desarrollo del proceso dificultando o retrasando el cumplimiento de sus objetivos, impidiendo que éste se desarrolle parcialmente en forma normal en el año en curso.
Menores	2	Riesgo cuya materialización puede generar pérdidas financieras ($) que tendrán un impacto menor en el presupuesto y/o comprometen de forma menor la imagen pública de la organización y del Gobierno. Su materialización causaría un bajo daño en el desarrollo del proceso y no afectaría el cumplimiento de los objetivos en el año en curso.
Insignificantes	1	Riesgo cuya materialización no genera pérdidas financieras ($) ni compromete de ninguna forma la imagen pública de la organización y del Gobierno. Su materialización puede tener un pequeño o nulo efecto en el desarrollo del proceso y que no afectaría el cumplimiento de los objetivos en el año en curso.

Cuadro 2 Categorías de impacto de Riesgos (fuente CAIGG N°70)

Valoración de Riesgos

En esta etapa se procede a realizar un ranking de los riesgos considerando su **severidad** que es la probabilidad de ocurrencia multiplicado por el impacto de la ocurrencia. De este cuadro se desprende que la categoría **impacto** tienen una mayor incidencia en el nivel de severidad asignado, puesto que, aunque la **probabilidad** de ocurrencia sea menor, al tratarse de riesgos con impactos altos, cualquier materialización del riesgo, tendrá consecuencia significativa en la disponibilidad, integridad o confidencialidad del activo de información bajo estudio.

NIVEL PROBABILIDAD (P)	NIVEL IMPACTO (I)	SEVERIDAD DEL RIESGO S = (P x I)
Casi Certeza (5)	Catastróficas (5)	EXTREMO (25)
Casi Certeza (5)	Mayores (4)	EXTREMO (20)
Casi Certeza (5)	Moderadas (3)	EXTREMO (15)
Casi Certeza (5)	Menores (2)	ALTO (10)
Casi Certeza (5)	Insignificantes (1)	ALTO (5)
Probable (4)	Catastróficas (5)	EXTREMO (20)
Probable (4)	Mayores (4)	EXTREMO (16)
Probable (4)	Moderadas (3)	ALTO (12)
Probable (4)	Menores (2)	ALTO (8)
Probable (4)	Insignificantes (1)	MODERADO (4)
Moderado (3)	Catastróficas (5)	EXTREMO (15)
Moderado (3)	Mayores (4)	EXTREMO (12)
Moderado (3)	Moderadas (3)	ALTO (9)
Moderado (3)	Menores (2)	MODERADO (6)
Moderado (3)	Insignificantes (1)	BAJO (3)
Improbable (2)	Catastróficas (5)	EXTREMO (10)
Improbable (2)	Mayores (4)	ALTO (8)
Improbable (2)	Moderadas (3)	MODERADO (6)
Improbable (2)	Menores (2)	BAJO (4)
Improbable (2)	Insignificantes (1)	BAJO (2)
muy improbable (1)	Catastróficas (5)	ALTO (5)
muy improbable (1)	Mayores (4)	ALTO (4)
muy improbable (1)	Moderadas (3)	MODERADO (3)
muy improbable (1)	Menores (2)	BAJO (2)
muy improbable (1)	Insignificantes (1)	BAJO (1)

Cuadro 3 Nivel de Severidad del Riesgo (fuente CAIGG N°70)

Tratamiento de Riesgos de Seguridad de la Información

Antes de considerar el tratamiento de un riesgo, la organización debe decidir criterios para determinar si los riesgos pueden ser aceptados. Por ejemplo, si se considera que un riesgo tiene una baja probabilidad de ocurrencia y su impacto es menor, la organización puede decidir que no es económicamente rentable el desarrollo de un proceso de mitigación del riesgo. La estrategia global descritas por el documento técnico N°70 del CAIGG para lidiar con los riesgos son: evitar, reducir, compartir y aceptar y corresponde a una decisión estratégica de la organización que debe ser documentada en la política general de gestión de riesgos.

Monitoreo y Revisión

Para esta fase del Proceso de Gestión de Riesgos, la organización debe establecer formalmente el monitoreo y formular estructuras de reportes útiles a la organización, que le permita a la dirección, obtener información relevante, en forma oportuna y periódica sobre el estado de los riesgos en cualquier etapa del proceso.

Este monitoreo es consistente con las directrices de La ISO27001:2013 en su cláusula especifica 9.1, medición, análisis y evaluación:

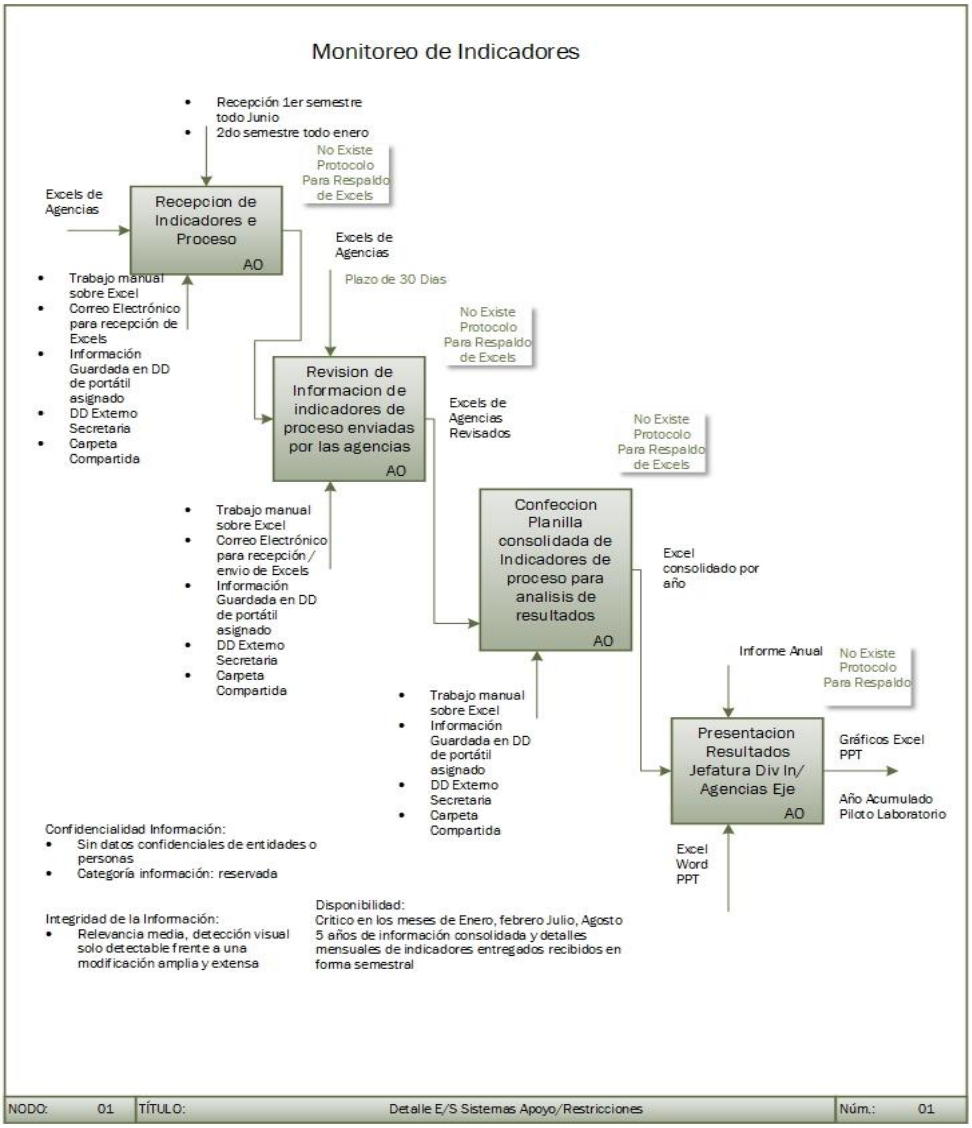
"La organización debe evaluar el desempeño de la Seguridad de la Información y la efectividad del sistema de gestión de la seguridad de la información

Comunicación

El objetivo fundamental de esta fase es entregar información confiable sobre el proceso de Gestión de Riesgos, para asegurar que los responsables de la implementación de las políticas y Procesos de Seguridad de la Información seleccionados producto de la aplicación del proceso de gestión del riesgo comprendan las bases que han servido para tomar las decisiones y las razones por las que son necesarias determinadas acciones.

ANEXO C IDENTIFICACIÓN DE INFORMACIÓN CON IDEF0,

En el ejemplo se muestra la información levantada del proceso FIC para realizar las tareas de monitoreo de indicadores de desempeño de los fondos de inversión para la competitividad. El centro del modelado, no está en determinar los flujos de información, sino en identificar la información que se utiliza produce y almacena en el proceso. Esta información corresponde a lo que hemos llamado Activos de información Primarios y es la base para el análisis descendente para la identificación de los activos de información que implementan, mantienen, modifican, almacenan la información.



ANEXO D INFORME DE BRECHAS PMG-SSI 2015

INFORME DE BRECHAS PMG-SSI 2015

Contenido

1. Introducción

En el año 2012 se diseñó un conjunto de controles en conformidad con la norma ISO27001:2005. Sin embargo, el sistema de seguridad de la información 2012 no logró resultados permanentes y fue abandonado, pues no se continuó haciendo seguimiento a los procesos de gestión de riesgos, no se institucionalizó la seguridad de la información ya que las políticas y controles solo quedaron definidos en papel, no encontrándose evidencia de su aplicación. Agravante a lo expuesto, es que la documentación del SSI-2012 esta desactualizada, incompleta en formato imagen de baja calidad lo cual dificulta su lectura y reproducción.

Creemos a la luz del estudio aportado por la realización PMG-SSI 2015, que el problema de abandono del SSI 2012, radicó principalmente, en la falta de una visión sistémica de procesos, dado que la iniciativa solo se centró en la escritura de controles indicados en el anexo A de la norma sin considerar la estructura organizativa del **Sistema de Gestión de Seguridad de la Infurción (SGSI)** y la institucionalización de políticas, procesos y controles de seguridad de la información.

La realización del PMG-SSI 2015, nos permitió identificar los elementos base para definir un sistema de gestión de seguridad de la información (SGSI) que va mucho más allá de la aplicación de los controles definidos en la norma en el "anexo A" e implica la definición de un conjunto de procesos de administración de la estructura organizacional que mantenga la dinámica de la seguridad de la información con un enfoque en la gestión de riesgos de los procesos organizacionales y en la información que permite la ejecución de estos. Importante para lograr este enfoque amplio, fue seguir los lineamientos de la norma ISO27003 que detallan como implementar la norma ISO27001:2013 y los lineamientos del CAIGG para gestión de riesgos Documento Técnico N° 70 en base a la norma ISO31000.

Con estos antecedentes establecimos el alcance inicial del SGSI al proceso estratégico Fondo para la Innovación Concursable FIC, para obtener la experiencia en la aplicación del modelo de gestión de riesgos, así como identificar los activos y, establecer las bases administrativas para la configuración del SGSI que nos permita:

- Seguir una hoja de ruta coherente para implementar la estructura administrativa y el conjunto de procesos y controles que constituyen el SGSI definido en la Norma ISO27001:2013 para proteger convenientemente la información y procesos que la recolectan, procesan, almacenan y distribuyen, frente a amenazas

- Evidenciar que los riesgos que ponen en peligro a la propia información, afectan la continuidad de los niveles de servicio, rentabilidad social y conformidad legal, necesarios para alcanzar los objetivos institucionales.

- Implementar un sistema que gestione la seguridad de la información, de manera que la Subsecretaría cumpla con la normativa ISO 27001:2013 y que a su vez, institucionalice la mejora continua de los procesos que componen el SGSI en apoyo a los procesos operacionales y estratégicos de la organización.

2. Brechas.

Actualmente del SSI que se implementó el 2012 bajo na norma ISO27001:2005, existen 34 procedimientos y 5 políticas que corresponden a 31 controles de la norma ISO27001:2013. Sin embargo estos procedimientos y políticas presentan los siguientes inconvenientes:

- Los documentos originales se perdieron.
- Solo existen copias en formato imagen.
- Los documentos no son de conocimiento del personal al cual están dirigidos.
- No han sido revisados ni actualizados desde el año 2012.
- No existe certeza si son las versiones finales.
- Los proceso actuales no se rigen por lo establecido en estas políticas y procesos
- No se encuentran firmados por la autoridad

Por estas razones se decidió utilizar estos documentos sólo como referencia para la implementación de los controles al estándar ISO27001:2013 y no como evidencia de la conformidad a la norma.

Procedimientos rescatados SSI-2012

DOCUMENTO	CONTROL
PR007 Procedimiento respaldo de usuarios.pdf	12.3.1 Copias de seguridad de la información
PR008 Procedimiento de acción contra código malicioso.pdf	12.2.1 Controles contra el código malicioso
PR009 Procedimiento de Control de Cambios.pdf	14.2.2 Procedimientos de control de cambios en los sistemas
PR011 Procedimiento para Asignar y Restringir el Acceso a los Proyectos de Desarrollo.pdf	14.2.6 Seguridad en entornos de desarrollo.

PR012 Procedimiento de Manipulación de Activos de Información 1.0.pdf	8.1.3 Uso aceptable de los activos.
PR013 Operación para Auditorías regulares de Servicios de Terceros.pdf	15.2.1 Supervisión y revisión de los servicios prestados por terceros
PR014 Protocolo de Salida de Bienes.pdf	8.2.3 Manipulación de activos
PR015 Procedimiento recepción de bienes informáticos.pdf	8.2.3 Manipulación de activos
PR016 Procedimiento Administración de Licencias.pdf	18.1.2 Derechos de propiedad intelectual (DPI).
PR017 Procedimiento Uso de Medios Removibles.pdf	8.3.1 Gestión de soportes extraíbles
PR018 Procedimiento para Informar y Exigir el Cumplimiento de los Requerimientos de Seguridad.pdf	7.2.2 Concienciación, educación y capacitación en seguridad de la información. 7.2.3 Proceso disciplinario.
PR019 Anexo Gestión de Incidentes de Seguridad.pdf	16.1.2 Notificación de los eventos de seguridad de la información.
PR020 Procedimiento de Almacenamiento y Respaldo.pdf	12.3.1 Copias de seguridad de la información.
PR021 Procedimiento Prueba de Respaldo.pdf	12.3.1 Copias de seguridad de la información.
PR022 Procedimiento de Acceso a la Información (Sistemas).pdf	9.2.1 Gestión de altas/bajas en el registro de usuarios
PR023 Procedimiento acceso a servicios de informacion.pdf	9.2.2 Gestión de los derechos de acceso asignados a usuarios
PR024 Procedimiento de Resguardo de los Registros.pdf	12.4.2 Protección de los registros de información
PR025 Procedimiento Elaboración Credenciales.pdf	9.2.4 Gestión de información confidencial de autenticación de usuarios
PR027 Procedimiento de Mantención del Equipamiento (Datacenter).pdf	11.2.4 Mantenimiento de los equipos
PR028 Procedimiento de Control de Cambios para la infraestructura TI.pdf	12.1.2 Gestión de cambios
PR029 Procedimiento para Proteger las Trasferencias de Información entre los Sistemas de Negocio.pdf	13.1.2 Mecanismos de seguridad asociados a servicios en red.
PR030 Procedimiento de Operaciones.pdf	12.1.1 Documentación de procedimientos de operación
PR031 Sincronización hora exacta.pdf	12.4.4 Sincronización de relojes.

PR032 Procedimiento Controles Criptográficos.pdf	10.1.1 Política de uso de los controles criptográficos.
PR033Procedimiento de Operación de Servicios de Terceros.pdf	15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores
PR034 Procedimiento de Monitoreo de Sistema de Operaciones y Sistemas.pdf	12.4.1 Registro y gestión de eventos de actividad.
PR035 Anexo Procedimiento Baja de Equipamiento informático.pdf	8.3.2 Eliminación de soportes.
PR036 Procedimiento Desvinculación.pdf	7.3.1 Cese o cambio de puesto de trabajo.
PR037 Procedimiento de Detección Automática y Autenticación de Equipos en la Red.pdf	9.1.2 Control de acceso a las redes y servicios asociados.
PR038 Provisión de Servicios de Terceros.pdf	15.2.1 Supervisión y revisión de los servicios prestados por terceros
PR040 Procedimiento de autorización para cambios y trazabilidad de los sistemas de procesamiento.pdf	14.2.2 Procedimientos de control de cambios en los sistemas
PR041 Procedimiento de Protección y Manejo Adecuado de la Información de Mensajería Electronica.pdf	14.2.2 Procedimientos de control de cambios en los sistemas
PR042 Procedimiento de Uso de Medios de Computación y Comunicación Móvil.pdf	6.2.1 Política de uso de dispositivos para movilidad.

Políticas

PO001 Política Control de Cambios.pdf	12.1.2 Gestión de cambios.
PO002 Política de Seguridad de Redes Informáticas v 1.2.pdf	9.1.2 Control de acceso a las redes y servicios asociados.
PO003 Política de Uso Aceptable de Recursos Informáticos v 1.2.pdf	8.1.3 Uso aceptable de los activos.
PO004 Política de Escritorio y Pantalla Limpia.pdf	11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.
PO005 Política Control de Acceso Lógico.pdf	9.1.1 Política de control de accesos

3. Plan de acción.

3.1. Generalidades

Indicamos a continuación, los compromisos para el 2016, relativos a los controles y políticas que se realizarán como parte de las actividades para implementar el SGSI en cumplimiento con los todos los "debes" de las cláusulas:

- **4 Contexto de la organización**
- **5 Liderazgo**
- **6 Planificación**
- **7 Apoyo**
- **8 Operación**
- **9 Evaluación de desempeño**
- **10 Mejora**

Todas estas cláusulas conforman la estructura organizativa del SGSI según lo indica la norma ISO27001:2013

3.2. Alcance del SGSI

Como lo expresa la Norma ISO27001:2013 en su punto "4.3 Determinar el alcance del sistema de gestión de la seguridad de la información" y en vista de los antecedentes entregados. La implementación de la norma ISO27001:2013 para nuestro caso no es una continuidad de lo realizado el 2013 de la norma ISO27001:2005, sino una implementación desde el cero.

Se ha definido como alcance del SGSI para 2016 el proceso estratégico FIC, dado la importancia estratégica para la subsecretaría de economía, por ser una meta alcanzable y realista que nos permitirá, posteriormente, en los planes del 2017, ir cubriendo con el alcance del SGSI los demás procesos estratégicos.

3.3. Implementación de Controles Anexo A NCHISO27001:2013

Del análisis los procesos y tareas propios del proceso FIC realizados sobre en base a la matriz de riesgos en conformidad lineamientos de las normas ISO27001:2013 y al documento técnico N°70 del CAIG sobre Gestión de Riesgos NCHISO31000 bajo el marco del PMG-SSI2015, se identificaron los siguientes controles a implementar durante el 2016:

A5.1.1 Políticas de seguridad de la información.

A5.1.2 Revisión de políticas para la seguridad de la información.

A6.1.1 Roles y responsabilidades para la segur de la información.

A6.1.2 Segregación de tareas.

A6.1.3 Contacto con las autoridades.

A6.2.1 Política de dispositivos Móviles.

A6.2.1 Política de dispositivos Móviles.

A6.2.2 Política de Teletrabajo.

A7.1.1 Selección.

A8.1.1 Inventario de activos.

A8.1.4 Devolución de activos.

A9.1.1 Política de control Acceso.

A9.1.2 Política acceso a las redes y los servicios de red.

A9.2.2 Gestión de los derechos de acceso asignados a usuarios.

A9.2.4 Gestión de información confidencialidad de autenticación de usuarios.

A9.2.5 Revisión de los derechos de acceso a los usuarios.

A9.4.2 Procedimientos seguros de inicio de sesión.

A11.1.1 Perímetro de seguridad física.

A11.2.1 Emplazamiento y protección de equipos.

A11.2.3 Seguridad del Cableado.

A11.2.4 Mantenimiento de los equipos.

A11.2.7 Seguridad en la reutilización o descarte de equipos.

A11.2.8 Equipo de usuario desatendido.

A12.1.1 Procedimientos de operación documentación.

A12.3.1 Copias de seguridad de la información (Política de Respaldo de información).

A12.4.2 Protección de los registros de información.

A12.4.4 Sincronización de relojes.

A12.5.1 Instalación del software en sistemas operacionales.

A13.1.1 Controles de red.

A13.1.2 Mecanismos de seguridad asociados a servicios en red.

A13.1.3 Segregación de redes.

A14.2.1 Política de desarrollo seguro de software.

A14.2.2 Procedimientos de control de cambios en los sistemas.

A15.1.1 Política de seguridad de la información para suministradores.

A15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.

A15.2.1 Supervisión y revisión de los servicios prestados por terceros.

A15.2.2 Gestión de cambios en los servicios prestados por terceros.

A16.1.2 Informe de los eventos de seguridad de la información.

A18.1.1 Identificación de la legislación vigente y los requisitos contractuales.

A18.1.3 Protección de los registros.

A18.1.4 Protección de datos y privacidad de la información personal.

ANEXO E ACTA CONSTITUCIÓN DE PROYECTO DE MONITOREO.

ACTA DE CONSTITUCIÓN DEL PROYECTO	
VERSION: 1.1	*FECHA REVISION : 18-junio-2015*
La aprobación de la presente acta de constitución del proyecto indica el entendimiento del propósito y contenido descrito en el presente documento, sus referencias y anexos. La firma de este documento, implica la conformidad de cada individuo con el mismo.	
Nombre del proyecto:	Sistema de Monitoreo Unificado
Cliente:	División de Desarrollo y Tecnología
Patrocinadores	Sub- Secretaria de Economía, Jefe de división Tecnológica.
Director del proyecto	Jefe Área Seguridad
Hito Iniciación	Aceptación por parte del cliente del acta
Descripción breve del proyecto	Revelar información del estado actual de la red de datos, para entender los problemas de comunicación existente, para buscar las mejores alternativas de solución.
Interesados	Sub-Secretaria de Economía y EMT.
Entregables	Informe levantamiento Estado Actual de la Red (Contingencia). Propuesta de Solución. Monitoreo constante a la red y servicios específicos.

Definición Del Proyecto

Enunciado del Problema

Contingencia.
Existe un problema de Red en el Backbone comprendido entre los pisos 01, 10, 11, 12.- Este problema genera una fuerte degradación en los servicios de red, afectando directamente a Internet, impresión, telefonía IP, etc. Por este motivo se ve afectado el trabajo diario de los usuarios de la plataforma.

La plataforma RES debe cumplir con las exigencias de cumplimiento en la norma ISO 27001 en el punto 9, y el Anexo A.12.4. Con esto se estaría dando cumplimiento a lo expresado en el PMG SSI 2015.

Descripción del Proyecto

Realizar el levantamiento de la situación actual del estado de la red. Construir una infraestructura de monitoreo constante para los dispositivos de red contenidos en el Backbone de los pisos 01, 10, 11, 12 de la Sub-Secretaria Economía y EMT. Identificar los problemas que afectan a los servicios, y recopilar la mayor cantidad de información para documentar dicho proceso.

Implementar sistemas de monitoreo que permitan cumplir con la normativa y generar valor agregado. (Nagios mas Cacti Y Zabbix)

Metas y Objetivos del Proyecto

- Implementar un sistema de monitoreo que ayudara a la detección y corrección de problemas de comunicación existente en la red de la Sub-Secretaria de Economía y EMT.
- Entregar una infraestructura de Monitoreo para a los dispositivos de comunicación en la Sub-Secretaria de Economía y EMT.
- Brindar el servicio de monitoreo para servidores y servicios de la Sub-Secretaria de Economía y EMT, incluyendo la plataforma RES (ResDB y ResWEB).
- Mantener informado del estado de la plataforma de forma periódica al departamento TI (y a los departamentos involucrados si fuera el caso).

Requisitos del proyecto

Los requisitos aportados por el cliente son:

- Un servidor para instalar los Software de Monitoreo.
  - Con un procesador de a lo menos dos núcleos.
  - Que cuente con unos 8 Gigas de RAM.
  - Un Espacio en disco no menor a 20 Gigas.
  - El servidor puede ser virtual o físico.
- Una estación de trabajo con un equipo acorde para las necesidades de las tareas a desempeñar.
  - Un escritorio de trabajo para el Analista que trabajara en los procesos de monitoreo
  - Un computador de escritorio o portátil que cuente con:
    - Un procesador mayor o igual a I5.
    - Que tenga a lo menos 4 Gigas de RAM
    - Y un disco de unos 150 Gigas para el sistema operativo, y un disco D para datos.
    - Tarjeta de red inalámbrica.
- Un Monitor grande o un televisor para proyectar la infraestructura de Monitoreo que cuente con dispositivo ChromeCast.
- Un Ingeniero de Redes para desempeñar el cargo de Analista, el cual estará dedicado a realizar labores de levantamiento, instalación, y monitoreo de la plataforma.

Alcance del Proyecto

El Proyecto Incluye:
• Levantamiento de situación actual de la Red de datos, enfocado en el Backbone de la Sub-Secretaria de Economía y EMT. • Mejoramiento de la infraestructura de Red de Datos. • Monitoreo constante para dispositivos de red contenidos en el Backbone de la Sub-Secretaria de Economía y EMT, servidores y servicios incorporados a servicio de Monitoreo como por ejemplo los servidores de RES y su portal www.empresaenundia.cl • Creación de informes frente a anomalías, detectadas he informadas por la plataforma de monitoreo. • Constante planteamiento de mejoras en procedimientos y servicios de la red de datos. • Entrega de informes de monitoreo a pedido por temas específicos.

El Proyecto no Incluye:
• Servicio 7 por 24. Solo se realizara monitoreo en horario hábil de 09:00 am a 18:00 pm. • La soluciones propuesta no necesariamente considera horas para realizar las actividades de mejoras en la red de datos o la infraestructura de red presente.. • Trabajo directo sobre los equipos, como por ejemplo: - Cambios de configuraciones. - Modificaciones de topología en el caso de dispositivos de red. - Incorporación de Equipos para el servicio de monitoreo..

Factores Críticos de Éxito

Los factores críticos para este proyecto están dados por:

- Entrega de requerimientos mínimos de materias de trabajo,
  - Un servidor que cuente con el mínimo de hardware y software según sea solicitado.
  - Una estación de Trabajo con un hardware y software acorde a lo solicitado.
- Colaboración de las partes,
  - Colaboración de los departamentos del Área TI, para una entrega oportuna de información y accesos a los dispositivos o servicios a Monitorear.
  - Colaboración para la entrega de Datos y recolección de nuevos antecedentes si se requieren.
- El Servicio de Monitoreo depende del trabajo coordinado entre el Analista encargado de este proceso y administrador de plataforma de redes, y ó el administrador de servidores, dependiendo de lo que se requiera incorporar al servicio de Monitoreo.
- Contar con toda la información que se solicite, y apoyo de las partes involucradas para el éxito del proyecto.
- Divulgación parcial o total de aspectos del proyecto.

Suposiciones

- No hay suposiciones relevantes.

Restricciones

- Respetar los plazos y ceñirse a cronograma para alcanzar todos los ítems del proyecto.

Criterios de aceptación

- Debe haber una plataforma estable realizando monitoreo

EDT Inicial

Se muestra a continuación las principales actividades y productos que se espera obtener durante la ejecución del proyecto “Sistema Monitoreo Unificado”. El detalle de las actividades así como la duración individual de cada una de ellas está registrada en la carta Gantt de proyecto

Fase 1: Creación Plan de trabajo.

Productos esperados:

- Levantamiento estado actual de la red Sub-Secretaria Economía y EMT.
- Plan de trabajo para el Monitoreo de la red de Sub-Secretaria Economía y EMT.

Fase 2: Análisis de situación actual.

Producto esperado:

- Informe de situación actual con plan de sugerencia para mejoramiento.

Fase 3: Implementación de Monitoreo.

Producto esperado:

- Manual de Procedimientos para herramienta de monitoreo CACTI
- Manual de Procedimientos para herramienta de monitoreo Zabbix
- Manual de procedimientos para herramienta de monitoreo Nagios.
- Manual de Procedimiento Ubuntu 14.04 relacionado con el monitoreo.

Fase 3: Ingresar al Monitoreo dispositivos de red, servidores de desarrollo y servicios solicitados.

Producto esperado:

- Cargar al monitoreo de CACTI, ZABBIX, NAGIOS dispositivos de Red, servidores y servicios.
- Manual de procedimiento carga de host a plataforma CACTI y administración.
- Manual de procedimiento carga de host a plataforma ZABBIX y administración.
- Manual de procedimiento carga de host a plataforma NAGIOS y administración.
- Respaldos.

Fase 4: Incorporación monitoreo RES, en todas las herramientas de Monitoreo.

Producto esperado:

Incorporación al monitoreo de los servidores de la plataforma RES, con la finalidad que se encuentren en contante observación, y esto permita identificar anomalías rápidamente y en lo posible antes de que afecten el servicio. Generación de informes frente a anomalías detectadas.

Hitos Principales del Proyecto

Hito/Artefacto Entregable	Fecha Entrega
Acta constitución de proyecto	15 Julio 2015
Inicio Proyecto Monitoreo	24 Julio 2015
Entrega Plan del Proyecto	3 Julio 2015
Implementación de Monitoreo CACTI	10 Julio 2015
Implementación de Monitoreo NAGIOS: - Carga de dispositivos de red - Servidores de desarrollo - Servicios solicitados - Servidores de RES	17 Julio 2015
Implementación de Monitoreo ZABBIX: - Carga de dispositivos de red - Servidores de desarrollo - Servicios solicitados - Servidores de servicio RES.	24 Julio 2015

Hito/Artefacto Entregable	Fecha Entrega
Entrega documentación de situación actual: - Informe Técnico Situación Actual - Armado de Diagrama de Red actual - Solución Propuesta.	7 Agosto 2015
Entrega de informe Técnico de Situación actual.	10 Agosto 2015
Configuración de Switch HP para departamento de Networking	14 Agosto 2015
Informes de Monitoreo para Plataforma RES	17 Agosto 2015
Entrega de Informe Nagios NRPE	28 Agosto 2015
Realización de pruebas en NAGIOS con el plugins NRPE	1 Septiembre 2015
Documentación de NAGIOS NRPE con: - Windows Server 2008 R2 - Windows Server 2012 R2	14 Septiembre 2015
Documentación de NAGIOS NRPE con: - Linux Ubuntu Server 14.04	22 Septiembre 2015
Fin de Proyecto Monitoreo	24 Septiembre 2015

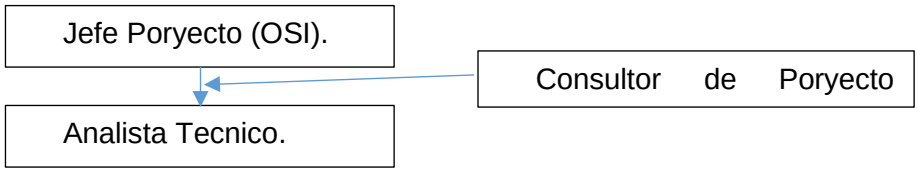
Estimación inicial de costes

La estimación de costes se realizará en base a los servicios prestados.

Horas Hombre	240
Licencias	No requeridas (uso software libre)
Capacitación	No requeridas

Organización del Proyecto

Estructura del Proyecto



Roles y Responsabilidades

[Resuma los roles y responsabilidades para el equipo de proyecto y otros participantes identificados en la estructura anterior.]

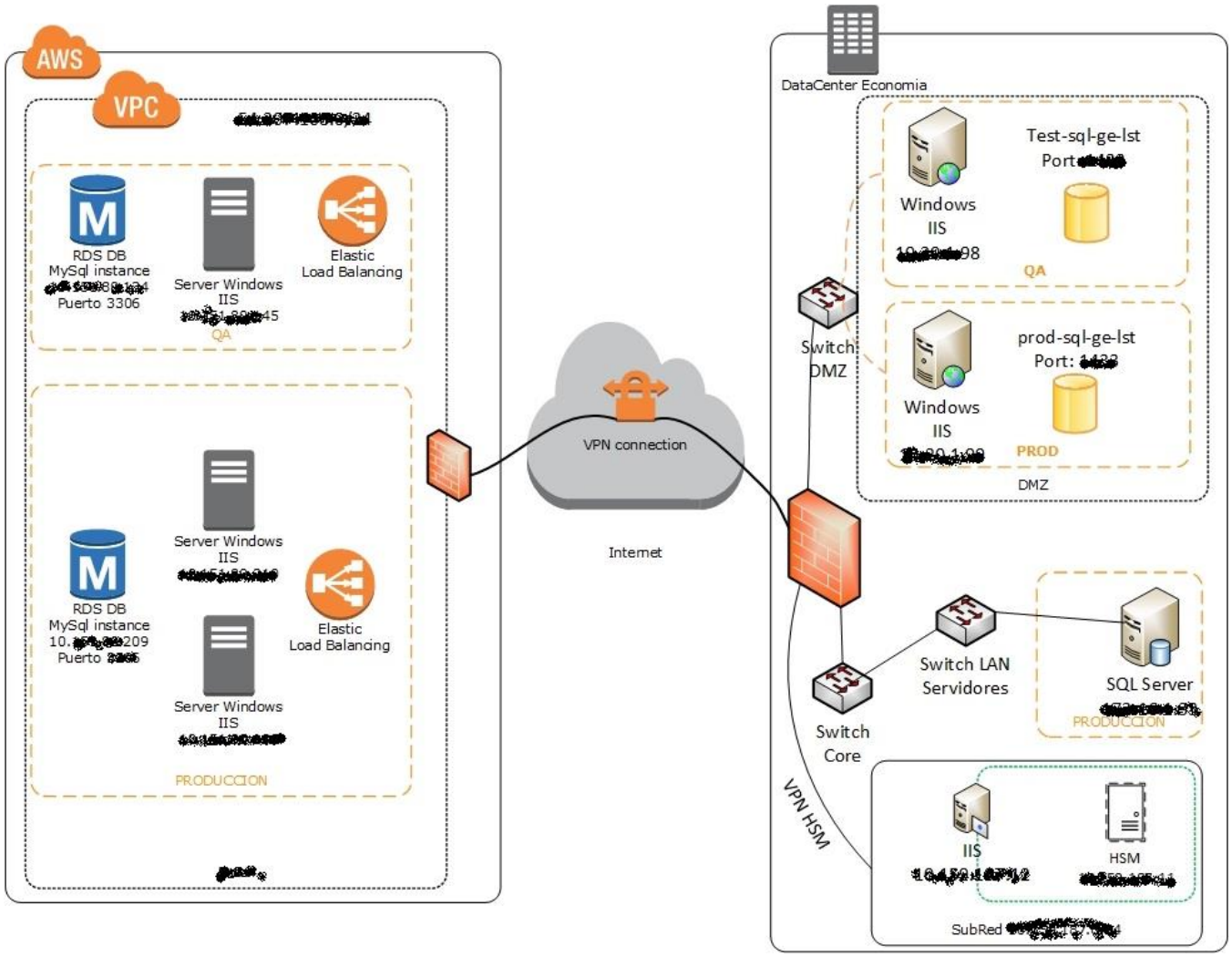
Rol	Responsabilidad
OSI	Encargado de supervisar el proyecto.
Analista Técnico	Néstor Reyes Avaria : Encargado de la ejecución del proyecto
Consultor de Poryecto PMBOK.	Favorecer la utilización de estándares y buenas prácticas de PMBOK en el desarrollo del proyecto

Comunicaciones Puntos de Contacto

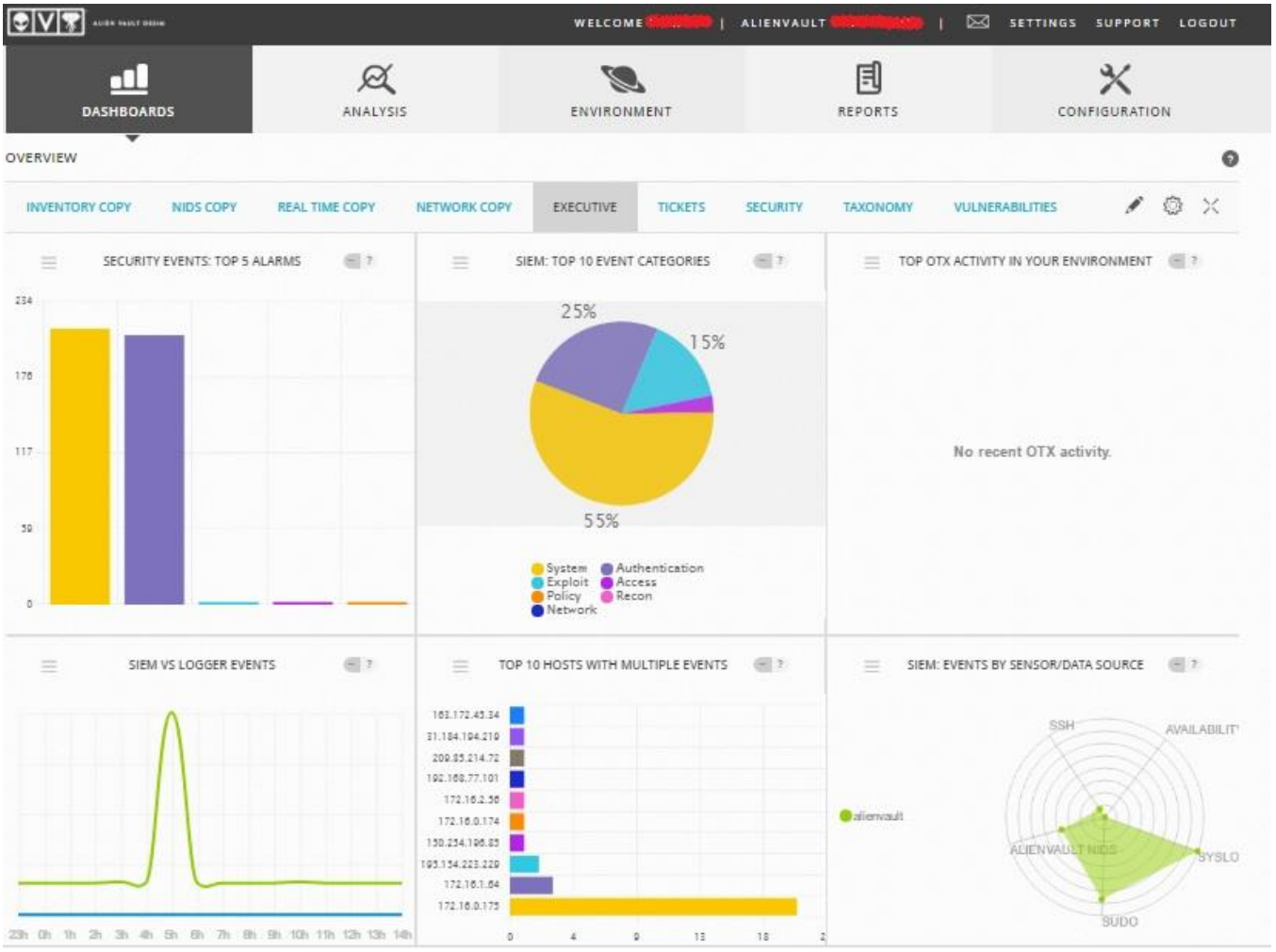
[Identificar y proveer la información de contacto de los principales interesados y miembros del equipo de proyecto.]

Rol	Nombre/Título/Organización	Teléfono	Email
Encargado del Proyecto			@economia.cl
Analista Técnico			@economia.com
Consultor PMBOK			
Sponsor			@economia.cl

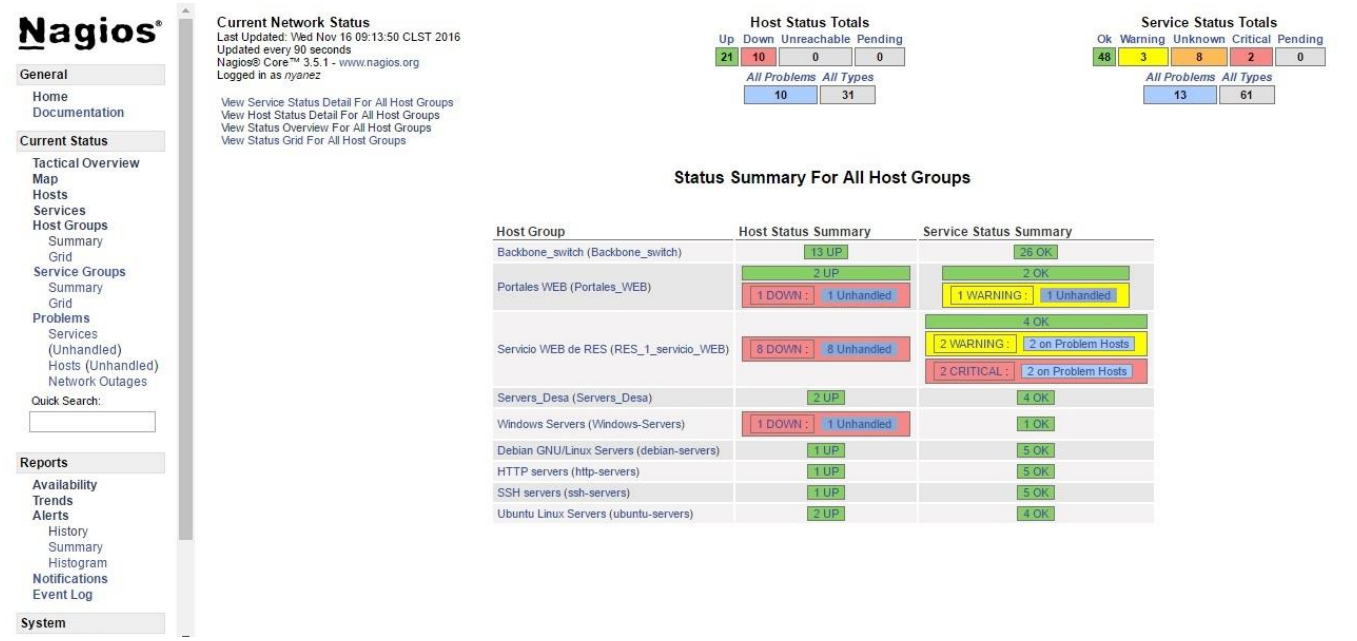
ANEXO F DIAGRAMA DE RED DE ECONOMÍA



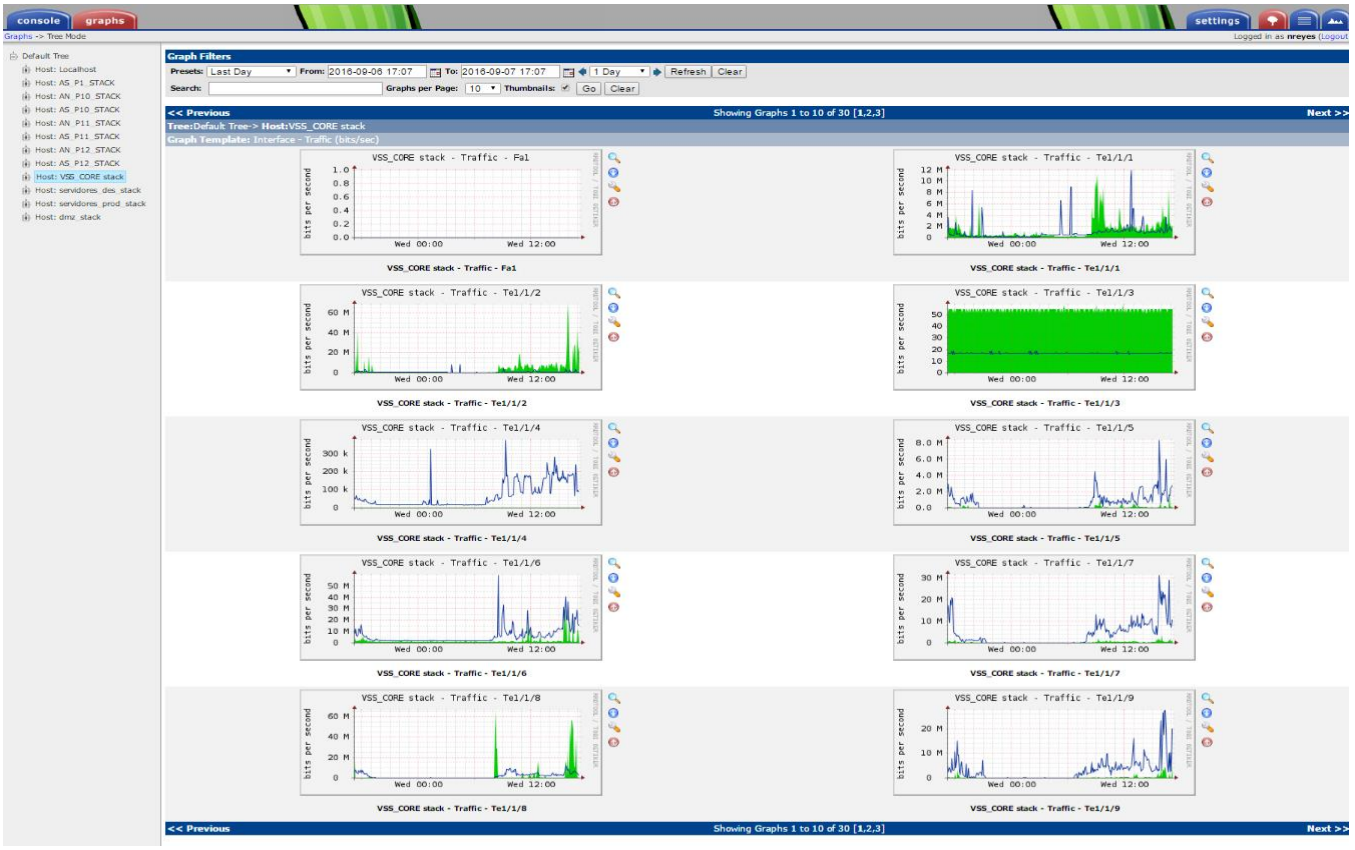
ANEXO G INFORMES DE SEGURIDAD.



Alien Vault Ossim



Nagios



CACTI

ANEXO H SITIO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

ANEXO J CONTROLES IMPLEMENTADOS

Del análisis los procesos y tareas propios del proceso FIC realizados sobre en base a la matriz de riesgos en conformidad lineamientos de las normas ISO27001:2013 y al documento técnico N°70 del CAIG sobre Gestión de Riesgos NCHISO31000 bajo el marco del PMG-SSI2015, se identificaron los siguientes controles a implementar durante el 2016:

A5.1.1 Políticas de seguridad de la información.

A5.1.2 Revisión de políticas para la seguridad de la información.

A6.1.1 Roles y responsabilidades para la segur de la información.

A6.1.2 Segregación de tareas.

A6.1.3 Contacto con las autoridades.

A6.2.1 Política de dispositivos Móviles.

A6.2.2 Política de Teletrabajo.

A7.1.1 Selección.

A8.1.1 Inventario de activos.

A8.1.4 Devolución de activos.

A9.1.1 Política de control Acceso.

A9.1.2 Acceso a redes y servicios de red

A9.2.2 Gestión de los derechos de acceso asignados a usuarios.

A9.2.4 Gestión de información confidencialidad de autenticación de usuarios.

A9.2.5 Revisión de los derechos de acceso a los usuarios.

A9.4.2 Procedimientos seguros de inicio de sesión.

A11.1.1 Perímetro de seguridad física.

A11.2.1 Emplazamiento y protección de equipos.

A11.2.3 Seguridad del Cableado.

A11.2.4 Mantenimiento de los equipos.

A11.2.7 Seguridad en la reutilización o descarte de equipos.

A11.2.8 Equipo de usuario desatendido.

A12.1.1 Procedimientos de operación documentación.

A12.3.1 Copias de Seguridad de la Información (Política de Respaldo de información).

A12.4.2 Protección de los registros de información.

A12.4.4 Sincronización de relojes.

A12.5.1 Instalación del software en sistemas operacionales.

A13.1.1 Controles de red.

A13.1.2 Mecanismos de seguridad asociados a servicios en red.

A13.1.3 Segregación de redes.

A14.2.1 Política de desarrollo seguro de software.

A14.2.2 Procedimientos de control de cambios en los sistemas.

A15.1.1 Política de Seguridad de la Información para suministradores.

A15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.

A15.2.1 Supervisión y revisión de los servicios prestados por terceros.

A15.2.2 Gestión de cambios en los servicios prestados por terceros.

A16.1.2 Informe de los eventos de seguridad de la información.

A18.1.1 Identificación de la legislación vigente y los requisitos contractuales.

A18.1.3 Protección de los registros.

A18.1.4 Protección de datos y privacidad de la información personal.

ANEXO K POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

Política General de Seguridad de la Información

Subsecretaria de Economía y Empresas de Menor Tamaño

Documento POGSI_01-10-2015

Historia del Documento	
Nombre del documento	Política General de Seguridad de la Información
Responsable del documento	Oficial de Seguridad de la Información
Aprobado Por	katia trusich subsecretaria

Control de Versiones			
versión	Fecha creación	Preparada por	Descripción
1.0	22-12-2008	Juan Pablo Chavol	
1.1	22-10-2009	Juan Pablo Chavol	
2.0	18-03-2011	E-Sign	
2.1	17-10-2011	Nicole Ogueta	
3.0	30-09-2015	Nelson Yáñez Mario Lemus	Reformulación en conformidad ISO27001:2013
3.1	21-09-2016	Nelson Yáñez Mario Lemus	Revisión Anual: Modificación de aprobación de Procedimientos y Políticas específicas de Seguridad de la Información

La presente versión substituye completamente a todas las precedentes, de manera que éste sea el único documento válido de entre todos los de la serie.

INTRODUCCIÓN

En la Subsecretaria de Economía y Empresas de Menor Tamaño la información es un activo fundamental para la prestación de sus servicios y la toma de decisiones eficientes, razón por la cual existe un compromiso expreso de protección de sus propiedades más significativas como parte de una estrategia orientada a la continuidad del servicio, la administración de riesgos y la consolidación de una cultura de seguridad.
Consciente de sus necesidades actuales, la Subsecretaria de Economía y Empresas de Menor Tamaño implementa un modelo de gestión de seguridad de la información como la herramienta que permite identificar y minimizar los riesgos a los cuales se expone la información, ayude a la reducción de costos operativos y financieros, establezca una cultura de seguridad y garantice el cumplimiento de los requerimientos legales, contractuales, regulatorios y normativos vigentes.
Este proceso será liderado de manera permanente por el Encargado de Seguridad de la Información.

OBJETIVO

El objetivo de este documento es establecer la política general de seguridad de la información de la subsecretaria de economía y empresas de menor tamaño, con el fin de regular la gestión de la seguridad de la información al interior de la entidad.

ALCANCE

Las políticas de seguridad de la información cubren todos los aspectos administrativos y de control que deben ser cumplidos por los directivos, funcionarios y terceros que laboren o tengan relación con el la Subsecretaria de economía y empresas de menor tamaño, para conseguir un adecuado nivel de protección de las características de seguridad y calidad de la información relacionada.

POLÍTICA

La Subsecretaria de Economía y Empresas de Menor Tamaño ha establecido las siguientes Políticas Generales de Seguridad de la Información, las cuales representan la visión de la Institución en cuanto a la protección de sus activos de Información:

1. Debe Existir un Comité de Seguridad de la Información, que será el responsable del mantenimiento, revisión y mejorar del Sistema de Gestión de Seguridad de la Información de la subsecretaria de economía y empresas de menor.

2. El Comité de Seguridad de la Información, debe tener a lo menos una reunión ordinaria trimestral. Sin perjuicio de lo anterior, se deben efectuar reuniones extraordinarias a solicitud de cualquiera de sus integrantes

3. La Subsecretaria de Economía y Empresas de Menor Tamaño en cada ámbito en particular, debe contar con políticas específicas y un conjunto de estándares y procedimientos que soportan la política general de seguridad de la información.

4. La Subsecretaria de Economía y Empresas de Menor Tamaño debe definir e implantará controles para proteger la información contra violaciones de autenticidad, accesos no autorizados, la perdida de integridad y que garanticen la disponibilidad requerida por los clientes y usuarios de los servicios ofrecidos por la Entidad.

5. Las violaciones a las Políticas y Controles de Seguridad de la Información deben ser reportadas, registradas y analizadas bajo un enfoque de mejora continua.

6. Los activos de información de la Subsecretaria de Economía y Empresas de Menor tamaño, deben ser identificados y clasificados para establecer los mecanismos de protección necesarios.

7. La información debe ser protegida, por sus custodios, de una manera consistente con su importancia, valor y criticidad, siguiendo las reglas establecidas en las políticas específicas de seguridad de la información, sus procedimientos asociados y en las recomendaciones dadas por el responsable designado de dicha información. Para ello, La subsecretaria de economía y empresas de menor tamaño deberá proveer los recursos que permitan implementar los controles necesarios para otorgar el nivel de protección correspondiente al valor de los activos.

8. Será de responsabilidad de cada una de las jefaturas de la institución, la difusión y cumplimiento de las normas establecidas en la Subsecretaria en materias de Seguridad de la Información.

9. Todos los funcionarios sean de, planta, contrata, honorarios y los contratistas, deben ser responsables de proteger la información a la cual accedan y procesen, para evitar su pérdida, alteración, destrucción o uso indebido.

10. Todos los accesos, usos y procesamientos de la información, deberán ser consistentes con las políticas, estándares y debe ser acorde a la clasificación de la información y las restricciones existentes sobre ella, vigentes en la Subsecretaria de Economía y Empresas de Menor Tamaño

11. Toda divulgación a terceros, de información confidencial o interna, debe ser acompañada de una declaración explícita del propietario, la cual describa exactamente la información que está restringida.

12. Ningún funcionario sean de, planta, contrata, honorarios y los contratistas deben actuar por cuenta propia en el caso de tener dudas sobre la clasificación de la información y su restricciones, debiendo consultar al propietario o de la información.

13. Se deben realizarán revisiones y controles periódicos sobre el modelo de gestión de Seguridad de la Información de la Subsecretaria de Economía y Empresas de Menor Tamaño.

14. Es responsabilidad de todos los funcionarios de planta, contrata, honorarios y contratistas de la Subsecretaria de Economía y Empresas de Menor Tamaño reportar los Incidentes de Seguridad, eventos sospechosos y el mal uso de los recursos que identifique

15. Todo equipo computacional (estación de trabajo, computador personal, servidor, periférico, Smartphone o dispositivo por el cual se pueda acceder, almacenar, transferir o modificar información), que sea de propiedad de la institución, este en arriendo o préstamo, deberá estar sujeto a las políticas, normas y procedimientos establecidos por la Subsecretaría de Economía y Empresas de Menor Tamaño.

16. La protección física del equipamiento tecnológico será de responsabilidad del usuario que recibe y/o utiliza el equipo, por lo tanto deberá informar oportunamente cualquier daño y/o comportamiento inesperado, a la unidad de informática de la Subsecretaría de Economía y Empresas de Menor Tamaño.

17. La Política General de Seguridad de la información de la Subsecretaría de Economía, ha sido diseñada de acuerdo al cumplimiento del marco legal, por ello cualquier exceso o conflicto que en ésta se detecte, debe ser informado de forma inmediata al Encargado de Seguridad de la Información.

18. Toda política debe contener las siguientes secciones:
    a) información de la Versión:
        i. -Autores
        ii. -Revisores
        iii. -N° de versión
        iv. -Fecha última Revisión
    b) Introducción
    c) Objetivos
    d) Alcance
    e) La política en si

19. Asociada a cada política se deben emitir los mecanismos de control y las sanciones cuando se viola la política respectiva.

20. La mantención de la presente política será realizada por el Encargado de Seguridad de la Información y sus cambios aprobados por el Comité de Seguridad de la Información y firmada por el o la Directora(a) Ejecutivo (a) de Subsecretaría de Economía.

21. Las políticas específicas y los procedimientos asociados, deberán ser aprobadas por el Comité de Seguridad de la información.

22. El presente documento debe ser revisado a lo menos 1 vez al año y actualizado cada vez que se realicen cambios relevantes en la Subsecretaría de Economía que afecten la adecuada protección de la información, considerando como tales entre otros, cambios en la misión, objetivos estratégicos, productos estratégicos, infraestructura, personal y/o procedimientos relacionados con la protección de la información.

***** Fin del Documento *****