GOBIERNO DE
CHILE

GUIA METODOLOGICA 2010

Programa de Mejoramiento de la Gestión

Sistema de Seguridad de la Información

Etapa I – Diagnóstico
Etapa II – Planificación

Red de Expertos
Subsecretaría del Interior – División Informática
Dirección de Presupuestos – División Tecnologías de la Información

Contenido

Introducción

El proceso de Modernización del Estado tiene como objetivo central realizar las adecuaciones necesarias, tanto en la estructura institucional del aparato estatal, como en la manera en que estas instituciones "hacen las cosas", para aumentar la eficacia y eficiencia en sus funciones de modo de servir mejor a la ciudadanía.

En el año 1998, con la implementación de la ley N° 19.553, se inició el desarrollo de Programas de Mejoramiento de la Gestión (PMG) en los servicios públicos, asociando el cumplimiento de objetivos de gestión a un incentivo en las remuneraciones de los funcionarios.

A partir del año 2010, el PMG incluye al sistema de "Seguridad de la Información" – dentro del área de Calidad de Atención a Usuarios – cuya asistencia y validación están a cargo de la Subsecretaría del Interior y la Dirección de Presupuestos.

La información es un bien que, como otros bienes de la organización, tiene gran valor y necesita ser protegida en forma apropiada. La Seguridad de la Información protege la información de una gran gama de amenazas con el fin de asegurar la continuidad de las operaciones, minimizar el daño de la institución y maximizar la eficiencia y las oportunidades de mejora de la gestión de la organización.

La información puede existir de muchas formas. Puede ser impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o medios electrónicos, mostrada en películas o hablada en una conversación. Cualquier forma que tome la información, o los dispositivos a través de los cuales es compartida o almacenada, siempre debe estar protegida en forma adecuada.

La Seguridad de la Información se logra mediante la implementación de un adecuado conjunto de controles, que pueden traducirse en políticas, procedimientos, prácticas, estructuras organizacionales y funciones de software. Se necesita establecer estos controles para asegurar que se cumplan los objetivos específicos de seguridad de la organización.

Con todo lo anterior, ha surgido la necesidad de que cada institución gubernamental cuente con un Sistema de Seguridad de la Información adecuado que permita asegurar la calidad, disponibilidad y oportunidad de la información, y la presente Guía ayudará a los mencionados organismos a alcanzar dicho objetivo.

Objetivo y Alcance de esta Guía Metodológica

El objetivo de esta Guía es presentar de manera detallada el desarrollo de cada uno de los requisitos técnicos asociados a las distintas etapas que componen el sistema, así como servir de herramienta para la confección del informe final que se debe presentar para verificar el cumplimiento de los objetivos de gestión comprometidos por los servicios públicos en el marco del Sistema Seguridad de la Información.

Alcances de la Guía Metodológica

Esta Guía le entregará lineamientos precisos para la presentación de los requisitos técnicos del Sistema de Seguridad de la Información. Sin embargo, no es un manual de gestión de proyectos. Por esta razón, el desarrollo de algunos requisitos pudiera requerir del uso de herramientas que no son descritas en profundidad en esta Guía y, en general, el empleo de conocimientos, capacidades y habilidades que se suponen existentes en cada uno de los servicios adscritos al sistema. Sin embargo, a lo largo de la Guía se enfatizan ciertos aspectos en los que se ha creído conveniente profundizar.

Cómo usar esta Guía Metodológica

El cuerpo central de la guía se divide en dos partes: La primera de ellas describe el SSI, sus objetivos y elementos constitutivos. En la segunda se detallan las etapas del Sistema, las acciones necesarias y los medios para reportar su cumplimiento a la Red de Expertos del PMG.

En forma anexa se incluye información que cada encargado del SSI deberá utilizar como referencia. Esto es, información que deberá ser estudiada en función del marco legal[1], que incorpora los decretos supremos y leyes que rigen el funcionamiento de los sistemas de información y el manejo de información en las instituciones.

La documentación facilitada para reporte del SSI[2] deberá ser cuidadosamente completada, de acuerdo a los formatos establecidos.

Además, se incluye documentación estandarizada[3], la cual cada servicio deberá adaptar de acuerdo a las necesidades propias.

[1] Ver carpeta Antecedentes Legales.
[2] Ver carpeta Evaluación.
[3] Ver carpeta Políticas de Seguridad y Lista de Contactos RCE.

El Sistema de Seguridad de la Información

Un Sistema de Seguridad de la Información (SSI) establece distintos controles de seguridad tanto a nivel de gobierno institucional y gestión, como de tecnologías de la información, todo esto con el objetivo de preservar:

- **La Integridad**: La información está completa, actualizada y es veraz, sin modificaciones inapropiadas o corrupción.
- **La Confidencialidad**: La información está protegida de personas/usuarios no autorizados.
- **La Disponibilidad**: Los usuarios autorizados pueden acceder a las aplicaciones y sistemas cuando lo requieran para utilizar la información apropiadamente al desempeñar sus funciones.

Las nuevas tecnologías, el desarrollo del conocimiento, la liberación de las comunicaciones y la disponibilidad de acceso libre a aplicativos, introducen nuevas amenazas para los activos de información, y la dependencia creciente de los recursos de Tecnologías de Información y Comunicación (TIC), aumenta considerablemente los impactos que la materialización de un incidente de seguridad pueda provocar en los activos de información.

No siempre se pueden eliminar los riesgos, por lo tanto es necesario **gestionar** la seguridad de la información a través de un programa de implementación de un sistema de gestión administrado.

Gestionar la seguridad de la información consiste en la realización de las tareas necesarias para garantizar los niveles exigibles en la organización, dentro del ámbito de protección de la integridad, la confidencialidad y la disponibilidad, como principio clave.

Según el Decreto Supremo N° 83 del 12 de enero de 2005 del Ministerio Secretaría General de la Presidencia (desde ahora en adelante DS-83), como también lo establecido en la Ley N° 20.285, las exigencias y recomendaciones que se proveen, tienen por finalidad garantizar estándares mínimos de seguridad en el uso, almacenamiento, acceso y distribución de documentos electrónicos, por lo que es necesario que cada uno de los órganos del estado cumpla con esta normativa a través de la implantación de un Sistema de Seguridad de la Información.

¿Qué se espera de este nuevo Sistema Seguridad de la Información?

Lo que se espera, en primer término, es que este nuevo Sistema constituya una herramienta para el ordenamiento de la gestión de cada institución desde el punto de vista del aporte efectivo de la tecnología a sus procesos institucionales relevantes, identificando primeramente sus activos de información críticos vinculados a sus procesos estratégicos y de soporte y, seguidamente, que se logre identificar y gestionar los riesgos asociados a estos activos, aterrizando en planes de contingencia y de recuperación frente a desastres tecnológicos, que permitan establecer una continuidad operacional de sus procesos relevantes a nivel institucional, de modo de asegurar la provisión de los productos y servicios que deben ser brindados a sus clientes / usuarios / beneficiarios.

Se espera que en el mediano plazo, este nuevo sistema actúe además como complemento y catalizador para el sistema PMG-Gobierno Electrónico (PMG-GE), introduciendo nuevas y mejores prácticas en la gestión de seguridad de la información en cada institución, así como en el gobierno de las TIC, para convertirse en un aporte efectivo a la gestión de las instituciones públicas.

En este contexto, lo que se espera de las entidades al adoptar el SSI, es que cumplan en un 100% con los dominios de seguridad establecidos en el DS 83. Los objetivos de dichos dominios se describen a continuación:

Tabla 1. Descripción de objetivos generales por dominio evaluado

Dominio 1: Política de Seguridad
El objetivo de este dominio es proporcionar a la institución la dirección y soporte para la seguridad de la información en concordancia con los requerimientos institucionales y las leyes y regulaciones pertinentes. La alta dirección debe establecer claramente el enfoque de la política en línea con los objetivos institucionales y demostrar su apoyo y su compromiso con la seguridad de la información, a través de la emisión y mantenimiento de una política de seguridad de la información en toda la organización.
Dominio 2: Seguridad Organizacional
El objetivo de este dominio es establecer un marco referencial a nivel directivo para iniciar y controlar la implementación de la seguridad de la información dentro de la institución. La dirección debe aprobar la política de seguridad de la información, asignar los roles de seguridad a los comités y al encargado de seguridad, además de coordinar y revisar la implementación de la seguridad en toda la institución. Si fuese necesario, se debe establecer una fuente de consultoría sobre seguridad de la información que esté disponible dentro de la institución. Se deben desarrollar contactos con los especialistas o grupos de seguridad externos, incluyendo las autoridades relevantes, para mantenerse actualizado con relación a las tendencias mundiales, monitorear los estándares, evaluar los métodos y proporcionar vínculos adecuados para el manejo de los incidentes de seguridad de la información. Se debe fomentar un enfoque multidisciplinario para la seguridad de la información.
Dominio 3: Clasificación, Control y Etiquetado de Bienes
El objetivo de este dominio es lograr y mantener una apropiada protección de los activos institucionales. Todos los activos deben ser inventariados y contar con un propietario nombrado. Los propietarios deben identificar todos los activos y deben asignar la responsabilidad por el mantenimiento de los controles apropiados. La implementación de controles específicos puede ser delegada por el propietario conforme sea apropiado, pero el propietario sigue siendo responsable por la protección de los activos. Adicionalmente se debe asegurar que la información reciba un nivel de protección adecuado. La información debe ser clasificada para indicar la necesidad, prioridades y grado de protección esperado en su manejo. La información tiene diversos grados de confidencialidad e importancia. Algunos ítems pueden requerir un nivel de protección adicional o manejo especial dependiendo de su criticidad y riesgo. Se debe utilizar un esquema de clasificación de información para definir un conjunto apropiado de niveles de protección y comunicar la necesidad de medidas de uso especiales.

Dominio 4: Seguridad del Personal
Antes de la contratación o formalización del servicio se debe asegurar que los empleados, contratistas y terceros entiendan sus responsabilidades, y sean idóneos para los roles para los cuales son considerados; y reducir el riesgo de robo, fraude y mal uso de los medios. Las responsabilidades de seguridad deben ser tratadas antes de la contratación en descripciones de trabajo adecuadas y en los términos y condiciones del empleo. Los antecedentes de todos los candidatos al empleo, contratistas y terceros deben ser adecuadamente investigados, especialmente para los trabajos confidenciales. Los empleados, contratistas y terceros usuarios de los medios de procesamiento de la información deben firmar un acuerdo sobre sus roles y responsabilidades con relación a la seguridad. Durante las labores se debe asegurar que los usuarios empleados, contratistas y terceras personas estén al tanto de las amenazas e inquietudes de la seguridad de la información, sus responsabilidades y obligaciones, y estén equipadas para apoyar la política de seguridad organizacional en el curso de su trabajo normal, y reducir el riesgo de error humano e incidentes de seguridad. Se debe proporcionar a todos los usuarios, empleados, contratistas y terceras personas un nivel adecuado de conocimiento, educación y capacitación en procedimientos de seguridad y uso correcto de los medios de procesamiento, activos y servicios de información para minimizar los posibles riesgos de seguridad. Se debe establecer un proceso disciplinario normal para manejar las fallas en la seguridad.
Dominio 5: Seguridad Física y del Ambiente
Prevenir el acceso no autorizado, daño e interferencia a las instalaciones de la institución y a la información. Los equipos de procesamiento de información crítica o sensible de la institución se deben mantener en áreas seguras, protegidos por un perímetro de seguridad definido, con barreras apropiadas de seguridad y controles de entrada. Éstos deben estar físicamente protegidos del acceso no autorizado, daño e interferencia. La protección provista debe estar en proporción con los riesgos identificados.
Se deben proteger físicamente los equipos de las amenazas de seguridad y riesgos del ambiente externo. Es necesaria la protección de los equipos, incluyendo los portátiles usados fuera de las dependencias, para reducir el riesgo de acceso no autorizado a datos y para prevenir la pérdida o daño. Esto también debe considerar la ubicación de los equipos y la eliminación de ítems en desuso. Se pueden necesitar controles especiales para protegerlos de riesgos o accesos no autorizados, y salvaguardar las instalaciones de apoyo, tales como el suministro eléctrico y la infraestructura de cables.
La información y los equipos de procesamiento de información se deben proteger de la divulgación, modificación o del robo por personas no autorizadas, y los controles se deben realizar in situ para minimizar la pérdida o daño.
Dominio 6: Gestión de las Operaciones y Comunicaciones
Se deben crear procedimientos y responsabilidades operacionales de manera de asegurar la operación correcta y segura de los medios de procesamiento de la información. Se deben establecer las responsabilidades y procedimientos para la gestión y operación de todos los medios de procesamiento de la información. Esto incluye el desarrollo de los procedimientos de operación apropiados. Cuando sea pertinente, se debe implementar la segregación de deberes para reducir el riesgo de negligencia o mal uso deliberado del sistema.
Se deben implementar medidas de protección contra el código malicioso y móvil a través de antivirus, de manera de proteger la integridad del software y la integración. El software y los medios de procesamiento de la información son vulnerables a la introducción de códigos maliciosos, como virus de cómputo, virus de red, caballos Troyanos y bombas lógicas. Los usuarios deben

estar al tanto de los peligros de los códigos maliciosos. Cuando sea apropiado, se deben introducir controles para evitar, detectar y eliminar los códigos maliciosos y controlar los códigos móviles.
Deben establecerse procesos de respaldo o Back-up con el objetivo de mantener la integridad y disponibilidad de la información y sus medios de procesamiento. Se deben establecer los procedimientos de rutina para implementar la política de respaldo acordada y la estrategia para tomar copias de respaldo de la data y practicar su restauración oportuna.
Se debe asegurar la protección de la información que viaja por correo electrónico y su infraestructura de soporte. La gestión segura del correo electrónico, requiere de la cuidadosa consideración de la información que es transmitida, su confidencialidad, implicancias legales, monitoreo y protección. También se pueden requerir controles adicionales para proteger la información confidencial que pasa a través de redes públicas.
Dominio 7: Control de Acceso
Se debe asegurar que el acceso del usuario es debidamente autorizado y evitar el acceso no autorizado a los sistemas de información. Se deben establecer procedimientos formales para controlar la asignación de los derechos de acceso a los sistemas y servicios de información. Los procedimientos deben abarcar todas las etapas en el ciclo de vida del acceso del usuario, desde el registro inicial de usuarios nuevos hasta la dada de baja de los usuarios que ya no requieren acceso a los sistemas y servicios de información. Cuando sea apropiado, se debe prestar atención especial a la necesidad de controlar la asignación de derechos de acceso privilegiados, lo que permite a los usuarios superar los controles del sistema.
La cooperación de los usuarios autorizados es esencial para una seguridad efectiva. Los usuarios deben estar al tanto de sus responsabilidades para mantener controles de acceso efectivos, particularmente con relación al uso de claves secretas y la seguridad del equipo del usuario. Se debe implementar una política de escritorio y pantalla limpios para reducir el riesgo de acceso no autorizado o daño a los papeles y medios de almacenamiento de la información.
Deben implementarse controles efectivos de manera de evitar el acceso no autorizado a los servicios de la red. Se debe controlar el acceso a los servicios de redes internas y externas. El acceso del usuario a las redes no debe comprometer la seguridad de los servicios de la red asegurando: a) Que existan las interfaces apropiadas entre la red de la institución y las redes de otras organizaciones, y redes públicas; b) Se apliquen los mecanismos de autenticación apropiados para los usuarios y el equipo; c) Que el control del acceso del usuario a la información sea obligatorio.
Se deben utilizar medios de seguridad para restringir el acceso a los sistemas operativos a los usuarios autorizados. Los medios deben tener la capacidad para: a) Autenticar a los usuarios autorizados, en concordancia con una política de control de acceso definida; b) Registrar los intentos exitosos y fallidos de autenticación del sistema; c) Registrar el uso de los privilegios especiales del sistema; d) Emitir alarmas cuando se violan las políticas de seguridad del sistema; e) Proporcionar los medios de autenticación apropiados; f) Cuando sea apropiado, restringir el tiempo de conexión de los usuarios.
Dominio 8: Desarrollo y Mantenimiento de Sistemas de Información
Se debe garantizar que la seguridad sea una parte integral de los sistemas de información. Los sistemas de información incluyen sistemas de operación, infraestructura, aplicaciones de negocio, servicios y aplicaciones desarrolladas por el usuario. El diseño e implementación del sistema de información que soporta el proceso de negocio puede ser crucial para la seguridad. Se deben identificar y acordar todos los requerimientos de seguridad antes del desarrollo y/o implementación de los sistemas de información en la fase de requerimientos de un proyecto; y deben ser justificados, acordados y

documentados como parte de las formalidades para un sistema de información.
Dominio 9: Gestión de la Continuidad del Negocio
Se deben considerar los aspectos de la seguridad de la información de la gestión de la continuidad del negocio de manera de hacer frente a las interrupciones de las actividades institucionales y proteger los procesos críticos de los efectos de fallas importantes o desastres en los sistemas de información y asegurar su reanudación oportuna. Se debe implementar el proceso de gestión de la continuidad del negocio para minimizar el impacto sobre la institución y lograr recuperarse de la pérdidas de activos de información (lo cual puede ser resultado de, por ejemplo, desastres naturales, accidentes, fallas del equipo y acciones deliberadas) hasta un nivel aceptable a través de una combinación de controles preventivos y de recuperación. Este proceso debe identificar los procesos institucionales críticos e integrar los requerimientos de gestión de la seguridad de la información de la continuidad del negocio con otros requerimientos de continuidad relacionados con aspectos como operaciones, personal, materiales, transporte y medios. Las consecuencias de los desastres, fallas en la seguridad, pérdida del servicio y la disponibilidad del servicio deben estar sujetos a un análisis del impacto en el negocio. Se deben desarrollar e implementar planes para la continuidad del negocio para asegurar la reanudación oportuna de las operaciones esenciales. La seguridad de la información debe ser una parte integral del proceso general de continuidad del negocio, y otros procesos gerenciales dentro de la organización. La gestión de la continuidad del negocio debe incluir controles para identificar y reducir los riesgos, además del proceso general de evaluación de riesgos, debe limitar las consecuencias de incidentes dañinos y asegurar que esté disponible la información requerida para los procesos institucionales.

¿Cuáles son objetivos del SSI en el PMG?

El nuevo Sistema de Seguridad de la Información 2010 permite identificar amenazas y vulnerabilidades que afectan a los activos de información que están vinculados a cada proceso de la institución. El énfasis está en desarrollar un plan para el tratamiento de riesgos, cautelando debidamente estos activos de información: Equipos, infraestructura tecnológica, software, bases datos, personas e información propiamente tal en sus múltiples formatos (papel, electrónica, audio, video, etc.).

El objetivo del SSI es "contar con un sistema de gestión de seguridad de la información que permita lograr niveles adecuados de integridad, confidencialidad y disponibilidad para todos los activos de información institucional considerados relevantes, de manera tal que se asegure la continuidad operacional de los procesos institucionales y la entrega de productos y servicios a los usuarios / clientes / beneficiarios"[4].

A través de SSI, los servicios públicos deberán elaborar un levantamiento pormenorizado de estos activos en dos planes: el Plan de Continuidad del Negocio y el Plan de Recuperación frente a Desastres Tecnológicos. En toda organización moderna, donde más del 90% de sus procesos descansan en TIC[5], los planes mencionados se transforman en elementos fundamentales para cumplir los objetivos principales de gestión de seguridad de la información (lograr que todos los activos de información institucional estén protegidos desde las perspectivas de Confiabilidad, Integridad y Disponibilidad).

[4] MINISTERIO de Hacienda – Dirección de Presupuestos. Programa de Mejoramiento de la Gestión (PMG). Año 2010. Programa Marco Básico. Documento Técnico. Septiembre de 2009. Pág. 6.

[5] MINISTERIO de Hacienda – Dirección de Presupuestos. Programa de Mejoramiento de la Gestión (PMG). Año 2010. Programa Marco Básico. Documento Técnico. Septiembre de 2009. Pág. 12.

Objetivos de las etapas del nuevo sistema:

- Etapa 1
  - Diagnosticar la situación de seguridad de la información institucional.
  - Identificar de todos aquellos aspectos de seguridad de la información que establece el Decreto Supremo N°83[6], estableciendo el nivel en que la institución se encuentra con respecto de ellos.
  - Determinar las brechas a ser abordadas en el Plan de Seguridad de la Información Institucional.

- Etapa 2
  - Definir el Plan General de Seguridad de la Información Institucional, para el año en curso y siguientes, considerando los resultados del diagnóstico y brechas detectadas en la Etapa I, y que comprenda la coordinación de todas las unidades vinculadas y los métodos para la implementación del DS-83.
  - Establecer el porcentaje de cumplimiento que se alcanzará cada año para cada uno de los dominios del DS-83.
  - Elaborar el Programa de Trabajo Anual para implementar el Plan de Seguridad de la Información definido, señalando el porcentaje de cada uno de los dominios del DS-83 que se alcanzará para el año, hitos, cronograma, plazos y responsables.
  - Difusión a los funcionarios del Plan de Seguridad de la Información y su Programa de Trabajo.

- Etapa 3
  - Implementar el Programa de Trabajo Anual definido en la etapa anterior, de acuerdo a lo establecido por el Plan General de Seguridad de la Información y porcentaje de cumplimiento del DS-83 comprometido.
  - Registrar y controlar los resultados de la implementación del Programa de Trabajo Anual considerando actividades, dificultades, holguras detectadas y las modificaciones realizadas respecto a lo programado.

- Etapa 4
  - Evaluar los resultados de la implementación del Plan General de Seguridad de la Información y Programa de Trabajo Anual, y formular recomendaciones de mejora.
  - Diseñar el Programa de Seguimiento a partir de las recomendaciones formuladas.
  - Implementar los compromisos establecidos en el Programa de Seguimiento, considerando plazos y responsables para superar las brechas aún existentes y debilidades detectadas.
  - Difundir a los funcionarios los resultados de la evaluación del Plan y Programa de Trabajo Anual.
  - Mantener del grado de desarrollo del sistema de acuerdo a cada una de las Etapas[7].

[6] Aspectos que establece el Decreto N°83 del Ministerio Secretaria General de la Presidencia de 3 de junio de 2004: Políticas de Seguridad, Seguridad Organizacional, Clasificación, Control y Etiquetado de Bienes, Seguridad Física y del Ambiente, Seguridad del Personal, Gestión de las Operaciones y de las Comunicaciones, Control de Acceso, Desarrollo y Mantenimiento de Sistemas, y Gestión de la Continuidad del Negocio.

7 Este objetivo es exigible sólo para aquellos servicios que ya hayan cumplido la cuarta etapa.

Ámbitos de interacción del SSI

El SSI interactúa estrechamente con diferentes áreas de la institución y sus procesos.

La entrega de productos, servicios e información institucional y procesos de soporte institucional, debe considerar:

i. **Provisión** de productos estratégicos a aquellos procesos que hacen factible el cumplimiento de los objetivos estratégicos de cada institución.

ii. **Productos** que se proveen a los ciudadanos y/o usuarios institucionales, directa o indirectamente (a través de empresas u otras instituciones).

iii. **Procesos tecnológicos** que se llevan a cabo en la generación, intercambio, transporte y/o almacenamiento de documentos electrónicos, ya sea entre los diferentes organismos de la administración del Estado y en las relaciones de éstos con los particulares, cuando éstas tengan lugar utilizando técnicas y medios electrónicos, o dentro de dichos organismos.

iv. **Normativa vigente,** incorporada en proyectos de Gobierno Electrónico u otros, relacionadas con la seguridad de la información, en particular:

- Ley N°19.553, febrero 1998. Concede asignación de modernización y otros beneficios que indica. Ministerio de Hacienda.
- Decreto N°475. Reglamento Ley 19.553 para la aplicación del incremento por Desempeño institucional del artículo 6° de la Ley y sus modificaciones.
- Ley N°20.212, agosto de 2007. Modifica las leyes N° 19.553, N° 19.882, y otros cuerpos legales, con el objeto de incentivar el desempeño de los funcionarios públicos. Ministerio de Hacienda.
- Ley N°19.799, abril de 2002. Sobre documentos electrónicos, firma electrónica y los servicios de certificación de dicha firma. Ministerio de Economía.
- DS N°181. Reglamento Ley 19.799 sobre documentos electrónicos, firma electrónica y la certificación de dicha firma.
- Instructivo Presidencial N° 05, mayo de 2001: Define el concepto de Gobierno Electrónico. Contiene la mayor parte de las instrucciones referidas al desarrollo de Gobierno Electrónico en Chile.
- Instructivo Presidencial N° 06, junio de 2004: Imparte instrucciones sobre la implementación de la firma electrónica en los actos, contratos y cualquier tipo de documento en la administración del Estado, para dotar así de un mayor grado de seguridad a las actuaciones gubernamentales que tienen lugar por medio de documentos electrónicos y dar un mayor grado de certeza respecto de las personas que suscriben tales documentos.
- DS N°77. Norma técnica sobre eficiencia de las comunicaciones electrónicas entre órganos de la Administración del Estado y entre éstos y los ciudadanos.
- DS N°81. Norma técnica para los órganos de la Administración del Estado sobre interoperabilidad de documentos electrónicos.
- DS N°158. Modifica D.S. N° 81 sobre norma técnica para la interoperabilidad de los documentos electrónicos.
- DS N°83. Norma técnica para los órganos de la Administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos.

- DS N°93. Norma técnica para minimizar la recepción de mensajes electrónicos masivos no deseados en las casillas electrónicas de los órganos de la Administración del Estado y de sus funcionarios.
- DS N°100. Norma técnica para el desarrollo de sitios web de los órganos de la Administración del Estado.
- Documentos elaborados por el Comité de Normas para el Documento Electrónico.
- Ley Nº 20.285, agosto de 2008. Regula el principio de transparencia de la función pública y el derecho de acceso a la información de los órganos de la administración del Estado. Ministerio Secretaría General de la Presidencia.
- Decreto N°13. Reglamento de la Ley Nº 20.285 sobre Acceso a la Información Pública.
- Instrucción General N°2, mayo de 2009, del Consejo para la Transparencia: Designación de Enlaces con el Consejo para la Transparencia.
- Instrucción General N°3, mayo de 2009, del Consejo para la Transparencia: Índice de Actos o Documentos calificados como secretos o reservados.
- Instructivo Presidencial N°08, diciembre de 2006: Imparte instrucciones sobre Transparencia Activa y Publicidad de la Información de la Administración del Estado.
- Circular Nº3, enero de 2007: Detalla las medidas específicas que deben adoptar los servicios y dispone los materiales necesarios para facilitar la implementación del instructivo presidencial sobre transparencia activa y publicidad de la información de la Administración del Estado.
- Ley Nº 19.880, mayo de 2003: Establece bases de los procedimientos administrativos que rigen los actos de los órganos de la administración del Estado. Ministerio Secretaría General de la Presidencia.
- Instructivo Presidencial N°4, junio de 2003: Imparte instrucciones sobre aplicación de la Ley de Bases de Procedimientos Administrativos.
- Ley N° 19.628, agosto de 1999. Sobre protección de la vida privada y datos personales. Ministerio Secretaría General de la Presidencia.
- Ley Nº 17.336, octubre de 1970: Sobre propiedad intelectual. Ministerio de Educación Pública.
- Ley Nº 19.223, junio de 1993: Sobre delitos informáticos. Ministerio de Justicia.
- Ley Nº 19.927, enero de 2004: Sobre delitos de pornografía infantil. Ministerio de Justicia.
- Guía Metodológica del Sistema Gobierno Electrónico.
- Guía Metodológica del Sistema Seguridad de la Información.

Para comprender en detalle el alcance de la legislación, revisar documentación en **"Anexo 3 - Referencias legales y normativas"**.

¿Quiénes deben estar involucrados en este PMG?

Para el desarrollo del SSI, será necesario aunar el aporte y trabajo de los profesionales de todas las áreas, con el fin de desarrollar adecuadamente los proyectos de interés institucional. Este equipo multidisciplinario permitirá dividir las responsabilidades, logrando la especialización en cada uno de los dominios del DS-83, obteniendo resultados de calidad satisfactoria.

Dentro del desarrollo del programa se deberá tener presente al siguiente personal:

1.- **Directivos.**

Dada la magnitud y relevancia de la tarea, se requiere de la participación activa de los más altos directivos de la institución, ya sea para entregar las orientaciones básicas, como para tomar las decisiones que influirán en el modo de operar del servicio público. Adicionalmente, es importante contar con un fuerte liderazgo y compromiso de los directivos que soporte la intervención de los procesos que se buscan mejorar. El rol que, en este sentido, juegan los directivos, no puede delegarse sin una significativa pérdida de credibilidad respecto a la seriedad del esfuerzo.

2.- **Profesionales y técnicos.**

Parte importante de este equipo multidisciplinario es la activa participación de profesionales y técnicos seleccionados, que entienden y manejan el desarrollo de los procesos dentro de la institución. Para lo anterior, es necesario que cumplan con los perfiles acordes al cargo, dado que ellos entregarán los antecedentes y atenderán los requerimientos en la práctica.

3.- **Otros funcionarios.**

Además, será necesario incluir a otro personal que pueda ser relevante para el correcto desarrollo del programa de implantación del SSI, ya sea directa o indirectamente. Cabe mencionar que también se debe incluir al personal a cargo de la Gestión de Calidad, dueños de procesos estratégicos del servicio o de procesos de provisión de productos y servicios, personal del área de gestión de riesgo; abogados/as del área jurídica y RRHH, entre otros.

Etapas del SSI

ETAPA I: Diagnóstico

¿En qué consiste?

La etapa de Diagnóstico es fundamental, ya que entrega los lineamientos para el trabajo a desarrollar en las etapas siguientes.

El diseño de proyectos de implementación de controles de seguridad dentro de la institución requiere de un adecuado diagnóstico de la situación que se busca intervenir.

Un diagnóstico deficiente casi necesariamente conduce a iniciativas que presentan resultados de poco o bajo impacto, si los hay, con lo que no se está resolviendo el problema que se pretendía abordar.

Un proyecto no surge de la nada, sino de una situación que se considera negativa, ineficaz o susceptible de modificar al reconocer una oportunidad de mejora. Desde el punto de vista de Seguridad de la Información, se enfatiza la capacidad de generar valor mediante el uso de políticas, procedimientos y estándares de seguridad que, en complemento con las Tecnologías de Información y Comunicaciones, conforman un sistema de gestión administrado. Sin embargo, el objetivo no es la incorporación de dichas tecnologías, de la normativa interna o el gobierno corporativo de seguridad, sino la mejora de la gestión de las instituciones a través de ellas. En este sentido, es indispensable que los servicios determinen si sus áreas y divisiones requieren mejoras antes de intervenir en sus procesos, de modo tal de no generar actividades de control que sean innecesarias, malgastando recursos que pueden aprovecharse en necesidades más urgentes en la institución.

Es importante destacar que uno de los aspectos relevantes para la aprobación de esta etapa es que el "nivel de completitud" sea consistente con el "estado real de la institución" y NO sobre/sub dimensionar los valores, siendo un nivel bajo o alto de completitud igualmente válido para la aceptación del Diagnóstico.

En esta etapa, utilizando los dominios de áreas de seguridad de acuerdo al DS-83, se realizará el diagnóstico de la situación actual de la institución, estableciendo los niveles en cada uno de ellos, de manera de determinar las brechas que deberán ser abordadas en el Plan de Seguridad especificado en la Etapa II del PMG-SSI.

Estos dominios o aspectos sobre los cuales se debe realizar el diagnóstico están descritos en la sección: El Sistema de Seguridad de la Información.

Tabla 2. Dominios DS 83

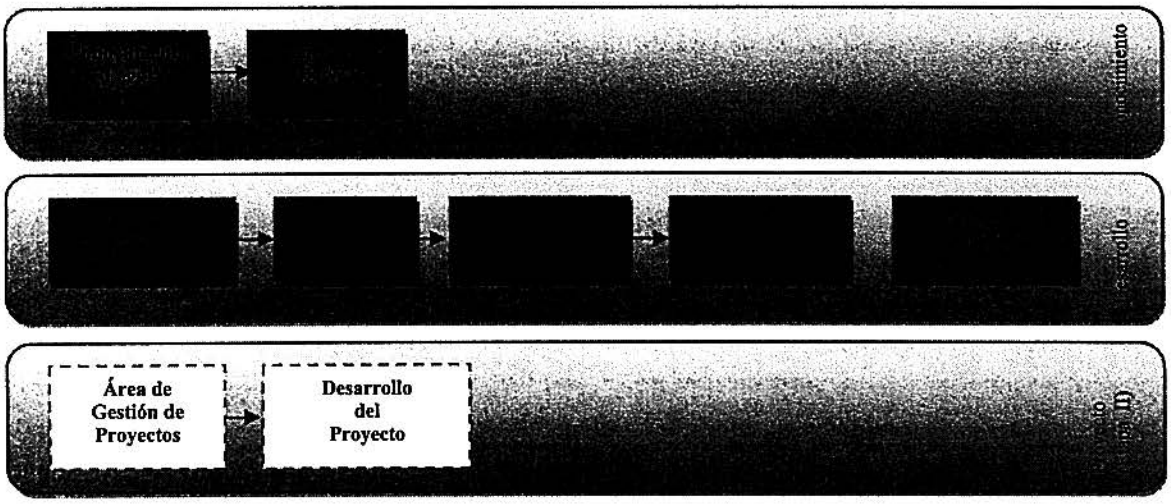
Dominio 1: Política de Seguridad
Dominio 2: Seguridad Organizacional
Dominio 3: Clasificación, Control y Etiquetado de Bienes
Dominio 4: Seguridad del Personal
Dominio 5: Seguridad Física y del Ambiente
Dominio 6: Gestión de las Operaciones y Comunicaciones
Dominio 7: Control de Acceso
Dominio 8: Desarrollo y Mantenimiento de Sistemas de Información
Dominio 9: Gestión de la Continuidad del Negocio

¿Cómo se hace el Diagnóstico?

En este apartado se describen una serie de acciones, actividades, consideraciones y requerimientos, los cuales deberán ser cumplidos en su totalidad. Cada acción se verá reflejada en un documento cuyo formato provee esta Guía, y da respuesta a cada uno de los requisitos técnicos del SSI en el PMG.

Para esto, la primera etapa (Diagnóstico) se divide en las sub-etapas que se muestran a continuación:

Figura 1. Sub- etapas – Diagnóstico PMG-SSI



Para el reporte de esta etapa se ha diseñado una **"Matriz de Diagnóstico"**. Este documento constituye el principal medio por el cual se informará a la Red de Expertos los requisitos de la etapa I. Cada elemento de esta matriz facilita la respuesta a los requisitos técnicos del SSI y permitirá dar continuidad al trabajo de las etapas restantes. Del mismo modo, a esta matriz se le deberá adjuntar toda la documentación solicitada para verificar el cumplimiento total de los requisitos.

Es necesario que el encargado PMG-SSI, como también todos los funcionarios que tengan participación en él, cumplan con la totalidad los pasos necesarios y requisitos técnicos, con el fin de lograr y asegurar un cumplimiento satisfactorio de la etapa de diagnóstico. Para esto, se precisa realizar la siguiente secuencia de actividades:

1. Definir a los responsables para cada uno de los dominios, quienes deberán conocer y comprender cada uno de los dominios del DS-83. Para facilitar la lectura, deberá leer el campo **"Definición"** del documento **"Matriz de Diagnóstico"** (Anexo 1).
   Además, una vez concluida esta etapa, ellos deberán defender el proyecto o sistema propuesto, el que deberá ser presentado al área de proyectos de su unidad, división o a quien le corresponda.

2. Igualmente, todos los participantes deberán conocer la totalidad de los documentos que tengan impacto dentro de la normativa legal. Para esto se adjunta compendio denominado **"Antecedentes Legales"**.

3. Luego de haber estudiado todos los antecedentes mencionados, se deberá proceder a realizar el diagnóstico utilizando el documento **"Matriz de Diagnóstico"**, en el cual tendrá que llenar lo solicitado para cada uno de los campos descritos en el documento. Este trabajo permitirá dar cumplimiento al requisito técnico "Revisión y verificación del nivel de cumplimiento de todos los requerimientos establecidos en el DS N°83, artículo primero, títulos I a V".

Tabla 3. Matriz de diagnóstico (Anexo 1 – Hoja "Dominios")

DOMINIO	PARRAFO	ARTICULO	SUB CATEGORÍA	DEFINICIÓN	COMPLETITUD	DESCRIPCIÓN DEL ESTADO ACTUAL	DESCRIPCIÓN DE LA BRECHA	ESTRATEGIA PRELIMINAR	OBJETIVOS ESPECÍFICOS (CORTO PLAZO)	DOCUMENTO REFERIDO	RESPONSABLE ASIGNADO	SISTEMA / PROYECTO	RELACIÓN CON GOBIERNO ELECTRÓNICO	PRIORIDAD
Políticas de Seguridad	**2**	**11**	**a**	**Una definición de seguridad del documento electrónico, sus objetivos globales, alcance e importancia.**										

Descripción de campos:

- **Dominio:** Nombre del dominio establecido en DS-83 a evaluar.
- **Párrafo:** Referencia a DS-83.
- **Artículo:** Referencia a DS-83.
- **Sub Categoría:** Referencia a DS-83.
- **Definición:** Texto extraído del DS-83, el cual corresponde, dentro del dominio, a lo que el encargado deberá evaluar dentro de la institución.

- **Completitud:** Espacio habilitado para la evaluación[8] en relación a cada uno de los dominios descritos.
- **Descripción del estado actual:** Breve descripción de cómo se encuentra actualmente la institución en relación al dominio correspondiente.
- **Descripción de la brecha:** Breve descripción de la brecha en la institución para poder cumplir con lo solicitado en el dominio de seguridad.
- **Estrategia preliminar:** Qué debería realizar la institución para cumplir con la reducción total de la brecha.
- **Objetivos específicos (corto plazo):** Breve descripción de las tareas específicas que la institución deberá realizar para cumplir con lo solicitado en el dominio correspondiente.
- **Documento referido:** Documentos que servirán de evidencia y respaldo para cada uno de los elementos evaluados.
- **Responsable asignado:** Designación de él o los responsables para realizar las actividades descritas en la columna "Estrategia Preliminar".
- **Sistema/Proyecto:** Descripción de algún sistema, actividad o proyecto que permita disminuir o mitigar la brecha.
- **Relación con Gobierno Electrónico:** Describir si la solución existe o se debe implementar como una actividad o desarrollar un proyecto dentro del ámbito del PMG de Gobierno Electrónico.
- **Prioridad:** Definir la criticidad de la brecha detectada en base a los criterios utilizados en la institución (ver tablas 5 y 6).

4. Como punto de partida, se deberá consignar el nombre de los responsables de cada dominio dentro del campo **"Responsable Asignado"**, de la Matriz, para luego, a través de entrevistas, estos funcionarios provean parte importante de la información requerida para el diagnóstico, dando respuesta al requisito técnico "Entrevistas a los responsables de los ámbitos de seguridad cubiertos por cada dominio de seguridad".

5. Otro insumo para completar la matriz será la revisión de los "documentos que soporten o entreguen más elementos al análisis, como por ejemplo, políticas, procedimientos, normas, registros, configuraciones de dispositivos, etc." que, en sí mismos, son requisitos técnicos del SSI, por tanto son parte del reporte para la Red de Expertos.

6. De igual forma ocurre con "la identificación de metodologías/normativas de gestión de riesgos, gestión de la calidad u otra metodología de gestión por procesos que se encuentre en uso en la Institución, señalando alcance y ámbito de aplicación". Esta identificación también es un requisito técnico que debe ser considerada para evaluar los diferentes dominios contenidos en la Matriz.

7. Con la información recopilada, lo último que debe ser llenado será el campo **"Completitud"**, el cual al momento de evaluar, el criterio a utilizar deberá ser:

[8] Ver tabla 4 "Criterios de evaluación"

Tabla 4 – Criterios de evaluación – Matriz de diagnóstico (Anexo 1)

VALOR	TIPO	DESCRIPCIÓN
0	No cumple	La institución no cuenta con procedimientos, sistemas, controles u otros que le permita cumplir con el DS-83.
1	Cumple parcialmente	La institución cuenta con algunos o varios procedimientos, sistemas, controles u otros que le permita cumplir con el DS-83.
2	Cumple	La institución cuenta con todos los controles, procedimientos, sistemas u otros requeridos por el DS-83.

8. Una vez realizado el diagnóstico, se deberá generar un informe utilizando el documento **"Brechas"**, sobre las diferencias encontradas entre lo estipulado en el DS-83 y la institución. Este reporte permitirá verificar el cumplimiento del requisito técnico de "establecer un registro de todas las brechas de seguridad por dominio detectadas".

9. Luego se debe desarrollar el requisito técnico de "priorizar las brechas identificadas, basándose para ello en los criterios de riesgo institucionales. Esta definición es fundamental para la segunda etapa, puesto que el trabajo a realizar se organizará sobre la base de los proyectos que respondan a las brechas priorizadas.

   A continuación, se presenta una descripción y algunos ejemplos de priorización que pueden ser utilizados para estimar actividades/proyectos a realizar de acuerdo a los riesgos de seguridad que involucra su no cumplimiento, y los indicadores (entregables) que nos certifican su cumplimiento.

Tabla 5. Criterio para la definición de prioridades

Prioridad	Descripción
Inmediata	Son actividades que deben ser llevadas a cabo en un corto plazo dado que involucran un alto riesgo de seguridad para la institución producto de sus vulnerabilidades asociadas.
Mediano Plazo	Las actividades de mediano plazo, se pueden considerar proyectos ya que requieren de una mayor programación, verificando su factibilidad, aprovisionamiento de recursos necesarios y designación de responsables. Estas actividades mitigan un conjunto de vulnerabilidades asociadas a distintos niveles de riesgo.
Largo Plazo	Estas actividades son proyectos con un horizonte de tiempo de desarrollo superior a un año y están orientadas a toda la organización, afectando gran parte de sus áreas.

Tabla 6. Ejemplos de prioridades y actividades a desarrollar

Dominio	Prioridad	Actividad o Proyecto
1	Actividad Inmediata	Desarrollar y sancionar directriz y Políticas de Seguridad.
2	Actividad Inmediata	Conformación del Comité de Seguridad Informática con apoyo de la Dirección.
2	Actividad Inmediata	Asignación formal de responsabilidad al Encargado de Seguridad.
3	Actividad Inmediata	Definición y difusión de Política de Clasificación de la Información.
3	Actividad Inmediata	Política de Respuesta ante Incidentes.
4	Actividad de Mediano Plazo	Habilitar servicio en Intranet para la Publicación y Mantención de Políticas.

Entiéndase por actividades inmediatas y mediano plazo a ejecutarse en el primer año y la primera mitad del segundo año, una vez iniciada la etapa de implementación. Las actividades de largo plazo, se desarrollarán desde la mitad del segundo año hasta términos del tercero.

10. Se deberá "establecer, de manera preliminar, la cartera de proyectos que le permitirán abordar las brechas detectadas", requisito técnico a ser reportado mediante un documento denominado "**Estrategias Preliminares**".

11. Toda la información antes mencionada, deberá almacenarse dentro de una carpeta llamada "**Documentos Referidos**", la cual constituirá la evidencia que respalda la evaluación de cada uno de los puntos del presente PMG.

¿Cómo hacer el Informe de Diagnóstico del SSI?

Para el llenado de la Matriz de Diagnóstico y su complementación con los otros documentos, se podrá seguir la estructura que a continuación se presenta, de modo de facilitar y ordenar la información:

Campo	Descripción	¿Qué se espera?	Entregable a la Red de Expertos
Análisis Situación Actual	• Realizar el análisis de los dominios descritos en los artículos que componen el DS-83.	• Se espera que en este punto el o los responsables adquieran la comprensión de cada uno de los dominios, entendiendo lo solicitado en ellos, permitiendo realizar el levantamiento de la situación actual de la institución.	• Informe de levantamiento de la situación actual de la institución (Basarse en Anexo 6 – Informe de diagnóstico institucional). • Matriz de Diagnóstico (campos "Completitud" y "Descripción del Estado Actual").
Brecha	• Se debe describir la diferencia entre la situación actual de la institución y lo requerido en cada uno de los dominios del DS-83.	• Se espera que en este punto el o los responsables identifiquen los elementos de los que carece la institución para cumplir con lo solicitado en cada uno de los dominios del DS-83.	• Informe que detalle por extensión los elementos que faltan para cumplir con lo solicitado por el DS-83 (Basarse en Anexo 6 – Informe de diagnóstico institucional). • Matriz de Diagnóstico (campo "Descripción de la Brecha").
Estrategia Preliminar	• Describir una estrategia de mitigación al corto plazo que facilite el desarrollo del diseño del plan de trabajo y que guarde relación con el PMG de Gobierno Electrónico y la matriz de riesgos institucional.	• Se espera que en este punto él o los responsables describan los elementos necesarios (descripción de alto nivel y referencial a un proyecto) que se requieran para lograr el objetivo específico.	• Informe que describa las estrategias consideradas, indicando los objetivos específicos de cada una de ellas. (Basarse en Anexo 6 – Informe de diagnóstico institucional).

Campo	Descripción	¿Qué se espera?	Entregable a la Red de Expertos
			• Matriz de Diagnóstico (campos "Estrategia Preliminar" y "Objetivos Específicos").
Asignación de Responsable(s)	• Para cada uno de los artículos descritos en el DS-83, se deberá asignar un responsable encargado de apoyar en el diagnóstico, diseño del plan de trabajo, ejecución y monitoreo de la implementación.	• Se espera que el encargado del PMG, designe y cree su red de apoyo.	• Cartera de proyectos. • Matriz de Diagnóstico (campo "Responsable Asignado").
Documentos Referidos	• Para cada uno de los artículos descritos en el DS-83, se deberá desarrollar la documentación que respalde (evidencia) cada uno de los aspectos solicitados.	• Desarrollar y almacenar de forma ordenada la documentación electrónica que da cuenta de las actividades, evaluaciones u otros requeridos por el SSI.	• Carpeta electrónica que contenga toda documentación relacionada con el SSI, siendo consistente con el marco regulatorio para el traspaso de información gubernamental. • Matriz de Diagnóstico (campo "Documento Referido").

TODA LA DOCUMENTACIÓN ENTREGADA POR LA INSTITUCIÓN DEBERÁ SER APROBADA POR LA AUTORIDAD SUPERIOR DEL SERVICIO Y ENVIADA A LA RED DE EXPERTOS.

ETAPA II: Planificación

La etapa de Planificación es muy importante pues aquí se definen claramente los objetivos de la implementación de soluciones o mejoras para resolver cada una de las brechas identificadas en la etapa de Diagnóstico, y se diseña un completo programa de trabajo que permite alcanzar dichos objetivos en los plazos establecidos. Además, permite la coordinación de esfuerzos y recursos al interior de las Instituciones garantizando el éxito de las iniciativas.

En esta etapa ya se han tomado las decisiones respecto del diagnóstico elaborado en la etapa anterior, en el cual se establecieron, de forma previa, las prioridades según las necesidades de la institución.

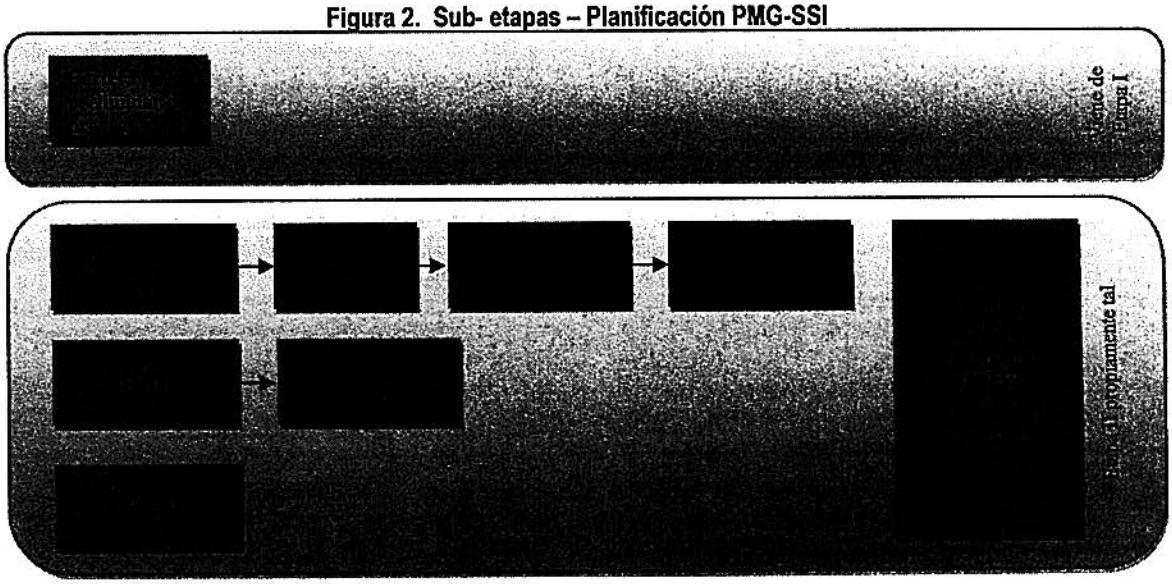
El resultado de la información levantada en la Etapa de Diagnóstico, será la guía para destinar los recursos institucionales disponibles.

¿Cómo se hace la planificación?

En el caso particular del Sistema de Seguridad de la Información, los proyectos/actividades que se incluyen en esta etapa adquieren la calidad de compromisos, a los cuales se les realizará un seguimiento que concluye en la etapa de Evaluación. Tales compromisos son la respuesta a las brechas priorizadas en el diagnóstico a través de la cartera preliminar de proyectos.

Para que la institución pueda cumplir tales compromisos debe trazar una ruta que organice el trabajo. Los elementos necesarios para desarrollar tal organización y garantizar su logro constituyen los requisitos técnicos de la segunda etapa.

Figura 2. Sub- etapas – Planificación PMG-SSI



1. Planificar acciones para llegar a definir una política de SI. Esto permite dar cumplimiento al requisito técnico de "Formulación de la documentación y las actividades necesarias para establecer en la institución

una Política General de SI". Se debe garantizar que se genere una declaración institucional que enfatice el compromiso de la dirección con los objetivos de gestión de SI.

2. Posteriormente, y en el marco del Plan General de SI, se debe elaborar la **"Cartera de proyectos"**. El producto de este punto, es la definición clara y operativa de los objetivos específicos que se buscan alcanzar para las actividades o proyectos resultantes del diagnóstico inicial, sobre aquellos ítems de los dominios que se califican con incumplimiento o cumplimiento parcial, y consiste en una breve descripción de cada aspecto a realizar, la especificación de un indicador de cumplimiento, las fechas estimadas de realización y la utilización aproximada de recursos de presupuesto. Para este propósito, se adjunta el anexo 2 "Cartera de Proyectos", cuya síntesis se describe en la tabla 2.1.

Tabla 7. Cartera de Proyectos

Nombre proyecto o actividad	Dominio PMG SSI	Proyecto PMG GE relacionado	Descripción	Evidencia de cumplimiento	Objetivo específico	Responsable	Fecha estimada inicio	Fecha estimada término	Prioridad	Presupuesto	Requiere asesoría externa	Nivel de Severidad	Comentarios

Descripción de campos a llenar

- **Nombre de proyecto o actividad:** Se debe definir una actividad o proyecto que resulte de una actividad calificada como "No cumple", o "Cumple parcialmente" del resultado obtenido en el diagnóstico (etapa I).
- **Dominio PMG SSI:** Se debe hacer referencia al dominio al cual dicho proyecto o actividad llevará a completar (ej.: Política de Seguridad, Control de Acceso, etc.).
- **Proyecto PMG GE relacionado:** Si se identifica un proyecto o actividad que se esté llevando a cabo en el Sistema Gobierno Electrónico, debe hacerse referencia al mismo.
- **Descripción:** Breve descripción de la actividad o proyecto a realizar.
- **Evidencia de cumplimiento:** Se debe describir la evidencia que se tendrá una vez realizado el proyecto o actividad (Ejemplo: Política de Seguridad confeccionada y sancionada por la autoridad).
- **Objetivo específico:** Se debe indicar qué objetivo se persigue al ejecutar esta actividad o proyecto de manera de ser considerado un indicador de eficacia del proyecto o actividad a realizar.
- **Responsable:** Indicar el responsable asignado para ejecutar el proyecto o actividad (puede ser un área o división específica, en cuyo caso la persona responsable es la jefatura).
- **Fecha estimada inicio:** Indicar la fecha aproximada de ejecución del proyecto.
- **Fecha estimada término:** Indicar la fecha aproximada de término de los trabajos.
- **Prioridad:** Indicar la prioridad de la actividad, teniendo en consideración los esfuerzos requeridos, el presupuesto existente y si es posible realizarlo con recursos propios (ejemplo: reconfiguración de manera segura de los sistemas de información, bases de datos, etc.).
- **Requiere asesoría externa:** Indicar si se requiere asesoría externa o se puede ejecutar con recursos propios.
- **Nivel de Severidad:** Se debe explicitar el nivel de severidad frente a la materialización del riesgo de no cumplir con la actividad o proyecto y como esta impacta a nivel institucional. Esto constituye un "Plan de Gestión de Riesgos del SSI" y se debe ejecutar considerando la metodología actual en

funcionamiento dentro del servicio. De no contar con ella, se sugiere implementar la metodología del Consejo de Auditoría Interna General de Gobierno (CAIGG).

- **Comentarios:** *Ingresar cualquier comentario adicional que sea de utilidad para la comprensión de la justificación de los proyectos y actividades por parte de la red de expertos.*

Para cada uno de los proyectos/actividades que se hayan priorizado se debe declarar uno o más objetivos específicos, que describen los logros concretos que se deben obtener para alcanzar el cumplimiento total de los dominios planteados anteriormente, en concordancia con los entregables definidos que conformarán la evidencia final. Estos objetivos se construyen a partir de los beneficios directos que se espera lograr con el proyecto y están, por tanto, directamente vinculados a los no cumplimientos o cumplimientos parciales identificados en la etapa de Diagnóstico. Los objetivos específicos muestran qué es lo que, en concreto, se pretende mejorar en cada uno de los dominios específicos evaluados, además de definir claramente cuál es el alcance del proyecto o actividad.

Para definirlos, primero debe cerciorarse de que existe una línea lógica consistente que parte con la identificación de no cumplimientos y oportunidades de mejora y llega a la definición de los beneficios esperados. De ser así, bastará que, a partir de los beneficios esperados, depure el alcance de su proyecto o actividad, determine claramente qué es lo que hará y qué no, y vuelva a redactarlos de tal forma que se transformen en los objetivos específicos. Una buena manera de hacerlo es comenzar con un verbo en infinitivo que indique la acción principal que se llevará a cabo en cada uno de los aspectos clave del proceso que se busca mejorar.

Cabe recordar que el proyecto o actividad no es el objetivo en sí, sino las mejoras que buscamos con su implementación, por lo tanto evite objetivos que sólo den cuenta de la implementación de las actividades o de alguna de las funcionalidades del proyecto (por ejemplo, "Contar con un set de políticas de seguridad de la información", "Contar con un comité de seguridad", etc.). Los objetivos que dan cuenta de los problemas y oportunidades de mejora que se busca con la intervención, constituyen quizás las definiciones más sensibles de su proyecto o actividad, pues reflejan de una forma concreta y medible el modo en que el servicio mejorará su gestión a través de la incorporación de controles de seguridad de la información, el cual es el propósito fundamental del Sistema de Seguridad de la Información del PMG. En este sentido, es especialmente relevante que los objetivos sean comprensibles, alcanzables y medibles, de forma tal que sea posible verificar su cumplimiento.

3. En orden a que los objetivos puedan ser medibles, se debe formular indicadores que permitan evaluar la eficacia en la implementación de las medidas tecnológicas y los controles de seguridad tendientes al cierre de las brechas detectadas en el diagnóstico. En este punto cabe tener presente que tales indicadores deben evaluar los resultados de la implementación en cuanto a su capacidad real de solucionar o mitigar las brechas, no sólo el hecho mismo de haber implementado la solución, teniendo presente que el sentido del SSI no es implementar los sistemas, sino que éstos finalmente cumplan el objetivo para el cual han sido diseñados.

4. La eficacia se refiere al grado de cumplimiento de los objetivos planteados, es decir, en qué medida el proyecto como un todo está cumpliendo con sus objetivos, sin considerar necesariamente los recursos asignados para ello9. Por eso, para medir la eficacia de un proyecto, es fundamental que haya claridad respecto de sus objetivos.

[9] Adaptado de: Guía Metodológica Sistema Planificación y Control de Gestión 2009 PMG. DIPRES.

5. Otras consideraciones importantes del diseño de los indicadores es la identificación adecuada de su temporalidad. Se debe considerar el momento en que los diferentes resultados deberían ocurrir y, por tanto, comenzar a medirse. Este momento dependerá de la naturaleza de los objetivos (proceso / productos / resultados).

6. Lo anterior es particularmente importante en el caso de objetivos cuyos resultados son de mediano y largo plazo y, por tanto, si bien es posible identificar indicadores, éstos no podrán ser medidos en lo inmediato. No obstante, esta identificación es útil para desarrollar los procesos necesarios para disponer de la información para las mediciones, cuando sea técnicamente recomendable realizarlas.

7. Todas las acciones mencionadas permitirán a la institución cumplir con el requisito técnico de "elaboración de la cartera de proyectos para la implementación de controles de seguridad de la información por dominio, priorizada a través de los criterios de gestión institucionales".

8. Uno de los requisitos a cumplir dentro de la segunda etapa es la "constitución del Comité de SI, roles e instancias de aprobación para el desarrollo del programa de implantación del SSI", lo cual se deberá reportar a través de un **acta constitutiva.** El Comité deberá ser presidido por la autoridad de la institución y al menos estar constituido por 1 integrante de Tecnologías de la Información, Recursos Humanos, El encargado de Seguridad y un asesor legal.

9. Como parte del trabajo de la segunda etapa está la "definición de una metodología de gestión de riesgos para los activos de información institucionales o adaptar una existente si es que se cuenta con ella". Este requisito técnico podrá reportarse obteniendo información respecto de qué técnicas y herramientas se utilizan actualmente en el servicio. Es posible que hayan algunas técnicas de gestión de riesgos aplicadas a otras materias del quehacer institucional, la cuales se pueden adaptar a las necesidades del SSI.

10. Una vez establecidos los objetivos y entregables de los proyectos o actividades, la institución estará en condiciones de determinar los recursos y el tiempo requerido para llevarlos a cabo. En este punto se debe elaborar un **Programa de Trabajo.** Este es una descripción detallada de los hitos y las actividades que se llevarán a cabo para implementar los proyectos. La información debe ser registrada en la tabla 8 "Programa de Trabajo" que se muestra a continuación:

Tabla 8. Programa de Trabajo

Nombre de la actividad o proyecto / Hitos y productos asociados	Actividades Asociadas	Fecha de Inicio	Fecha de Término	Actividad Precedente

Descripción de los campos a llenar

- **Nombre del Proyecto o Actividad e Hito Asociado:** Se debe completar con el proyecto o actividad definida e indicar el hito a cumplir una vez terminado el conjunto de actividades.
- **Actividades Asociadas:** Se debe desagregar el proyecto/actividad en todas las posibles actividades que sean involucradas.
- **Fecha de Inicio:** Fecha estimada de inicio de la actividad específica.
- **Fecha de Término:** Fecha estimada de término de la actividad específica.

- **Actividad Precedente:** se debe especificar si existe una actividad a desarrollar previo a la ejecución, para poder determinar posibles atrasos.

Para establecer los hitos y sus actividades, es útil pensar en el proyecto como una suma de etapas intermedias que entregan algún producto o marcan un hito en el desarrollo del mismo, y luego especificar las actividades necesarias para terminarlos. Es importante que el programa de trabajo tenga un nivel de detalle apropiado para chequear el avance de su desarrollo.

Es importante destacar que, para efectos del sistema de Seguridad de la Información del PMG, se entenderá finalizada la implementación de un proyecto o actividad cuando ésta se encuentre en régimen de operación, por lo que es de suma importancia que se estimen adecuadamente los plazos y recursos que permitan cumplir con los requisitos y compromisos asumidos en esta etapa de Planificación. Por tal razón, el planteamiento de hitos debe considerar entregables que permitan verificar que los proyectos se encuentran implementados y operando.

11. Aún cuando la información requerida para este punto es sólo la descrita, es altamente recomendable el uso de herramientas que han sido especialmente diseñadas para la planificación y seguimiento de proyectos, como por ejemplo:

    - Carta Gantt: Diagrama que muestra, con diferentes niveles de detalle, las actividades de un proyecto, su calendarización, recursos, responsables, interrelaciones y/o dependencias.
    - Línea crítica o CPM (Critical Path Method): Secuencia de los elementos terminales de la red de actividades de un proyecto, con la mayor duración agregada, de tal forma que la duración de la ruta crítica determina la duración del proyecto entero y cualquier retraso en un elemento terminal en la ruta crítica impacta directamente la fecha de término planificada del proyecto.
    - Técnica de Revisión y Evaluación de Programas o PERT (Program Evaluation Review Technique): Modelo para la administración y gestión de proyectos, que permite analizar las tareas necesarias para completar un proyecto dado, especialmente la duración de cada tarea, identificando el tiempo mínimo necesario para completar el proyecto.

Ejemplo de Carta Gantt:

- Desarrollar y Sancionar Política General de Seguridad	80 días	mié 04-02-09	mar 26-05-09	100%
- Definición de temas relevantes para a Política General de Seguridad	80 días	mié 04-02-09	mar 26-05-09	100%
Declaración Institucional sobre el Gobierno de Seguridad de la Información (Compromiso)	62 días	mié 04-02-09	jue 30-04-09	100%
Definición del ámbito	5 días	mié 04-02-09	mar 10-02-09	100%
Definición de los controles y sanciones por incumplimiento de la política	5 días	mié 11-02-09	mar 17-02-09	100%
- Definición de roles y responsabilidades	6 días	mié 18-02-09	mié 25-02-09	100%
Definición Comité de Seguridad de la Información	2 días	mié 18-02-09	jue 19-02-09	100%
Definición de Encargado de Seguridad de la Información	2 días	vie 20-02-09	lun 23-02-09	100%
Definición de Comité de Incidentes	2 días	mar 24-02-09	mié 25-02-09	100%
- Definición de Reglas para las Políticas de Seguridad de la Información	16 días	mar 03-03-09	mar 24-03-09	100%
Modelo - Metodología a utilizar	2 días	mar 03-03-09	mié 04-03-09	100%
Estructura y contenido de las políticas de seguridad	2 días	jue 05-03-09	vie 06-03-09	100%
Definición de cumplimiento desde el punto de vista legal (Decretos Supremos y Legislación vigente)	2 días	lun 09-03-09	mar 10-03-09	100%
Definición de formato estándar de políticas	2 días	mié 11-03-09	jue 12-03-09	100%
Definición de gestación de políticas	2 días	vie 13-03-09	lun 16-03-09	100%
Definición de aprobación de políticas	2 días	mar 17-03-09	mié 18-03-09	100%
Definición de difusión de políticas	2 días	jue 19-03-09	vie 20-03-09	100%
Definición de revisión de políticas	2 días	lun 23-03-09	mar 24-03-09	100%
Acta de aprobación	1 día	mié 01-04-09	mié 01-04-09	100%
Revisión por miembros Comité de Seguridad	1 día	jue 09-04-09	jue 09-04-09	100%
Ejecución de cambios	5 días	vie 10-04-09	jue 16-04-09	100%
Liberación versión N°1	1 día	vie 17-04-09	vie 17-04-09	100%
Confección presentación para difusión a alta dirección	5 días	lun 20-04-09	vie 24-04-09	100%
Presentación y aprobación Director	2 días	lun 27-04-09	mar 28-04-09	100%
Política aprobada - Publicación y Difusión en Intranet Corporativa - Mail Masivo	20 días	mié 29-04-09	mar 26-05-09	100%
Hito 1 - Política General de Seguridad de la Información Implantada.	0 días	mar 26-05-09	mar 26-05-09	100%

El uso de este tipo de herramientas permitirá el reporte del requisito técnico "identificación de una ruta crítica que asegure que se complete cada proyecto".

12. Dentro de las medidas que se deben tomar para asegurar que cada proyecto se llevará a cabo, se debe establecer un "Plan de mitigación de riesgo que defina los riesgos asociados a cada proyecto y sus acciones para resolverlos". Este requisito técnico debe consignar el estado actual del riesgo, nivel de criticidad, las personas responsables de la mitigación, etc. La información debe ser registrada en la tabla 9 "Programa de Trabajo" que se muestra a continuación:

Tabla 9. Plan de Mitigación de Riesgos.

Riesgo	Frecuencia	Severidad	Impacto	Causa	Daño	Acción de Mitigación	Responsable

Descripción de campos a llenar

- **Riesgo:** Específica el ámbito en donde se observa el riesgo, puede ser:
  - *Personas* (clientes, usuarios finales, actores involucrados, equipo de trabajo, personas de la organización, experiencias, habilidades, etc.)
  - *Procesos* (objetivos, características del proyecto, presupuesto, costos y cronograma, requerimientos, diseño, desarrollo, testing, etc.)
  - *Tecnología* (seguridad, ambiente de desarrollo y testing, herramientas de desarrollo, ambiente de operación y soporte, etc.)

- *Ambiental* (aspectos legales, regulaciones económicas, tecnológicas o de negocio, etc.).

- **Frecuencia:** Indica las veces que dicho evento puede presentarse durante el desarrollo del proyecto. Asignar un valor entero, siendo:
  - 4=Muy Alta
  - 3=Alta
  - 2=Media
  - 1=Baja
- **Severidad:** Magnitud apreciada del daño sobre el beneficio u objetivos del Proyecto, si el evento se presenta. Valor entero entre 1 y 4, siendo:
  - 1=No Significativo
  - 2=Significativo
  - 3=Importante
  - 4=Catastrófico
- **Impacto:** Producto de la Frecuencia y Severidad, lo cual es usado como una base para ordenar y priorizar los riesgos.
- **Causa:** Identifica la causa del riesgo.
- **Daño:** Identifica los potenciales resultados de la ocurrencia del riesgo.
- **Acción de Mitigación:** Describe las acciones a llevar a cabo para mitigar el riesgo
- **Responsable:** Indica el responsable de observar el estado del riesgo y si este cambió en términos de su probabilidad o impacto.

13. Es necesario definir un programa de seguimiento que contenga el calendario de mediciones parciales para observar la evolución de los resultados esperados y posibles desviaciones, el cual servirá de insumo para el desarrollo de la Etapa de Evaluación. Este seguimiento se orienta a la observación de resultados obtenidos y se realiza una vez que ha concluido la implementación de las actividades propuestas. Para este fin es necesario considerar un tiempo de medición de, al menos, cuatro meses para obtener resultados estables de la operación de los proyectos o actividades desarrolladas, considerando un mínimo de 2 meses por cada objetivo comprometido.

    El producto final de este punto es un calendario de mediciones parciales de cada actividad/proyecto comprometido, el que además registra los valores esperados a la fecha de cada medición. Dicha información debe ser registrada en la tabla 2.4 "Programa de Seguimiento", que se muestra a continuación:

Tabla 10. Programa de Seguimiento

Nombre de Actividad o Proyecto	Dominio PMG SSI	Fecha de Medición	Valor (%) de Avance Esperado	Valor (%) de Avance Real

Descripción de campos a llenar

- **Nombre de Proyecto o Actividad:** Se debe completar con el proyecto o actividad definida.
- **Dominio PMG SSI:** Se debe hacer referencia al dominio al cual dicha actividad o proyecto llevará a completar (ej.: Política de Seguridad, Control de Acceso, otros).
- **Fecha de Medición:** son las fechas estimadas en las cuales se medirá el estado de avance de cada actividad o proyecto definido.
- **Valor (%) de Avance Esperado:** Es el valor del porcentaje de avance esperado al momento de realizar la proyección inicial
- **Valor (%) de Avance Real:** Es el valor del porcentaje de avance real a la fecha de la medición.

14. Teniendo claridad respecto de la planificación y sus objetivos, se debe poner en marcha un "plan de capacitación del personal clave, y sensibilización de todos los funcionarios, con el detalle de las actividades a realizar para instalar en las personas la importancia de contar con un SSI", lo que constituye un requisito técnico. Éste apunta fundamentalmente a gestionar de manera efectiva el cambio organizacional que amerita la puesta en marcha del SSI, incorporando nuevas prácticas y rutinas de trabajo a las cuales las personas no necesariamente estarían habituadas.

15. En esta misma línea la institución desarrolla un "plan de difusión del Programa de Trabajo Anual, aprobado por la autoridad superior del servicio", el que unido a la capacitación, está atendiendo a la premisa de que finalmente serán las personas quienes van a garantizar el logro de los resultados esperados para cada proyecto. Aunque los medios tecnológicos y los procesos estén diseñados adecuadamente, si las personas no los ponen en práctica, si no los comprenden ni valoran, definitivamente no habrá resultados favorables.

16. Finalmente se debe mostrar evidencia de la difusión realizada, considerando el "objetivo general y específico de las iniciativas y los proyectos a implementar"; el "mensaje central que debe ser conocido e internalizado por los funcionarios involucrados"; los "canales de comunicación escogidos para difundir el mensaje"; y la "fecha de ejecución de las actividades consideradas para la difusión". Todos estos elementos constituyen requisitos técnicos del SSI.

¿Cómo se hace el informe de Planificación del SSI?

Campo	Descripción	¿Qué se espera?	Entregable a la Red de Expertos
Política de Seguridad de la Información	Declaración institucional que enfatiza el compromiso de la dirección con los objetivos de gestión de SI.	Apoyo y compromiso de la autoridad con la seguridad de la información, a través de la emisión y mantenimiento de una política de seguridad de la información en toda la organización.	Política de Seguridad de la Información
Proyectos	Breve descripción de cada aspecto a realizar, la especificación de un indicador de cumplimiento, las fechas estimadas de realización y la utilización aproximada de recursos de presupuesto.	Definición clara y operativa de los objetivos específicos que se buscan alcanzar para las actividades o proyectos resultantes del diagnóstico inicial, sobre aquellos ítems de los dominios que se califican con incumplimiento o cumplimiento parcial.	Cartera de proyectos
Conformación del Comité de Seguridad	Roles e instancias de aprobación para el desarrollo del programa de implantación del SSI.	Instalación del Comité de SI a través de un acta, que incorpore a la autoridad de la institución, 1 integrante de Tecnologías de la Información, Recursos Humanos, El encargado de Seguridad y un asesor legal.	Acta constitutiva del Comité de SI.
Gestión de Riesgo	Conjunto de técnicas y herramientas destinadas a mitigar riesgos para los activos de información institucionales	Definición de un Plan de Gestión de Riesgos del SSI	Metodología de Gestión de Riesgos (ya existente en el servicio) Plan de mitigación de riesgo (de acuerdo a tabla 9) Plan de Gestión de Riesgos del SSI (de acuerdo al anexo 2, campo "Nivel de Severidad")
Programa de Trabajo	Detalle de los hitos y las actividades que se llevarán a cabo para implementar los proyectos.	Para cada proyecto, los hitos, actividades, fechas de inicio y término.	Programa de trabajo
Programa de Seguimiento	Es la ruta crítica definida para asegurar que el proyecto se lleve a cabo.	Uso de herramientas de gestión y seguimiento de proyectos para verificar su cumplimiento.	Carta Gantt, Diagramas PERT, CPM, etc.

Campo	Descripción	¿Qué se espera?	Entregable a la Red de Expertos
Capacitación y Difusión	Conjunto de actividades estructuradas para dar a conocer a los funcionarios el Programa de Trabajo para la implementación del SI y contar con su colaboración.	La realización de tales actividades debe facilitar la implementación, producto de la sensibilización de los funcionarios, que con diferentes niveles de responsabilidad deberán participar en los proyectos.	Plan de capacitación, plan de difusión y evidencias (listados de participación en cursos, piezas gráficas utilizadas, etc.)
Documentos referidos	Para cada uno de los requisitos técnicos se deberá desarrollar la documentación que los respalde (evidencia).	Desarrollar y sistematizar la documentación electrónica que da cuenta de la planificación para la puesta en marcha del SSI.	Carpeta electrónica que contenga toda documentación relacionada con la planificación del SSI, siendo consistente con el marco regulatorio para el traspaso de información gubernamental.

Plazos y Medios

Los informes de Estado de Avance (detallados en la guía metodológica, sección Ejecución del Diagnóstico) deben ser enviados en formato electrónico, a través de un acceso Web que será informado oportunamente.

Se debe entregar un informe de pre-validación a mediados de año y un informe final, al término del año. Sin embargo, se recomienda un monitoreo mensual a los encargados PMG, con énfasis en el primer semestre para que en base a esa información se pueda apoyar la formulación presupuestaria con miras al siguiente periodo administrativo.

Los plazos específicos serán informados oportunamente por el organismo técnico validador.

Recuerde que para eximirse de alguna etapa o solicitar cualquier modificación a los objetivos de gestión comprometidos por su institución con el sistema, debe hacerlo directamente a la Dirección de Presupuestos en los plazos y formas establecidos para ello. Para mayor información sobre el particular, por favor visite el sitio www.dipres.cl.

Este documento y todas sus futuras revisiones serán publicados en el sitio Web:
http://pmg.ssi.gov.cl
Y en el sitio de DIPRES:
http://www.dipres.gov.cl/572/propertyvalue-15533.html

Este documento de origen electrónico, una vez impreso, pasa a ser copia no controlada y puede quedar obsoleto. Para la versión vigente, ir a los sitios señalados previamente.

Historial de revisiones

Nº Revisión	Fecha Aprobación	Motivo de la revisión	Páginas Modificadas	Autor
1	04/02/2010	Elaboración inicial	Todas	Pablo Morán Hernán Espinoza Jorge Sanchez
2	15/02/2010	Correcciones de contenido, estilo, lenguaje, ordenamiento y presentación de temas.	Todas	Waldo Gómez (DIPRES) Jimena Zenteno (DIPRES)
3	15/02/2010	Correcciones ortográficas y reemplazo de palabras	10, 13, 22, 23	Pablo Morán
4	19/02/2010	Correcciones de puntuación, ortografía, inserción dominio 6.	Todas excepto portada	Jimena Zenteno (DIPRES)
5	04/03/2010	Correcciones de contenido, ordenamiento y presentación de temas.	Todas	Carola Córdova
6	08/03/2010	Reordenamiento y presentación de los contenidos; incorporación de requisitos técnicos a las etapas I y II.	Todas	Carola Córdova
7	09/03/2010	Incorporación ítems de gestión de riesgos	22 y 26	Waldo Gómez
8	11/03/2010	Cambio de Logo Nuevo Gobierno Compaginación – Índice - Anexos	Todas	Jimena Zenteno
9	15/03/2010	Títulos, referencias, revisión completa	1,12,32	Felipe Morales
10	19/03/2010	Ajustes de formato y diagramas de cada etapa	Todas	Carola Córdova