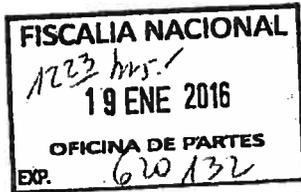




E8638/2015



ORD. N° 164

ANT.: Su oficio FN N° 855/2015, de 29 de diciembre de 2015

11

MAT.: Convenio de Desempeño Institucional 2016.

SANTIAGO, 18 ENE 2016

DE : MINISTRO DE HACIENDA

A : SEÑOR FISCAL NACIONAL DEL MINISTERIO PÚBLICO

Se ha recibido en esta Secretaría de Estado su oficio del Ant., mediante el cual Ud., en el marco de lo dispuesto en la Ley N° 20.240, en particular de los artículos 6° y demás pertinentes, manifiesta que corresponde refrendar el Convenio de Desempeño Institucional del Ministerio Público correspondiente al año 2016, que Ud. acompaña, el que ha sido trabajado por la Instancia Técnica que establece la ley.

Al respecto, cumplesme transmitir a Ud. la conformidad del Ministro de Hacienda infrascrito a los términos de dicho convenio, que se adjunta al presente oficio debidamente firmado.

Saluda atentamente a Ud.,

  
REPUBLICA DE CHILE  
MINISTERIO DE HACIENDA  
**RODRIGO VALDÉS PULIDO**  
Ministro de Hacienda



C.c.:  
- Sr. Director de Presupuestos  
- Coordinación de Gestión Subsecretaría de Hacienda



## **CONVENIO DE DESEMPEÑO INSTITUCIONAL PARA EL AÑO 2016.**

En Santiago, a 31 de diciembre de 2015, entre el Ministerio Público, representado por el Fiscal Nacional, don Jorge Abbott Charne, chileno, abogado, Cédula de Identidad N° 5.982.815-0, ambos con domicilio en Avenida General Mackenna 1369, piso 2, de la comuna y ciudad de Santiago, y el Ministerio de Hacienda, representado por don Rodrigo Valdés Pulido, chileno, casado, Cédula de Identidad N° 8.267.804 - 2, ambos domiciliados en calle Teatinos N° 120, piso 12, se suscribe el siguiente Convenio de Desempeño Institucional.

### **PRIMERO: Antecedentes**

1.- Que, de conformidad con lo dispuesto en la Ley N° 19.640 y sus reglamentos y lo dispuesto en la Ley N° 20.240, el bono de gestión institucional a que tiene derecho el personal del Ministerio Público se concederá en relación a la ejecución de un Compromiso de Gestión Institucional (CGI).

2.- Que para la formulación del Compromiso de Gestión Institucional, se debe tener presente que, de acuerdo con la Constitución Política de la República y la Ley 19.640, el Ministerio Público es un organismo autónomo, por lo que no forma parte de la Administración del Estado y, en consecuencia, no le son aplicables, por regla general, las leyes, reglamentos, instrucciones u otras normas dictadas para esta última. No obstante dicho carácter de autónomo del Ministerio Público, de conformidad a la Ley N° 20.240, corresponde que formule los Compromisos de Gestión Institucional.

✓ Los organismos técnicos responsables de los sistemas y los requisitos técnicos establecidos por éstos para la Administración del Estado en el Programa de Mejoramiento de la Gestión (PMG) del Ministerio de Hacienda, podrán ser considerados un apoyo y/o referente para los sistemas que son materia de este convenio, sin ser necesariamente obligatorio sujetarse a sus disposiciones.

3.- Que dicho Compromiso de Gestión Institucional será propuesto anualmente por el Fiscal Nacional del Ministerio Público al Ministro de Hacienda, especificando las áreas prioritarias y las metas anuales de gestión, con sus respectivos indicadores o elementos de similar naturaleza que permitan la medición de su grado de cumplimiento.

4.- Que sobre la base de las áreas prioritarias, el Compromiso de Gestión Institucional debe quedar anualmente refrendado en un Convenio de Desempeño Institucional que suscribirá el Fiscal Nacional del Ministerio Público con el Ministro de Hacienda.

5.- Una entidad evaluadora de origen externo, tendrá como función efectuar el proceso de verificación del grado de cumplimiento de las metas contenidas en el Compromiso de Gestión Institucional, sobre la base de los informes que respecto a la materia haya elaborado el Fiscal Nacional.

6.- Que, conforme a los antecedentes expuestos, las partes del presente Convenio de Desempeño Institucional acuerdan lo siguiente:

**SEGUNDO: Áreas Prioritarias.**

Las partes definen las siguientes áreas prioritarias para el año 2016:

**MISIÓN INSTITUCIONAL:** Dirigir en forma exclusiva las investigaciones criminales, ejercer cuando resulte procedente la acción penal pública instando por resolver adecuada y oportunamente los diversos casos penales, adoptando las medidas necesarias para la atención y protección de víctimas y testigos; todo ello a fin de contribuir a la consolidación de un Estado de Derecho, con altos estándares de calidad.

PROGRAMA MARCO DEL MINISTERIO PÚBLICO		
ÁREAS PRIORITARIAS, OBJETIVOS Y SISTEMAS		
ÁREA PRIORITARIA	SISTEMAS	OBJETIVO
USUARIOS Y COMUNIDAD	SISTEMA DE INFORMACIÓN Y ATENCIÓN A USUARIOS	Contar con un Sistema de Información y Atención a Usuarios que coordine los espacios de atención del Ministerio Público a fin de permitir el acceso a la información relativa a la función institucional, la transparencia de los actos administrativos y que contemple: a) Procesos de Trabajo definidos con sus respectivos estándares y protocolos. b) Sistemas de registro y gestión de requerimientos. c) Mecanismos de evaluación de procesos y de resultados.
	SISTEMA DE INFORMACIÓN PARA LA COMUNIDAD UTILIZANDO TIC	Poner a disposición de la comunidad sistemas de información que garanticen el acceso oportuno y transparente a la información que genera la institución y que es de relevancia para la comunidad, utilizando Tecnología de Información y Comunicación (TIC).
	SISTEMA DE SEGURIDAD DE LA INFORMACIÓN	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.
GESTIÓN ORGANIZACIONAL	PLANIFICACIÓN Y CONTROL DE GESTIÓN	Contar con un Plan Estratégico Institucional de largo plazo y un Sistema de Control de Gestión que disponga de información relevante y oportuna, que permita direccionar la gestión institucional hacia el cumplimiento de los objetivos estratégicos definidos por el Ministerio Público.

ÁREA USUARIOS Y COMUNIDAD			
SISTEMA DE INFORMACIÓN Y ATENCIÓN A USUARIOS			
<b>OBJETIVO</b>		<p>Contar con un Sistema de Información y Atención a Usuarios que coordine los espacios de atención del Ministerio Público a fin de permitir el acceso a la información relativa a la función institucional, la transparencia de los actos administrativos y que contemple:</p> <p>a) Procesos de Trabajo definidos con sus respectivos estándares y protocolos;</p> <p>b) Sistemas de registro y gestión de requerimientos;</p> <p>c) Mecanismos de evaluación de procesos y de resultados.</p>	
Etapa 1	Etapa 2	Etapa 3	Etapa 4
<p>1. Mantener vigente el diagnóstico del Sistema de Información y Atención a Usuarios del Ministerio Público, o actualizarlo si se registran cambios.</p> <p><b>ETAPA EGRESADA</b></p>	<p>1. Mantener vigente el Diseño del Sistema de Información y Atención a Usuarios (SIAU), o actualizarlo si se registran cambios.</p> <p>2. Mantener vigente, el Plan General de Implementación del Sistema de Información y Atención a Usuarios (SIAU), o actualizarlo si se registran cambios.</p> <p>3. Elaborar el programa de trabajo para el año siguiente.</p> <p><b>ETAPA EGRESADA</b></p>	<p>1. Implementar gradualmente el Sistema de Información y Atención a Usuarios, en base al Plan General de Implementación vigente.</p> <p><b>ETAPA EGRESADA</b></p>	<p>1. Evaluar el funcionamiento de los espacios de atención del SIAU formulando recomendaciones de mejora para el año siguiente, si corresponde.</p> <p>2. Ejecutar los compromisos establecidos en el Programa de Seguimiento de las recomendaciones de mejora definido el año anterior.</p> <p>3. Elaborar un programa de seguimiento de la implementación de las recomendaciones de mejora que se seleccionen para ser ejecutadas en el año siguiente.</p> <p><b>ETAPA COMPROMETIDA AÑO 2016</b></p>

SISTEMA DE INFORMACIÓN PARA LA COMUNIDAD UTILIZANDO TIC

**OBJETIVO**

Poner a disposición de la comunidad sistemas de información que garanticen el acceso oportuno y transparente a la información que genera el Ministerio Público y que es de relevancia para la comunidad, utilizando Tecnología de Información y Comunicación (TIC).

Etapa 1	Etapa 2	Etapa 3	Etapa 4
<p>Mantener vigente el Diagnóstico del Sistema de Información para la comunidad utilizando TIC, o actualizándolo si se registran cambios vinculados a los requisitos técnicos de la etapa, considerando:</p> <p>1. La identificación de las modificaciones a los procesos de provisión de los productos estratégicos del Ministerio Público, que utilizarán TIC, de modo de mejorar los servicios e información a los ciudadanos.</p> <p>2. La identificación de las modificaciones a los procesos de soporte institucional que utilizarán TIC.</p> <p>3. El desarrollo de un levantamiento de los modelos y procesos de operación, con los siguientes alcances:</p> <ul style="list-style-type: none"> <li>- Identificación de Mejores Prácticas.</li> <li>- Identificación de Procesos Estandarizables a Nivel Nacional que requieran el uso de TIC para mejorarlos.</li> </ul> <p>4. La identificación de los proyectos TIC que surjan del diagnóstico, e identificar las actualizaciones a la Cartera de Proyectos y su cronograma.</p> <p><b>ETAPA EGRESADA</b></p>	<p>Mantener vigente la Planificación del Sistema de Información para la Comunidad utilizando TIC, considerando los resultados del diagnóstico y la normativa vigente<sup>1</sup>, a saber:</p> <p>1. Priorización y/o secuenciación de los proyectos TIC.</p> <p>2. Identificación de mejores prácticas a replicar en las Fiscalías.</p> <p>3. Elaboración y/o actualización de los programas de trabajo de implementación anual, para la ejecución de los proyectos priorizados en base al Plan de Mejoramiento con uso de TIC, que considere al menos: cronogramas de trabajo, principales hitos, requerimientos de recursos, etapas, plazos y responsables para cada uno de ellos.</p> <p><b>ETAPA COMPROMETIDA AÑO 2016</b></p>	<p>1. Implementar los Programas de Trabajo de los proyectos comprometidos para el año 2016, de acuerdo al Plan de Mejoramiento con uso de TIC, aprobado en la Etapa anterior, señalando los hitos identificados en la planificación.</p> <p>2. Registrar los resultados de la implementación de los proyectos priorizados y, comprometido su inicio en el año en curso, considerando, al menos, las actividades ejecutadas e hitos cumplidos, las dificultades y las modificaciones realizadas respecto de lo programado.</p> <p><b>ETAPA COMPROMETIDA AÑO 2016</b></p>	<p>1. Evaluar la implementación de los Programas de Trabajo para el Sistema de Información para la Comunidad Utilizando TIC implementado, considerando al menos:</p> <ul style="list-style-type: none"> <li>- Análisis de la implementación realizada considerando actividades desarrolladas, descripción y justificación de eventuales modificaciones a lo programado originalmente. Lo anterior, de acuerdo a los resultados obtenidos en relación a la evaluación de los indicadores de desempeño.</li> </ul> <p>2. Realizar un programa de seguimiento que incluya recomendaciones, compromisos, plazos y responsables. Lo anterior con la finalidad de cerrar las brechas y debilidades detectadas por la evaluación de los proyectos ejecutados.</p> <p><b>ETAPA NO COMPROMETIDA AÑO 2016</b></p>

<sup>1</sup> La normativa a considerar, que sin ser obligatoria para el Ministerio Público puede usarse como referencia en esta etapa, se refiere a las comunicaciones electrónicas, interoperabilidad de documentos electrónicos y su seguridad-confidencialidad (DS: 77, 81, 83 respectivamente), mensajes electrónicos masivos no solicitados, desarrollo de sitios WEB (DS. 93 y 100 respectivamente) y nuevas normativas definidas por el comité de normas para el documento electrónico. Además, se deben considerar las leyes siguientes: Ley N° 19.628 sobre protección de la vida privada y datos personales, Ley N° 19.799 sobre documentos electrónicos y firma electrónica, Ley N° 19.880 sobre bases de procedimientos administrativo.

AREA USUARIOS Y COMUNIDAD			
SISTEMA DE SEGURIDAD DE LA INFORMACIÓN			
<b>OBJETIVO</b>	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.		
Etapa 1	Etapa 2	Etapa 3	Etapa 4
<p>1. La institución realiza un diagnóstico de la situación de seguridad de la información institucional, e identifica en éste los activos de información que dan sustento a una selección de sus procesos de provisión, estableciendo los controles necesarios para mitigar riesgos que puedan afectar a los activos de información críticos, considerando para esto todos aquellos dominios de seguridad de la información que establece el DS 83 y la NCh-ISO 27001-2009, determinando el nivel en que la institución se encuentra respecto de: Políticas de Seguridad, Seguridad Organizacional, Clasificación, Control y Etiquetado de Bienes, Seguridad Física y del Ambiente, Seguridad del Personal, Gestión de la Operaciones y de las Comunicaciones, Control de Acceso, Desarrollo y Mantenimiento de Sistemas, Gestión de Incidentes en la Seguridad de la Información, Gestión de la Continuidad del Negocio y Cumplimiento.</p> <p>2. La institución compara los resultados del Diagnóstico con los controles establecidos en los dominios de seguridad del DS 83 y la NCh-ISO 27001-2009, y determina las brechas que deberán ser abordadas y cerradas a través de la implementación de un Plan de Seguridad de la Información Institucional.</p> <p><b>ETAPA COMPROMETIDA AÑO 2016</b></p>	<p>1. La institución establece su Política de Seguridad de la Información debidamente formalizada por el Jefe Superior del Servicio.</p> <p>2. La institución, en el marco de la Política de Seguridad de la Información establecida, elabora un Plan General de Seguridad de la Información Institucional, para el año en curso y siguientes, de acuerdo a los resultados del diagnóstico y las brechas detectadas, que comprende, al menos, la coordinación de todas las unidades de la institución vinculadas a los aspectos de seguridad de la información, a través del nombramiento de responsables de la implementación del Plan, y el establecimiento de los controles para cumplir los requisitos del DS 83 y la NCh-ISO 27001-2009.</p> <p>3. La institución, en el marco de la Política de Seguridad de la Información establecida, elabora un Programa de Trabajo Anual para implementar el Plan de Seguridad de la Información definido, señalando al menos, los principales hitos de su ejecución y un cronograma que identifique actividades, plazos y responsables, indicadores de desempeño; difundiéndolo al resto de la organización.</p> <p><b>ETAPA NO COMPROMETIDA AÑO 2016</b></p>	<p>1. La institución implementa el Programa de Trabajo Anual definido en la etapa anterior, de acuerdo a lo establecido en el Plan General de Seguridad de la Información, registrando y controlando los resultados de las actividades desarrolladas, las dificultades y holguras encontradas y las modificaciones realizadas respecto a lo programado.</p> <p><b>ETAPA NO COMPROMETIDA AÑO 2016</b></p>	<p>1. La institución evalúa y difunde los resultados de la implementación del Plan General de Seguridad de la Información y el Programa de Trabajo Anual, considerando el porcentaje de cumplimiento en los dominios de seguridad del DS 83 y la NCh-ISO 27001-2009 logrado, respecto de las brechas detectadas en el diagnóstico, y formula recomendaciones de mejora.</p> <p>2. La institución diseña un Programa de Seguimiento a partir de las recomendaciones formuladas en la evaluación de los resultados de la ejecución del Plan General de Seguridad de la Información y Programa de Trabajo Anual, señalando los compromisos, plazos y responsables, que permitan superar las causas que originaron las brechas aún existentes y las debilidades detectadas de aquellas priorizadas.</p> <p>3. La institución, implementa los compromisos establecidos en el Programa de Seguimiento definido.</p> <p><b>ETAPA NO COMPROMETIDA AÑO 2016</b></p>

SISTEMA DE PLANIFICACION Y CONTROL DE GESTION

<p><b>OBJETIVO</b></p>	<p>Contar con un Plan Estratégico Institucional de largo plazo, y un Sistema de Planificación y Control de Gestión que disponga de información relevante y oportuna que permita direccionar la gestión institucional hacia el cumplimiento de los objetivos estratégicos definidos por el Ministerio Público.</p>			
	<p>Etapa 1</p>	<p>Etapa 2</p>	<p>Etapa 3</p>	<p>Etapa 4</p>
<p>1. Mantener vigente el Plan Estratégico del Ministerio Público, o actualizándolo si se registran cambios vinculados a los componentes definidos.</p> <p><b>ETAPA EGRESADA</b></p>	<p>1. Mantener vigente el Diseño del Sistema de Control de Gestión, en base a las definiciones establecidas en la etapa anterior, actualizando si se registran cambios vinculados a los componentes definidos.</p> <p>2. Elaborar un programa de trabajo anual para el año siguiente orientado a la implementación del Sistema de Planificación y Control de Gestión.</p> <p><b>ETAPA EGRESADA</b></p>	<p>Implementar el Sistema de Planificación y Control de Gestión, considerando:</p> <p>1. Medición de los indicadores de desempeño comprometidos para el año en curso.</p> <p>2. Identificación de los elementos del sistema necesarios de ajustar para su pleno funcionamiento para el año en curso.</p> <p>3. Identificación de los elementos del sistema necesarios de ajustar para su pleno funcionamiento para el año siguiente.</p> <p><b>ETAPA EGRESADA</b></p>	<p>1. Evaluar el resultado de los indicadores de desempeño seleccionados, cumpliendo las metas entre 75 % y 100 %, logrando un porcentaje de cumplimiento global de los indicadores del Anexo 2, en al menos un 75 %.</p> <p>2. Establecer las principales directrices institucionales que permitan direccionar la gestión del Ministerio Público, elaborando para ello su Plan Estratégico para el período 2016-2023.</p> <p><b>ETAPA COMPROMETIDA AÑO 2016</b></p>	

N

A

**TERCERO:** Compromiso de Gestión Institucional (CGI).

Por este Convenio, las partes definen las Metas de Gestión Institucional para el año 2016, estableciendo los Requisitos Técnicos que deben cumplirse, con sus respectivos Medios de Verificación, que constan en Anexo N° 1.

Las Metas de Gestión Institucional que corresponde a la etapa de desarrollo que alcanzará en el año, los objetivos de gestión de cada etapa y sus respectivos requisitos técnicos, éstos últimos definidos en el Anexo N° 1, fueron establecidas conforme lo definido en el Programa Marco del numeral anterior, y de acuerdo con el estado de avance de cada una de sus etapas.

En cumplimiento de lo establecido en el artículo 7° de la Ley N° 20.240, las Metas definidas para cada Sistema en el Anexo N° 1, son priorizadas y se les asigna las ponderaciones que se indican a continuación:

**METAS DE GESTIÓN  
ETAPAS, PRIORIDADES Y PONDERADORES DEL CONVENIO DE GESTIÓN (CGI)  
DEL AÑO 2016**

ÁREA PRIORITARIA	SISTEMAS	METAS DE GESTIÓN					
		ETAPA DE DESARROLLO O ESTADO DE AVANCE				PRIORIDAD	PONDERADOR %
		1	2	3	4		
USUARIOS Y COMUNIDAD	SISTEMA DE INFORMACIÓN Y ATENCIÓN A USUARIOS				0	BAJA	10%
	SISTEMA DE INFORMACIÓN PARA LA COMUNIDAD UTILIZANDO TIC		0	0		MEDIA	15%
CALIDAD DE ATENCIÓN A USUARIOS	SISTEMA DE SEGURIDAD DE LA INFORMACIÓN	0				BAJA	10%
GESTIÓN ORGANIZACIONAL	PLANIFICACIÓN Y CONTROL DE GESTIÓN				0	ALTA	65%

Adicionalmente, en el Anexo N° 2 que forma parte de este Convenio, las partes acuerdan los indicadores de desempeño que el Ministerio Público compromete para el período de ejecución correspondiente al año 2016.

**CUARTO:** Período de Ejecución.

El período de Ejecución de las Metas de Gestión Institucional para el año 2016 será aquél comprendido entre el 1 de enero de 2016 y el 31 de diciembre de 2016.

**QUINTO:** Fórmulas que vinculan la magnitud del bono de gestión institucional, con el conjunto de los resultados de los distintos indicadores e instrumentos de similar naturaleza.<sup>2</sup>

<sup>2</sup> El artículo 8 de la Ley 20.240 establece que "Podrán establecerse porcentajes mínimos de cumplimiento para cada una de las metas comprometidas. De no lograrse dicho mínimo, el grado de cumplimiento de esa meta particular será

El artículo 4 de la Ley N° 20.240 estableció la fórmula que vincula el grado de cumplimiento del Compromiso de Gestión Institucional, con la magnitud del bono de gestión institucional a que tendrán derecho los funcionarios señalados en el inciso primero del artículo 2 de dicha ley.

Para estos efectos, se entenderá que el grado de cumplimiento del Compromiso de Gestión Institucional corresponde a la suma de las ponderaciones acreditadas por los distintos sistemas.

La ponderación acreditada a cada sistema, será la ponderación que la cláusula TERCERA establece para ese sistema, multiplicada por la suma de las ponderaciones acreditadas a las etapas del mismo sistema.

La ponderación acreditada a cada etapa, será la ponderación que establece el cuadro presentado al final de esta cláusula, multiplicada por la suma de las ponderaciones acreditadas a los requisitos técnicos que pertenecen a dicha etapa.

La ponderación acreditada a cada requisito técnico será la ponderación que establece el **Anexo N° 1** de este Convenio para dicho requisito técnico, si este es cumplido en un 100%, y será cero en caso contrario. Los requisitos técnicos tendrán un valor equivalente dentro de cada etapa. Excepción de lo anterior serán los Requisitos Técnicos de la etapa 4 del Sistema de Planificación y Control de Gestión, en cuyo caso, la ponderación acreditada se determinará del modo que establecen los dos párrafos siguientes.

✓  
La ponderación acreditada al Requisito Técnico N° 2 de la etapa 4 del Sistema de Planificación y Control de Gestión será 70%, multiplicada por la suma de las ponderaciones acreditadas a los indicadores que pertenecen a dicho Requisito Técnico. Los Requisitos Técnicos N° 1 y N° 3 por su lado, tendrán una ponderación de 10% y 20% respectivamente.

La ponderación acreditada a cada indicador que pertenece al Requisito Técnico N° 2 de la etapa 4 del Sistema de Planificación y Control de Gestión, será la ponderación que establece el **Anexo N° 2** de este Convenio para dicho indicador, multiplicada por aquél cociente donde el numerador es el resultado del indicador y el denominador es la meta comprometida para el mismo, en caso de que dicho cociente exceda o iguale 75%. En aquellos indicadores donde dicho cociente sea inferior a 75%, la ponderación acreditada será cero.<sup>3</sup>

De este modo, los requisitos mínimos de cumplimiento serán 75% para los indicadores que conforman el Requisito Técnico N° 2 de la etapa 4 del Sistema de Planificación y Control de Gestión, y serán 100% para los demás requisitos técnicos contenidos en este Convenio.

---

igual a cero." En consecuencia, el establecimiento de porcentajes mínimos de cumplimiento es opcional, y puede establecerse para algunos indicadores o instrumentos de similar naturaleza.

<sup>3</sup> Los valores proyectados como numerador y denominador en la meta de cada indicador (Anexo 2 de este documento) constituyen información de carácter referencial, por lo que en el caso que los valores efectivos alcanzados en el período no se ajusten a dichas proyecciones no constituye incumplimiento del indicador, siempre que la meta comprometida haya sido alcanzada.

PONDERACIÓN ETAPAS PARA CADA UNO DE LOS SISTEMAS CGI 2016				
SISTEMAS	ETAPA 1	ETAPA 2	ETAPA 3	ETAPA 4
SISTEMA DE INFORMACIÓN Y ATENCIÓN A USUARIOS	0	0	0	100 %
SISTEMA DE INFORMACIÓN PARA LA COMUNIDAD UTILIZANDO TIC	0	50 %	50%	0
SEGURIDAD DE LA INFORMACIÓN	100 %	0	0	0
PLANIFICACIÓN Y CONTROL DE GESTIÓN	0	0	0	100 %

**SEXTO:** Revisión o Reformulación del Convenio.

Las partes acuerdan que el presente Convenio podrá ser revisado o reformulado mediante modificación del mismo, en la medida que en el período de ejecución se presenten causas externas calificadas y no previstas, que limiten seriamente su logro o se produzcan reducciones en el presupuesto destinado a financiar ítems relevantes para su cumplimiento.

La Calificación de las referidas causas y posterior revisión de las metas, será realizada, previa solicitud del Fiscal Nacional del Ministerio Público, por el Ministro de Hacienda y de acogerse las referidas causas, éstas quedarán señaladas expresamente en el Convenio Modificatorio.

**SEPTIMO:** Documentos.

Las partes dejan constancia que en el Anexo N° 1 se encuentra el documento "Requisitos Técnicos y Medios de Verificación, Compromiso de Gestión Institucional Año 2016", el que establece el estándar mínimo a alcanzar para cada requisito técnico por cada sistema.

En el Anexo N° 2, se encuentra el documento "Indicadores de Desempeño 2016", el que establece el nombre del mismo, fórmula de cálculo, meta, dimensión/ámbito, medio de verificación, ponderador, supuesto y nota técnica.

Estos dos anexos forman parte integrante del presente convenio.

**OCTAVO:** Personerías.

La personería de don Jorge Abbott Charne, para actuar en representación de la Fiscalía Nacional del Ministerio Público, el nombramiento consta en el Decreto Supremo del Ministerio de Justicia N° 792 de fecha 26 octubre 2015, publicado en el Diario Oficial de 23 de noviembre de 2015, en tanto que la personería de don Rodrigo Valdés Pulido,

ANEXO 1

REQUISITOS TÉCNICOS Y MEDIOS DE VERIFICACIÓN, COMPROMISO DE GESTIÓN INSTITUCIONAL AÑO 2016

Sistema de Información y Atención a Usuarios (SIAU)		
ETAPA 4	Requisitos Técnicos (RT)	Medios de Verificación
<p>1. Evaluar el funcionamiento de los espacios de atención del SIAU formulando recomendaciones de mejora para el año siguiente, si corresponde.</p> <p>2. Ejecutar los compromisos establecidos en el Programa de Seguimiento de las recomendaciones de mejora definido el año anterior.</p> <p>3. Elaborar un programa de seguimiento de la implementación de las recomendaciones de mejora que se seleccionen para ser ejecutadas en el año siguiente.</p>	<p>El Ministerio Público:</p> <ol style="list-style-type: none"> <li>1. Evalúa el funcionamiento de los espacios de atención telefónico, presencial, virtual implementados en todo el país.</li> <li>2. Formula recomendaciones de mejora a los espacios de atención evaluados, si corresponde.</li> <li>3. Ejecuta el o los compromiso(s) establecido(s) en el Programa de Seguimiento de las recomendaciones de mejora definido en el año 2015 a implementar en el año 2016.</li> <li>4. Elabora un programa de seguimiento de la implementación de las recomendaciones de mejora que se seleccionen para ser ejecutadas el año 2017, si corresponde, señalando al menos: los compromisos, los responsables y plazos.</li> </ol>	<ol style="list-style-type: none"> <li>1. Informe de evaluación del funcionamiento de los espacios de atención telefónico, presencial y virtual. (RT 1)</li> <li>2. Informe de recomendaciones de mejora, si corresponde. (RT 2)</li> <li>3. Informe de ejecución de los compromisos establecidos en el Programa de Seguimiento. (RT 3)</li> <li>4. Programa de Seguimiento de la implementación de las recomendaciones de mejora a ser ejecutadas en el año 2017, si corresponde. (RT 4)</li> </ol>

consta en Decreto Supremo N° 593, de fecha 11 de Mayo de 2015 del Ministerio del Interior y Seguridad Pública.

  
**JORGE AROT CHARME**  
**FISCAL NACIONAL MINISTERIO PÚBLICO**

  
  
**RODRIGO VALDÉS PULIDO**  
**MINISTRO DE HACIENDA**

  
**JEFE DE GABINETE**

  
  
**DIRECCIÓN DE GESTIÓN DE SERVICIOS**

Sistema de Información para la Comunidad Utilizando TIC		
ETAPA 2	Requisitos Técnicos (RT)	Medios de Verificación
<p>Mantener vigente la Planificación del Sistema de Información para la Comunidad utilizando TIC, considerando los resultados del diagnóstico y la normativa vigente<sup>4</sup>, a saber:</p> <ol style="list-style-type: none"> <li>1. Priorización y/o secuenciación de los proyectos TIC.</li> <li>2. Identificación de mejores prácticas a replicar en las Fiscalías.</li> <li>3. Elaboración y/o actualización de los programas de trabajo de implementación anual, para la ejecución de los proyectos priorizados en base al Plan de Mejoramiento con uso de TIC, que considere al menos: cronogramas de trabajo, principales hitos, requerimientos de recursos, etapas, plazos y responsables para cada uno de ellos.</li> </ol>	<p>El Ministerio Público mantiene vigente la Planificación del Sistema de Información para la Comunidad utilizando TIC, o lo actualiza, si se identifican cambios en alguno de los siguientes requisitos técnicos:</p> <ol style="list-style-type: none"> <li>1. El Plan de Mejoramiento con uso de TIC para la ejecución y evaluación de cada proyecto de mejoramiento con uso de TIC comprometido en la provisión de productos estratégicos y proceso de soporte institucional, si se identifican cambios en la priorización y/o secuenciación de la Cartera de Proyectos.</li> <li>2. Los programas de trabajo deberán incluir al menos los siguientes aspectos por cada proyecto priorizado, que dará cuenta de las actividades planificadas de los años siguientes:             <ol style="list-style-type: none"> <li>2.1. Objetivo general de cada proyecto.</li> <li>2.2. Objetivos específicos de cada proyecto.</li> <li>2.3. Indicadores de Desempeño para evaluar la operación del proyecto de mejoramiento con uso de TIC.</li> <li>2.4. Identificación secuencial de tareas:                 <ol style="list-style-type: none"> <li>2.4.1. Hitos principales.</li> <li>2.4.2. Cronograma de trabajo que incorpore plazos y responsables de la implementación.</li> </ol> </li> <li>2.5. Identificación de ruta crítica, entendida como la secuencia básica de tareas que asegure que se complete el proyecto.</li> <li>2.6. Plan de mitigación de riesgos (define los riesgos asociados al proyecto y sus acciones para resolverlos).</li> </ol> </li> <li>3. Programa de Monitoreo y control de la implementación de acuerdo al programa de trabajo para cada proyecto de mejoramiento con uso de TIC comprometido, que incluya:</li> </ol>	<p>1. Informe de Planificación del Sistema de Información para la Comunidad utilizando TIC vigente o su actualización. (Contiene RTs 1, 2 y 3)</p>

<sup>4</sup> La normativa a considerar, que sin ser obligatoria para el Ministerio Público puede usarse como referencia en esta etapa, se refiere a las comunicaciones electrónicas, interoperabilidad de documentos electrónicos y su seguridad-confidencialidad (Decreto Supremo N° 14/2014 del Ministerio de Economía, Fomento y Turismo - Subsecretaría de Economía y Empresas de Menor Tamaño (que deroga Decretos Supremos N°s 77/2004 y 81/2004, ambos del Ministerio Secretaría General de la Presidencia) y el Decreto Supremo N° 83/2005 del Ministerio Secretaría General de la Presidencia, respectivamente), mensajes electrónicos masivos no solicitados, desarrollo de sitios WEB (Decreto Supremo N° 83/2005 del Ministerio Secretaría General de la Presidencia, Decreto Supremo N° 14/2014 del Ministerio de Economía, Fomento y Turismo - Subsecretaría de Economía y Empresas de Menor Tamaño (que deroga Decreto Supremo N° 100/2006 del Ministerio Secretaría General de la Presidencia, respectivamente) y Decreto Supremo N° 1/2015 del Ministerio Secretaría General de la Presidencia, que Aprueba Norma Técnica sobre Sistemas y Sitios WEB de los Organos de la Administración del Estado) y nuevas normativas definidas por el comité de normas para el comité de normas para el documento electrónico. Además, se deben considerar las leyes siguientes: Ley N° 19.628 sobre protección de la vida privada y datos personales, Ley N° 19.798 sobre documentos electrónicos y firma electrónica, Ley N° 19.880 sobre bases de procedimientos administrativo.

	<p>3.1 Mecanismos de control. 3.2 Frecuencia de control. 3.3 Hitos de control. 3.4 Requisitos de aceptación conforme por cada hito de control (entregables). 3.5 Fecha de implementación planificada. 3.6 Responsable de cumplimiento.</p>	
--	--	--

Sistema de Información para la Comunidad Utilizando TIC

ETAPA 3	Requisitos Técnicos (RT)	Medios de Verificación
<p>1. Implementar los Programas de Trabajo de los proyectos comprometidos para el año 2016, de acuerdo al Plan de Mejoramiento con uso de TIC, aprobado en la Etapa anterior, señalando los hitos identificados en la planificación.</p> <p>2. Registrar los resultados de la implementación de los proyectos priorizados y, comprometido su inicio en el año en curso, considerando, al menos, las actividades ejecutadas e hitos cumplidos, las dificultades y las modificaciones realizadas respecto de lo programado.</p>	<p>El Ministerio Público:</p> <p>1. Implementa los Programas de Trabajo actualizados para la ejecución de cada proyecto comprometido para el 2016 de mejoramiento con uso de TIC en la provisión de sus productos estratégicos y procesos de soporte institucional.</p> <p>2. Registra los resultados de la implementación de los proyectos, en ejecución o terminados durante el año 2016, considerando lo siguiente:</p> <p>2.1. Aplicar un programa de monitoreo y control de la implementación del programa de trabajo para cada proyecto de mejoramiento con uso de TIC,</p> <p>2.2. Reconocer y declarar las dificultades encontradas en la implementación de las actividades, atribuibles a factores externos e internos.</p> <p>2.3. Justificar eventuales modificaciones a lo programado originalmente de acuerdo a los resultados obtenidos y dificultades en los cumplimientos de compromisos por parte de proveedores y a factores externos e internos.</p>	<p>1. Informe de resultado de la implementación de los programas comprometidos para el año 2016. (Contiene RTs 1 y 2)</p>

Sistema de Seguridad de la Información		
ETAPA 1	Requisitos Técnicos (RT)	Medios de Verificación
<p>1. La Institución realiza un diagnóstico de la situación de seguridad de la información institucional, e identifica en éste los activos de información que dan sustento a una selección de sus procesos de provisión, estableciendo los controles necesarios para mitigar riesgos que puedan afectar a los activos de información críticos, considerando para esto todos aquellos dominios de seguridad de la información que establece el DS 83 y la NCh-ISO 27001-2009, determinando el nivel en que la institución se encuentra respecto de: Políticas de Seguridad, Seguridad Organizacional, Clasificación, Control y Etiquetado de Bienes, Seguridad Física y del Ambiente, Seguridad del Personal, Gestión de la Operaciones y de las Comunicaciones, Control de Acceso, Desarrollo y Mantenimiento de Sistemas, Gestión de Incidentes en la Seguridad de la Información, Gestión de la Continuidad del Negocio y Cumplimiento.</p> <p>2. La Institución compara los resultados del Diagnóstico con los controles establecidos en los dominios de seguridad del DS 83 y la NCh-ISO 27001-2009, y determina las brechas que deberán ser abordadas y cerradas a través de la implementación de un Plan de Seguridad de la Información institucional.</p>	<p>1. El Ministerio Público realiza un diagnóstico del estado actual de la seguridad de la información para sus activos de información críticos, para lo cual deberá:</p> <p>a. Identificar los activos de información para un conjunto seleccionado de procesos de provisión de productos estratégicos, de acuerdo al alcance definido, señalando su nivel de criticidad.</p> <p>b. Analizar los riesgos de seguridad de aquellos activos de información declarados con criticidad media y alta.</p> <p>2. Para aquellos activos de información con criticidad media y alta, el Ministerio Público:</p> <p>a. Identifica los controles (requisitos normativos Norma ISO NCh-ISO 27001 – 2009 y del DS 83 o buenas prácticas) ya cumplidos (o por dominio de seguridad de la información<sup>5</sup>, para mitigar riesgos.</p> <p>b. Identifica los controles o requisitos normativos de los dominios de seguridad, que falta implementar para mitigar los riesgos.</p>	<p>1. Informe de Diagnóstico que contenga Inventario de activos actualizado y el análisis de los riesgos detectados. (Contiene RTs 1 y 2)</p>

Fuente referencial: Documentos Requisitos Técnicos y Medios de Verificación Programa de Mejoramiento de la Gestión años 2012, 2013 y 2014

<sup>5</sup> Los dominios de seguridad de la información son 11: 1) Política de Seguridad (declaración general de voluntad por parte del Jefe de Servicio); 2) Seguridad Organizacional (formalización de estructura y responsabilidades, ejemplo: Encargado y Comité de seguridad de la información); Gestión de activos de información (procedimientos de manejo de la información de acuerdo a su clasificación); Seguridad Física y del Ambiente (medidas y procedimientos de acceso físico, protecciones en cuanto a temperatura, luz u otras variables ambientales); Seguridad del Personal (procedimientos de gestión de RRHH que incorporen medidas de protección para los conocimientos que tienen las personas, en la contratación, capacitación, etc.); Gestión de la Operaciones y de las Comunicaciones (procedimientos asociados a la gestión de antivirus, correo electrónico y respaldo, fundamentalmente); Control de Acceso (procedimientos de manejo de contraseñas para los sistemas, redes, etc.); Desarrollo y Mantenimiento de Sistemas (procedimientos para la creación de software, su actualización o la contratación de estos servicios a terceros); Gestión de Incidentes en la Seguridad de la Información (procedimientos para la creación de software, su actualización o la Continuidad del Negocio (planes para proveer estabilidad a los procesos críticos) y Cumplimiento (chequeo de que las medidas adoptadas satisfacen las leyes y normativas vigentes).

Sistema de Planificación y Control de Gestión

Etapa 4	Requisitos Técnicos (RT)	Medios de Verificación
<p>1. Evaluar el resultado de los Indicadores de desempeño seleccionados, cumpliendo las metas entre 75% y 100%, logrando un porcentaje de cumplimiento global de los Indicadores del Anexo 2, en al menos un 75%.</p> <p>2. Establecer las principales directrices institucionales que permitan direccionar la gestión del Ministerio Público, elaborando para ello su Plan Estratégico para el período 2016-2023.</p>	<p>1. La autoridad del Ministerio Público informa al Ministerio de Hacienda, en el contexto del proceso de evaluación del CGI correspondiente al año 2016, el valor efectivo de cada uno de los indicadores comprometidos a evaluar en el año en curso y dispone de los medios de verificación que respaldan los valores informados de cada indicador.</p> <p>2. El porcentaje de cumplimiento<sup>6</sup> global de los indicadores definidos en el Anexo 2, corresponderá a la sumatoria de los porcentajes acreditados para cada indicador cumplido y parcialmente cumplido. Para todos los indicadores, se considerará:</p> <ul style="list-style-type: none"> <li>• <u>Cumplido</u> cuando su porcentaje de cumplimiento sea igual o mayor al 95%, por lo cual se acredita el 100% de la ponderación de dicho indicador.</li> <li>• <u>Cumplido parcialmente</u> cuando su porcentaje de cumplimiento sea igual o superior a 75% y menor a 95%. En dicho caso, el porcentaje acreditado al ponderador del indicador será el resultado de la multiplicación de su respectivo ponderador por el porcentaje de cumplimiento del indicador.</li> <li>• <u>No cumplido</u> cuando su porcentaje de cumplimiento sea inferior a 75% o cuando no sea posible verificar los valores a través de sus medios de verificación y por tanto no permitan determinar el valor efectivo informado. En este caso el ponderador acreditado a ese indicador será igual a cero.</li> </ul> <p>3. El Ministerio Público establece sus principales definiciones estratégicas y las principales líneas de acción a desarrollar para el período 2016-2023, para lo cual elabora su Plan Estratégico el cual contendrá al menos la visión, misión, objetivos estratégicos y líneas de acción que permitan direccionar la gestión institucional.</p>	<p>1. Informe de resultados de los indicadores comprometidos a evaluar (valores efectivos y grado de cumplimiento). (RT 1 y 2)</p> <p>2. Medios de verificación de cada uno de los indicadores comprometidos. (RT 2)</p> <p>3. Plan Estratégico del Ministerio Público para el período 2016-2023. (RT 3)</p>

<sup>6</sup> El sobrecumplimiento de los indicadores no afecta el cumplimiento de la meta definidas, por ende se consideran como "cumplidos".

ANEXO 2 CGI 2016

<p>1</p> <p>Porcentaje de solicitudes ingresadas en el año t por el espacio de atención presencial del SIAU que requieren evaluación interna respondidas al usuario dentro del plazo establecido desde su fecha de ingreso, respecto del número total de solicitudes ingresadas en el año t por el espacio de atención presencial del SIAU que requieren evaluación interna.</p>	<p>(Número de solicitudes ingresadas por el espacio de atención presencial del SIAU que requieren evaluación interna respondidas al usuario dentro del plazo establecido desde su fecha de ingreso / Número total de solicitudes ingresadas por el espacio de atención presencial del SIAU que requieren evaluación interna)*100</p>	<p>ND</p> <p>ND</p> <p>Calidad / Producto</p>	<p>83,7% (123.329 / 147.379)</p> <p>No hay (no se mide como indicador el año 2015)</p>	<p>80% (240.685 / 300.856)</p> <p>10%</p>	<p>Informe consolidado de solicitudes ingresadas a SIAU emitido por la División de Atención a Víctimas y Testigos.</p> <p>- La posibilidad de realizar la medición se encuentra sujeta a la disponibilidad y suficiencia de los datos, que se encuentran contenidos en el sistema Informático SIAU, cuya plataforma de servicio se encuentra externalizada, por ende se requiere que dicho sistema presente continuidad y estabilidad en su funcionamiento.</p> <p>(1)</p>
<p>2</p> <p>Porcentaje de solicitudes ingresadas en el año t por el espacio de atención virtual del SIAU que requieren evaluación interna respondidas al usuario dentro del plazo establecido desde su fecha de ingreso, respecto del número total de solicitudes ingresadas en el año t por el espacio de atención virtual del SIAU que requieren evaluación interna.</p>	<p>(Número de solicitudes ingresadas por el espacio de atención virtual del SIAU que requieren evaluación interna respondidas al usuario dentro del plazo establecido desde su fecha de ingreso / Número total de solicitudes ingresadas por el espacio de atención virtual del SIAU que requieren evaluación interna)*100</p>	<p>ND</p> <p>ND</p> <p>Calidad / Producto</p>	<p>89,9% (6.552 / 7.285)</p> <p>No hay (no se mide como indicador el año 2015)</p>	<p>80% (87.186 / 108.982)</p> <p>10%</p>	<p>Informe consolidado de solicitudes ingresadas a SIAU emitido por la División de Atención a Víctimas y Testigos.</p> <p>- La posibilidad de realizar la medición se encuentra sujeta a la disponibilidad y suficiencia de los datos, que se encuentran contenidos en el sistema Informático SIAU, cuya plataforma de servicio se encuentra externalizada, por ende se requiere que dicho sistema presente continuidad y estabilidad en su funcionamiento.</p> <p>(2)</p>

<sup>1</sup> Los valores del operando sobre los que se calculan las metas de todos los indicadores del Anexo 2 2016, corresponden solo a estimaciones de carácter referencial y no son parte de la evaluación.

18



REPUBLICA DE COLOMBIA  
 MINISTERIO DE JUSTICIA Y DEL DERECHO  
 DIRECCIÓN DE ADMINISTRACIÓN DE JUSTICIA  
 DIVISIÓN DE ESTADÍSTICA Y ANÁLISIS DE DATOS

Porcentaje de casos NO TCMC Ingresados por delitos de abusos sexuales y violaciones con víctimas mayores de edad con imputado conocido más los casos de robos con violencia e intimidación y robos en lugar habitado con imputado sometido a ACD por flagrancia que cumplen con el registro de declaración de la víctima en la fiscalía en plazo inferior o igual a 30 días, en el año t.	(Número de casos NO TCMC Ingresados por delitos de abusos sexuales y violaciones con víctimas mayores de edad con imputado conocido más los casos de robos con violencia e intimidación y robos en lugar habitado con imputado sometido a ACD por flagrancia que cumplen con el registro de declaración en la fiscalía en plazo inferior o igual a 30 días) / (Número total de casos NO TCMC Ingresados por delitos de abusos sexuales y violaciones con víctimas mayores de edad con imputado conocido	Eficiencia / Proceso	55,4% (2.480 / 4.475)	NA	51% (4.958 / 9.721)	10%	Informe consolidado emitido por la División de Estudios.	- Modificación legal de las facultades de fiscales y policías para la realización de diligencias de investigación. - Disponibilidad y suficiencia de los datos, que se encuentran contenidos en el sistema Informático SAF, se requiere que dicho sistema presente continuidad y estabilidad en su funcionamiento.
5		ND						Implican el funcionamiento anormal de la empresa adjudicada para la realización del estudio, como por ejemplo, huelgas o paros, término del contrato, siniestros que la inhabiliten, etc.; o bien cuando se verifique el incumplimiento reiterado y contumaz por parte de la empresa de los acuerdos básicos de servicio, a pesar de que el Ministerio Público haya adoptado las medidas correctivas de su facultad de acuerdo a lo establecido en el contrato.



Pago Oportuno a Proveedores	a (Nº de pagos asociados a la operación (Subtítulo 22) y la inversión (Subtítulos 29 y 31) efectuados dentro de un plazo de 30 días corridos, en compras o contrataciones relevantes en el Ministerio Público, durante el año 2016)/(Total de pagos efectuados asociados a compras o contrataciones relevantes vinculados a la operación (Subtítulo 22) y la inversión (Subtítulos 29 y 31) en el Ministerio Público, efectuados durante el año 2016)*100.	Eficacia / proceso	96,6% <sup>2</sup> (8.366/ 8.658)	97% (6.964 7.182)	86,5%  90% (13.954 / 15.505)	10%	(8)

Informe consolidado emitido por la División de Administración y Finanzas.

Para proceder al pago de facturas por parte del Ministerio Público, es necesario que se den las siguientes condiciones:

- 1) Que los bienes o servicios hayan sido recepcionados a conformidad por parte del Ministerio Público.
- 2) Que los documentos de cobro (facturas, boletas, etc.), emitidas por los proveedores respectivos, sean correctamente emitidas.
- 3) Que los pagos se inicien una vez que los respectivos contratos están totalmente tramitados. Esto en el caso de tratarse de contratos suscritos por ambas partes.
- 4) Que los documentos de cobro sean emitidos una vez que los respectivos contratos están totalmente tramitados. Esto en el caso de tratarse de contratos suscritos por ambas partes.
- 5) Que los documentos de cobro sean emitidos una vez que las respectivas órdenes de compra o servicio asociadas hayan sido emitidas y enviadas.

<sup>2</sup> Para el caso del Indicador "Pago Oportuno a Proveedores", este fue medido durante el segundo semestre de 2014 dado que el primer semestre de dicho año se efectuó la construcción de su línea base.

GOBIERNO GENERAL DE LA REPUBLICA VENEZOLANA MINISTERIO DEL PODER JUDICIAL TRIBUNAL UNICO ELECTORAL SECCION DE RECURSOS ELECTORALES CARACAS, VENEZUELA	NÚMERO DE EXPEDIENTE: 0116 FECHA: 2011	NÚMERO DE FOLIO: 0116 FECHA: 2011									
<p>6) Que los documentos de cobro sean emitidos una vez que los respectivos bienes o servicios hayan sido recibidos a conformidad por el Ministerio Público.</p> <p>7) Que los emisores de los documentos de cobro, en los casos que correspondan, hayan informado oportunamente respecto de la entrega de dichos documentos a un factoring y que las notificaciones notariales asociadas hayan llegado también oportunamente.</p> <p>8) Que se haya efectuado previamente la identificación de fondos (a través de Decreto Supremo) por parte del Ministerio de Hacienda, en el caso de los pagos asociados al Subtítulo 31.</p> <p>9) Que exista presupuesto suficiente, en la o las cuentas presupuestarias respectivas, para efectuar el pago asociado.</p> <p>10) Que todos los Certificados de Cumplimiento de Obligaciones Laborales y Previsionales asociados a pagos de contratos suscritos por servicios acogidos a Ley de Subcontratación, hayan sido</p>											

recibidos a conformidad por el Ministerio Público a más tardar dentro de los 23 días corridos siguientes a la recepción conforme de los respectivos documentos de cobro.

11) No se registren, en el año, situaciones imprevistas, fuera del ámbito de control del Ministerio Público, que afecten los plazos de pago de pagos relevantes.

En el caso que no se cumpla cualquiera de los supuestos anteriores, el pago asociado no será considerado en la medición del indicador.

ND: No Disponible  
NA: No Aplica

**Notas:**

- (1) - El Sistema de Información y Atención a Usuarios (SIAU) del Ministerio Público es un sistema transversal que coordina los espacios de atención existentes, a fin de facilitar a los usuarios el acceso a los servicios que presta la Institución a través de la entrega de información, recepción y gestión de sus requerimientos y su correspondiente respuesta.
- Dar respuesta a una solicitud implica las actividades de resolver la solicitud y comunicarla al usuario.
  - Se entenderá que una solicitud es comunicada cuando el encargado que corresponde informe al usuario lo resuelto respecto a su solicitud, dejando registro de dicha comunicación en el sistema de registro.
  - El plazo para dar respuesta a las solicitudes que requieren de evaluación interna es hasta los cinco días hábiles siguientes desde su fecha de Ingreso. En tanto, en el caso de solicitudes correspondientes a "solicitud de diligencias de investigación", "solicitud de devolución de especies/dinero" y "solicitud de reapertura de una causa con nuevos antecedentes", el plazo se extenderá hasta los 10 días hábiles siguientes a la fecha de su Ingreso.
  - Se excluyen las solicitudes del tipo "Aporte de antecedentes asociados a una causa", ya que no requieren una comunicación con el usuario con posterioridad a la recepción de dichos antecedentes.
  - Los días hábiles que señala este Indicador corresponden a días calendario, sin considerar hora de Ingreso, es decir, si un requerimiento Ingresado el día hábil N°1, los días hábiles se emplean a contabilizar desde el día hábil siguiente de realizado el requerimiento.
  - Se entenderá como días hábiles de lunes a viernes, exceptuando los días feriados.
  - La evaluación del cumplimiento de este Indicador estará referida al resultado acumulado del año 2016 a nivel nacional.
- (2) - El Sistema de Información y Atención a Usuarios (SIAU) del Ministerio Público es un sistema transversal que coordina los espacios de atención existentes, a fin de facilitar a los usuarios el acceso a los servicios que presta la Institución a través de la entrega de información, recepción y gestión de sus requerimientos y su correspondiente respuesta.
- Dar respuesta a una solicitud implica las actividades de resolver la solicitud y comunicarla al usuario.
  - Se entenderá que una solicitud es comunicada cuando el encargado que corresponde informe al usuario lo resuelto respecto a su solicitud, dejando registro de dicha comunicación en el sistema de registro.
  - El plazo para dar respuesta a las solicitudes que requieren de evaluación interna es hasta los cinco días hábiles siguientes desde su fecha de Ingreso. En tanto, en el caso de solicitudes correspondientes a "solicitud de diligencias de investigación", "solicitud de devolución de especies/dinero" y "solicitud de reapertura de una causa con nuevos antecedentes", el plazo se extenderá hasta los 10 días hábiles siguientes a la fecha de su Ingreso.
  - Se excluyen las solicitudes del tipo "Aporte de antecedentes asociados a una causa", ya que no requieren una comunicación con el usuario con posterioridad a la recepción de dichos antecedentes.
  - Los días hábiles que señala este Indicador corresponden a días calendario, sin considerar hora de Ingreso, es decir, si un requerimiento Ingresado el día hábil N°1, los días hábiles se emplean a contabilizar desde el día hábil siguiente de realizado el requerimiento.
  - Se entenderá como días hábiles de lunes a viernes, exceptuando los días feriados.
  - La evaluación del cumplimiento de este Indicador estará referida al resultado acumulado del año 2016 a nivel nacional.
- (3) - Se consideran las Víctimas VIF mayores de dieciocho años, Ingresadas en casos VIF, por un Parte Policial o Denuncia Directa, con evaluación de riesgo medio o alto.
- Se excluyen víctimas menores de dieciocho años, víctimas sin registro de edad y casos asociados a delitos sexuales.
  - Se consideran medidas de protección autónomas y cautelares, excepto las que se indican a continuación:
    - o Medidas sin especificar o tipificadas como "Otra".
    - o Contacto telefónico prioritarlo con la policía.
    - o Impedir que se tome fotografía o que por cualquier otro medio se capte su imagen.
    - o Solicitud de biombo.

- o Solicitud de circuito cerrado de TV.
  - o Elabora Plan de Autoprotección en conjunto con la víctima.
  - o Entrega número telefónico del Plan cuadrante.
  - o Medida cautelar personal artículo 196 f (retención del permiso para conducir).
- El modelo establece que el plazo de otorgamiento de las medidas de protección es hasta dos días hábiles siguientes desde la fecha de evaluación de riesgo medio o alto.
- (4) • La Información de este Indicador corresponde a la evaluación de la Satisfacción General del servicio presencial del SIAU entregado en la Fiscalía. Específicamente se refiere a la aplicación de la pregunta: ¿Qué tan satisfecho quedó usted con el servicio en general que le entregó la Fiscalía cuando concurrió a sus oficinas? u otra pregunta equivalente.
- Las respuestas se organizan de acuerdo a una escala de notas de uno a siete, donde la nota uno representa la peor evaluación "muy insatisfecho", y la nota siete representa la mejor evaluación "muy satisfecho".
  - Se considera que las notas uno a cuatro representan evaluaciones negativas; en tanto, las notas cinco, seis y siete, corresponden a evaluaciones positivas.
  - Se encuestará a usuarios mayores de edad atendidos por el espacio presencial del SIAU en fiscalías locales, cuyos requerimientos o solicitudes de información, se encuentren respondidas o concluidas, esto es, que ya se ha completado el ciclo de atención y que sus datos de dirección o teléfono (fijo o celular) se encuentren registrados en el SAF o en el sistema de registro del SIAU.
  - Se excluirá de la muestra a usuarios imputados.
  - Para el cálculo del nivel de satisfacción general, las evaluaciones efectivas (cuestionarios aplicados) se deben ponderar por los factores de proporcionalidad que se estime adecuado conforme a la metodología del estudio, a fin de asignarle a cada caso el peso real que le corresponde según su segmento.
  - Para la evaluación de este indicador se debe considerar el valor resultante de todos los ajustes y ponderaciones que defina la metodología del estudio.
  - La muestra será representativa de los usuarios atendidos por el SIAU presencial en un periodo cercano a la aplicación de la encuesta, según lo defina la metodología del estudio, para resguardar el grado de recordación de los usuarios respecto a los aspectos que les son consultados.
  - El período t, corresponde a un espacio de aproximadamente dos meses, inmediatamente anteriores al inicio de la etapa de aplicación de las encuestas, de modo que los cuestionarios se aplican a una muestra de los usuarios atendidos en dicho período.t

- (5) Tramitación de Casos No TCMC: Se refiere a aquellos casos que no cumplen con los atributos definidos para ser clasificados como "Casos Menos Complejos", es decir, corresponden a los casos de tramitación compleja y se opera en base a los instructivos generados por el Fiscal Nacional.
- Se consideran los casos NO TCMC ingresados por los siguientes delitos:
    - o Abusos sexuales y violaciones (en todas sus formas) cometidos en contra de víctimas mayores de edad y donde el imputado es conocido.
    - o Respecto a los robos con violencia, robos con intimidación y robos en lugar habitado debe existir un imputado sometido a ACD (Audencia Control de Detención) por flagrancia. Para este segmento se considera el total de víctimas directas, es decir, menores y mayores de edad.
  - Respecto al cálculo del plazo del registro de la declaración, se debe considerar éste como aquel comprendido desde la fecha de recepción hasta la fecha del registro de declaración, salvo en las siguientes situaciones:
    - Para aquellos casos donde la fecha del registro de declaración es menor a la fecha de recepción, y la digitación se realizó en la misma fiscalía, el cálculo se realizará entre la fecha de la denuncia (fec\_fiscalía) y la fecha del registro de declaración; o bien,
    - Si la víctima fue ingresada posteriormente a la fecha de recepción o fecha de denuncia, el cálculo se realizará entre la fecha de ingreso de la víctima y la fecha de la declaración; o bien,
    - Si la fecha del registro de declaración es menor a la fecha de recepción, y la digitación se realizó en otra fiscalía, se verificará si hubo una transferencia del caso. Si es así, el cálculo se realizará entre la fecha de la denuncia (fec\_fiscalía) y la fecha del registro de declaración. Si el registro de declaración es ejecutado dentro del plazo establecido entonces, y antes de la transferencia del caso, se

agregará al numerador y denominador de la fiscalía que realizó el registro la actividad en el SAF, en cambio, si el registro de declaración fue ejecutado, pero posterior al plazo establecido, y antes de la transferencia del caso, no se considerará en ninguna de las partes.

- Si en el caso existe más de un registro de declaración se considerará en el cálculo la primera ingresada.

(6) **Tramitación de Casos Menos Complejos (TCMC):** Corresponde a un modelo de trabajo mediante el cual se estandariza el proceso de evaluación inicial de los casos ingresados para la posterior asignación a los equipos de trabajo de la Fiscalía y se basa en la identificación de los tipos de término (Salidas Judiciales y Salidas No Judiciales) asociados al respectivo caso.

- Se consideran los casos TCMC Ingresados por los siguientes delitos:

- o Robo con intimidación
- o Robo con violencia
- o Robo en lugar habitado destinado a la habitación.
- Se consideran actividades de contacto válidas para la medición:
  - comunicación telefónica (se incluyen las comunicaciones Ingresadas en el SAF, como también los registros de contacto Ingresados en el Sistema OPA);
  - citación;
  - toma de declaración;
  - registro de aporte de antecedentes por sistema SIAU.

- Para las actividades de contacto, se consideran las víctimas directas, independiente de su edad (menores y mayores de edad).
- Respecto al cálculo del plazo, se debe considerar éste como aquel comprendido desde la fecha de recepción hasta la fecha de la primera actividad de contacto, salvo en las siguientes situaciones:

- Para aquellos casos donde la fecha de la primera actividad de contacto es menor a la fecha de recepción, y la digitación se realizó en la misma fiscalía, el cálculo se realizará entre la fecha de la denuncia (fec\_fiscalía) y la fecha de la primera actividad de contacto; o bien,
- Si la fecha de la primera actividad de contacto es menor a la fecha de recepción, y la digitación se realizó en otra fiscalía, se verificará si hubo una transferencia del caso. Si es así, el cálculo se realizará entre la fecha de la denuncia (fec\_fiscalía) y la fecha de la primera actividad de contacto. Si la primera actividad de contacto es ejecutada dentro del plazo establecido y antes de la transferencia del caso, entonces, se agregará al numerador y denominador de la fiscalía que realizó la actividad en el SAF, en cambio, si la primera actividad de contacto fue ejecutada posterior al plazo establecido, y antes de la transferencia del caso, no se considerará en ninguna de las partes.

- Se excluirán de la medición del indicador las Fiscalías Locales de Arica, Alto Hospicio, Calama, Copiapó, Ovalle, La Ligua, San Fernando, Parral, Coronel, Carahue, Valdivia, Puerto Varas, Coyhaique, Punta Arenas, Mollilla, las Condes, Centro de Justicia y TCMC San Miguel, en la medida que se vayan incorporando durante el año 2015 a un proyecto piloto de ajustes a los procesos de ingreso y tramitación de casos, como parte de las acciones de mejoramiento que se enmarcan en la ley de fortalecimiento.

(7) Los Pilotos a Implementar son cuatro (4), cada uno correspondiente a las siguientes Fiscalías Regionales: Valparaíso, del Libertador Bernardo O'Higgins, Del Biobío y De la Araucanía, según lo dispone el DS N°1564 del Ministerio de Hacienda del 23 de octubre de 2015 y lo contemplado en el Plan de Implementación.

**Plan de Implementación:** Se refiere a las actividades asociadas a las áreas de RRHH; Infraestructura y Modelo de Operación, necesarias para iniciar el funcionamiento de las 4 regiones comprometidas y que ingresan en el primer año de gradualidad al Sistema de Análisis Criminal. Estas regiones corresponden las definidas en el Decreto Supremo respectivo suscrito entre los Ministerios de Hacienda y Justicia. Las áreas y actividades más relevantes del Plan, son las siguientes:

- o RECURSOS HUMANOS: Proceso de contratación de funcionarios y fiscales asignados al proyecto y capacitación de los mismos.
- o INFRAESTRUCTURA: Diagnóstico de necesidades regionales (fiscalías regionales que integran el Plan Piloto) y entrega de espacios habilitados arquitectónicamente para el Sistema de Análisis Criminal.
- o MODELO DE OPERACIÓN DEL SISTEMA DE ANÁLISIS CRIMINAL: Reuniones de trabajo con Fiscalías Regionales Piloto para la definición del modelo de operación.

- (8) Las compras o contrataciones relevantes serán aquellas asociadas a la operación (Subtítulo 22) y la Inversión (Subtítulos 29 y 31) del Ministerio Público, cuyo monto total sea igual o superior a 150 UTM (Ciento cincuenta Unidades Tributarias Mensuales).
- Para efectos del cálculo del indicador, se consideraran todos los pagos de la Fiscalía Nacional y Fiscales Regionales, Independiente de su cuantía, asociados a las compras o contrataciones relevantes antes definidas.
  - Se incluirán, dentro de estas contrataciones relevantes, aquellas de carácter permanente, como son los servicios básicos (luz, agua, gas), además de los pagos por arriendos, gastos comunes, pasajes (emitidos en virtud del contrato de administración de viajes institucionales) y telepeajes (tag), entre otros, conforme a las instrucciones que entregue a este efecto la División de Administración y Finanzas.
  - Los pagos a considerar para efectos del indicador serán exclusivamente con cargo al presupuesto 2016.
  - Para efectos del indicador, cada documento de cobro genera un pago, es decir, cada factura, boleta o similar, será la unidad básica de medida.
  - Los pagos de contratos escritos y suscritos por ambas partes, podrán efectuarse sólo una vez que los mismos estén totalmente tramitados y los respectivos bienes o servicios hayan sido recibidos a conformidad por el Ministerio Público, según visto bueno otorgado por los responsables o usuarios.
  - La periodicidad de cálculo será mensual.
  - Para cada pago, la fecha de pago efectivo, para efectos del indicador, es la siguiente: a) el día hábil siguiente de la fecha de aviso al proveedor en que se le indica que el cheque está disponible para ser retirado o, de no haber registro de dicho aviso, la fecha efectiva de retiro del cheque, cuando el cheque de pago es retirado por el proveedor o su representante para estos efectos; b) la fecha del depósito bancario, cuando el cheque de pago es depositado en la cuenta bancaria del proveedor; c) la fecha de emisión del respectivo comprobante de pago o timbre de pago, cuando se efectúa el pago en algún Centro de Pago del proveedor o de terceros autorizados por éste; d) la fecha de pago indicada en la transferencia electrónica, cuando se efectúa la transferencia electrónica de fondos desde la cuenta de Banco Estado del Ministerio Público a la cuenta bancaria del proveedor; e) la fecha de la carta de envío del cheque, cuando el cheque es enviado por carta al proveedor.
  - El plazo de 30 días corridos para efectuar oportunamente los pagos se contará, a partir de la fecha de recepción conforme en el Ministerio Público de los documentos de cobro (boletas, facturas y/o estados de pago).
  - Para cada pago, la fecha de recepción conforme del documento de cobro, para efectos del indicador, es la fecha indicada en el timbre de recepción que figura en el mismo documento. De no existir este timbre o estar ilegible, se usará la fecha de emisión del documento de cobro.
  - El valor de la UTM a considerar para definir si las compras o contrataciones son relevantes, es la correspondiente al mes de la Resolución de Adjudicación o Contratación Directa, al mes de la Orden de Compra u Orden de Servicio, o de la fecha de suscripción del contrato respectivo, lo que ocurra antes.
  - En el caso de los pagos asociados a Estados de Pago de proyectos de Infraestructura (Subtítulo 31), se considera como fecha de recepción conforme del documento de cobro la fecha de recepción del Oficio conductor que envía el respectivo Estado de Pago al Ministerio Público, la que figura en el respectivo timbre de recepción en el documento. De no existir este timbre o estar ilegible, se considera la fecha de emisión del Oficio conductor como fecha de recepción conforme del documento de cobro.
  - Debe utilizarse el formato de informe de reporte que la División de Administración y Finanzas defina para estos efectos.
  - Cada reporte mensual debe incluir todos los pagos de compras y contrataciones relevantes con fecha de pago efectivo dentro del mes a reportar.
  - El reporte mensual del indicador se realizará los días 20 (ó el día hábil siguiente) del mes siguiente al reportado.
- Casos especiales:
- Contratos de Salas Cunas: Estos pagos deben ser incorporados sólo en caso que correspondan a un convenio suscrito con una empresa en particular, en cuyo marco acudían varios menores, de modo que el monto total contratado iguale o supere las 150 UTM. Por lo mismo, no deben ser informados en el caso que se suscriban contratos con salas cuna distintas por cada menor en cuanto no igualen o superen las 150 UTM en total. En el caso de existir convenios de carácter permanente con alguna Sala Cuna, los pagos debieran ser incorporados, independientemente de la cantidad de niños que asistan a la misma.

- Renovación de Contratos que inicialmente y hasta la fecha no superan las 150 UTM pero, como resultado de su renovación, sí superan dicho monto total contratado al considerar los pagos efectuados previamente: En estos casos deberán incorporarse los pagos del contrato a partir de la renovación que implicó que la contratación superase las 150 UTM al considerar los pagos previos. No deberán informarse o incorporarse pagos previos a dicha renovación pues, antes de la renovación, la contratación era por menos de 150 UTM.
- Peritos psicólogos externos: Los pagos asociados deben ser incluidos sólo en caso que correspondan a convenios suscritos, los cuales, por su período de vigencia, pudieran implicar un monto a contratar total igual o superior a 150 UTM.
- Otros peritajes: Los pagos asociados deben ser incluidos sólo si la contratación es igual o superior a 150 UTM.
- Anticipos a proveedores: No procede informar los pagos asociados por cuanto el pago se efectúa con anterioridad a la emisión de la factura o boleta (documento de cobro). Ejemplos son la compra de combustible en el marco del convenio "Cupón Electrónico Copec" (en la medida que se pague en forma anticipada de la manera descrita); y el pago de peritajes ADN a la Dirección de Logística de Carabineros de Chile, ya que dicha Institución emite la factura con posterioridad a la realización del pago.
- Pago de Comisiones a Banco del Estado de Chile en el marco del Convenio de Pago Electrónico: Si corresponde incorporar estos pagos, pues se considera una contratación permanente, que implica pagos por más de 150 UTM asociadas al convenio señalado.



M. HACIENDA OF PARTES  
18.07.2016 10:50



OFICIO FN N° 432/2016

**ANT.: Convenio Desempeño  
Institucional año 2016, Ministerio  
Público.**

**MAT.: Remite modificación que  
indica.**

**Santiago, 15 de julio de 2016**

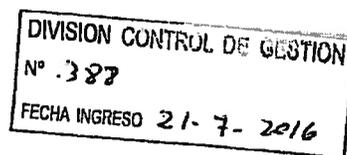
**DE : SR. JORGE ABBOTT CHARME  
FISCAL NACIONAL DEL MINISTERIO PÚBLICO**

**A : SR. RODRIGO VALDÉS PULIDO  
MINISTRO DE HACIENDA**

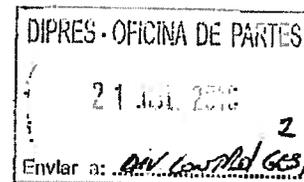
En relación con el Convenio de Desempeño Institucional del Ministerio Público para el año 2016, la Instancia Técnica, formada por representantes del Ministerio de Hacienda y del Ministerio Público conforme con el artículo 15 de la ley 20.240, ha estimado necesario modificar ese Convenio con el fin de dar respuesta a las actualizaciones que se desarrollan en el documento adjunto. Las modificaciones propuestas se refieren a la actualización de Norma ISO 27001, ajuste al periodo de vigencia del nuevo Plan Estratégico Institucional, y publicación en el Diario Oficial de la ley N° 20.931, que facilita la aplicación efectiva de las penas establecidas para los delitos de robo, hurto y receptación y mejora la persecución penal en dichos delitos.

Coincidiendo este Fiscal Nacional con las propuestas de la Instancia Técnica, adjunto para su consideración, debidamente suscrito en tres ejemplares, texto de las modificaciones aludidas, según propuesta de los representantes de la instancia antes mencionada.

Saluda atentamente a UD.,



**JORGE ABBOTT CHARME  
FISCAL NACIONAL DEL MINISTERIO PÚBLICO**



**OF DE PARTES DIPRES  
21.07.2016 10:16**

General Mackenna 1369 - piso 2 - Santiago  
Fono: (56-2) 22 965 9500 - www.fiscaliadechile.cl

Primer PDC/camp

c.c.: Sr. Patricio Leiva, Representante Instancia Técnica Ministerio de Hacienda.  
Dirección Ejecutiva Nacional.  
Unidad de Planificación y Coordinación Estratégica.  
- Archivo

06747/2016

**MODIFICACIÓN AL CONVENIO DE DESEMPEÑO INSTITUCIONAL DEL  
MINISTERIO PÚBLICO PARA EL AÑO 2016, POR ACTUALIZACIÓN DE  
NORMA ISO 27001, AJUSTE AL PERIODO DE VIGENCIA DEL NUEVO PLAN  
ESTRATÉGICO INSTITUCIONAL, Y PUBLICACIÓN EN EL DIARIO OFICIAL DE  
LA LEY N° 20.931, QUE FACILITA LA APLICACIÓN EFECTIVA DE LAS PENAS  
ESTABLECIDAS PARA LOS DELITOS DE ROBO, HURTO Y RECEPCIÓN Y  
MEJORA LA PERSECUCIÓN PENAL EN DICHS DELITO**

En Santiago, a 15 julio de 2016, entre el Ministerio Público, representado por el Fiscal Nacional, don Jorge Abbott Charme, chileno, abogado, Cédula de Identidad N° 5.982.815-0, ambos con domicilio en Avenida General Mackenna 1369, piso 2, de la comuna y ciudad de Santiago, y el Ministerio de Hacienda, representado por don Rodrigo Valdés Pulido, chileno, casado, Ingeniero Comercial, Cédula de Identidad N° 8.267.804-2, ambos domiciliados en calle Teatinos N° 120, piso 12, comuna de Santiago, se efectúa la siguiente modificación al Convenio de Desempeño Institucional del Ministerio Público para el año 2016, suscrito con fecha 31 de diciembre de 2015.

La Instancia Técnica, formada por representantes del Ministerio de Hacienda y del Ministerio Público, de acuerdo al artículo 15 de la Ley N° 20.240, han acordado proponer las modificaciones al Convenio de Desempeño Institucional del Ministerio Público para el año 2016, respecto de la referencia realizada a la versión 2009 de la Norma Chilena ISO 27.001, respecto del período de vigencia del Plan Estratégico del Ministerio Público, y respecto de las materias en que incide la ley N° 20.931, que facilita la aplicación efectiva de las penas establecidas para los delitos de robo, hurto y recepción y mejora la persecución penal en dichos delito, recientemente publicada en el Diario Oficial de 5 de julio del presente año.

Con relación a la Norma Chilena ISO 27.001, se propone modificar la referencia a la versión 2009 por aquella versión 2013, en las páginas 5 y 15 del Convenio de Gestión Institucional relacionado con el Sistema de Seguridad de la Información, por existir actualmente vigente una nueva versión correspondiente al año 2013.

Lo anterior, debido a que conforme la información disponible, tenida a la vista respecto a lo elaborado por el Instituto Nacional de Normalización (INN), la norma en comento se encuentra actualizada respecto a la versión 2009. Es esta última versión sobre la cual se redactó el objetivo del Sistema, sus requisitos técnicos y el respectivo medio de verificación. En consecuencia, la Instancia Técnica estima necesario adecuarlos a la versión del año 2013. Ello, con la finalidad que el Diagnóstico que debe realizar el Ministerio Público sobre Seguridad de la Información, se establezca sobre estándares que permitan una evaluación del riesgo lo más actualizada posible, y de esa manera se puedan adoptar los controles imprescindibles para lograr mitigar o eliminar tales riesgos.

Respecto a la vigencia del nuevo plan estratégico Institucional, la Constitución de la República de Chile, establece en su Capítulo VII, específicamente en su artículo 85, que el Fiscal Nacional durará ocho años en el ejercicio de sus funciones y que le será aplicable lo dispuesto en el inciso segundo del artículo 80, en lo relativo al tope de edad, esto es los 75 años. En el caso particular del Fiscal Nacional Sr. Jorge Abbott Charme, la segunda restricción (edad), prima por sobre la primera, por cuanto cumplirá los 75 años en octubre del año 2022, es decir, poco más de un año antes que se cumpla el periodo de los 8 años. Conforme a lo anterior, se estima pertinente que el nuevo Plan Estratégico del Ministerio Público tenga una vigencia de siete años, esto es, hasta el año 2022 y no como lo establece actualmente el CGI 2016, hasta el año 2023, en las páginas 6 y 16 relacionadas con el Sistema de Planificación y Control de Gestión.

Finalmente, con fecha 5 de julio recién pasado, se publicó en el Diario Oficial la Ley N° 20.931, que facilita la aplicación efectiva de las penas establecidas para los delitos de robo, hurto y receptación y mejora la persecución penal en dichos delitos. Uno de los aspectos relevantes de esta normativa legal, dice relación, específicamente, con la modificación al artículo 183 del Código Procesal Penal que, en lo relativo a la solicitud de diligencias de investigación, dispone que el fiscal, respecto de ellas "...deberá pronunciarse dentro de los 10 días siguientes a la solicitud...".

Sobre esta materia, se debe tener en consideración el impacto que la modificación legal generará en los procesos de trabajo del Ministerio Público y, en consecuencia, en lo comprometido en el Anexo N° 2 (notas 1 y 2 relacionadas con los Indicadores 1 y 2 del SIAU respectivamente).

La norma referida tiene incidencia en el servicio del SIAU denominado "*Solicitud de diligencias*", que se encuentra regulado en los protocolos del SIAU, los que disponen que tal solicitud debe ser derivada al fiscal de la causa para su evaluación y que ésta, una vez resuelta, se debe comunicar al usuario, todo ello en un plazo máximo de 10 días hábiles desde el ingreso de la solicitud. Teniendo en consideración que la modificación normativa impone un plazo de respuesta a esta solicitud específica en 10 días, sin referencia a días hábiles, corresponde computar el nuevo plazo legal de 10 días como días corridos.

Para el año en curso, los Indicadores de porcentaje de solicitudes ingresadas en los espacios de atención presencial y virtual del SIAU, que requieren evaluación interna, respondidas al usuario dentro del plazo establecido desde su fecha de ingreso, se encuentran definidos de la siguiente manera: "*El plazo para dar respuesta a las solicitudes de diligencias de investigación se extenderá hasta los 10 días hábiles siguientes a la fecha de su ingreso.*"

Al respecto, se ha estimado que procede modificar la metodología de cálculo de este indicador a fin de que sea ajustado conforme al estándar que fija la nueva ley desde el 05 de julio del año 2016, fecha en la cual entró en vigencia, por lo que su cálculo se realizará contabilizando los días corridos. Por ello, teniendo presente lo señalado respecto a la naturaleza de compromiso CGI de este indicador, se ha estimado conveniente modificarlo a fin de fijar en 9 DÍAS CORRIDOS EL CÁLCULO DEL PLAZO PARA DAR RESPUESTA A LAS SOLICITUDES DE DILIGENCIAS DE INVESTIGACIÓN, conforme a la regulación de la ley.

Atendido lo expuesto, la Instancia Técnica ha estimado necesario efectuar una modificación a lo señalado en el Convenio de Desempeño Institucional para el año 2016, con vigencia a contar del 1º de enero de 2016, en el sentido de:

- 1) Sustituir la referencia a la versión año 2009 de la norma ISO 27.001 por una referencia a la versión 2013, con el fin de obtener un Diagnóstico de la Seguridad de la Información en el Ministerio Público lo más acorde a los actuales estándares existentes en la materia;
- 2) Ajustar el periodo de vigencia del nuevo Plan Estratégico hasta el año 2022, en atención a lo señalado en el inciso tercero del artículo 85 de la Constitución Política de la República de Chile, y;
- 3) Modificar las notas técnicas 1 y 2, establecidas en el Anexo N°2 dada la entrada en vigencia de la Ley N° 20.931.

A continuación se describe el detalle de las modificaciones propuestas:

**I.- Respecto a sustituir la referencia a la versión año 2009 de la norma ISO 27.001 por una referencia a la versión 2013.**

**Sistema de Seguridad de la Información.**

- a. La Etapa 1 del Sistema de Seguridad de la Información de la página 5, se sustituye por la siguiente:

1. La Institución realiza un diagnóstico de la situación de seguridad de la Información Institucional, e identifica en éste los activos de Información que dan sustento a una selección de sus procesos de provisión, estableciendo los controles necesarios para mitigar riesgos que puedan afectar a los activos de Información críticos, considerando para esto todos aquellos dominios de seguridad de la Información que establece el DS 83 y la NCh-ISO 27001 versión 2013, determinando el nivel en que la institución se encuentra respecto de: Políticas de Seguridad, Seguridad Organizacional, Clasificación, Control y Etiquetado de Bienes, Seguridad Física y del Ambiente, Seguridad del Personal, Gestión de la Operaciones y de las Comunicaciones, Control de Acceso, Desarrollo y Mantenimiento de Sistemas, Gestión de Incidentes en la Seguridad de la Información, Gestión de la Continuidad del Negocio y Cumplimiento.

2. La institución compara los resultados del Diagnóstico con los controles establecidos en los dominios de seguridad del DS 83 y la NCh-ISO 27001 versión 2013, y determina las brechas que deberán ser abordadas y cerradas a través de la Implementación de un Plan de Seguridad de la Información Institucional.

**ETAPA COMPROMETIDA AÑO 2016**

- b. El punto 2 de la Etapa 2 del Sistema de Seguridad de la Información de la página 5, se sustituye por la siguiente:

2. La Institución, en el marco de la Política de Seguridad de la Información establecida, elabora un Plan General de Seguridad de la Información Institucional, para el año en curso y siguientes, de acuerdo a los resultados del diagnóstico y las brechas detectadas, que comprenda, al menos, la coordinación de todas las unidades de la institución vinculadas a los aspectos de seguridad de la información, a través del nombramiento de responsables de la implementación del Plan, y el establecimiento de los controles para cumplir los requisitos del DS 83 y la NCh-ISO 27001 versión 2013.

- c. El punto 1 de la Etapa 4 del Sistema de Seguridad de la Información de la página 5, se sustituye por el siguiente:

1. La Institución evalúa y difunde los resultados de la Implementación del Plan General de Seguridad de la Información Institucional y el Programa de Trabajo Anual, considerando el porcentaje de cumplimiento en los dominios de seguridad del DS 83 y la NCh-ISO 27001 versión vigente 2013, respecto de las brechas detectadas en el diagnóstico, y formula recomendaciones de mejora.

- d. La Etapa 1 del Sistema de Seguridad de la Información de la página 15, se sustituye por la siguiente:

1. La Institución realiza un diagnóstico de la situación de seguridad de la Información institucional, e identifica en éste los activos de Información que dan sustento a una selección de sus procesos de provisión, estableciendo los controles necesarios para mitigar riesgos que puedan afectar a los activos de Información críticos, considerando para esto, todos aquellos dominios de seguridad de la Información que establece el DS 83 y la NCh-ISO 27001 versión 2013, determinando el nivel en que la institución se encuentra respecto de: 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, Gestión de Incidentes en la Seguridad de la Información, Gestión de la Continuidad del Negocio y Cumplimiento.

2. La Institución compara los resultados del Diagnóstico con los controles establecidos en los dominios de seguridad del DS 83 y la NCh-ISO 27001 versión 2013, y determina las brechas que deberán ser abordadas y cerradas a través de la implementación de un Plan de Seguridad de la Información Institucional.

- e. Requisito Técnico 2 del Sistema de Seguridad de la Información de la página 15, se sustituye por lo siguiente:

2. Para aquellos activos de información con criticidad media y alta, el Ministerio Público:

a. Identifica los controles (requisitos normativos Norma ISO NCh-ISO 27001 versión 2013 y del DS 83 o buenas prácticas) ya cumplidos (o

abordados) por dominio de seguridad de la Información<sup>1</sup>, para mitigar riesgos.

b. Identifica los controles o requisitos normativos de los dominios de seguridad, que falta implementar para mitigar los riesgos.

## **II.- Respecto al ajuste del periodo de vigencia del nuevo Plan Estratégico hasta el año 2022.**

### **Sistema de Planificación y Control de Gestión:**

a. El punto 2 de la Etapa 4 del Sistema de Planificación y Control de Gestión de la página 6, se sustituye por el siguiente:

2. Establecer las principales directrices institucionales que permitan direccionar la gestión del Ministerio Público, elaborando para ello su Plan Estratégico para el período 2016-2022.

b. El punto 2 de la Etapa 4 del Sistema de Planificación y Control de Gestión de la página 16, se sustituye por el siguiente:

2. Establecer las principales directrices institucionales que permitan direccionar la gestión del Ministerio Público, elaborando para ello su Plan Estratégico para el período 2016-2022.

c. El Requisito Técnico (RT) 3 de la página 16, se cambia por el siguiente:

3. El Ministerio Público establece sus principales definiciones estratégicas y las principales líneas de acción a desarrollar para el período 2016-2022, para lo cual elabora su Plan Estratégico el cual contendrá al menos la visión, misión, objetivos estratégicos y líneas de acción que permitan direccionar la gestión institucional.

d. El Medio de Verificación 3 de la página 16 se cambia por el siguiente:

3. Plan Estratégico del Ministerio Público para el periodo 2016-2022. (RT 3).

---

<sup>1</sup> Los dominios de seguridad de la Información son 11: 1) Política de Seguridad (declaración general de voluntad por parte del Jefe de Servicio); 2) Seguridad Organizacional (formalización de estructura y responsabilidades, ejemplo: Encargado y Comité de seguridad de la Información), Gestión de activos de Información (procedimientos de manejo de la Información de acuerdo a su clasificación), Seguridad Física y del Ambiente (medidas y procedimientos de acceso físico, protecciones en cuanto a temperatura, luz u otras variables ambientales), Seguridad del Personal (procedimientos de gestión de RRHH que incorporen medidas de protección para los conocimientos que tienen las personas, en la contratación, capacitación, etc.), Gestión de la Operaciones y de las Comunicaciones (procedimientos asociados a la gestión de antivirus, correo electrónico y respaldo, fundamentalmente), Control de Acceso (procedimientos de manejo de contraseñas para los sistemas, redes, etc.), Desarrollo y Mantenimiento de Sistemas (procedimientos para la creación de software, su actualización o la contratación de estos servicios a terceros), Gestión de Incidentes en la Seguridad de la Información (procedimientos de manejo de eventos que afectan la seguridad de la Información, su registro y análisis posterior), Gestión de la Continuidad del Negocio (planes para proveer estabilidad a los procesos críticos) y Cumplimiento (chequeo de que las medidas adoptadas satisfacen las leyes y normativas vigentes).

**III. Respecto a la modificación de las notas técnicas 1 y 2, establecidas en el Anexo N°2 dada la entrada en vigencia de la Ley N° 20.931.**

**Sistema de Planificación y Control de Gestión:**

Anexo 2, Notas Técnicas N° 1 y 2 en la página 8, la viñeta 4 de ambas notas se cambia por la siguiente:

- El plazo para dar respuesta a las solicitudes que requieren de evaluación Interna es hasta los cinco días hábiles siguientes a la fecha de ingreso. En tanto, para las siguientes solicitudes los plazos se extienden a:
  - **Solicitud de diligencias de investigación:** hasta los 9 días corridos siguientes a la fecha de su Ingreso. La medición de este plazo se realizará sólo a contar del 05 de julio del año 2016.
  - **Solicitud de devolución de especies/dinero:** hasta los 10 días hábiles siguientes a la fecha de su Ingreso.
  - **Solicitud de reapertura de una causa con nuevos antecedentes:** hasta los 10 días hábiles siguientes a la fecha de su Ingreso.

Coincidiendo en la conveniencia de efectuar las modificaciones precedentes, el Sr. Fiscal Nacional del Ministerio Público y el Sr. Ministro de Hacienda, vienen en suscribir el presente documento, con el fin de formalizar las precisiones referidas, entendiéndolas incorporadas legalmente como parte integrante del Convenio de Desempeño Institucional suscrito el 31 de diciembre del 2015.

  
**RODRIGO VALDÉS PULIDO**  
**MINISTRO DE HACIENDA**

  
  
**JORGE ABBOTT CHARME**  
**FISCAL NACIONAL**  
**MINISTERIO PÚBLICO**





ASESORIA JURÍDICA  
MBV/BPR  
E6747/2016



ORD. N° 2 8 3 3 /

ANT.: Oficio DEN N° 257/2016, de la Directora Ejecutiva Nacional del Ministerio Público.

MAT.: Da respuesta que indica.

2865

SANTIAGO, 12 DIC 2016

DE : **JORGE VALVERDE CARBONELL**  
**JEFE DE GABINETE SUBSECRETARIO DE HACIENDA**

A : **FRANCISCA WERTH WAINER**  
**DIRECTORA EJECUTIVA NACIONAL MINISTERIO PÚBLICO**

Se ha recibido en esta Secretaría de Estado el Oficio señalado en ANT. de la Directora Ejecutiva Nacional del Ministerio Público, en el que se consulta la pertinencia de firmar una nueva modificación del Convenio de Desempeño Institucional de 2016, del Ministerio Público.

En relación a su consulta, cúpleme en señalar que analizado los antecedentes a los que hace mención en su presentación, esta Subsecretaría es de la opinión que no resulta necesario realizar una nueva modificación del Convenio referido, toda vez que el mismo ya fue modificado con fecha 15 de julio de 2016.

Saluda atentamente a Ud.,

  
★ REPUBLICA DE CHILE ★  
JEFE DE GABINETE **JORGE VALVERDE CARBONELL**  
Subsecretario de Hacienda  
SUBSECRETARIA DE HACIENDA



**Distribución:**  
Destinataria  
Patricio Leiva I.  
Archivo.



**OFICIO DEN N° 257/2016**

M.HACIENDA OF PARTES  
14.11.2016 10:32

**ANT: No Hay.**

**MAT.: Remite consulta e información referente al CGI Sistema de Seguridad de la Información 2016.**

**ADJ.: Convenio de Desempeño Institucional 2016, Ministerio Público.**

**Oficio FN N° 432/2016 Modificación Convenio de Desempeño Institucional 2016.**

**Metodología Diagnóstico empresa INGENIA GLOBAL LTDA.**

**Santiago, 03 de noviembre de 2016**

**DE : FRANCISCA WERTH WAINER  
DIRECTORA EJECUTIVA NACIONAL  
MINISTERIO PÚBLICO**

**A : PATRICIO LEIVA IRIGOYEN  
DIRECTOR DE COORDINACIÓN DE SERVICIOS  
SUBSECRETARÍA DE HACIENDA  
REPRESENTANTE INSTANCIA TÉCNICA MINISTERIO DE HACIENDA**

Junto con saludarlo, a través del presente oficio y en el contexto de los Compromisos de Gestión Institucional 2016, remito a usted, en su calidad de representante de la Instancia Técnica del Ministerio de Hacienda, consulta e información respecto al Sistema de Seguridad de la Información:

1. Como es de su conocimiento, el Convenio de Desempeño Institucional del Ministerio Público, fue firmado el 31 de Diciembre de 2015, entre el Ministro de Hacienda y el Fiscal Nacional. Particularmente, en lo que se refiere al Sistema de Seguridad de la Información, se estableció que la Etapa 1 de Diagnóstico se debía ejecutar tomando como Modelo de Referencia la Norma ISO NCh-ISO 27001, en su versión 2009. Esta norma establece 11 Dominios en la Seguridad de Información.

Luego, con fecha 15 de julio de 2016, el Convenio de Desempeño Institucional fue modificado por las mismas autoridades. En particular para el Sistema de Seguridad de la Información (SSI), se formalizó que la Etapa 1 de Diagnóstico se debía ejecutar tomando como Modelo de Referencia la Norma ISO NCh-ISO 27001, en su versión 2013, la cual se encuentra vigente. Esta norma establece 14 Dominios en la Seguridad de Información.

Sin embargo, la modificación del Convenio, omitió reemplazar los 11 Dominios de Seguridad de la Información, definidos por la Norma ISO NCh-ISO 27001/2009, por los 14 Dominios de Seguridad de la Información establecidos por la Norma ISO

**06747/2016**

NCh-ISO 27001/2013; tanto en el objetivo de la Etapa 1 (contenido en la página 5 del cuerpo del Convenio firmado originalmente), y en el objetivo de la Etapa 1 y pie de página del CGI SSI (contenido en la página 15, Anexo N° 1 del Convenio firmado originalmente).

Dado lo anterior, amerita consultar, la pertinencia de firmar una nueva modificación del Convenio de Desempeño Institucional del año 2016, para evitar eventuales complicaciones en la revisión del cumplimiento del CGI SSI 2016 por parte del auditor externo.

2. Es necesario señalar, que para la Etapa 1 de Diagnóstico del CGI SSI, en el Anexo N° 1 del Convenio en su página 15, se señala textualmente: *"Fuente referencial: Requisitos Técnicos y Medios de Verificación. Programa de Mejoramiento de la Gestión años 2012, 2013 y 2014"*.

Adicionalmente, y dada la necesidad de contar con apoyo externo técnico especializado para la ejecución del CGI SSI 2016, el Ministerio Público licitó la ejecución de la mencionada Etapa de Diagnóstico, el cual fue adjudicado a la empresa INGENIA GLOBAL LTDA., la cual cuenta con una vasta experiencia en el análisis e implantación de Sistemas de Seguridad de la Información, tanto en el ámbito público como en el privado. Esta empresa aplica en el diagnóstico de Sistema de Seguridad de Información una metodología distinta, pero mejorada en relación a las herramientas del PMG SSI 2014, la cual (es decir, la mencionada metodología de la empresa Ingenia Global Ltda), en general, consiste en:

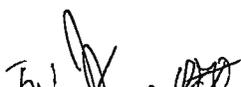
- Disponer de un Inventario de activos de información, detallado y actualizado,
- Conocer las dependencias entre los diferentes activos de información,
- Determinar el nivel de criticidad de los activos en función de sus aspectos de Confidencialidad, Integridad y Disponibilidad,
- Determinar el grado de cumplimiento de la Institución respecto a los controles del Anexo A de la Norma NCh-ISO 27001:2013 (y buenas prácticas NCh-ISO 27002:2013),
- Determinar la Declaración de Aplicabilidad (SoA) en función de los controles aplicables,
- Determinar los Riesgos sobre los activos de información, en base a la metodología MAGERIT, reconocida y utilizada internacionalmente,
- Mediante la herramienta computacional PILAR, realizar un Análisis de Riesgos y evaluar el cumplimiento normativo sistemático, disponiendo de diferentes reportes y gráficos, permitiendo obtener la información en diferentes formatos (html, cvs, xml, db) para su posterior explotación de forma más amplia,
- Obtener un alineamiento con la matriz de instrumentos del PMG 2014, al incluir la información que en ella se indica, siendo más manejable el formato de representación, mantención y explotación, y
- Conocer el grado de madurez y de apego de la Institución a las Normas de Seguridad de la Información y, por consiguiente, priorizar los esfuerzos para aplicar las salvaguardas sobre los activos más críticos y cuyo nivel de riesgo requiere una mejoría.

Dado lo anteriormente descrito, informamos a Uds., que se aplicará la Metodología propuesta por el consultor especialista; ya que, permite a nuestra Institución, cumplir con los instrumentos del PMG SSI 2014 (establecidos como referencia en el CGI SSI 2016), además de obtener conclusiones, productos y herramientas que permitan al Ministerio Público gestionar de mejor forma el diseño y la implementación del Sistema de Seguridad de Información. Entre las más relevantes se pueden mencionar la utilización de la Metodología MAGERIT, la herramienta computacional de análisis de riesgo PILAR, contar como producto entregable con una Base de Datos que contiene los activos de información, los parámetros de evaluación y los escenarios de riesgo cuantificados, simular en función de los distintos planes de seguridad propuestos los riesgos residuales asociados.

Se adjunta como Anexo al presente Oficio, una Descripción detallada de la Metodología, que la empresa INGENIA GLOBAL LTDA. a esta fecha ya se está ejecutando al interior de nuestra Institución.

Saluda atentamente a UD.,

MINISTERIO PÚBLICO  
DIRECTORA  
EJECUTIVA  
NACIONAL  
FRANCISCA WERTH WAINER  
DIRECTORA EJECUTIVA NACIONAL



FWM/MHS/VBC/OZD/amp  
c.c: - Sra. Luna Israel – Jefa del Departamento de Control de Gestión Pública – DIPRES  
- Archivo