GUÍA METODOLÓGICA 2015

INDICADOR TRANSVERSAL SSI

SISTEMA DE SEGURIDAD DE LA INFORMACIÓN
PROGRAMA MARCO PMG 2015

Versión 1, Abril 2015

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

Contenido

Objetivo y Alcance de esta Guía Metodológica

Objetivo

El objetivo de esta Guía es presentar de manera detallada el desarrollo de cada uno de los requisitos técnicos asociados a las distintas actividades necesarias para la medición del Indicador Transversal del Sistema de Seguridad de la Información, en el contexto del Programa Marco de los Programas de Mejoramiento de la Gestión para el año 2015 (PMG/MEI SSI)[1], según lo establecido en el Decreto Exento N° 239/2014 del Ministerio de Hacienda, facilitando a los servicios públicos verificar el cumplimiento de los objetivos comprometidos.

Alcance de la Guía Metodológica

Esta Guía entrega los lineamientos para la presentación de los requisitos técnicos del Sistema de Seguridad de la Información (SSI), en el contexto de los objetivos de gestión establecidos en el Decreto(E) N° 239 para el sistema de Monitoreo del Desempeño, y en particular para el Objetivo N° 2, que dice relación con el indicador de gestión transversal (N°6) para el SSI.

Las instituciones que a la fecha hayan comprometido etapas para seguir desarrollando el Sistema de Seguridad de la Información durante el presente año (y que por tanto no hayan egresado aun de su etapa 4), deberán remitirse a los antecedentes de Guía Metodológica 2014 e instrumentos asociados, los cuales se encuentran disponibles y publicados en el sitio web de DIPRES (www.dipres.cl) sección “Sistema Seguridad de la Información”, apartado “Antecedentes 2014”

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 comprometidos en el Sistema. Sin embargo, a lo largo de la Guía se enfatizan ciertos aspectos en los que se considera conveniente profundizar.

Cómo usar esta Guía Metodológica

El cuerpo central de la Guía se divide en tres partes: La primera de ellas describe el SSI, sus objetivos y elementos constitutivos. En una segunda parte, más extensa, se detallan las etapas de Diagnóstico y Planificación del Sistema, sus interrelaciones, las acciones necesarias para su desarrollo y los medios para reportar la medición del indicador transversal a la Red de Expertos del PMG/MEI.

Una vez estudiados tales antecedentes, en el anexo I de la Guía se entregan instrucciones sobre la forma en que se debe completar los instrumentos dispuestos por la Red de Expertos para verificar el cumplimiento de los requisitos técnicos en las diferentes etapas. Es recomendable ajustarse a tales instrucciones con el objeto de dar cuenta de manera completa y coherente a los requisitos.

[1] Cuando este documento menciona el Sistema de Seguridad de la Información (SSI), se refiere al mismo en el marco del PMG y las MEI, indistintamente.

Sistema de Seguridad de la Información

Antecedentes

A raíz de la publicación de la Ley Nº 19.799 Sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de dicha firma, en el año 2004 se publicaron una serie de Decretos Supremos a fin de reglamentar distintos aspectos de la mencionada ley, en el marco del concepto de "Gobierno Electrónico" y del proceso de modernización del Estado. Uno de esos instrumentos, el Decreto Supremo N° 83 / 2005 - SEGPRES, planteó un código de prácticas para la gestión de la seguridad de la información en los órganos del Estado.

Hacia el año 2007 el Ministerio del Interior, en su rol de Coordinador del Subcomité de Gestión de Seguridad y Confidencialidad de Documentos Electrónicos, detectó que en las instituciones del sector público persistían algunas falencias respecto de estos temas, entre las cuales se menciona: aplicaciones y sistemas informáticos con configuración inadecuada, sitios web de gobierno implementados deficitariamente y con vulnerabilidades conocidas, redes informáticas institucionales con debilidades en sus mecanismos de control de acceso y de regulación del tráfico de datos, problemas de continuidad operacional frente a incidentes de índole recurrente, como cortes de energía eléctrica, e inexistencia de políticas de seguridad institucionales.

A mediados del año 2009 el Comité de Ministros que rige el desarrollo del Programa de Mejoramiento de la Gestión (PMG), en el marco de la ley Nº 19.553, toma la decisión de incluir a partir de 2010, al Sistema de "Seguridad de la Información" como parte del Área de Calidad de Atención a Usuarios, con el fin de enfrentar los problemas de seguridad detectados y cuya asistencia técnica queda a cargo de la Red de Expertos, conformada por analistas de la Secretaría y Administración General del Ministerio del Interior y de la Dirección de Presupuestos del Ministerio de Hacienda, para darle el debido impulso a la implementación de las normativas de gestión de seguridad.

Igualmente, durante el año 2011, en el contexto de la Ley 20.212, se realiza lo propio para las Metas de Eficiencia Institucional, a ser incorporadas a partir del 2012.

En este contexto se incluyó la Norma Chilena NCh-ISO 27001.Of2009 como referente normativo, cuya propuesta incorpora todo tipo de activos de información, complementando al DS 83.

Actualmente, el ya mencionado Decreto Exento N° 239/2014 del Ministerio de Hacienda, establece como requisito técnico para el Indicador Transversal del SSI la utilización los controles de seguridad establecidos en la normativa vigente, esto es la NCh-ISO 27001.Of **2013**

Objetivo del SSI

El objetivo del Sistema de Seguridad de la Información (SSI) es "*lograr niveles adecuados de integridad, confidencialidad y disponibilidad para toda la información institucional relevante, con el objeto de asegurar continuidad operacional de los procesos y servicios, a través de un sistema de gestión de seguridad de la información*".

Ventajas de contar con un SSI

El SSI es una herramienta de apoyo a la gestión de una institución pública. Dado que la información es uno de los componentes más importantes de toda organización moderna, requiere ser protegida convenientemente (junto a los procesos y sistemas que la manejan) frente a amenazas que puedan poner en peligro la continuidad de los niveles de servicio, rentabilidad social y conformidad legal, necesarios para alcanzar los objetivos institucionales.

Hoy en día, el conjunto de activos de información institucional (documentos, bases de datos, sistemas y software de aplicación, personas, equipos informáticos, redes de transmisión de datos, datacenter, soportes de almacenamiento, y otros elementos de infraestructura) están sujetos a diferentes tipos de amenazas e inseguridades, tanto desde dentro de la propia organización como desde fuera de ella.

Una adecuada gestión de la seguridad de la información, da la posibilidad de disminuir en forma significativa el impacto de los riesgos a los que están expuestos los activos de información. Para ello se hace necesario conocerlos y afrontarlos de manera ordenada, y a través de la participación proactiva de toda la institución, establecer los procedimientos adecuados y planificar e implantar **controles de seguridad** basados en una evaluación de riesgos y en una medición de la eficacia de los mismos.

Por otra parte, el SSI permite ir conformando un marco de gobierno para la seguridad de la información institucional, al establecer políticas, procedimientos y controles en relación a los objetivos estratégicos de la institución, con objeto de mantener siempre el riesgo por debajo del nivel aceptable por la propia organización. Para ello se contempla la designación del Encargado de Seguridad de la Información, la conformación de un Comité de Seguridad y la aprobación de una Política General de Seguridad Institucional, que exprese adecuadamente el compromiso del alto directivo público.

A nivel estratégico, para los directivos de la institución, el SSI es una herramienta que les ofrece una visión global sobre el estado de sus activos de información, las medidas de seguridad que se están aplicando y los resultados que se están obteniendo de dicha aplicación. Todos estos datos permiten a la dirección una toma de decisiones sobre la estrategia a seguir. Mediante el SSI, la organización puede **conocer los riesgos** a los que está sometida su información **y gestionarlos mediante una planificación** definida, documentada y conocida por todos, que debe ser revisada y mejorada constantemente, atendiendo a los controles y objetivos de control que propone la normativa NCh-ISO 27001.Of2013.

Desde el punto de vista del desempeño institucional, facilita la entrega fluida de los bienes y servicios a los clientes/usuarios/beneficiarios, mediante la formulación de un **Plan de Continuidad Institucional**, que permite asegurar de forma correcta la **continuidad operacional** para los procesos institucionales relevantes, la **contingencia tecnológica**, especificando escenarios de catástrofe y fallas a enfrentar, y el **manejo de crisis**, estableciendo la estrategia de gestión en situaciones de contingencia.

Roles y responsabilidades en el SSI Institucional

Para el desarrollo del SSI, será necesario aunar el trabajo de los profesionales y técnicos de todas las áreas, con el fin de implementar adecuadamente los proyectos de interés institucional. Este equipo multidisciplinario permitirá establecer las responsabilidades, logrando la especialización en cada uno de los dominios de la NCh-ISO 27001, obteniendo resultados de calidad satisfactoria.

Dentro del desarrollo del Sistema se debe 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 soporten la intervención de los procesos que se buscan mejorar. El rol que cumplen, no puede delegarse sin una significativa pérdida de credibilidad respecto a la seriedad del esfuerzo.

   En el caso específico del **Jefe de Servicio**, concretamente es quien aprueba las políticas de seguridad y valida el proceso de gestión de Seguridad de la Información, sanciona las estrategias y mecanismos de control para el tratamiento de riesgos que afecten a los activos de información institucionales, que se generen como resultado de los reportes o propuestas del Comité de Seguridad de la Información (CSI), así como los recursos necesarios para su ejecución.

2. **Comité de Seguridad de la Información (CSI).**
   Tiene la responsabilidad de supervisar la implementación de procedimientos y estándares que se desprenden de las políticas de seguridad de la información, proponer estrategias y soluciones específicas para la implantación de los controles necesarios para materializar las políticas de seguridad establecidas y la debida solución de las situaciones de riesgo detectadas, arbitrar conflictos en materia de seguridad de la información y los riesgos asociados, y proponer soluciones sobre ello, coordinarse con los Comités de Calidad y de Riesgos de la institución, para mantener estrategias comunes de gestión y reportar a la Alta Dirección, respecto a oportunidades de mejora en el SGSI, así como de los incidentes relevantes y su gestión.

   Se recomienda que el CSI esté integrado por los siguientes funcionarios:
   a) Jefe Operaciones o Tecnologías de Información.
   b) Jefe de Recursos Humanos.
   c) Encargado de Calidad.
   d) Encargado de Riesgos.
   e) Asesor Jurídico (Abogado de la Institución).
   f) Jefes de Áreas Funcionales o encargados de procesos, si corresponde.
   g) Encargado de Seguridad de la Información (ESI).

3. **Encargado de Seguridad de la Información (ESI).**
   Es un funcionario nombrado por el Jefe de Servicio como su asesor directo en materia de seguridad de la información. Debe organizar las actividades del CSI, coordinar la debida

respuesta y priorización al tratamiento de incidentes y riesgos vinculados a los activos de información de los procesos institucionales y sus objetivos de negocio, monitorear el avance general de la implementación de las estrategias de control y tratamiento de riesgos, tener a su cargo el desarrollo inicial de las políticas de seguridad al interior de la institución, controlar su implementación y velar por su correcta aplicación, así como mantener coordinación con otras unidades del Servicio para apoyar los objetivos de seguridad y establecer puntos de enlace con los Encargados de Seguridad de otros organismos públicos y especialistas externos, que le permitan estar al tanto de las tendencias, normas y métodos de seguridad pertinentes.

4. **Profesionales y técnicos.**
   Un elemento importante en el equipo multidisciplinario que implementa y opera en el SSI 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 a los cargos, dado que ellos entregarán los antecedentes y atenderán los requerimientos en la práctica.

5. **Otros funcionarios.**
   Además, será necesario incluir al personal que pueda ser relevante para el correcto desarrollo del programa de implantación del SSI, ya sea directa o indirectamente, entre otros: personal a cargo de la gestión de calidad, dueños de procesos estratégicos de la institución o de procesos de provisión de productos y servicios, abogados/as del área jurídica, profesionales del área de tecnologías de la Información, personal del área de recursos humanos y de gestión de riesgo.

Rol de la Red de Expertos

La Red de Expertos del SSI, tiene como misión fundamental brindar asistencia técnica a las instituciones que comprometen etapas del SSI. Para ello contempla las siguientes funciones:

1. Proponer los Requisitos Técnicos del Sistema al Comité de Ministros del PMG/MEI.
2. Diseñar la Guía Metodológica e instrumental para el desarrollo del Sistema.
3. Realizar labores de asistencia técnica directa en el desarrollo del SSI, al personal encargado por parte de cada institución.
4. Elaborar un cronograma de trabajo global para establecer hitos en la asistencia técnica, que permitan conocer el avance de las instituciones participantes.
5. Evaluar el avance presentado por las instituciones durante la ejecución del SSI.
6. Asesorar a la Secretaría Técnica del PMG/MEI, en materias relacionadas con la preparación del proceso de validación final del Sistema.

Factores críticos de éxito

La experiencia ha demostrado que los siguientes factores con frecuencia son críticos para una exitosa implementación de la seguridad de la información dentro de una organización:

1. Una política de seguridad debidamente formalizada por el Jefe de Servicio, que establezca el alcance, objetivos, roles, responsabilidades y actividades que permitan gestionar la seguridad de la información, para proteger los activos relevantes y lograr el debido cumplimiento de la la misión institucional.
2. Un enfoque de gestión para implementar, mantener, monitorear y mejorar la seguridad de la

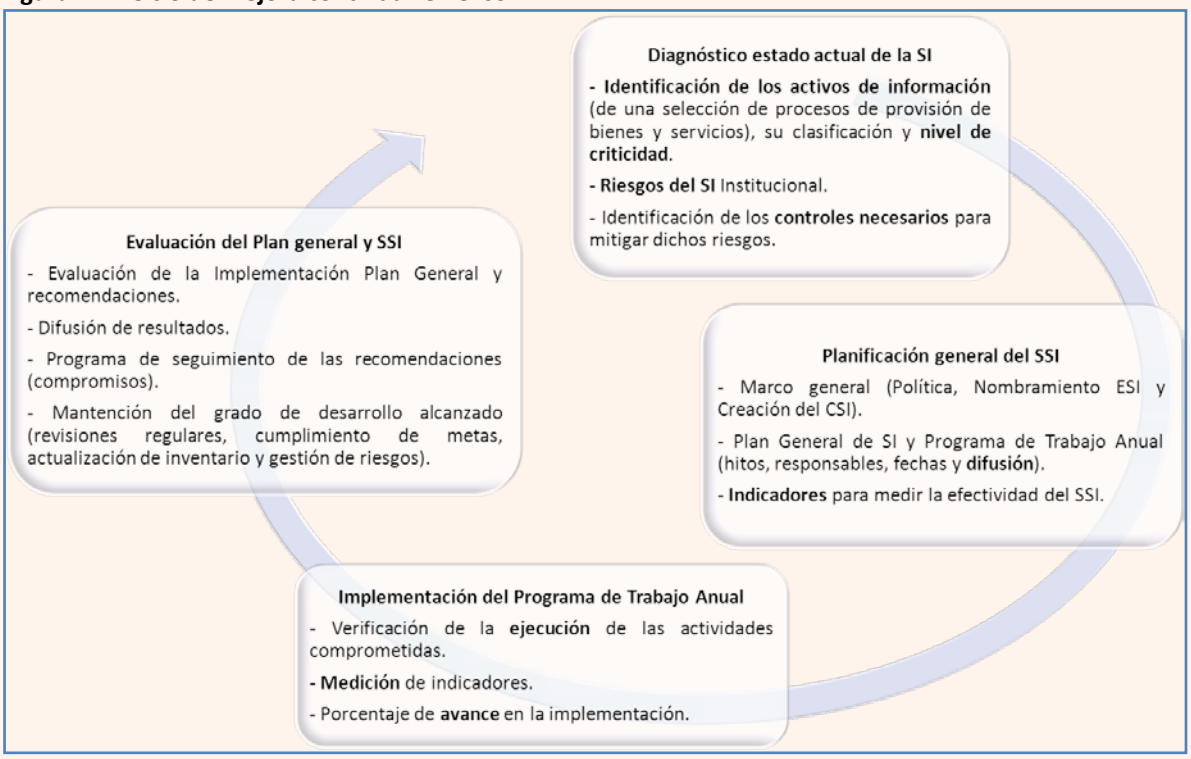
información que sea consistente con la cultura institucional.
3. El apoyo visible y compromiso constante de la alta dirección con el enfoque anterior.
4. Comprensión de los requisitos de seguridad, de evaluación del riesgo y de su gestión.
5. Comunicación efectiva en la seguridad de la información con todos los directivos, jefes de división, funcionarios y otras partes interesadas.
6. Distribución de lineamientos sobre la política de seguridad de la información para todos los jefes de división, funcionarios y otras partes involucradas.
7. Provisión de recursos para las actividades de gestión de la seguridad de la información.
8. Provisión del conocimiento, capacitación y educación apropiados para lograr conciencia sobre el tema.
9. Un proceso de gestión de incidentes de seguridad de la información.
10. Implementación de un método de medición para evaluar el desempeño en la gestión de la seguridad de la información y adoptar las sugerencias de mejoramiento.

Estos factores se tornan operativos a través de los controles, procedimientos o estándares que se deben ir implementando progresivamente en el SSI.

Descripción general del ciclo de mejora para el Sistema

El SSI ha sido concebido con una estructura compuesta de cuatro etapas que son de carácter progresivo y acumulativo: Diagnóstico, Planificación, Implementación y Evaluación. Estas cuatro etapas reflejan el ciclo de mejora continua (PDCA: Plan – Do – Check - Act), como se observa en la figura1, integrando en ellas los principales elementos constitutivos del SSI.

Figura N°1: Ciclo de mejora continua en el SSI



Fuente: Elaboración propia.

TAREA DE MEDICION del INDICADOR TRANSVERSAL DEL SSI

¿Que es necesario hacer en 2015, para poder medir el indicador propuesto?

El indicador transversal 2015 mide simplemente el grado de adherencia institucional a la normativa NCh-ISO 27001.Of 2013, una vez que la institución ha logrado realizar al menos un ciclo completo de mejora continua para el SSI.

Para ello se debe considerar que el **Indicador Transversal** del SSI se calcula como un cociente entre los **controles efectivamente cumplidos** versus el **Total de Controles** establecidos en la normativa.

En la etapa de **Diagnóstico** institucional, se identifican y priorizan los activos relevantes de información que sustentan los procesos de provisión institucionales. Dicha identificación debe considerar información que fluye en las principales etapas de dichos procesos, las personas que participan en dichas etapas y la infraestructura asociada, de modo tal que se llegue a conformar

un Inventario de activos de información, debidamente caracterizado. Asimismo, esta etapa exige la realización de un análisis de los riesgos que afectan a tales activos, posibilitando identificar controles y objetivos de control, a partir de los elementos señalados en la NCh-ISO 27001.Of2013

Como producto de esta etapa se obtiene un **inventario de activos estructurado** que debe ser objeto de actualización permanente, a lo largo del ciclo de vida del Sistema. Esta es la base para comenzar con el correspondiente **Análisis de Riesgos**, que debe ser construido a partir del análisis de las amenazas y vulnerabilidades a los que se encuentran expuestos cada uno de los activos identificados en el inventario.
Para el presente año, se admiten también otras metodologías de análisis y gestión de riesgos corporativos, siempre y cuando permitan presentar un análisis de riesgo con el mayor grado de detalle posible, enfocado en los procesos de provisión institucional, sus actividades, actores y activos.
Para profundizar en análisis de riesgos corporativos, se puede acudir a las siguientes fuentes:

- CAIGG, revisar apartado Líneas de Acción / Gestión de Riesgos, en el sitio web http://www.auditoriainternadegobierno.cl/
- Norma NCh-ISO 31000:2012 - Principios y Directrices para la Gestión de Riesgos.
- Marco COSO ERM - www.coso.org.

Una vez realizado el Diagnostico, se realiza la **Planificación**, donde se toman aquellos controles que se hayan declarado como NO cumplidos en la etapa de diagnóstico, y en base a los productos esperados que se señalen para abordarlos, se formulan iniciativas para su adecuada implementación, que deberían ser volcadas en programas de trabajo de carácter anual. En esta etapa además se deben establecer los elementos del marco de gobierno para la seguridad de la información institucional, y adicionalmente formular los indicadores de desempeño que se usarán posteriormente para realizar mediciones sobre la efectividad del SSI.

En la etapa de **Implementación**, se ejecutan las iniciativas incluidas en el programa de trabajo anual y se miden los indicadores de desempeño formulados.

Para el reporte del **INDICADOR TRANSVERSAL** se debe presentar los documentos correspondientes que permitan dar cuenta del cumplimiento de los requisitos técnicos del SSI:

-Análisis de Riesgo (y Hoja de Inventario de Activos cuando corresponda)
-Medios de verificación asociados a los cumplimientos declarados
-Informe de Justificación de Brechas

En la siguiente figura se especifican para cada una de ellas:

Figura N°2: Documentos a presentar por etapas del SSI

- **Planilla de instrumentos:**
  Hoja Análisis de Riesgos
  Hoja Plan General
  Hoja Inventario de Activos (opcional)

- Conjunto de Archivos correspondientes a los **Medios de Verificación** para cada **control cumplido**.

- **Informe Final** de **Justificaciones** (Brechas)**.**

Diagnóstico

Acciones a realizar

1. Seleccionar un conjunto de procesos de provisión institucional que defina el alcance del sistema. Dicha selección deberá justificarse en el Informe Final de Justificaciones (Brechas) y presentarse a la Red de Expertos.

2. Diagnosticar la situación de Seguridad de la Información institucional, poniendo énfasis en la adecuada identificación de los **activos de información** que estén vinculados a las diferentes etapas relevantes de los procesos (y eventualmente Sub-procesos) de provisión seleccionados, para lo cual se deben considerar los elementos de información (Bases de Datos, Documentos, etc.) que fluyen en las principales etapas de dichos procesos, las personas que participan en dichas etapas y la infraestructura asociada (oficinas, espacios de trabajo, equipos, sistemas informáticos, etc.) , así como las características básicas de tales activos, que incluyan además el respectivo análisis de criticidad de cada uno de ellos, en función de los niveles de confidencialidad, integridad y disponibilidad. Lo anterior debe permitir la conformación de un **inventario** de activos de información debidamente priorizado en términos de su criticidad.

3. Para cada uno de los activos declarados con criticidad media o alta, se deberán especificar el o los riesgos más relevantes. Asimismo, para cada riesgo identificado, se le deberá asociar uno o más controles de mitigación (de los dominios de seguridad normativos que sean pertinentes), considerando para ello la naturaleza del riesgo, el tipo de activo y la criticidad declarada para el activo.

4. Con respecto a cada uno de tales controles de mitigación de riesgos, se deberá señalar el debido **cumplimiento**, es decir declarando que el control se encuentra cumplido cuando se encuentra implementado y operando al momento del diagnóstico, o bien que dicho control no se encuentra implementado y constituye en consecuencia una brecha por abordar.

5. Cada control no cumplido, genera una brecha que debe ser abordada posteriormente en el Plan General de Seguridad de la Información institucional.

Documentos a entregar

D1. Alcance del SSI.
El diagnóstico se focaliza en la correcta identificación y caracterización de los activos de información de la institución, que están vinculados en especial a sus **procesos de provisión** los permiten la obtención de los productos estratégicos (ver Ficha de Definiciones Estratégicas, formulario A1 de cada servicio, en el sitio www.dipres.gob.cl).

Para comenzar con las actividades requeridas en el diagnóstico, es preciso establecer el alcance del Sistema, esto es decidir si se ampliará la selección de los procesos de provisión de bienes y servicios realizada el año anterior o se realizará una mejora al diagnóstico. Para tomar tal decisión se debe adoptar como referencia aquellos declarados por la institución en sus definiciones estratégicas vigentes (Ficha A1).

La decisión que tome el servicio deberá comunicarla a la Red de Expertos – DIPRES mediante la sección inicial del Informe de Justificaciones (Brechas). Se recomienda que este documento sea trabajado previamente con la Red de Expertos – DIPRES a través del/la Analista correspondiente, a fin de que la fundamentación sea la más precisa y conduzca a la institución hacia un trabajo acotado a sus capacidades y con el impacto necesario.

D2. Inventario de Activos de Información (planilla).

La realización de cada uno de los procesos estratégicos de provisión, involucra **activos de información específicos** que son generados / modificados / utilizados en cada una de las etapas relevantes de tales procesos.

La Red de expertos del SSI considera importante identificar y caracterizar adecuadamente los activos de información vinculados a los procesos de provisión considerados en el alcance, porque de esta forma permite mostrar las condiciones en las cuales éstos se encuentran, dadas las diferentes etapas de los procesos en los que participan. Indicar bajo qué circunstancias está cada activo en la institución, ya sea en cuanto a su tipificación, condiciones físicas, responsabilidades asociadas, procedimientos para su tratamiento y sus requerimientos en confidencialidad, integridad y disponibilidad, conducente a definir la **criticidad** del activo. Es relevante tener en cuenta que la descripción de tales condiciones, y la criticidad definida, determinan el análisis de riesgos que puede afectar a cada uno de los activos del inventario, centrados en aquellos declarados con criticidad alta o media.

Es necesario que el encargado PMG/MEI-SSI, como también todos los funcionarios que tengan participación en el llenado del Inventario de Activos, cumplan con la totalidad de los pasos necesarios, a fin de asegurar las consistencia requerida para pasar al análisis de riesgos.

D3. Análisis de Riesgo (planilla):

En el mismo archivo de planilla electrónica donde se especifica el inventario de activos de información, en una hoja separada denominada "*Análisis de Riesgos*", se debe registrar todo el detalle del análisis de los riesgos. Una vez que han sido identificados los activos de información, se requiere caracterizar los riesgos que los amenazan, cuantificando el nivel de severidad y el tratamiento necesario. Para cada riesgo vinculado a un activo especifico, **se asocia uno o más controles para su mitigación** sobre la base de los dominios de seguridad que sean pertinentes (según lo que propone la NCh-ISO 27001.Of2013), considerando para ello la naturaleza del riesgo, el tipo y criticidad declarada para el activo**.**

En este punto es preciso señalar que cada institución, producto de la implementación de un ciclo de mejora con las 4 etapas establecidas para el SSI, debe haber logrado un análisis de

riesgos, cuyos controles de mitigación estaban expresados en términos de la normativa NCh-ISO 27001.Of **2009.** Dado que el presente año se requiere trabajar con la normativa versión **2013,** la Red de expertos ha incluido dentro de la planilla de instrumentos la hoja denominada "*Transición*", donde se detalla la equivalencia control a control de cada uno de los controles de la norma versión 2009 hacia el o los controles correspondientes de la nueva versión 2013. Esto debiera facilitar en gran medida el tema de la "traducción" de las hojas de riesgos desarrolladas en años anteriores, para que sus controles mitigantes queden actualizados y expresados en la nueva versión vigente.

Por otra parte, se incluye también la hoja "*NCh-ISO 27001.Of2013*", con el detalle de los 14 nuevos dominios y 114 controles de la normativa vigente, señalando para cada control una especificación de:

- El Objetivo de Control
- El Requisito de Control
- La Verificación del Requisito de Control: esta especificación debiera tomarse como guía al momento de declarar cumplimientos.

Al determinar los controles que se necesitan para mitigar cada riesgo, se debe señalar para cada uno de ellos si los productos asociados se encuentran implementados (y operando) en la institución. En ese caso afirmativo, se señala como un control **cumplido**; al contrario, si un control no se ha implementado, éste representa una brecha a superar y se debe señalar como NO-cumplido. Esto determina el **nivel de cumplimiento** que tiene el Servicio en su diagnóstico por cada dominio de seguridad, el cual se verá reflejado en la hoja Resumen del Diagnóstico del instrumento. Esto permitirá definir directamente el valor que toma el Indicador Transversal del SSI.

Cabe señalar que para aquellos controles en los que se declare cumplimiento se debe explicitar la evidencia (el o los Medios de Verificación) que permita evidenciarlo, de modo que la Red de Expertos, u otro ente interno o externo a la Institución pueda solicitar esa evidencia de forma inequívoca. Se debe entender que los productos establecidos para el tratamiento del Riesgo son las políticas, procedimientos, instrucciones de trabajo, estándares u otros elementos formales que instauren un determinado control, creando la institucionalidad necesaria para su sustentabilidad en el tiempo.

Este análisis se traducirá en un conjunto de controles, que denominaremos **Cobertura** la cual representa el conjunto de controles mínimo requerido para mitigar los riesgos identificados por la institución**,** y que por tanto constituye el universo de referencia para el cálculo de los cumplimientos ya señalados por cada dominio de seguridad.

Planificación

Acciones a realizar

La etapa de planificación entrega la organización de las actividades, uso de recursos y productos a generar en las etapas siguientes. Los productos y sus actividades asociadas incluidas en esta etapa adquieren la calidad de compromisos, a los cuales se les realizará un seguimiento que debiese ser incluido en una etapa de Evaluación posterior post-implementación.
Las acciones concretas son:

1. Definir el Plan General de Seguridad de la Información institucional, para el año en curso y siguientes, el cual debe considerar al menos los productos (iniciativas) que permitan implementar las acciones de mitigación de riesgo que correspondan a las brechas detectadas en el diagnóstico, es decir aquellos asociados a los controles declarados como NO cumplidos.

2. Se recomienda elaborar un Programa de Trabajo Anual (con un subconjunto de las iniciativas definidas en el Plan) que permita iniciar la implementación de aquellas iniciativas(productos) que sean relevantes para lograr alguna mejora en el año en curso.

Documentos a entregar

P1. Plan General de Seguridad de la Información (planilla).

Teniendo el marco institucional que implica la política general, el nombramiento del Encargado y la conformación del CSI, se debe dar forma al Plan General de Seguridad de la Información, para el año en curso y siguientes**.** Esta es la definición clara y operativa de los productos que se busca alcanzar y que permitan implementar las acciones de mitigación de riesgo que correspondan a las brechas detectadas en el diagnóstico.

Este plan se puede registrar en la misma planilla de instrumentos que se ha trabajado el inventario de activos y el análisis de riesgos, en la hoja correspondiente a “Plan General”, dado que se deben considerar los resultados del diagnóstico, riesgos y brechas detectados en el Diagnóstico.

La identificación de los productos en el Plan debe ser consistente con la descripción de los productos esperados ya definidos en la fase de análisis de riesgos, en la hoja “Análisis de Riesgos” de la planilla de instrumentos, y debe especificar además a los responsables de su desarrollo (cargo y nombre).

P2. Programa de Trabajo Anual.

Se recomienda elaborar un Programa de Trabajo Anual, con objeto de estructurar las acciones del año en curso del plan de seguridad de la información definido.

Se deberá especificar - para cada producto incluido en el programa- el detalle de sus actividades, sus plazos de ejecución y sus responsables (cargo y nombre). Se debe incluir en este detalle de actividades la debida señalización de los hitos (obtención de producto intermedio o final), y por otra parte las acciones orientadas a difusión/capacitación/sensibilización a todos los funcionarios sobre el programa de trabajo y sus productos.

Aparte de lo anterior, esta red de expertos recomienda incluir un apartado especial del programa de trabajo con actividades de base que incluyan entre otras:

- Revisiones internas del Sistema
- Auditorías internas o Externas
- Revisión del Cumplimiento de la Política.

Este programa de trabajo se puede reportar en la misma hoja donde se presenta el plan general, “Plan General” de la planilla de instrumentos, pero se debe cuidar de incluir el detalle de actividades solamente para aquellos productos comprometidos dentro del año en curso.

Implementación

Acciones a realizar

1. En caso de que se haya optado por establecer un Programa de Trabajo, lo que se espera entonces es Implementar dentro del año en curso el programa de trabajo anual definido en la etapa anterior.

2. Registrar y controlar los resultados de la implementación del programa de trabajo, verificando el avance en el nivel de cumplimiento de los controles que requiere el servicio para mitigar sus riesgos versus la cobertura de controles declarada en el diagnóstico. Esto debe hacerse en la Hoja "implementación" de la planilla de instrumentos.

I1. Ejecución de actividades (planilla).

En la misma planilla de trabajo del SSI, en la hoja "Implementación", se debe registrar el término real de las actividades cuantificando las desviaciones. Se debe prever que las desviaciones admisibles son aquellas que no implican el incumplimiento del compromiso en el año de implementación (enero a diciembre).

El registro de la implementación de un determinado producto, asociado a uno o más controles desde el diagnóstico, se debe plasmar señalando la evidencia de ello, en el último hito del producto. Dicha evidencia debe contener el control para el cual fue definida, de lo contrario no es válida como tal.

ANEXO I: Instrumentos 2015

Recomendaciones Generales

La planilla de instrumentos que ha sido confeccionada para su llenado contiene vínculos entre las hojas, así como también parámetros, por lo que se recomienda no alterarla para no afectar estas características.

Fue creada de esta forma para dar cuenta del ciclo de mejora continua y la relación entre las etapas de diagnóstico-planificación-implementación, traspasando los datos que vinculan estas etapas entre las hojas del archivo instrumentos.

Etapa de Diagnóstico

1. **Hoja "Inventario".**
   Este instrumento tiene por objetivo recoger el conjunto de los activos de información asociados a los procesos de provisión de bienes y servicios de la institución, cuyos productos estratégicos se encuentran en la Ficha A1. En él se deben considerar todos los activos de información de los procesos.

   El inventario organiza los atributos de los activos en las tres secciones que se describen a continuación.

   1.a Sección "DESCRIPCIÓN DE PROCESOS"
   Esta sección permite caracterizar el o los procesos del alcance en los que el activo participa.

   Proceso: Corresponde al nombre del proceso de negocio (de provisión de productos/servicios estratégicos) al cual pertenecen los activos de información a incluir en el inventario.
   Estos procesos deben ser consistentes con los mencionados en el Oficio de alcance.

   Subproceso: Son aquellos subprocesos en los que puede estar dividido el proceso transversal mencionado en la columna anterior, dependiendo de la complejidad del mismo.

   Etapa relevante: Detalle de las fases más importantes que se deben desarrollar en cada subproceso para dar origen a los productos.

   1.b Sección "IDENTIFICACION DE LOS ACTIVOS DE INFORMACIÓN"
   Esta sección permite caracterizar la naturaleza de cada activo y sus condiciones de preservación y manejo, que servirán de insumo para el posterior análisis de riesgos.
   Los atributos básicos se describen en lo que sigue:

   Nombre Activo: Nombre del activo de información, en este campo debe incluirse todos los activos de información identificados para la etapa, independiente de su medio de soporte y sus características. Esta columna se encuentra destacada con azul pues es una de las que dan consistencia entre esta hoja y la siguiente.
   Se deben detallar activos para los 3 niveles: Información, Infraestructura y Personas.

Se debe evitar repetir el mismo activo en diferentes líneas.

Identificador o código: En este campo se debe incluir el código dado por la institución al activo (nuevo o preexistente). Este atributo debe permitir identificar en forma única al activo.

Tipo: este atributo permite establecer la naturaleza del activo, calificándolo según los siguientes valores:

- "Base de Datos": Es la información sistematizada y organizada.
- "Documento": Corresponde a un escrito que refleja el resultado de una acción determinada y sustenta la toma de decisiones por parte de quien la administra y accede a ella, pudiendo ser físico o electrónico
- "Equipo": Objetos o dispositivos que realizan o apoyan la realización de un proceso y contienen información. A este tipo no le aplica los siguientes atributos: Soporte y Persona Autorizada para Copiar.
- "Expediente": Conjunto de documentos y formularios dispuestos en estricto orden de ocurrencia, de ingreso o egreso. Este puede ser físico o electrónico, en cuyo caso la definición está dada por el DS 81: "*Documento electrónico compuesto por una serie ordenada de actos y documentos representados en formato electrónico, dispuestos en estricto orden de ocurrencia, de ingreso o egreso en aquél, y que corresponde a un procedimiento administrativo o asunto determinado*".
- "Formulario": Corresponde a documentos utilizados para recoger información, pudiendo ser físico o electrónico.
- "Infraestructura Física": Estructura que permite almacenar y/o custodiar activos de información del proceso, tales como: datacenter, oficinas de partes, bodegas, caja fuerte, etc. A este tipo no le aplica los siguientes atributos: Soporte, Persona Autorizada para Copiar, Medio de Almacenamiento, Tiempo de Retención, Disposición y Criterio de Búsqueda.
- "Persona": personal de la institución que participa en un proceso de provisión. A este tipo no le aplica los siguientes atributos: Soporte, Persona Autorizada para Manipular, Persona Autorizada para Copiar, Medio de Almacenamiento, Tiempo de Retención, Disposición y Criterio de Búsqueda.
- "Sistema": Programa computacional desarrollado a medida, por la institución o por un externo, cuyo objetivo es apoyar un proceso de negocio.
- "Software": Programa computacional licenciado, producido por una empresa externa que lo distribuye o comercializa.

Ubicación: Corresponde al lugar físico o lógico donde se encuentra el activo mientras es utilizado en el proceso, esta descripción debe ser lo suficientemente detallada como para determinar a partir de esta información las condiciones de seguridad física en las que se encuentra el activo.

Responsable/dueño: Corresponde al rol o cargo de la persona autorizada para tomar decisiones respecto del activo. Esto no implica necesariamente derecho de propiedad sobre el activo.[2]

Soporte: Corresponde al medio en el cual se encuentra el activo, este puede ser en papel o digital. Esta característica no aplica a los activos de tipo "Persona", "Infraestructura física" ni "Equipo".

Persona Autorizada para Manipular: Corresponde al rol o cargo de la(s) persona(s) autorizada(s) para usar el activo de información, ya sea modificándolo, actualizándolo, trasladándolo o limpiándolo.

Los últimos 5 atributos que se describen en lo que sigue son opcionales (se pueden omitir), y sirven cuando se quiera lograr una caracterización más en profundidad.
Persona autorizada para copiar: Corresponde al rol o cargo de la(s) persona(s) autorizada para copiar el activo (aplicable al activo de información en papel y copias en medios magnéticos).

Medio de almacenamiento: Descripción de la forma de guardar el activo durante el tiempo de retención.

Tiempo de retención: Corresponde al tiempo en el cual el activo de información debe ser mantenido por la Institución en el medio de almacenamiento

Disposición: Corresponde al destino que se le da al activo de información una vez transcurrido el tiempo de retención.

Criterio de Búsqueda: Forma en la cual se debiera buscar el activo de información. Corresponde al criterio de ordenamiento o indexación definido por la institución para el activo, que permite un acceso rápido y eficiente.

1.c Sección "ANÁLISIS DE CRITICIDAD"

El atributo de criticidad permitirá establecer una priorización de los activos del inventario, en función de los requerimientos de Confidencialidad, integridad y disponibilidad, cuyos valores consideran la caracterización previamente realizada para cada activo. Los valores que pueden tomar cada uno de estos tres atributos se encuentran detallados en la Tabla 1.

Confidencialidad: Necesidad de permitir el acceso al activo sola a las personas debidamente autorizadas de acuerdo a lo definido por la institución. El acceso no autorizado tiene impacto para la institución o terceros.
Para establecer este atributo, se debe considerar las leyes 20.285, y 19.628, así como también la etapa del proceso en la cual se realiza el análisis del activo.

[2] Considerar la definición establecida en la NCH-ISO 27002

Integridad: necesidad de preservar la configuración y contenido de un activo de Información. Su modificación no deseada tiene consecuencias que generan distintos niveles de impacto para la institución o terceros. El Valor de este atributo está directamente relacionado con la magnitud de dicho impacto.

Disponibilidad: necesidad de preservar el tiempo de acceso al activo bajo un umbral predefinido por la institución. Sobrepasar dicho umbral implica indisponibilidad del activo la que genera distintos niveles de impacto para la institución o terceros. El Valor de este atributo está directamente relacionado con la magnitud de dicho impacto.

Tabla 1: Valores para Cálculo de Criticidad

Variables asociadas a la criticidad	Grado	Significado
CONFIDENCIALIDAD	Pública	El activo no tiene restricciones de acceso.
	Reservada	Activo de información cuyo acceso no autorizado tiene impacto para la institución o terceros.
INTEGRIDAD	Baja	Activo de Información cuya modificación no deseada tiene consecuencias con impacto leve para la institución o terceros.
	Media	Activo de Información cuya modificación no deseada tiene consecuencias con impacto significativo para la institución o terceros.
	Alta	Activo de Información cuya modificación no deseada tiene consecuencias con impacto grave para la institución o terceros
DISPONIBILIDAD	Baja	Activo de Información cuya inaccesibilidad, tiene impacto leve para la institución o terceros.
	Media	Activo de Información cuya inaccesibilidad, tiene impacto significativo para la institución o terceros.
	Alta	Activo de Información cuya inaccesibilidad, tiene impacto grave para la institución o terceros.

Los impactos para la institución o terceros pueden ser cuantificables (monto monetario o entrega de servicio) y no cuantificables (imagen, valor estratégico de la información, obligaciones contractuales o públicas, disposiciones legales, etc.).

Criticidad: Esta columna se encuentra destacada con azul pues es una de las que dan consistencia entre esta hoja y la siguiente. Esta columna es calculada automáticamente en la planilla de instrumentos, en función de la tríada Confidencialidad-Integridad-Disponibilidad y puede tomar los siguientes Valores:

- "Baja" : Ninguno de los valores asignados a la triada supera el valor "público" o "bajo".
- "Media": Alguno de los valores asignados a la triada es "medio".
- "Alta" : Alguno de los valores asignados a la triada es "Reservado" o "Alto".

Observación: el valor de Criticidad calculado por la planilla no debe ser alterado.

2. Hoja "Análisis de Riesgos".

Este instrumento tiene por objetivo identificar los riesgos potenciales que amenazan los activos inventariados en la institución. Éstos pueden ser identificados ya sea por haberse materializado y haber afectado la seguridad de los activos, independiente de que exista registro de dicho incidente o porque el activo se encuentra en una situación de vulnerabilidad.

2.a Sección "CARACTERIZACION DEL ACTIVO"

Inicialmente, esta hoja aparece pre-cargada con los activos identificados en la hoja "**Etapa 1 – Inventario**" (de los cuales se detalla el proceso al que pertenece, el nombre del activo de información, su confidencialidad, integridad, disponibilidad y criticidad). Los activos identificados con criticidad "baja" aparecerán difuminados para indicar que para ellos no se requiere realizar el análisis.

Por el contrario, para todos aquellos activos cuya criticidad tiene el valor "media" o "alta", se debe realizar el análisis de riesgos correspondiente.

Los atributos de esta sección de la hoja son los siguientes:

Proceso – Activo – Confidencialidad – Integridad – Disponibilidad - Criticidad: Corresponden a atributos declarados en el Inventario de Activos, que permiten dar continuidad al análisis, no se deben cambiar las fórmulas que referencian los contenidos de estos atributos desde la hoja de inventario.

2.b Sección "IDENTIFICACIÓN Y CARACTERIZACION DE LOS RIESGOS"

Dependiendo de la criticidad declarada en el inventario, en este análisis es posible identificar varios riesgos, asociados a un activo. Para registrar cada uno de ellos, se debe insertar las filas que se requieran.

A su vez, para cada riesgo se debe asociar uno o más controles que permitan su mitigación. Asimismo, cada control requerirá la definición de un producto esperado para su implementación.

Amenaza: Evento generado a partir de un agente externo o interno de la institución, que tenga el potencial de generar algún grado de daño (ya sea en relación a la Confidencialidad, Integridad o Disponibilidad) en uno o más activos de información institucional.

Vulnerabilidad: Se refiere a alguna **"**Condición de debilidad o fragilidad que se encuentra presente en el activo identificado". Usualmente se traduce en una debilidad o ausencia de control, que posibilita la ocurrencia de eventos no deseados y que pueden afectar a uno o más activos de información.

Descripción del Riesgo: Descripción de la consecuencia que existiría para el proceso, en el caso de que la Amenaza descrita afectase concretamente alguna vulnerabilidad del activo de información identificado.

En caso de que el Análisis de riesgo se base en el inventario de activos, las Amenazas y Riesgos descritos deben ser consistentes con el análisis de criticidad del activo y con su naturaleza (tipo de activo).

Probabilidad de ocurrencia: Posibilidad de que el riesgo se materialice. Los valores posibles son:

- Casi Certeza
- Probable
- Moderado
- Improbable
- Muy Improbable

Impacto: Corresponde a los efectos que tiene en la institución la materialización del riesgo. Los valores posibles son:

- Catastróficas
- Mayores
- Moderadas
- Menores
- Insignificantes

Severidad: Corresponde al nivel de gravedad del riesgo, este será calculado por la planilla y corresponde a la probabilidad de ocurrencia por el impacto (Tabla 2). Los resultados posibles son:

- Extremo
- Alto
- Moderado
- Bajo

2.c Sección "MEDIDAS DE MITIGACION"

Esta sección permite caracterizar cada uno de los controles seleccionados para mitigar los riesgos identificados

Control para mitigar el riesgo: Corresponde a las medidas que propone la NCh-ISO 27001.Of2013, cuya implementación permitirá mitigar el riesgo identificado. Se debe agregar filas en caso de requerirse más de una.

Cumplimiento: Corresponde a la declaración (afirmativa o negativa) respecto al cumplimiento del "Control para mitigar el riesgo" definido en la columna M.

Nombre del producto esperado: Corresponde al tratamiento del riesgo identificado, cuya implementación permite dar por cumplido(s) el(los) control(es) asociado(s)

NOTA: La realización de un producto puede permitir la implementación de más de un control. No obstante, se debe evitar asociar más de un producto a la implementación de un mismo control. En la eventualidad de requerirse esto, se debe cuidar de especificar los

distintos tratamientos como un solo producto en esta hoja, y evidenciar - en el Programa de Trabajo- los distintos subproductos a generar, estableciéndolos como hitos intermedios.

Nombre del Archivo Evidencia: Nombre del archivo complementario que se presenta como medio de verificación de los controles que se declaren cumplidos, es decir, con un "SI" en la columna "Cumplimiento".

Tabla 2: Niveles de severidad del riesgo

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)

Fuente: Guía Técnica Nº 53. CAIGG

Etapa de Planificación

1. **Hoja "Etapa 2 – Plan General".**

Este instrumento tiene por objetivo registrar la planificación -en términos generales– que permitirá la obtención de los productos identificados en la etapa anterior en la hoja Riesgos - a desarrollar durante el 2014 y los años siguientes, si corresponde, así como también las actividades de difusión de los productos desarrollados y las actividades de control básicas destinadas a la evaluación de los resultados de la implementación.
El diseño de la planilla considera 4 zonas identificadas con diferentes colores:

1.a. Sección ZONA AMARILLA

En esta zona se debe registrar los productos a desarrollar el 2015 que constituyen el programa de trabajo. Los atributos que la componen son:

Producto Esperado: Corresponde al tratamiento del riesgo identificado, cuya implementación permite dar por cumplido(s) el(los) control(es) asociado(s). Es importante mantener la continuidad y consistencia entre la hoja Riesgos y la del Plan General, lo que significa mantener el mismo nombre del producto esperado en ambas hojas (por los que se recomienda copiarlos y pegarlos.). Adicionalmente, se debe cuidar la incorporación de todos los productos asociados a controles declarados como "NO" cumplidos en la hoja de riesgos al Plan general.

Responsable del Producto: Nombre y cargo del responsable de la implementación del producto.

Actividades o Hitos: Secuencia de actividades que la Institución debe realizar para la obtención del producto. Se recomienda identificarlas en forma consecutiva de acuerdo al orden de ejecución de las mismas. Dentro de ellas se debe resaltar el momento de la entrega del producto, esto se realiza incorporando un hito final, el cual se identifica con la glosa "Hito Final: <*Nombre del Producto*>".
NOTA: Se debe considerar que los hitos no corresponden a actividades por lo que no se debe establecer como una acción a realizar.

Fecha Inicio: Corresponde a la fecha de inicio de la actividad, se debe considerar formato dd-mm-yy.

Fecha Término: Corresponde a la fecha de término de la actividad, se debe considerar formato dd-mm-yy. En el caso de los hitos se debe establecer una fecha de término igual a la fecha de inicio.

Responsable de la Actividad: Corresponde al nombre y cargo de la persona que ejecutará actividad. En el caso de los hitos el responsable de éstos es el responsable del producto.

1.b. Sección ZONA VERDE
En esta zona se debe registrar las actividades de difusión de los productos de Programa de Trabajo 2014, actividades de capacitación y actividades de sensibilización, las que forman parte del Programa de Trabajo. Los atributos que la componen son:

Producto Esperado: En la planilla de Instrumentos aparece desplegado un título genérico. En caso de requerirse es posible – en esta columna - agrupar un conjunto de actividades de difusión, identificándolas con un título más específico

Responsable del Producto: No aplica

Actividades o Hitos: Secuencia de actividades que la Institución debe realizar para la obtención del producto. Se recomienda identificarlas en forma consecutiva de acuerdo al orden de ejecución de las mismas. Dentro de ellas se debe resaltar el momento de la entrega del producto, esto se realiza incorporando un hito final, el cual se identifica con la glosa "Hito Final: <*Nombre del Producto*>".
NOTA: Se debe considerar que los hitos no corresponden a actividades por lo que no se debe establecer como una acción a realizar.

Fecha Inicio: Corresponde a la fecha de inicio de la actividad, se debe considerar formato dd-mm-yy.

Fecha Término: Corresponde a la fecha de término de la actividad, se debe considerar formato dd-mm-yy.

Responsable de la Actividad: Corresponde al nombre y cargo de la persona que ejecutará actividad. En el caso de los hitos el responsable de éstos es el responsable del producto.

Difusión/Sensibilización: Corresponde a las instancias de difusión y/o sensibilización planificadas para el año, ya sea para difundir los productos esperados o sensibilizar respecto a la implementación del sistema.

Capacitación: Corresponde a las instancias de capacitación definidas para el año.

1.c. Sección ZONA CELESTE
En esta zona se puede registrar las actividades de control básicas recomendadas para las Instituciones en etapa IV.

Producto Esperado: En la planilla de Instrumentos aparece desplegado un título genérico.

Responsable del Producto: No aplica

Actividades o Hitos: Corresponde a las actividades de control requeridas para las Instituciones que se encuentran en etapa IV, las que incluyen:
- Revisiones internas del Sistema

- Auditorías internas o Externas
- Revisión del Cumplimiento de la Política

Fecha Inicio: Corresponde a la fecha de inicio de la actividad, se debe considerar formato dd-mm-yy.

Fecha Término: Corresponde a la fecha de término de la actividad, se debe considerar formato dd-mm-yy.

Responsable de la Actividad: Corresponde al nombre y cargo de la persona que ejecutará actividad.

1.d. Sección ZONA ROSA
En esta zona se debe registrar los productos que serán realizados el 2016 o posteriores, en caso que corresponda.

Producto Esperado: Corresponde al tratamiento del riesgo identificado, cuya implementación el 2016 o posteriores, permitirá dar por cumplido(s) el(los) control(es) asociado(s).
Responsable del Producto: Nombre y cargo del responsable de la implementación del producto.

Justificación: Esta columna debe utilizarse para indicar las razones por las que dichos productos se desfasan para los años siguientes, tales como: prioridad de la Institución, nivel de severidad del riesgo que mitiga, requerimientos presupuestarios, etc.

Fecha Inicio: Corresponde a la fecha aproximada de inicio de la implementación del producto, se debe considerar formato dd-mm-yy.

Fecha Término: Corresponde a la fecha aproximada de término de la implementación del producto, se debe considerar formato dd-mm-yy.

Etapa de Implementación

En caso de que la institución opte por implementar el Programa de trabajo definido en la etapa anterior, con el fin de obtener mejoras dentro del año en curso, se debe considerar llenado de la siguiente hoja en la planilla de instrumentos.

1. **Hoja "Etapa 3 – Implementación".**
   El objetivo de esta hoja es controlar la ejecución del Programa de Trabajo, registrando la realización de los hitos o actividades comprometidas en la etapa de planificación.
   Los atributos de esta hoja son los siguientes:

   Productos esperados: Corresponde al producto definido en la Zona Amarilla de la hoja del Plan General, el cual se copia por fórmula a esta hoja de Implementación. Los productos desfasados para el 2016 o posteriores no deben formar parte de este registro.

Actividades o Hitos: Corresponde a las actividades e hitos necesarios para implementar los productos del Programa de Trabajo 2015, de acuerdo a lo comprometido por la Institución en la Planificación.

Fecha Término: Las dos columnas bajo este rótulo permiten comparar la fecha en la cual se había definido el término de la actividad o hito, con la fecha en que esto realmente ocurrió.

- **Estimado:** Es la fecha en que se había definido serían terminadas las actividades o hitos, según el Plan General, la cual se copia por fórmula a esta hoja de Implementación.
- **Real:** Es la fecha en que efectivamente finalizó la actividad que generó el producto que da cumplimiento al control para el cual había sido definido. Se debe considerar formato dd-mm-yy.

Desviaciones (días): Es una fórmula que calcula la diferencia entre la fecha estimada y la real. Cuando una actividad se haya terminado antes de lo programado, este valor será positivo. Si la actividad tuvo retrasos, será negativo.

Justificación: Esta columna permite señalar causas de desviaciones significativas. Se considera que una desviación es significativa si ella supera el 20% del tiempo total estimado para la ejecución del producto esperado de acuerdo al Programa de Trabajo.
Cabe señalar que las desviaciones admisibles no pueden exceder el año 2015, salvo situaciones cuya causalidad sea externa a la Institución y verificable.

Nombre del archivo evidencia: Corresponde al nombre del(los) archivo(s) complementario(s) que constituye(n) el medio de verificación del producto, cada nombre de archivo debe ser registrado en la celda que corresponda al hito final. Se debe mantener la consistencia entre el nombre así registrado en esta columna y el nombre del archivo complementario. Es importante que el contenido del archivo sea lo requerido por el(los) control(es) asociado(s), al producto porque esta evidencia es la que permitirá considerar que tal(es) control(es) está(n) cumplido(s), incrementando el porcentaje de logro del servicio en la etapa de implementación.

ANEXO II: Activos de Información y la Normativa NCh-ISO 27001

Los **Activos de Información** corresponden a todos aquellos elementos relevantes en la producción, procesamiento, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la institución.

De esta forma podemos distinguir 3 niveles básicos de activos de información:

- La Información propiamente tal, en sus múltiples formatos (papel, digital, texto, imagen, audio, video, etc.)
- Los Equipos/Sistemas/infraestructura que soportan esta información
- Las Personas que utilizan la información, y que tienen el conocimiento de los procesos institucionales.

Dado que los activos de información poseen valor para la organización, necesitan por tanto, ser protegidos adecuadamente para que la misión institucional (o "negocio" en términos normativos) no se vea perjudicada. Esto implica identificar para cada activo sus riesgos asociados, detectar vulnerabilidades y establecer los controles de seguridad que sean necesarios para mitigarlos, tanto a nivel de gobierno institucional y de gestión de procesos, como a nivel de tecnologías de la información utilizadas.

El Sistema de Seguridad de la Información (SSI) establece distintos controles tanto a nivel de gobierno y gestión, como de tecnologías de la información, con el objeto de garantizar que los activos de información cumplan con preservar las siguientes condiciones:

- **La Integridad**: Los activos de información se encuentran completos, actualizados y son veraces, sin modificaciones inapropiadas o corruptas.
- **La Confidencialidad**: Los activos de información se encuentran protegidos de personas/usuarios no autorizados.
- **La Disponibilidad**: Los usuarios autorizados pueden acceder a los activos de información cuando lo requieran, para utilizarlos apropiadamente al desempeñar sus funciones.

Las nuevas tecnologías, el desarrollo del conocimiento, la liberación de las comunicaciones y la posibilidad de acceso libre a diversos aplicativos, requieren de un sistema que permita gestionar la seguridad de la información, lo cual consiste en la realización de las tareas necesarias para garantizar los niveles exigibles en la organización, dentro del ámbito de protección de las condiciones de integridad, confidencialidad y disponibilidad de los activos de información, como principio clave.

Según el Decreto Supremo N° 83 / 2004 del Ministerio Secretaría General de la Presidencia (desde ahora en adelante DS-83), la Norma Chilena Oficial NCh-ISO 27001.Of2013, como también lo establecido en la Ley N° 20.285, y otras normativas presentes en el SSI del PMG/MEI, las exigencias y recomendaciones que se proveen, presentan desafíos en cuanto a la necesidad de garantizar estándares mínimos de seguridad en el uso, almacenamiento, acceso y distribución de información, por lo que es necesario que cada uno de los órganos del Estado cumpla con estas normativas a través de la implantación de un Sistema de Seguridad de la Información.

El DS-83, provee de un marco regulatorio para incorporar mayores niveles de seguridad a la información de los servicios públicos, sin embargo, su principal objetivo apunta al documento electrónico para facilitar la interoperabilidad en el Estado. Dado que el documento electrónico constituye sólo una parte de la información relevante a proteger, es que el Sistema de Seguridad de la Información debe abarcar progresivamente a todos los Activos de Información asociados a los procesos de provisión de las instituciones públicas, valiéndose de los dominios que establece la NCh-ISO 27001.Of2013

ANEXO III Normativa vigente

El siguiente corresponde al listado de la normativa vigente relacionada con el SSI:

- 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 Nº 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 Nº 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°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°14, 27 de febrero de 2014, Ministerio de Economía, Fomento y Turismo. Modifica Decreto Nº 181 de 2002.
- 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.
- 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 sitio Web: http://www.dipres.gob.cl, sección Sistema Seguridad de la Información.