Defensoría
Sin defensa no hay Justicia

MANUAL DE PROCEDIMIENTOS TECNOLÓGICOS

DEFENSORÍA PENAL PÚBLICA

DEPARTAMENTO DE INFORMÁTICA Y ESTADÍSTICA

Versión 2.0

Septiembre de 2015

Elaborado por:	Revisado por:	Aprobado por:
Jefe Departamento de Informática y Estadísticas	Director Administrativo Nacional	Defensor Nacional
Fecha: 03/09/2015		

Defensoría
Sin defensa no hay Justicia

CONTROL DE CAMBIOS

Fecha	Versión	Ámbitos	Cambio
Agosto 2013	1.0	Aprobación del Manual, mediante Res. N° 439/2013	
Agosto 2015	2.0	Cambios Generales	Reordenamiento de contenidos. Correcciones de redacción y mejoramiento de formatos. Actualización de versiones de productos de software.
		Comité Tecnológico	Se actualiza composición y ámbitos a abordar.
		Políticas	Se incluyen Políticas sobre *Entrega de Información* y *Uso de Carpetas Compartidas*. Se actualiza Política de *Creación de Casillas de Correo Electrónico*.
		Procedimientos	Se actualizan Procedimientos de *Servicios Informáticos*, de *Sistemas de Información*, de *Contrataciones* y de *Seguridad de la Información*.

Defensoría
Sin defensa no hay Justicia

Contenido

I. Antecedentes

La Defensoría Penal Pública a contar del año 2009 ha procedido a definir un conjunto de Políticas, Procedimientos y Protocolos tendientes a establecer criterios y formas de proceder respecto a diferentes situaciones que se producen, producto del uso de servicios y sistemas informáticos. En los últimos 2 años, además se han introducido un conjunto de definiciones, estructuras y controles, a partir del uso y aplicación de la Norma ISO 27.001:2013, relacionada con la Seguridad de la Información.

Finalmente y producto de la Auditoría Interna efectuada en Diciembre de 2012, se determinó que existe la necesidad y conveniencia de hacer un ordenamiento de esta información, actualizarla, concentrarla y aplicar una estructura única de presentación. Por otra parte surge la necesidad de explicitar procedimientos relacionados con el acceso de usuarios a los servicios y sistemas informáticos que provee la Defensoría.

En consecuencia, el Departamento de Informática y Estadística de la Defensoría Nacional, en adelante DIE, efectuó una compilación y actualización de la Política Informática y de Seguridad de la Información y, en orden a sistematizar las tareas, se ha efectuado una revisión de los procedimientos y protocolos vigentes y los presenta a través de este manual.

Esta versión surge tras el levantamiento efectuado por el DIE y que fue sometida a consideración del Comité Tecnológico y aprobado por éste en sus reuniones de Abril y Mayo del año 2015.

II. Objetivos

1. General

Fijar principios orientadores, políticas y procedimientos que regulen el funcionamiento y uso de la tecnología en la Defensoría Penal Pública.

2. Específicos

- Consolidar los procedimientos necesarios para efectuar una adecuada prestación de los servicios tecnológicos y sistemas informáticos.
- Facilitar el control del cumplimiento de las actividades asociadas al uso de la tecnología a cargo del Departamento de Informática y Estadística y Encargados de Informática Regionales.
- Disponer de Políticas y Procedimientos para la Seguridad de la Información.
- Establecer ámbitos y focos para las actividades de Auditoría Tecnológica.
- Establecer los procedimientos que regirán el trabajo de los funcionarios del DIE y los Encargados de Informática Regionales.
- Disponer de Políticas y Procedimientos para el uso de los servicios tecnológicos y sistemas informáticos por parte de los funcionarios y usuarios de la Defensoría.

III. Alcance

Este manual está orientado a todos los usuarios de la Defensoría Penal Pública, y a aquellos que por razón de la prestación de sus servicios, requieran hacer uso de los servicios tecnológicos y sistemas informáticos de la Defensoría y de forma específica al personal que cumple funciones dentro del DIE y los Encargados de Informática Regionales.

Las áreas de aplicación son las de asignación y uso de los servicios tecnológicos y sistemas informáticos, desarrollo y mantención de sistemas de información, contrataciones, acceso a internet, seguridad de la información y cumplimiento, actualización y auditorías, y los procesos relacionados con el cumplimiento de las leyes y regulaciones aplicables a la Defensoría.

IV. Vigencia

Este documento entrará en vigencia a contar de la fecha de la Resolución Exenta que lo aprueba y deberá ser revisado al menos una vez al año.

V. Principios Orientadores

La prestación de los servicios informáticos se sustenta en los siguientes principios orientadores:

- **Universalidad**: Todo funcionario de la Defensoría ya sea en su calidad de planta, contrata u honorarios dispondrá de una estación de trabajo y acceso a los servicios tecnológicos y sistemas informáticos que apoyen las actividades que le corresponde efectuar, de acuerdo, al cargo que desempeña.

- **Facilidad de Uso**: El uso de los sistemas informáticos deberán ser de carácter intuitivo para los usuarios. Para ello, se utilizará en su prestación, tecnología de uso masivo y que se encuentre ya probada en el país.

- **Accesibilidad**: Los sistemas informáticos deben estar disponibles para el usuario desde cualquier lugar con acceso a Internet, con la sola excepción de aquéllos que la Institución haya decidido no publicar.

- **Alta Disponibilidad**: El funcionamiento de los sistemas informáticos de la Defensoría, será bajo una modalidad de alta disponibilidad y en un horario (7 x 24 x 365), 7 días por 24 horas los 365 días del año.

- **Seguridad**: La información, servicios tecnológicos y sistemas informáticos que se provean considerarán administrar los riesgos de seguridad asociados, buscando impedir que sean accedidos o alterados por personas no autorizadas.

- **Confidencialidad**: La información y los datos personales de los usuarios de los sistemas informáticos de la Defensoría serán de carácter reservado.

- **Externalización**: Los servicios informáticos que requiera la Defensoría serán contratados, mediante los procesos de compras públicas que establece la normativa vigente, con empresas especializadas, quienes los proveerán en la modalidad que corresponda dependiendo de las necesidades de la Institución.

VI. Roles y Responsabilidades

Para el presente Manual de Procedimientos se consideran los siguientes roles y las siguientes responsabilidades asociadas:

a. **Alta Dirección:** Aprobar las políticas institucionales, evidenciar su compromiso con el cumplimiento de las mismas y asegurar la disponibilidad de recursos para su implementación y mejoras.

b. **Comité Tecnológico:** Asegurar la protección, conservación, retención y disposición de los registros de seguridad de la información. Mantener actualizado el inventario de activos de la institución e implementar controles a los riesgos asociados a los activos de la Institución. Proponer actividades que aseguren niveles de seguridad adecuados a los procesos de la Defensoría y a las tareas que ejecutan los usuarios.

c. **Departamento de Informática y Estadística:** Asegurar el adecuado funcionamiento de los servicios informáticos de la Defensoría Penal Pública, a través de la aprobación, aplicación y seguimiento de procedimientos y controles adecuados, para evitar su uso indebido o con propósitos no autorizados. Establecer los controles de seguridad necesarios en cada caso y asegurar el uso de controles criptográficos en los casos pertinentes.

d. **Defensores Regionales, Directivos de Departamentos y Unidades de la Defensoría Penal Pública y Jefes de Estudio Regionales:** Velar y supervisar el cumplimiento de lo establecido en las políticas tecnológicas y de los requisitos establecidos por las leyes, regulaciones y reglamentos aplicables. Proponer mejoras, actualizaciones y automatización de los procesos que les atañen.

e. **Directores Administrativos Regionales:** Velar y supervisar el cumplimiento de lo establecido en las políticas tecnológicas y de los requisitos establecidos por las leyes, regulaciones y reglamentos aplicables. Controlar la creación o eliminación de usuarios internos y externos de la Región. Supervisar el cumplimiento de las obligaciones de los Encargados Informáticos Regionales. Administrar y verificar el correcto funcionamiento del equipamiento de uso general instalado en la Región.

f. **Encargados de Informática Regionales:** Asegurar el adecuado funcionamiento de los servicios informáticos en las dependencias de las Defensorías en cada Región. Brindar el soporte de primer nivel a los usuarios internos de la Región. Dar cumplimiento a lo establecido en los procedimientos tecnológicos.

g. **Unidad de Asesoría Jurídica:** Velar por la correcta aplicación e interpretación de las normas jurídicas vigentes en lo concerniente al derecho administrativo y ejercer un oportuno control de legalidad de los actos administrativos emanados de la Defensoría y también de aquéllos que dicen relación con las actividades asociadas al uso de la tecnología a cargo del DIE.

h. **Unidad de Auditoría Interna:** Velar por el cumplimiento de los procedimientos descritos en este manual, específicamente en lo concerniente al proceso de auditorías tecnológicas y promover actualizaciones y mejoras.

i. **Funcionarios de la Defensoría Penal Pública:** Cumplir con lo establecido en las políticas tecnológicas y asegurar que sus actividades den cumplimiento de lo establecido en las leyes, regulaciones y reglamentos aplicables, así como en los controles de seguridad establecidos. Para los fines del presente Manual, los funcionarios de la Defensoría Penal Pública son todas aquellas personas que mantienen una relación de contrata, planta u honorarios con la Defensoría y ejecutan sus labores en las dependencias de ésta.

j. **Usuarios de Servicios Tecnológicos y Sistemas Informáticos:** Corresponden a todos aquellos que hacen uso total o parcial de los servicios tecnológicos y sistemas informáticos que dispone la Defensoría Penal Pública. Existirán 2 tipos de usuarios; *Internos* correspondiente a todos aquéllos que acceden a los sistemas y servicios en las dependencias físicas de la Defensoría Penal Pública, entre estos se consideran a los funcionarios de la Defensoría, al personal de proveedores externos (guardias, técnicos residentes) y estudiantes en práctica, *y Externos* correspondientes a todos aquéllos que acceden a los sistemas desde fuera de las dependencias de la Defensoría Penal Pública, entre estos se consideran administradores de contratos de servicio, defensores licitados, asistentes licitados, profesionales de instituciones con las cuales la Defensoría ha suscrito convenio para compartir información.

   Todos los usuarios deberán cumplir con lo establecido en las políticas tecnológicas y asegurar que sus actividades den cumplimiento a lo establecido en las leyes, regulaciones y reglamentos aplicables, así como en los controles de seguridad establecidos.

VII. Políticas Tecnológicas

1. Políticas de Asignación de Servicios Informáticos

a. Derechos de los Usuarios

- Utilizar los servicios y sistemas informáticos que disponga la Defensoría y sean de su competencia, conforme el rol que cumplen en la Defensoría.
- Disponer del espacio de almacenamiento necesario en su estación de trabajo, que le permitan guardar y mantener sus documentos y correos, al menos durante un año calendario.
- Ser capacitado en el uso de los Servicios y Sistemas Informáticos requeridos para el rol que cumple y en los mecanismos de respaldo.
- Requerir soporte, ayuda o capacitación frente a problemas técnicos.
- Estar informado acerca de los cambios en nuevas versiones licenciadas y de los sistemas informáticos que disponga la Defensoría y sobre las ventajas y desventajas que estas presenten.
- Contar con continuidad y estabilidad en los servicios y sistemas informáticos y que se asegure la confiabilidad, integridad y disponibilidad de sus archivos y correos.
- Poder revisar y enviar correos electrónicos y acceder a los sistemas informáticos.
- Que se respondan sus consultas o requerimientos.
- Conocer y disponer del nombre de todas las cuentas de correo de la institución y que la suya esté publicada entre ellos.
- Exigir privacidad en sus mensajes.
- Expresar su conformidad o insatisfacción con los servicios tecnológicos y sistemas informáticos y presentar propuestas de mejora a ser evaluadas por el DIE.
- Solicitar capacitación, instrucciones, manuales o ayuda, sobre los sistemas o servicios que deba utilizar.

b. Deberes de los Usuarios

- Informarse y dar cumplimiento a las políticas y procedimientos tecnológicos definidos por la Institución.
- Utilizar los servicios tecnológicos y sistemas informáticos para los fines propios del trabajo que efectúa en la Defensoría y mantener actualizada la información de los sistemas de manera oportuna y fidedigna.
- Efectuar el respaldo de la información del equipo computacional estacionario y/o portátil que le haya sido asignado.
- Mantener limpio y en óptimas condiciones el equipamiento asignado y su cuenta de correo electrónico.
- Usar el correo electrónico institucional para fines propios de las funciones que efectúa en la Defensoría y no para usos privados (bancos, casas comerciales, suscripciones, etc.)
- Leer los correos que son enviados y efectivamente recibidos en su casilla electrónica.
- Respaldar sus correos y documentos para mantenerlos al menos por un año calendario.
- Mantener informados a los demás usuarios y personas que le envíen correos electrónicos a su casilla de los cambios en su cuenta de correo, horarios de atención, vacaciones o ausentismo prolongado, dejando mensajes de aviso indicando los datos de la persona que lo suplirá, indicando el nombre, teléfono y casilla de correo electrónico a la que pueden dirigirse.
- Evitar riesgos de contaminación y propagación de virus.
- Avisar de todo mensaje sospechoso y solicitar ayuda o soporte para su tratamiento.

c. Prohibiciones para los Usuarios

- Utilizar los sistemas y servicios informáticos que les hayan sido asignados para cualquier propósito ajeno a los fines institucionales o las funciones que ejerce.
- Extraer y compartir todo tipo de información de carácter institucional ya sea en forma total o parcial, con personas o entidades externas, y sin autorización previa.
- Utilizar las cuentas de otros usuarios.
- Compartir con otras personas sus claves personales de los servicios tecnológicos y sistemas informáticos.
- Instalar software no autorizado.
- Participar en la propagación de correos electrónicos encadenados o similares dentro y fuera de la Defensoría.
- Acceder a sitios web o distribuir correos con contenidos impropios y/o lesivos, o representen cadenas, o actividades de activismo digital o político; para participar, organizar, inducir y promover prácticas de intolerancia religiosa o racial o que generen conflictos que puedan producir daños a terceros.
- Inscribir sus casillas de correo en sitios Web de juego, sexo, pornografía de todo tipo, comercio por Internet, sitios promocionales, listas de distribución, foros, notificación periódica, política, entre otros, que no guarden directa relación con los productos estratégicos definidos por la institución o vinculados a sus fines; a menos que sea expresamente autorizado por la jefatura respectiva y quede constancia escrita de ello.
- Enviar mensajes electrónicos a "todos los usuarios" de la institución o envíos masivos parciales con motivos promocionales, campañas u otro tipo de motivo, sin la previa autorización del Defensor Nacional o el/la Directora(a) Administrativo(a) Nacional. Las casillas autorizadas para el envío de correos masivos serán las que el Defensor Nacional establezca.
- Acceder a servicios chat o sitios que ofrecen servicios de intercambio en línea de música, videos, redes sociales y otros archivos.

d. Recomendaciones a los Usuarios

- Modificar periódicamente su contraseña para acceder a los servicios y sistemas informáticos.
- Eliminar los correos tipo cadena, ya que generalmente adjuntan archivos de gran tamaño, que afectan el espacio disponible en la casilla.
- Disminuir los archivos adjuntos utilizando el software de compresión de archivos instalados en todos los equipos.
- Rechazar archivos adjuntos provenientes de remitentes desconocidos o que contengan un asunto u origen no confiable, en especial si el origen es de fuera de la Defensoría.
- Eliminar sin ser leídos los mensajes marcados como SPAM.
- Evitar adjuntar imágenes o información innecesaria en su pie de firma de correo.
- En caso de recibir promociones indeseables de distribución masiva, se recomienda no responder o solicitar su eliminación de la lista de distribución, porque ello sólo sirve a la empresa de promoción para confirmar que su casilla es una casilla válida y le permitirá confirmarlos en las listas de distribución. En estos casos deberán eliminar los mensajes recibidos y clasificar al remitente como "Correo No Deseado" para que no vuelva a aparecer en la casilla de recepción principal.
- Todos los accesos vía Web a servicios públicos o privados, y otros, con la finalidad de obtener información, realizar pagos, u otras actividades, utilizando infraestructura de la Defensoría, se sugiere realizarlos fuera del horario de trabajo.

2. Política de Uso de Servicios Informáticos

a. Política de Uso de Computadores

Los usuarios que tengan a su cargo un computador o notebook serán responsables, de su adecuado uso, mantenimiento y custodia. En relación a la información en dichos equipos deberán evitar dejar documentos y/o archivos en el escritorio o en pantalla de los computadores y toda información contenida en equipos pertenecientes a la institución podrá ser administrada y monitoreada por el DIE, con excepción, de las definidas por el/la Directora(a) Administrativo Nacional.

El respaldo de información de computadores de escritorio y portátiles deberá realizarse por lo menos cada 6 meses y será de responsabilidad del usuario que tenga a cargo el equipo.

b. Política de Uso de Telefonía y Telefonía Móvil

El usuario interno será el responsable del adecuado uso, mantenimiento y custodia de los equipos de telefonía, y deberá informar sobre daños, robos o cualquier situación que vulnere las *Políticas de Seguridad de la Información*. La administración de los equipos de telefonía y su asignación será regulada a través de un medio formal y estará a cargo del DIE.

c. Política de Uso del Equipamiento en General

La Defensoría asignará equipamiento a la Defensorías Regional, Defensorías Locales y Departamentos y Unidades de la Defensoría Nacional, de acuerdo a sus necesidades para el desempeño de sus funciones (equipos de videoconferencia, impresoras, relojes biométricos, UPS, WIFI, proyectores, telefonía), conforme los criterios establecidos en la Política de Clasificación de Oficinas.

Cada Defensoría Regional, Local, Departamento y Unidad de la Defensoría Nacional será responsable por los equipos asignados, en cuanto a su uso, mantenimiento y custodia. Además deberá adoptar las medidas que sean necesarias para resguardarlos y mantenerlos en las mejores condiciones, debiendo reportar las pérdidas que se produzcan y cualquier tipo de daño o fallas que los afecten a los Encargados de Informática Regionales o funcionarios del DIE según corresponda, quienes señalarán las acciones a seguir en cada caso. La entrega y uso de los equipos se encuentran sujetos a las normas sobre responsabilidad administrativa en el sector público, sin perjuicio de la responsabilidad civil y penal contenidas en nuestro ordenamiento jurídico.

d. Política de Uso de Correo Electrónico

La Defensoría adopta como herramienta base de sus comunicaciones internas el correo electrónico, de modo que tiene la misma validez que un oficio o memorándum. De esta forma, los usuarios, tendrán derecho a disponer de una casilla de correo electrónico para el intercambio de información y lo harán mediante las herramientas provistas formalmente por el DIE. De este modo, se garantiza

la seguridad y confiabilidad de la información. Las herramientas de intercambio de ella deberán estar protegidas con firma electrónica simple, es decir, nombre de usuario y contraseña.

e. Política de Uso de Licencias de Software

Todo software que se requiera para apoyar las funciones, actividades y tareas de los usuarios de la Defensoría Penal Pública será provisto mediante el proceso respectivo, a través del área de Adquisiciones del Departamento de Administración y Finanzas de la Defensoría Nacional, previa autorización del DIE. Los productos contratados deberán contar con su respectiva licencia de uso, el material bibliográfico necesario para comprender el proceso de instalación y el manual de usuario que permita entender su uso y aplicabilidad. Dependiendo de la complejidad del producto adquirido, se deberá también solicitar servicios de instalación y capacitación; y deberá incluir los servicios de respaldo técnico que se requieran para asegurar su continuidad operativa y su funcionalidad.

El software necesario para el funcionamiento de los servicios críticos de la Defensoría deberá tener su licenciamiento respectivo donde la Institución será la propietaria de dichas licencias, además estos servicios deberán disponer de contratos de soporte y actualización.

Se dispondrán de los siguientes tipos de licencias en función de su naturaleza:

Servidor de Aplicaciones	WebLogic
Base de datos	Oracle 11g
Correo electrónico	MS Exchange 2010 SP3 MS Office 365 E3
Productividad	MS Office Profesional Plus 2013
Antivirus	McAfee
Virtualización	WMware Sphere V.5.1
Sistema Operativo	Windows 2008 o Centos 6.0

La instalación de cualquier programa deberá ser efectuado sólo por personal del DIE o los Encargados de Informática Regionales. No obstante ello, las estaciones de trabajo dispondrán del siguiente conjunto de aplicaciones que abarcan las necesidades básicas para la realización de las actividades de todos los funcionarios.

Estaciones de Trabajo

Sistema Operativo	Windows 7 Profesional SP1
Herramienta de Productividad	Microsoft Office Pro Plus 2013 SP1 (incluye: Word, Excel, PowerPoint y Outlook)
Lector de documentos PDF	Adobe Reader XI
Compresor de archivos	7-Zip 9.38

Antivirus	Agente McAfee
Navegador	Internet Explorer versión 11.0.15 (usuarios SIGFE versión 9) Chrome versión 42.0.2311.90
Grabador de DVD	Contenido en Windows 7
Complementos	Microsoft Silverlight
	Windows Media Player activado
	Parche cambio de hora instalado
	Java Runtime Environment 6 (JRE)
	Adobe Flash Plugin 13, para permitir la completa navegación en sitios web que lo exigen
	Agente Sistema de Gestión de Activos
	Codec K-Lite Codec Pack v10, para la reproducción de la gran mayoría de formatos de archivos multimedia utilizados
	Drivers de impresoras: que permite el uso de todos los modelos de impresoras disponibles dentro de la DPP

Servidores Regionales

Sistema Operativo	Windows Server 2008 Standard R2 SP1
Herramienta de Productividad	Windows Server Update Services Active Directory Super Agente Mc Afee
Antivirus Corporativo DPP	Agente McAfee
Grabador de DVD	Contenido en Windows Server
Contenidos	Master de microcomputadores
	Parche cambio de hora
Discos	RAID 0, se dispondrán de 4 Tb de espacio Se deben efectuar respaldos periódicos en equipo NAS

f. Política de Uso de Sistemas Informáticos

El acceso y uso de los sistemas informáticos de la institución deberá ser autorizado por los respectivos Jefes de Departamento y Unidades de la Defensoría Nacional y por los Directores Administrativos Regionales en el caso de las Defensorías Regionales. Los usuarios autorizados deberán ser capacitados para su uso y las contraseñas que se entreguen a propósito del acceso serán personales, nominativas y confidenciales.

La información que se registre en los sistemas informáticos debe ser completa, oportuna y fidedigna. Asimismo, la información que consulten o extraigan los usuarios de dichos sistemas debe ser utilizada exclusivamente para los fines propios de la función que ejercen en la institución.

g. Política de Soporte a Usuarios

Para abordar las necesidades de cada región del país, el DIE, dentro de su estructura y organización territorial dispone de Encargados Informáticos Regionales que cubren las necesidades de las dependencias de la DR y DL respectivas, y su administración regional, y por lo tanto son los encargados de aplicar los procedimientos tecnológicos, en directa relación con la administración regional respectiva, como también en estrecha comunicación con los integrantes del DIE de la DN. El soporte a los usuarios tendrá tres niveles:

- **Soporte Nivel 1:** Es el único que involucra al usuario y es brindado por el Encargado de Informática Regional en el caso de las DR e Inspectorías Zonales ubicadas en su zona y por el DIE en el caso de la Defensoría Nacional e Inspectoría Zonal Centro.
- **Soporte Nivel 2:** Requerido solo por los Encargados de Informática Regionales o funcionarios del DIE y corresponde al levantamiento de ticket de atención a los proveedores de servicio.
- **Soporte Nivel 3:** Utilizado solo por el DIE.

3. Políticas de Servicios Informáticos

a. Política de Categorización de Servicios Informáticos

Los Servicios Informáticos que se encuentren en operación serán clasificados en 3 grupos. La categorización considerara:

Servicios	Descripción	Servicios Informáticos
CENTRAL	Considera los servicios cuya implementación y funcionamiento se efectúan a partir de nodos centrales y que requieren para su funcionamiento la acción de contrapartes de funcionarios del DIE, en forma exclusiva	Plataforma Central Oracle Infraestructura Virtual Correo Electrónico Videoconferencia Housing Bases de Datos Antivirus Sitio Web
LOCAL	Considera los servicios cuya implementación y funcionamiento se efectúan a en las oficinas de la Defensoría y que requieren para su funcionamiento la acción de contrapartes de los encargados informáticos regionales, en forma principal	Telecomunicaciones Telefonía Computadores Impresoras UPS Telefonía Móvil Instalaciones y Mantención de Cableados Mantención y Soporte de Licencias MS
SISTEMAS	Considera las aplicaciones informáticas que prestan apoyo a la Defensoría, en cuanto al registro, almacenamiento y gestión de los procesos de negocios y soporte administrativo	Sistemas de Alto Impacto Sistemas de Impacto Medio Sistemas de Bajo Impacto

El DIE efectuará un levantamiento y actualización en la clasificación de los servicios informáticos, de tal forma de identificar aquellos que tienen un rol crítico y determinar planes de mejora.

b. Política de Redes y Telecomunicaciones

La Defensoría dispondrá de una red privada que conecte a todas las dependencias que tiene a nivel nacional. El DIE será responsable de gestionar, proveer y administrar los servicios que garanticen una adecuada cobertura en comunicaciones e implementar planes de contingencia que permitan mantener la conectividad en todas las oficinas y dependencias de la Defensoría.

c. Política de Housing

Para el alojamiento del equipamiento asociado a los servicios centrales y sistemas de alto e impacto medio; se mantendrá un servicio de housing que asegure las debidas condiciones de protección, monitoreo y continuidad del servicio y que cumpla con estándares de alta disponibilidad. Adicionalmente, y cuando exista disponibilidad presupuestaria se deberá contar con servicios de monitoreo que vigilen y controlen el comportamiento de las aplicaciones, sistemas operativos, bases de datos, enlaces de telecomunicaciones, comunicaciones asociadas a cada sistema y equipos.

d. Política de Continuidad de los Servicios Tecnológicos y Servicios Informáticos

Se deberá contar con un plan de contingencia que permita mantener operativos los sistemas informáticos ante la ocurrencia de fallas mayores en los servicios y/o sistemas críticos, el que deberá considerar una copia actualizada de los programas y sus ambientes operativos, y respaldos de datos, que permita asegurar la continuidad de funciones. Este plan deberá ser revisado y probado anualmente.

e. Política de Nuevas Versiones o Actualizaciones

Se deberán mantener actualizados todos los servicios informáticos que utiliza la Defensoría, siempre y cuando se verifique la compatibilidad con lo instalado actualmente, de manera que los usuarios siempre dispongan de nuevas herramientas y utilidades, y sobre todo para disminuir los errores. Los costos asociados deberán estar considerados en los respectivos contratos de prestación de servicios.

f. Política de Clasificación de Oficinas

Como estrategia de servicio las oficinas de la Defensoría serán clasificadas, de acuerdo a su impacto en el funcionamiento y factibilidad de provisión de servicios, en cinco tipos:

Aspecto	Esencial	Alto Impacto	Mediano-Bajo Impacto	Extrema	Básica
Descripción	Oficinas con gran volumen de causas, una gran cantidad de funcionarios y donde se desempeñan Directivos	Defensorías Locales u oficinas con gran volumen de causas o actividad, y 5 o más funcionarios	Defensorías Locales con volumen medio de causas, y entre 2 y 5 funcionarios	Defensorías Locales distantes con un volumen bajo de causas, y con 1 o 2 funcionarios	Oficinas de Atención de baja demanda, y con 1 funcionario
Velocidad Enlace	6 a 100 Mbps	1 a 2 Mbps	1 a 2 Mbps	512 Kbps a 2 Mbps	Banda Ancha / Servicio Domiciliario
Punto de Conexión	Santiago	Santiago	Santiago	Santiago	Internet
Enlace Respaldo	DN y CJS	No	No	No	No
WiFi	Si	Si	No	No	No
Videoconferencia	Si	Si (software)	No	No	No
Cantidad y tipo de teléfonos	Tipo A: Secretarias Tipo B: Jefatura Consola Visualizadora	Tipo A: 1 Tipo B: 2 a 6	Tipo A: 0 Tipo B: 2 a 5	Tipo A: 0 Tipo B: 1 a 2	Línea local
Troncales Planta Telefónica	8 máximo	2	2	2	-
Servidor	Si	No	No	No	No
Computadores	20 o más	5 a 7	2 a 5	1 o 2	1
Impresoras	Color + B/N multifuncional Incluyen scanner y fax	B/N multifuncional Incluyen scanner y fax	B/N multifuncional Incluyen scanner y fax	B/N multifuncional Incluyen scanner y fax	B/N impresora

Reloj Biométrico	Si	Si	No	No	No
Pistolas Lectoras	Si	Si	Si	Si	No
Data-Show	Si	Si	No	No	No
Defensorías Locales	Arica, Iquique, Antofagasta, Copiapó, La Serena, Valparaíso, Rancagua, Talca, Concepción, Temuco, Valdivia, Puerto Montt, Coyhaique, Punta Arenas, Centro Justicia, DN y Los Héroes	Calama, Coquimbo, Viña del Mar, Quilpué, Quillota, Curicó, Talcahuano, Chillán, Los Ángeles, Temuco (Indígena), Valdivia, Osorno, Puerto Montt (UDJ), Puente Alto, San Bernardo, Talagante, Melipilla, Colina, Inspectorías Zonales Norte, Centro y Sur	Tocopilla, Tal-Tal, Chañaral, Vallenar, Ovalle, Los Andes, San Antonio, Curacaví, San Fernando, Rengo, Santa Cruz, Pichilemu, Cauquenes, Parral, San Javier, Constitución, Linares, Angol, Arauco, Cañete, Collipulli, Ancud, Castro, Coronel, Villarrica y Puerto Natales	Isla de Pascua, Chaitén, Puerto Cisnes, Cochrane, Chile Chico, Puerto Aysén y Porvenir	Futaleufú

4. Política de Sistemas de Información

La Defensoría adoptará un estándar tecnológico como plataforma, que regulará los desarrollos dentro de la institución. Ese estándar en el área de desarrollo corresponde a Java y PHP y en cuanto al motor de base de datos a Oracle. Debido al grado de dispersión geográfica de las oficinas de la institución a lo largo del país; las aplicaciones o sistemas de información que se desarrollen deberán estar basados en tecnología Web, con el objeto de facilitar los procesos de mantención y actualización de las aplicaciones, mejorar los estándares de seguridad en el ingreso y almacenamiento de información, y la disponibilidad de acceso a los sistemas de información así como a los datos registrados en ellos.

a. Política de Categorización de Sistemas Informáticos

Los sistemas que se encuentran actualmente en operación serán clasificados en función de su vinculación y el impacto en los procesos de negocio de la Defensoría Penal. Los Sistemas serán clasificados de la siguiente forma:

- **Alto Impacto:** considera los sistemas que se relacionan directamente con el giro de la Defensoría y se definen como esenciales.
- **Impacto Medio:** considera los sistemas que relacionándose con su giro, provocan un impacto medio o estacional en la organización.
- **Bajo Impacto:** considera los sistemas que provocan un bajo nivel de impacto a nivel de la organización, o es altamente focalizado en alguna unidad de ésta.

Criterios	Sistemas Alto Impacto	Impacto Medio	Bajo Impacto
Localización	Housing	Housing	Housing / Servidores Regionales
Accesibilidad	Cualquier equipo con acceso a Internet	Cualquier equipo con acceso a Internet	Dependencias Defensoría
Herramientas de Programación	Java / PHP	Java / PHP (excepto sistemas contratados)	
Base de Datos	Oracle	Oracle	Oracle/MySQL
Respaldo de Recuperación	Obligatorio	Obligatorio	Obligatorio
Respaldo Histórico	Obligatorio	Opcional	Sin respaldo
Modalidad de construcción	A medida en 3 capas	A medida en 3 capas Licenciado	
Browser	IE 11.0 o posterior Chrome 43 o posterior	IE 11.0 o posterior Chrome 43 o posterior	IE 11.0 o posterior Chrome 43 o posterior

El DIE en forma periódica efectuará un levantamiento y actualización en la clasificación de los Sistemas de Información que utiliza la Defensoría, con el fin de disponer de información relevante para la confección de planes de mejora o de contingencia.

b. Política de Desarrollo y Mantención de Sistemas de Información

La guía que regula los desarrollos, implementación y explotación de sistemas deberá cumplir con estándares técnicos de mercado; de modo que el desarrollo de sistemas informáticos en general deberá ser concordante con dicha plataforma; y todo sistema que soporte una línea de negocio, deberá ser único a nivel nacional, sin existir sistemas locales aislados, paralelos o replicados.

Para la atención de requerimientos a los sistemas existentes, y su posterior desarrollo y puesta en marcha, se establece que el DIE será quien determine la factibilidad técnica de implementación.

En cuanto a los ambientes de desarrollo se establece que existirán tres, con diferentes niveles de acceso, y estos son:

- *Ambiente de Producción*: solo tendrá acceso personal del área de Operaciones del DIE.
- *Ambiente de Desarrollo*: tendrán acceso personal del área de Desarrollo del DIE y programadores externos.
- *Ambiente de Prueba*: tendrán acceso los usuarios del grupo de pruebas funcionales.

c. Política de Metodologías de Desarrollo de Sistemas

Todo desarrollo de sistemas deberá utilizar metodología que asegure el éxito de la implantación de las aplicaciones, utilizando conceptos modulares, iterativos e incrementales, que permitan revisar cada etapa de desarrollo, actualizar aplicaciones y mejorarlas en función de su dinamismo. Además se debe aplicar la segregación de funciones que permita reducir el riesgo de mal uso de los sistemas. Y exigir que las etapas del desarrollo sean documentadas.

d. Política de Prueba de los Sistemas

Los sistemas informáticos desarrollados o mantenidos por la Defensoría deberán cumplir con las actividades de revisión y validación de su funcionalidad, etapa que siempre debe ser supervisada por funcionarios del Departamento de Informática y Estadística de la Defensoría Nacional o los Encargados de Informática Regionales y será efectuada por el área que formuló el requerimiento a objeto de minimizar el impacto en los usuarios de la puesta de producción de nuevas aplicaciones de los sistemas.

e. Política de Instalación de Nuevas Versiones y Actualizaciones

Antes de la instalación de versiones nuevas de sistemas informáticos, se debe garantizar la continuidad operacional del servicio, para ello el Departamento de Informática y Estadística de la Defensoría Nacional deberá velar que estos procesos sean debidamente realizados.

f. Política de Respaldo de Sistemas de Información

Los datos asociados a todos los sistemas informáticos y los definidos en los Decretos Supremos N°s 77, 81 y 83; deberán ser respaldados y sus copias deberán ser almacenadas en recintos que cumplan con los estándares establecidos en la Norma ISO 27.001:2013 para seguridad de datos; es decir, ser almacenados en forma separada en edificios geográficamente distantes; con una periodicidad al menos mensual (respaldos semanales y diarios son menos riesgosos) y serán responsabilidad del DIE.

Los tipos de respaldos que se efectuarán son:

Respaldo de Recuperación: orientados a restablecer sistemas tras algún tipo de falla o desastre. Se consideran en este caso 2 tipos de respaldo:

- **Primarios**: son los que deberán garantizar la continuidad operacional y estarán insertos en los contratos de prestación, estarán efectuados a disco.
- **Secundarios:** corresponde a una réplica del respaldo primario y efectuarse a un medio de almacenamiento ubicado fuera de las dependencias del Housing.

Respaldo Histórico: orientado a guardar información para casos de consultas que puedan requerirse en el futuro o dar cumplimiento a normativa existente.

En cuanto a la *Retención de Respaldos*, de acuerdo a la capacidad de los recursos existente se deberá disponer de respaldos completos de las bases de datos con una retención de un mes, de programas y configuración con una retención de 3 meses e Histórica con una retención de 10 años.

5. Políticas de Contratación

a. Política del Arriendo del Equipamiento Informático

La Defensoría Penal Pública proveerá del equipamiento tecnológico necesario para apoyar las funciones de la institución por la vía del arriendo de tecnología sin compromiso de compra y asociado a planes y programas de mantención y soporte que permitan asegurar la continuidad operativa normal y, ante fallas o interrupciones del servicio, responder con la agilidad necesaria de manera de evitar o mitigar tales discontinuidades.

Las empresas que presten el servicio deberán tomar las medidas y precauciones necesarias para asegurar la continuidad del servicio (por ejemplo, seguros, redundancia de equipamiento, alertas y monitoreo, mantención preventiva y correctiva, asistencia técnica y soporte) en conformidad al respectivo contrato. Para asegurar la calidad del servicio, la Defensoría establecerá los plazos de respuesta y límites de servicio en condiciones de falla, que estime convenientes y necesarios para asegurar la continuidad y la calidad en la prestación del servicio.

b. Política de Control de Inventario

La mayoría de los equipos inventariables están asociados a servicios arrendados a empresas externas, con un tiempo predeterminado de operación y renovables, a través de procesos licitatorios de contratación. En base a lo anterior, se debe considerar como parte del servicio contratado con las empresas proveedoras, mantener un detalle del inventario de equipos y módulos asociados, lo cual formará parte del proceso de recepción en conformidad del proyecto.

Será función del DIE notificar al Departamento de Administración y Finanzas de la Defensoría Nacional (DAF) de "Altas", "Bajas" y "Modificaciones" que experimenten los equipos objeto de los servicios contratados y con respecto de todos los bienes informáticos adquiridos por la Institución, entre los que se cuentan las licencias de software y los equipos informáticos no sujetos a contrato de arriendo. Su control de inventario regirá según lo normado por el DAF.

c. Política de Mantención y Soporte del Equipamiento

Los contratos de prestación de servicios tecnológicos deberán considerar la realización en terreno de mantenciones preventivas y correctivas del equipamiento. La periodicidad de dicha mantención deberá ser al menos anual y ser ejecutada por personal certificado en la marca del equipamiento.

La Defensoría deberá diseñar y proveer planes y programas de mantención, actualización y soporte de equipamiento, que en cualquier caso, deberán ser realizadas en terreno.

d. Política de Obsolescencia Tecnológica

Con el objeto de evitar la obsolescencia del equipamiento, la Defensoría establece como política mantener en operación equipos computacionales de uso frecuente solo por tres (3) años y hasta cuatro (4) años en equipos de uso ocasional y al efectuar la contratación de un bien o servicio requerir las mejores características, en ningún caso se podrá adquirir tecnología obsoleta.

e. Política al Término de un Contrato

El DIE deberá efectuar antes de terminar el contrato con un proveedor, un informe de planificación, que incluya a lo menos una descripción del servicio prestado, características del contrato actual, recursos involucrados, requerimientos y recursos, periodo de contrato, mejoras e identificación del Encargado del Proyecto.

f. Política de Adquisiciones

La adquisición de software o hardware estará supeditada a la consistencia técnica con la plataforma tecnológica de la institución y sus planes informáticos y estratégicos, por lo tanto será el DIE quien deberá dar autorización para las adquisiciones. El equipamiento adquirido solo corresponderá a aquel cuyas características de mercado no recomiende arrendarlo y deberá incluir un período de garantía. Queda prohibida la adquisición e instalación de cualquier solución informática que no cuente con la autorización del DIE.

6. Políticas de Acceso de Internet

Todo el desarrollo, modernización o adaptación de los sitios Web de la institución se harán en función de las recomendaciones para el desarrollo de sitios Web del Estado y respetando los estándares sugeridos en la Guía Web del Estado.

a. Política de Uso de Internet

Todas las estaciones de trabajo tendrán acceso a Internet, para propiciar acciones de búsqueda y estudios que enriquezcan las funciones realizadas por los funcionarios de la Defensoría. Se podrá acceder a todo tipo de sitio que contenga información relacionada directa o indirectamente con las actividades que desempeña la institución. También se podrá acceder a sitios de noticias, bancos y otros fuera de los horarios de trabajo, el horario de trabajo corresponderá al determinado por la jefatura correspondiente y el Estatuto Administrativo.

Los funcionarios deberán abstenerse de acceder a sitios que hagan un fuerte uso del ancho de banda, en especial, sitios que presenten videos (ej. www.youtube.com) o que permitan escuchar radios on-line, para fines que no sean propios de su rol en la Defensoría.

b. Política de Uso de Intranet (Red Interna)

Todas las estaciones de trabajo tendrán acceso obligado a la Intranet de la Defensoría cada vez que abran el navegador adoptado como estándar por la Institución. Por lo tanto será obligatorio para cada funcionario la visita a la Intranet y se entenderá como el mecanismo formal y oficial utilizado por la institución para difundir resoluciones, decretos, oficios, instrucciones, reglas, normas, políticas, estrategias, metas y compromisos, resultados, decisiones, noticias y en general todo tipo de documentos que sean de interés y obligación institucional conocer y difundir.

Todas las políticas, normas y estándares que afectan, rigen o regulan los procesos y procedimientos informáticos, deberán ser publicados, comunicados y notificados a todos los funcionarios de la institución, y se entenderán conocidas por ellos.

c. Política de Uso de Accesos a Extranet

La Defensoría pondrá a disposición de las personas o empresas que prestan servicio de defensa penal pública licitada, un ambiente WEB que será el mecanismo mediante el cual se podrá acceder a los diferentes servicios tecnológicos y sistemas informáticos que se requiere para prestar sus servicios a la Defensoría. Todo documento publicado por este medio se entenderá y dará por conocido por dichas personas o empresas.

d. Política de Uso de Redes Sociales

En virtud del riesgo asociado a la posible contaminación por virus y las demandas a los anchos de banda de la red de telecomunicaciones, no se permitirá el acceso y uso de Facebook, u otros sitios de redes sociales, o cualquier tipo de sitio web cuya finalidad no se encuentre relacionada con las actividades propias del cargo, específicamente desde el equipamiento institucional.

Las redes sociales serán un canal de comunicación oficial de la Defensoría para con sus usuarios y clientes, el cual será administrado por la Unidad de Comunicaciones de la Defensoría. Dichas redes sociales a utilizar son: Twitter; Facebook; Youtube; LinkedIn; WhatsApp.

7. Políticas de Seguridad de la Información

Permite garantizar los niveles de seguridad de la información que se maneja, intercambia, genera, procesa y almacena en la institución, a fin de lograr la adecuada confidencialidad, integridad y disponibilidad para los activos de información considerados relevantes, de manera de permitir la continuidad operacional de los procesos y la entrega de servicios a usuarios.

La Defensoría declara su compromiso de adoptar las medidas necesarias y disponibles para lograr niveles adecuados de integridad, confidencialidad y disponibilidad de todos los activos de información considerados relevantes.

a. Política de Administración y Autenticación de Usuarios

A toda persona se le deberá asignar una contraseña de autenticación que le permita acceder a los servicios tecnológicos y sistemas informáticos. En otras palabras, un nombre de usuario y una clave cifrada, personal y confidencial. Para ello, cada incorporación de un nuevo funcionario que se integre a la Defensoría deberá ser informada por el Departamento de RR.HH. y D.O. de la Defensoría Nacional al DIE. En el caso de abogados licitados y otras entidades externas, cualquiera sea su naturaleza y finalidad, la solicitud será enviada por la Dirección Administrativa Nacional o Regional según corresponda. El DIE o los Encargados de Informática Regionales, según corresponda, dispondrán de dos días hábiles para habilitar las claves respectivas, las que serán entregadas personalmente al nuevo usuario.

En el mismo acto, el usuario será instruido por parte de un representante calificado del DIE a ejecutar él o los cambios de claves en él o los sistemas asignados. La creación, ingreso y responsabilidad de la nueva clave será del nuevo usuario.

De igual manera, el Departamento de RR.HH. y D.O. de la Defensoría Nacional y/o las Defensorías Regionales deberán comunicar al DIE el cese o cambio de funciones por parte de un funcionario, que implican su suspensión o eliminación de un sistema. El DIE centralizadamente, procederá a la eliminación de las cuentas respectivas.

b. Política de Uso de Información

La Institución se compromete a asegurar la confidencialidad de la información que se genere, procese, transmita y almacene en las bases de datos o aplicaciones, la que tendrá el carácter de confidencial, de acuerdo a la Ley N°19.628 sobre Protección de datos de carácter personal. Solo podrá ser utilizada para fines estadísticos y estudios, y en ningún caso se podrán publicar datos de carácter personal.

c. Política de Creación de Casillas de Correo Electrónico

Es política de la Defensoría Penal Pública crear y asignar una casilla de correo electrónico a toda persona que haya sido formalmente contratada para prestar servicios en forma directa (Defensores Locales, Directivos, Profesionales, Técnicos, Administrativos y Auxiliares de Planta, Contrata u Honorarios asimilados a grado), o indirecta (Defensores Licitados, Convenio Directos, etc.).

Estas casillas se podrán utilizar para transmitir comunicaciones oficiales entre usuarios de la organización. Existirán tres tipos de casillas:

- **Institucionales**: Se crearán basadas en el nombre de la función o departamento que representa. Su mantención estará a cargo del DIE.

- **Personales**: Se crearán basándose en el nombre del usuario y se podrán utilizar para intercambio de información de todo orden entre usuarios de la institución y entre éstos y terceros ajenos de la organización. Su mantención estará a cargo del correspondiente usuario. Se asignarán cuentas personales de correo electrónico a funcionarios de la institución y a defensores licitados.

- **Genéricas**: Respecto de personas y profesionales externos a la Defensoría (asistentes de empresas licitadas, estudiantes en práctica y recepción de notificaciones de tribunales), se asignarán cuentas genéricas asociadas a cada región y rol que cumpla la persona respecto de la institución. Su mantención estará a cargo del Encargado Informático Regional en Regiones y del DIE en Defensoría Nacional.

La creación y cierre de casillas de correo electrónico es responsabilidad del Encargado Informático Regional en cada Región, y del DIE en la Defensoría Nacional.

Espacio máximo y condiciones de uso de casillas de correo electrónico:

- **Tamaño casillas**: 0,5 Gb para Estudiantes en Práctica, 2 Gb General, 4 Gb para Directivos, Oficinas de Parte, Receptoras de Notificaciones.

- **Tamaño archivos adjuntos**: 15 Mb para enviar, 5 Mb para recibir desde dominios externos.

d. Política de Protección de Estaciones de Trabajo

Las estaciones de trabajo deberán protegerse de amenazas externas e internas; de riesgos ambientales, pérdidas o daños físicos. Del mismo modo, es necesario proteger los medios de apoyo e instalaciones y dispositivos de comunicaciones, de suministro eléctrico, y en general todos los elementos directa o indirectamente relacionados con el funcionamiento de los equipos computacionales.

Además, estarán protegidas con nombre de usuario y contraseña para evitar ingresos no autorizados a sus contenidos y con protector de pantalla que se active a lo más cada 15 minutos de inactividad para proteger la información visible. En este mismo sentido, los equipos estarán protegidos con antivirus local y perimetral para evitar ataques de código malicioso que perjudiquen

o destruyan su contenido. En estaciones de trabajo consideradas críticas, se protegerán adicionalmente a través de control de acceso por dirección IP.

e. Política de Protección de Servidores

Todos los servidores y ambientes de desarrollo, sistemas de almacenamiento de datos, dispositivos de protección lógicos y físicos (antivirus y cortafuegos), dispositivos de comunicación, dispositivos de suministro eléctrico y dispositivos de refrigeración deberán protegerse físicamente de amenazas externas e internas como pérdida, hurto, robo o daño físico, y de riesgos ambientales tales como inundaciones, humedad, humo, fuego, elementos tóxicos, inestabilidad del suministro eléctrico, entre otros.

Las instalaciones y los accesos a través de la red deberán estar protegidos de accesos no autorizados, por lo tanto, los trabajos de aseo y mantención podrán realizarse solo en forma controlada y quedará estrictamente prohibido el consumo de bebidas y alimentos en las cercanías a estas áreas, las que se deberán clasificar como áreas de seguridad.

f. Política de Entrega de Información

La Defensoría Penal Pública hará pública la información estadística que da cuenta del accionar de la Institución, acorde a las exigencias de la Ley N°20.285 de Transparencia y Acceso a la Información y la Ley N°19.628 de Protección de Datos de Carácter Personal.

La información a publicar considerará al menos 3 grandes universos de información: causas ingresadas, terminadas y vigentes; desglosando dicha información en variables socio-demográficas relevantes. En el caso de subconjuntos de datos inferiores a 10 casos, solo se hará pública información agrupada.

En los casos que sea necesario entregar información detallada a terceros para fines de investigaciones que éstos realicen y que la Institución considere beneficiosa desarrollar, será obligatoria la suscripción de un Acuerdo de Confidencialidad, que explicite la obligatoriedad del tercero a guardar reserva de la información entregada, utilizarla exclusivamente para los fines para los que fue solicitada, y destruirla una vez concluida la investigación.

g. Política de Uso de Carpetas Compartidas

El uso de carpetas compartidas en los computadores de los usuarios es una práctica que, aunque puede ser una herramienta útil de trabajo, tiene implícitos algunos riesgos que pueden afectar los principios de confidencialidad, integridad y disponibilidad de la información, por lo tanto su uso y aplicación debe ser controlado. Con este propósito se definen los siguientes lineamientos para su uso seguro:

- No se permitirá el uso de carpetas compartidas en computadores de usuarios.
- Los Encargados Informáticos Regionales en Regiones y el DIE en Defensoría Nacional, establecerán e implementarán, en los casos aprobados, la configuración de acceso a la carpeta,

previo requerimiento formal de la misma, por parte del Director Administrativo Regional o del Jefe de Departamento o Unidad de la Defensoría Nacional.

- El usuario que autoriza y dispone el recurso compartido es el responsable por las acciones y los accesos sobre la información contenida en dicha carpeta.
- Se debe definir el tipo de acceso y los roles estrictamente necesarios sobre la carpeta (lectura, escritura, modificación y borrado).
- Debe tenerse claramente especificado el límite de tiempo durante el cual estará publicada la información y compartido el recurso en el equipo.
- Si se trata de información confidencial o crítica, deben utilizarse carpetas destinadas para tal fin en un servidor de archivos de usuarios, para que sean incluidos en los respaldos de información.
- El acceso a carpetas compartidas debe delimitarse a los usuarios que las necesitan y deben ser protegidas con contraseñas en caso de escritura, modificación o borrado.
- No está permitido el acceso a dichas carpetas a usuarios que no formen parte de la red institucional.

h. Política de Cumplimiento de Requisitos Legales

Se debe asegurar el cumplimiento de la legislación vigente incluyendo, especialmente, las leyes que se señalan a continuación:

- Ley N°19.718 Crea la Defensoría Penal Pública
- Ley N°20.285 Acceso a la Información Pública
- Ley N°19.039 De Propiedad Industrial
- Ley N°17.336 sobre Propiedad Intelectual y sus modificaciones
- Ley N°19.628 Sobre Protección de la Vida Privada y Protección de Datos de Carácter Personal

De igual forma es política de la Defensoría, el cumplimiento de los reglamentos, regulaciones y compromisos emanados de Tratados Internacionales, asociados a sus actividades y relacionados con la seguridad de la información, para lo cual se asegura de que la información relativa a los mismos se mantiene actualizada, de forma tal, de poder incorporar en los procesos y procedimientos institucionales, las mejores prácticas que conduzcan a su cumplimiento.

La Defensoría declara su compromiso de cumplir los acuerdos y compromisos contractuales en materia de seguridad de la información, así como asegurar la adecuada protección, preservación, retención de los registros que se generan como resultado de las actividades de los procesos de la Defensoría, y de su disposición según lo establecido en acuerdos contractuales, en las leyes y regulaciones y en los procedimientos de la organización relativos a su control.

Como parte de esta política de cumplimiento de requisitos legales, la Defensoría Penal Pública, declara su compromiso con la adopción y seguimiento de prácticas adecuadas y técnicamente confiables para asegurar la prevención del uso inadecuado o con propósitos no autorizados, de las instalaciones de procesamiento de la información. Se incluyen en estas actividades, las auditorías a los sistemas de información como vía para verificar el cumplimiento de los controles establecidos a nivel del sistema de seguridad de la información y los acuerdos de confidencialidad y de acceso a recursos de información celebrados con los usuarios externos.

De igual forma como parte esencial de esta política, se declara el compromiso de la Defensoría y de sus Directivos, funcionarios y personal de asegurar el cumplimiento de los controles de seguridad establecidos, como vía para mitigar los riesgos de seguridad de la información y para asegurar la continuidad operacional.

Como vía para asegurar el cumplimiento de esta y las demás políticas del sistema de seguridad de la información, la alta Dirección declara su compromiso de trabajar de manera continua en el perfeccionamiento de las competencia de los funcionarios y prestadores a honorarios y personas externas que desarrollan sus actividades en la Defensoría, así como de asegurar, en la medida de su relevancia, los recursos necesarios para la implementación de los controles y procedimientos relacionados.

8. Política de Cumplimiento, Actualización y Auditorías

El DIE incluirá en sus evaluaciones periódicas la revisión del cumplimiento del Manual de Procedimientos Tecnológicos.

Como una forma de adoptar medidas correctivas, detectar errores y documentar información relevante para el área de operaciones del DIE, se efectuarán auditorías sobre el cumplimiento de procedimientos vigentes, estado y mantenimiento de las salas de servidores, configuraciones de equipos y administración de usuarios en los distintos sistemas, entre otros.

Las Políticas y Procedimientos Tecnológicos serán revisados y actualizados en periodos anuales, de tal forma de incorporar aspectos de mejora resultantes de las Auditorías efectuadas, incorporar aspectos asociados al avance tecnológico producido y los cambios que la propia Defensoría haya adoptado en dicho periodo.

Asimismo, a través del sistema de evaluación selectiva de la Unidad de Auditoría Interna podría ser incluida una auditoría a los Departamentos y Unidades de la DN, Defensorías Regionales o Defensorías Locales sobre lo indicado en este documento y según el nivel de riesgo que se defina para cada periodo.

VIII. Comité Tecnológico

Se considera la existencia de un Comité Tecnológico, cuyo rol y responsabilidades serán las siguientes:

a. Objetivo

Revisar las políticas; procedimientos; plan anual de trabajo y velar por la correcta aplicación de las directrices establecidas, en materia tecnológica, como conocer los temas asociados a la Seguridad de la Información.

b. Estructura

El comité estará conformado por el/la DAN, quien lo presidirá y actuará institucionalmente como Encargado del comité; el Jefe del Departamento de Informática y Estadísticas quien actuará como su Secretario Ejecutivo; los Jefes de los Departamentos de Estudios y Proyectos (DEP), Evaluación Control y Reclamaciones (DECR), Administración y Finanzas (DAF) y Recursos Humanos (RRHH) de la Defensoría Nacional; 1 Defensor Regional y 2 Directores Administrativos Regionales.

Podrán ser invitados a participar a sus sesiones, todos aquellos funcionarios que se considere conveniente para el mejor decidir del Comité.

c. Funciones

- Proponer políticas tecnológicas y determinar las responsabilidades generales y específicas.
- Realizar seguimiento a los cambios que afecten las políticas y procedimientos vigentes en la materia y definir mecanismos de actualización.
- Proponer mejoras a los planes vigentes.
- Revisar y dar seguimiento al Plan Tecnológico Institucional.
- Revisar y dar seguimiento al Plan de Continuidad de las Operaciones.
- Monitorear los incidentes de seguridad de la información, revisar amenazas, niveles de riesgo, acciones preventivas o correctivas y capacitaciones.
- Difusión de las actividades o cambios tecnológicos.

d. Funcionamiento

El Comité se reunirá al menos una vez al año, mediante convocatoria de su Secretario Ejecutivo, debiendo sesionar con la asistencia de sus titulares y al menos 5 de sus miembros. Anualmente, deberán revisarse los siguientes temas:

- Modificaciones al Manual de Procedimientos Tecnológicos.
- Seguimiento al Plan Tecnológico.
- Resultado de Auditorías.
- Aprobación de Planes Anuales Tecnológicos de Trabajo.

IX. Procedimientos Tecnológicos

1. Procedimiento de Asignación de Servicios Informáticos

a. Objetivo

Describir las acciones asociadas a la asignación, modificación y suspensión del uso de los Servicios Informáticos que utiliza la Defensoría.

b. Alcance

Este documento describe las acciones necesarias para asignar a los usuarios acceso a los servicios informáticos de la Defensoría, se entenderán como servicios, los enunciados en la *Política de Categorización de Servicios Informáticos*, y se clasifican en Centrales, Locales y Sistemas. Los Centrales corresponden a Telecomunicaciones, Telefonía, Videoconferencia, Housing, Plataforma Central Oracle, Infraestructura Virtual, Bases de Datos, Correo Electrónico, Antivirus y Sitios Web. Los Locales corresponden a Computadores, Impresoras, Scanner, UPS, Telefonía Móvil, Instalaciones y Mantención de Cableados y finalmente Mantención y Soporte de Licencias. Y los de Sistemas corresponden a los sistemas de Alto Impacto, Impacto Medio y Bajo impacto.

Además los servicios descritos en algunos casos incluyen la asignación de equipamiento como son los proyectores, notebook, relojes biométricos y WIFI.

c. Base Legal

Según lo que establece la Ley N° 10.336 sobre Organización y Atribuciones de la Contraloría General de la República, en sus arts. N°s 60 y siguientes, todo funcionario que tenga, use, custodie o administre bienes fiscales será responsable de éstos, de su uso, abuso o empleo ilegal, y de toda pérdida o deterioro de los mismos que se produzca, imputables a su culpa o negligencia.

La entrega y uso de equipos computacionales pertenecientes a la institución están sujetos a las normas sobre responsabilidad administrativa contenidas en la Ley N° 18.834 sobre Estatuto Administrativo y las normas sobre Probidad Administrativa contenidas en el D.F.L. N° 1/19.653 de 2000, que fija texto refundido, coordinado y sistematizado de la Ley 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado, sin perjuicio de la responsabilidad civil y penal contenidas en nuestro ordenamiento jurídico.

d. Responsabilidades

- **Personal de la Defensoría Penal Pública y Usuarios:** Cumplir con lo establecido en este procedimiento y asegurar que sus actividades en cumplimiento a lo establecido en las leyes, regulaciones y reglamentos aplicables, así como en los controles de seguridad establecidos.
- **Departamento de Informática y Estadística de la Defensoría Nacional:** Asegurar la adecuada y oportuna asignación de servicios informáticos, y establecer los procedimientos necesarios frente a pérdidas, robos y frente al deterioro del equipamiento a través de la aprobación, aplicación y seguimiento de procedimientos y controles adecuados.
- **Directores Administrativos Regionales y Jefes de Departamento y Unidades:** Solicitar para los usuarios de su dependencia la asignación, modificación o eliminación de acceso a los servicios informáticos. Los Directores Administrativos Regionales respecto de su Defensoría Regional, incluidas las Inspectorías Zonales, Empresas de Abogados Licitados y usuarios externos correspondientes a su región y los Jefes de Departamento y Unidades respecto de sus usuarios.
- **Encargado de Informática Regional:** Velar por el cumplimiento del presente instructivo, y el funcionamiento de los servicios y sistemas informáticos a nivel regional, capacitar a los usuarios en el uso de los servicios y encargarse del soporte de 1er nivel.

e. Descripción de Actividades

1. **Asignación:** La asignación de servicios a los usuarios va a estar determinada por el cargo que desempeña y en algunos casos por requerimientos temporales, la solicitud de acceso debe ser remitida vía correo electrónico al Encargado de Informática Regional, cuando se trate de usuarios de una DR y al DIE cuando se trate de usuarios de la DN.

   Los datos requeridos para esta solicitud, son: Nombre completo, RUT, Defensoría/Departamento/Unidad, Cargo, Perfil, Sistemas a los que requiere acceso, fecha de inicio y fecha de término si corresponde y en el caso que se solicite la asignación de un equipo perteneciente a la Defensoría, por ejemplo: notebook, celular, etc. deberá indicarse el usuario y el cargo. De esta manera se podrá determinar los recursos disponibles para el usuario según su perfil, dicha comunicación deberá ser a nivel local para luego ser remitida al DIE, que evaluará la asignación. En el caso que corresponda asignar algún tipo de equipamiento el usuario deberá firmar el acta de entrega respectiva. En el *anexo A* se adjunta el *Formulario de Servicios* que debe ser utilizado por el DAR o el Jefe de Departamento/Unidad en el caso de la DN. La confección de este formulario puede ser apoyada por el Encargado de Informática Regional o por el DIE, según corresponda.

   En el caso de correos electrónicos, su asignación se hará conforme a la *Política de Creación de Casillas de Correo Electrónico*.

   Y en el caso de los perfiles para la asignación de servicios que se identifica en el *formulario de servicios*, corresponden a los tipos de usuarios más comunes que acceden los sistemas, se

determinaron los más representativos, según la cantidad de usuarios, los perfiles disponibles y se encuentran detallados en el *Anexo D* Perfiles de Usuarios.

Responsable de las solicitudes: El DAR cuando se trate de usuarios de las Defensorías Regionales y el Jefe del Departamento o Unidad cuando se trate de usuarios de la DN.

2. **Modificación:** Para efectuar una modificación en la asignación de los servicios, la comunicación debe partir del DAR o del Jefe de Departamento o Unidad, y ser efectuada por vía formal indicando los servicios que serán modificados o los servicios que deben incorporarse, dirigida al Encargado de efectuar las modificaciones, como se indica en el punto anterior de Asignación.

3. **Eliminación:** La eliminación en la asignación de los servicios, es prioritaria para mantener la seguridad en el acceso a los servicios de la Defensoría, por lo tanto, debe ser efectuada inmediatamente se comunica o se toma conocimiento de ello y la responsabilidad de la comunicación es de los DAR y de los Jefes de Departamento o Unidades, según corresponda. Esta comunicación debe ser realizada vía formal, indicando los servicios que se van a dar de baja y los motivos permaneciendo un registro escrito sobre este proceso.

   Anualmente, el DIE procederá a efectuar la eliminación física de los registros en los sistemas de las solicitudes efectuadas el año anterior al que termina, esto para mantener un control adecuado de la información.

4. **Capacitación:** La capacitación de los usuarios en materia de uso de los servicios será de responsabilidad de los Encargados Regionales de Informática y del DIE según corresponda. Y debe efectuarse cada vez que un usuario se incorpora a la Defensoría y al asignarse los recursos tecnológicos y también en el caso que se efectúe una modificación de la asignación. De este proceso debe quedar consignada un acta de capacitación.

f. Registros

- Para la asignación, modificación y eliminación en el acceso de los servicios de la Defensoría, deberá quedar un registro, es decir, correo electrónico, providencia, memo u oficio de la solicitud, donde se adjunte el *Formulario de Servicios*, incluido en el *anexo A*.
- *Acta de capacitación*, incluido *anexo B*.
- *Perfiles de Usuarios*, incluido anexo C.

g. Referencias

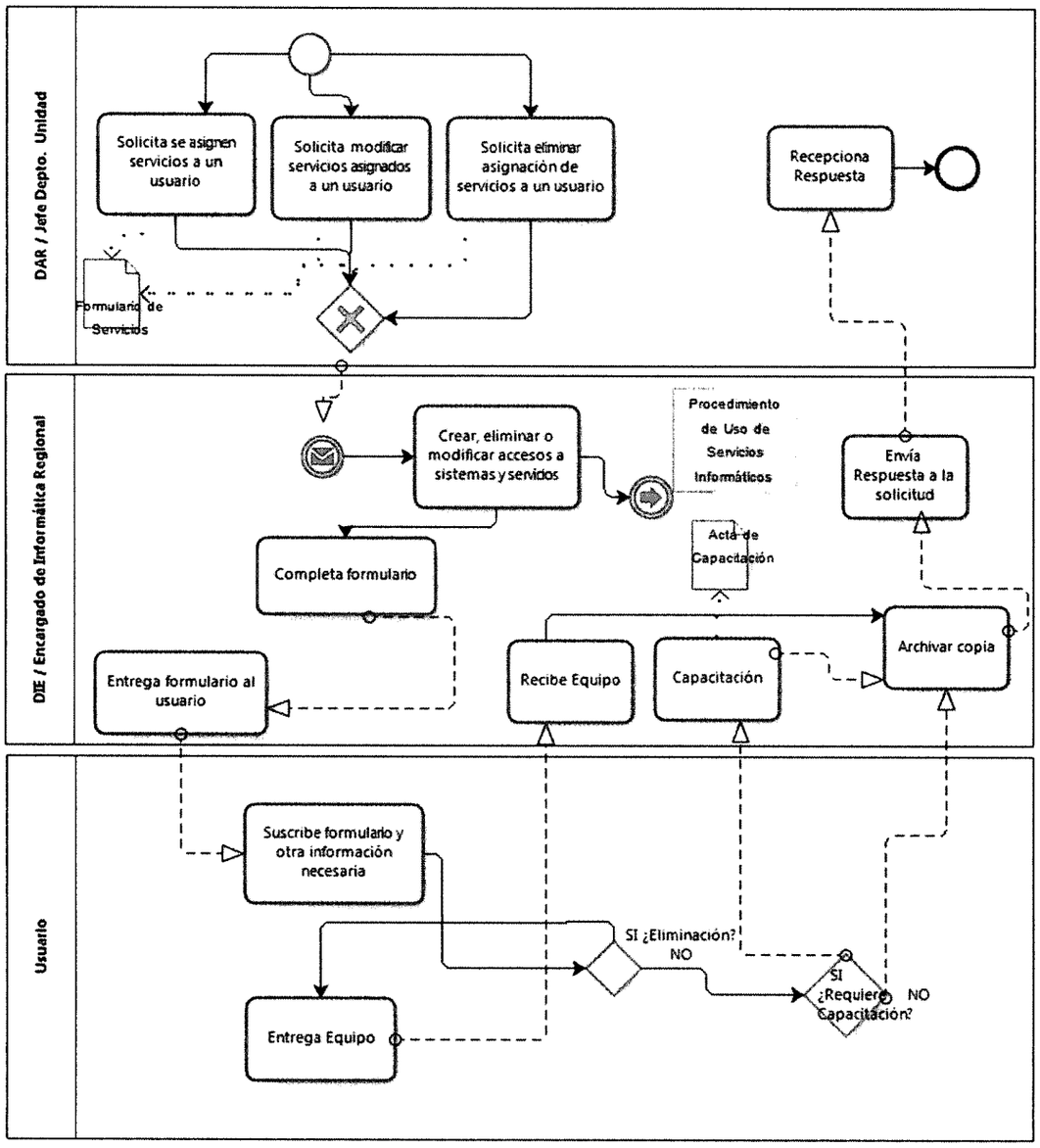
- Política Tecnológica, Política de Asignación de los Servicios Informáticos.
- Ley 18.334 sobre Estatuto Administrativo.
- DFL N° 1/19.653, de 2000, que fija texto refundido, coordinado y sistematizado de la Ley 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado

h. Indicadores

- No hay

i. Diagrama de Flujo

Diagrama de Asignación de Servicios Informáticos



j. Anexos

Anexo A

Formulario de Asignación de Servicios

Formulario de Asignación de Servicios	Defensoría Sin defensa no hay Justicia

Uso DAR/Jefe Depto/Jefe Unidad

Nombre Completo **(*) Tipo de Movimiento (N/E/M)**

Apellido Paterno	Apellido Materno	Nombres

Perfil **RUT**

Lugar de Trabajo y Región **Responsable de la solicitud** (Nombre y Apellido)

			Uso DIE		
Fecha			**Fecha**		
Día	Mes	Año	Día	Mes	Año

Servicios		**Observaciones**	**(N/E/M)**	**Observaciones**
Estación de Trabajo				N° Inventario
Teléfono				N°
Teléfono Móvil				N°
Notebook				N° Inventario
Correo Electrónico				email
Sistemas				
SIGDP				
SIACD				
SIAR				
SIGO				
SCD				
SIED				
SIGPER				
REDMINE				
Otras aplicaciones				
Ms Office Profesional				
Project				
Acrobat				
SPSS				
PhotoShop				
Autocad				

Otros (especificar)	Otras Observaciones

Uso USUARIO

Acta de entrega: **Fecha**

Día Mes Año

Usuario Encargado DIE/Regional DAR/Jefe Depto/Jefe Unidad

NOTA: Una vez recibida la información sobre sus contraseñas, deberá ingresar a los sistemas y cambiarla. Su contraseña inicial son los primeros 6 dígitos de su rut.

(*) N asignación nueva, E elimina asignación y M modifica asignación.

Anexo B

Acta de Capacitación

ACTA DE CAPACITACIÓN			Defensoría Sin defensa no hay Justicia
Fecha			
Relator			
Contenidos			
Lugar			
Nombre	**RUT**	**Oficina/Defensoría**	**Firma**

Anexo C
Perfiles de Usuarios

PERFIL	SIGDP	SIACD	SIAR	REDMINE	OTROS
Directivo	Consultas	Consultas	Consultas / Aprobación	Consultas	Lo define el jefe directo
Defensor	Todo		Todo		
Asistente Administrativa	Ingreso / Consultas				
Inspector	Consultas	Todo	Todo		
Profesionales DEP	Consultas	Consultas	Consultas		
Profesionales DECR	Consultas	Todo	Consultas		
Otros	Lo define el jefe directo				

2. Procedimientos de Uso de Servicios Informáticos

2.1 Procedimiento de Resguardo del Equipamiento Computacional

a. Objetivo

Describir las acciones necesarias para el uso, custodia, seguridad y resguardo del equipamiento institucional que se encuentra asignado a los usuarios.

b. Alcance

Se entenderá por equipamiento los siguientes: Computadores de Escritorio, Notebooks, Teléfonos, Celulares y Equipamiento en General. Además considera el equipamiento de uso general asignado por unidad, es decir, impresoras, UPS, data-show y reloj biométrico.

La responsabilidad del uso recaerá en el usuario que tenga asignado el equipamiento o el servicio.

c. Base Legal

Según lo que establece la Ley N° 10.336 sobre Organización y Atribuciones de la Contraloría General de la República, art. N°60 y siguientes.

La entrega y uso de equipos computacionales pertenecientes a la institución están sujetos a las normas sobre responsabilidad administrativa contenidas en la Ley N° 18.834 sobre Estatuto Administrativo y normas sobre Probidad Administrativa contenidas en el D.F.L. N° 1/19.653 que fija texto refundido, coordinado y sistematizado de la Ley 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado, sin perjuicio de la responsabilidad civil y penal contenidas en nuestro ordenamiento jurídico.

d. Responsabilidades

- **Todo el personal de la Defensoría Penal Pública y Usuarios:** Cumplir con lo establecido en este procedimiento y asegurar que sus actividades dan cumplimiento a lo establecido en las leyes, regulaciones y reglamentos aplicables, así como en los controles de seguridad establecidos.
- **Departamento de Informática y Estadística:** Asegurar el soporte y establecer los procedimientos y controles necesarios frente a pérdidas, robos y frente al deterioro del equipamiento, encargarse del soporte de 2do nivel y requerir el soporte de 3er nivel.
- **Encargado de Informática Regional:** Velar por el cumplimiento del presente instructivo, capacitar a los usuarios en el uso de los servicios, encargarse del soporte de 1er nivel y requerir el soporte de 2do nivel.

e. Descripción de Actividades

1. Uso de Computadores Personales, Telefonía y Telefonía Móvil

- **Uso:** Los usuarios que tengan a su cargo un computador de escritorio, notebook, aparato telefónico o móvil, deberán velar por su uso, custodia, seguridad y resguardo. Y deberán informar a su soporte de 1er nivel cualquier anomalía o mal funcionamiento, tanto del hardware como del software. Para los teléfonos móviles el usuario tendrá asignada una cantidad de minutos para llamadas y una bolsa de datos para navegación, de acuerdo a su perfil y cargo. Y para los teléfonos fijos los usuarios tendrán asignado un perfil que permitirá llamadas locales, a celulares y/o a larga distancia. En ambos casos los usuarios tienen la obligación de respetar y ajustarse a la cantidad asignada.

- **Incidentes equipos de uso personal:** El usuario que sufra de un incidente con su computador de escritorio, notebook, teléfono fijo o teléfono móvil, deberá reportarlo a su jefe directo y al soporte de 1er nivel, quienes tomarán las acciones administrativas y técnicas que correspondan. Cuando el incidente se trate de robo o hurto el usuario deberá dejar una constancia en carabineros o una denuncia en el Ministerio Público. Antes de efectuar un reporte de fallas deberá realizar las pruebas indicadas en el *anexo A*, esto permitirá al soporte de 1er nivel tomar acciones de acuerdo al caso.

- **Incidentes equipos de uso común:** Cuando el incidente corresponda a equipamiento de uso compartido, el responsable del equipamiento deberá efectuar el reporte al Soporte 1er nivel. El responsable será el que se encuentre consignado en el Sistema de Inventario.

- **Escalabilidad:** El soporte de 1er nivel deberá reportar las fallas o incidentes a la empresa que presta el servicio, de acuerdo a lo establecido en el contrato de prestación del servicio, si a pesar que se efectuó el reporte, no se resuelve el incidente se deberá recurrir al soporte de 2do nivel, cabe mencionar que el soporte de 1er nivel deberá velar por los plazos de respuesta del soporte y mantener informado al soporte de 2do nivel sobre cumplimientos o incumplimientos.

- **Soporte y plazos:** Los tipos de soporte para los servicios son los determinados en la *Política de Soporte a Usuarios*. Y los plazos de respuesta estarán determinados por los contratos de servicios vigentes. En cuanto al plazo para derivar los incidentes entre los diferentes tipos de soporte este será de 48 horas posteriores al reporte del usuario.

- **Pruebas:** Como se mencionó anteriormente en el *anexo A* se presentan algunas pruebas básicas que puede efectuar el usuario para verificar el funcionamiento de su aparato telefónico, teléfono móvil y computador de escritorio.

2. Uso del Equipamiento en General

- **Uso:** El uso del equipamiento en general deberá ajustarse a las necesidades de los usuarios, quienes deberán hacer un uso adecuado y racional de los mismos. Cabe hacer mención que por regla general no se impondrán restricciones de uso, siempre y cuando, no se constate que se está efectuando un uso inadecuado de los recursos.

- **Capacitación:** El encargado del soporte de 1er nivel realizará capacitaciones permanentes del uso de los servicios tecnológicos y sistemas informáticos.

f. Registros

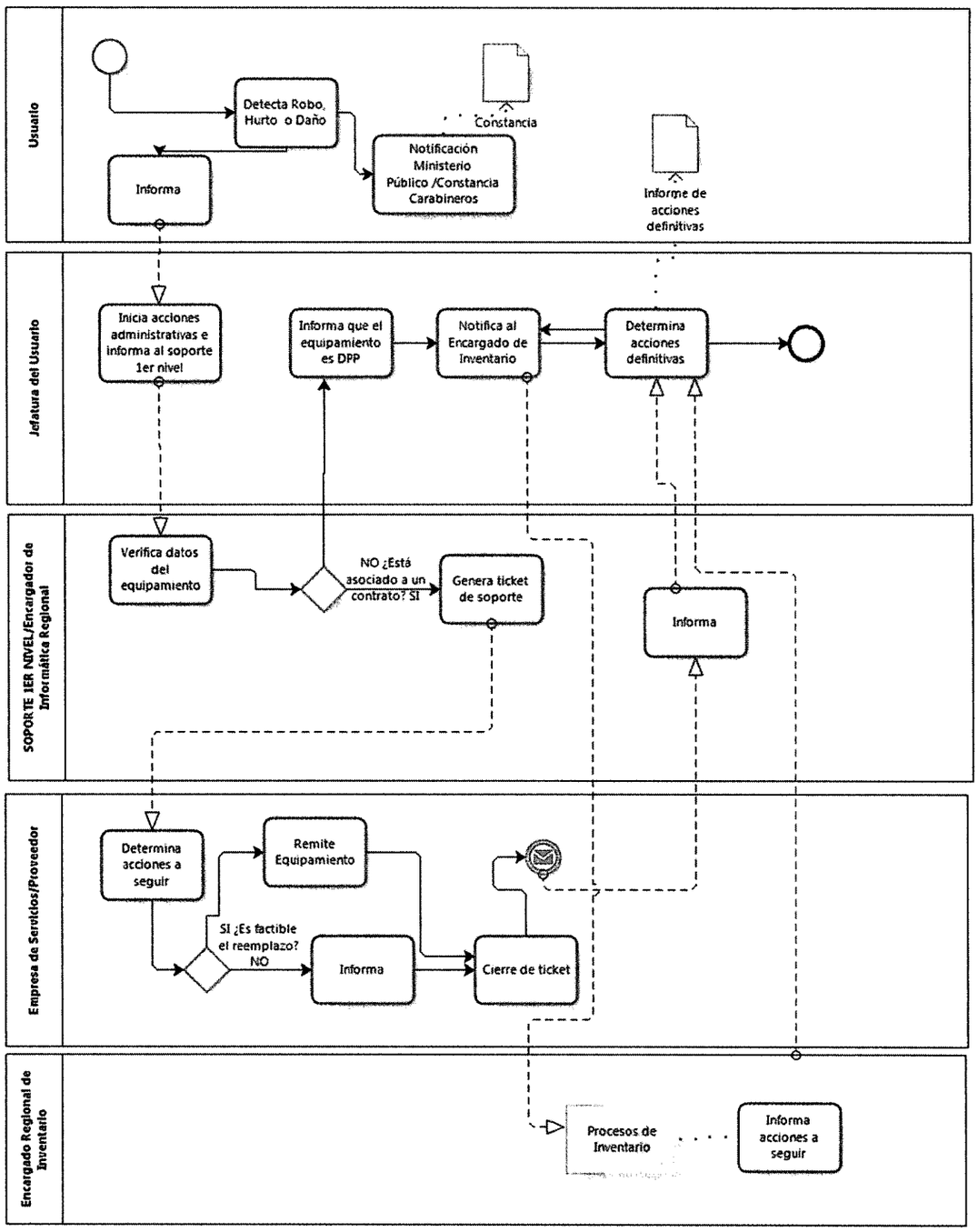
- Pruebas para verificar el funcionamiento de los servicios de telefonía fija, telefonía móvil y computadores de escritorio, incluido *anexo A*.
- Constancia en carabineros, en caso de Robo o Hurto, emitido por Carabineros de Chile.

g. Referencias

- Política Tecnológica, Política Uso de los Servicios Informáticos
- Ley 18.334 sobre Estatuto Administrativo.
- DFL N° 1/19.653 de 2000, que fija texto refundido, coordinado y sistematizado de la Ley 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado.

h. Diagrama de Flujo

Diagrama de Flujo Robos, Hurtos o Daños del Equipamiento



i. Anexo

Anexo A
Pruebas para verificar el funcionamiento de los servicios

Teléfono Fijo	Teléfono Móvil	Computador Personal
Verificar si existe tono de marcado	Verificar si puede realizar llamadas, navegar y si tiene WIFI	Verificar si enciende el monitor y la CPU
Verificar si el equipo está conectado en la roseta telefónica	Verificar si carga la batería	Verificar si todo el cableado está debidamente ajustado
Verificar si el equipo se encuentra en buenas condiciones	Verificar estado de la batería	Verificar si existe internet y hacer pruebas con la intranet institucional v/s otra página externa
Solicitar al soporte 1er nivel que verifique que la central telefónica está encendida y tiene suministro eléctrico	Verificar si muestra algún mensaje de alerta	Verificar con el soporte 1er nivel si no existen inconveniente con el suministro eléctrico
Verificar si tiene comunicación local, entre anexos	Verificar la cobertura	
Verificar si las líneas externas funcionan		
Verificar si el visor entrega un mensaje de error		

2.2 Procedimiento de Reportes y Soportes de los Usuarios

a. Objetivo

Normar el proceso de reportes de los usuarios y establecer como herramienta única de administración de los reportes el sistema REDMINE.

b. Alcance

Este procedimiento es extensivo a todos los usuarios de la defensoría, ya sea que utilicen los sistemas que cuenta la institución y/o los servicios de correo, telefonía, red de datos, intranet, entre otros.

c. Definiciones

- REDMINE: Herramienta para la gestión de proyectos que incluye sistema de seguimiento de incidentes, calendario de actividades, diagramas de Gantt para la representación visual de la línea del tiempo de los proyectos, wiki, foro, visor del repositorio de control de versiones, control de flujo de trabajo basado en roles, integración con correo electrónico, entre otros.
- Requerimientos: Es una necesidad documentada sobre el contenido, forma o funcionalidad de un producto o servicio. Los requerimientos son declaraciones que identifican atributos, capacidades, características y/o cualidades que necesita cumplir un servicio tecnológico o sistema informático para que tenga valor y utilidad para el usuario. En otras palabras, los requerimientos muestran qué elementos y funciones son necesarias para un proyecto. En el modelo clásico de desarrollo de sistemas, la etapa de requerimientos viene antecedida de la etapa de factibilidad y precedida por la etapa de diseño.
- Consultas: Corresponde a las inquietudes emanadas de los usuarios sobre el uso de los servicios tecnológicos y sistemas informáticos, o de carácter jurídico operativos sobre el correcto ingreso de la información.
- Soporte: Asistencia con el hardware o software en general, el servicio de soporte sirve para ayudar a resolver los problemas que puedan presentárseles a los usuarios, mientras hacen uso de servicios, programas o dispositivos.
- Ticket: Número que identifica el reporte levantado en REDMINE.

d. Responsabilidades

Usuario: Reportar cualquier falla en los servicios tecnológicos y sistemas informáticos, y solicitar por las vías establecidas la información estadística relevante para su gestión, puede validar las soluciones entregadas por el soporte de REDMINE.

Encargado de Informática Regional: Recibir por parte de los usuarios los requerimientos de soporte o de solicitudes de información y derivarlos a quienes sean los responsables de entregar el soporte

o la información, respetando los procedimientos y protocolos establecidos. A cargo de levantar los tickets en REDMINE.

Director Administrativo Regional: Garantizar el soporte de usuarios en sus defensorías regionales reportar cualquier anomalía ya sea de los servicios tecnológicos o sistemas informáticos de la institución, así como canalizar las solicitudes de información de sus usuarios, de acuerdo al procedimiento adscrito.

Encargado del área de Desarrollo: Garantizar la respuesta oportuna a los requerimientos de soporte a usuarios y a mantener una base actualizada de las mejoras propuestas por los usuarios en relación a los sistemas informáticos con el fin de canalizarlos a los departamentos técnicos de la defensoría. Administrar Soporte Desarrollo.

Encargado del área de Operaciones: Garantizar la respuesta oportuna a los requerimientos de soporte de los usuarios y a mantenerlos informados sobre el estado de los ticket. Administrar Soporte de los Servicios Tecnológicos.

Encargado del área de Estadística: Garantizar la respuesta oportuna a los requerimientos de información de los usuarios y a mantenerlos informados sobre el estado de los ticket. Administrar Soporte de Información Estadística.

Equipo REDMINE: Responder los requerimientos en el plazo establecido, entregar información al usuario sobre el ticket y canalizar los requerimientos nuevos por la vía establecida en el presente documento.

Jefe de Departamento de Informática y Estadística: Velar por el cumplimiento del procedimiento contenido en este documento. Administrar Soporte DIE.

e. Descripción de Actividades

1. Una vez al año se designarán los encargados del Equipo REDMINE quienes estarán a cargo de responder los incidentes ingresados, y podrán solicitar ayuda y soporte a los integrantes de su respectiva área para resolverlos. Además tendrán que informar directamente a su encargado de área.
   La designación del equipo será efectuada vía correo electrónico por cada encargado de área, y comunicada al interior del DIE y al Jefe DIE.
2. Reporte de incidente: Todos los usuarios de la institución podrán reportar anomalías sobre el funcionamiento de los sistemas informáticos o servicios tecnológicos que son de su competencia, para esto deberán por correo electrónico enviar un detalle del incidente a su encargado de informática regional y/o al director administrativo regional indicando lo siguiente:
   a. Sistema o Servicio involucrado.
   b. Funcionalidad utilizada al momento de la ocurrencia del problema.
   c. Pantalla del error, mensaje o síntoma.
   d. Fecha y hora de la ocurrencia del problema.

e. Usuario que se vio afectado del problema, cuenta de usuario, rut o perfil. En caso de tratarse de problemas telefónicos o de celulares indicar número de anexo o celular. Si corresponde reportar problemas de correo electrónico indicar la casilla de correo correspondiente.

3. El encargado de informática regional deberá analizar y resolver el problema reportado. Solo en el caso que no pueda resolver el incidente personalmente o con el apoyo de los proveedores externos locales que prestan servicio, proceder a escalarlo al Soporte nivel 2 (DIE), vía REDMINE.
4. El encargado de informática regional deberá generar un ticket de REDMINE con los datos proporcionados por el usuario, indicando además el correo electrónico del usuario. Los ticket deberán ser ingresados en alguna de las cuatro carpetas existente o proyectos, de acuerdo, a la denominación entregada por el sistema, los cuales son:
    a. Soporte Desarrollo: Cuando se trate de incidentes o consultas sobre los sistemas informáticos de la institución. Este proyecto será gestionado por la encargada del área de desarrollo del DIE.
    b. Soporte Operaciones: Cuando se trate de incidentes o consultas sobre los servicios tecnológicos de la institución, correo electrónico, telefonía, comportamiento de la red de datos, impresoras, ups, cortes de servicios, entre otros. Este proyecto será gestionado por el encargado de operaciones del DIE.
    c. Soporte Estadística: Cuando se trate de aclaraciones, consultas o solicitudes de información estadística. Este proyecto será gestionado por la encargada del área estadística.
    d. Soporte DIE: Cuando se trate de consultas o aclaraciones sobre los procedimientos del DIE, el Plan Tecnológico, las condiciones de los servicios prestados por la institución, este proyecto será gestionado por el Jefe de Departamento.
5. Una vez generado el ticket el encargado de cada proyecto podrá asignarlo a alguno de los profesionales de su área, esta derivación debe ser realizada en un plazo no mayor a las 24 horas de generado el ticket, además se indicará la prioridad. El estado inicial de este ticket será de *Nuevo*.
6. Luego de asignado el ticket el responsable deberá responder dando acuse recibo e indicar un plazo de 'x' días para resolver su reclamo, en el caso de incidentes o consultas que sean de mero trámite la respuesta deberá ser ingresada dentro de un plazo no mayor a las 24 horas. Los 'x' días mencionado no podrán superar los 10 días corridos desde la generación del ticket. En los tickets donde el usuario solicite información o corresponda a un requerimiento de desarrollo, deberán traer adjunto un documento con las especificaciones del requerimiento y la firma del Defensor Regional que confirma la solicitud. Lo mismo para las solicitudes de información deberán ceñirse a lo indicado en el protocolo de solicitud de información estadística. En el caso de los requerimientos de desarrollo informático, estos estarán supeditados a la disponibilidad de recursos para atenderlos por lo que quedarán almacenados en una carpeta distinta *Desarrollos Nuevos* y a la espera de lo que determine el Comité Tecnológico quienes tendrán la responsabilidad de guiar y priorizar la líneas de trabajo, de acuerdo, objetivos planteados por la institución, si de acuerdo a los

antecedentes procede se efectué el desarrollo de una modificación o mejora a algún sistema el tiempo necesario y los recursos serán determinados por el área de desarrollo. Para efectos de este procedimiento los requerimientos de información o aclaraciones deberán ser consideradas de mero trámite, a menos que el área involucrada determine que el costo de su extracción sea mayor.

7. La etapa anterior contempla aclaraciones sobre los tickets lo que corresponderá cuando no exista información suficiente o necesaria para gestionarlos o existan dudas sobre lo solicitado, esto quedará plasmado en el sistema cambiando el estado del ticket de *Nuevo* a Feedback IR, de lo contrario al ingresar el acuse recibo con la indicación de días de respuesta el ticket pasará al estado *Asignado.*
8. Una vez resuelto el incidente o cuando se tenga la información solicitada se deberá ingresar la respuesta quedando en un estado de *Validación* donde el encargado de informática o quien haya ingresado el ticket deberá validar con el usuario que reportó el incidente y cambiar el estado del ticket a *Cerrado,* de acuerdo, a lo indicado por el usuario.

f. Registros

- Formularios de requerimientos.
- Reportes de REDMINE.
- Correo del usuario.
- Correo de designación Equipo REDMINE

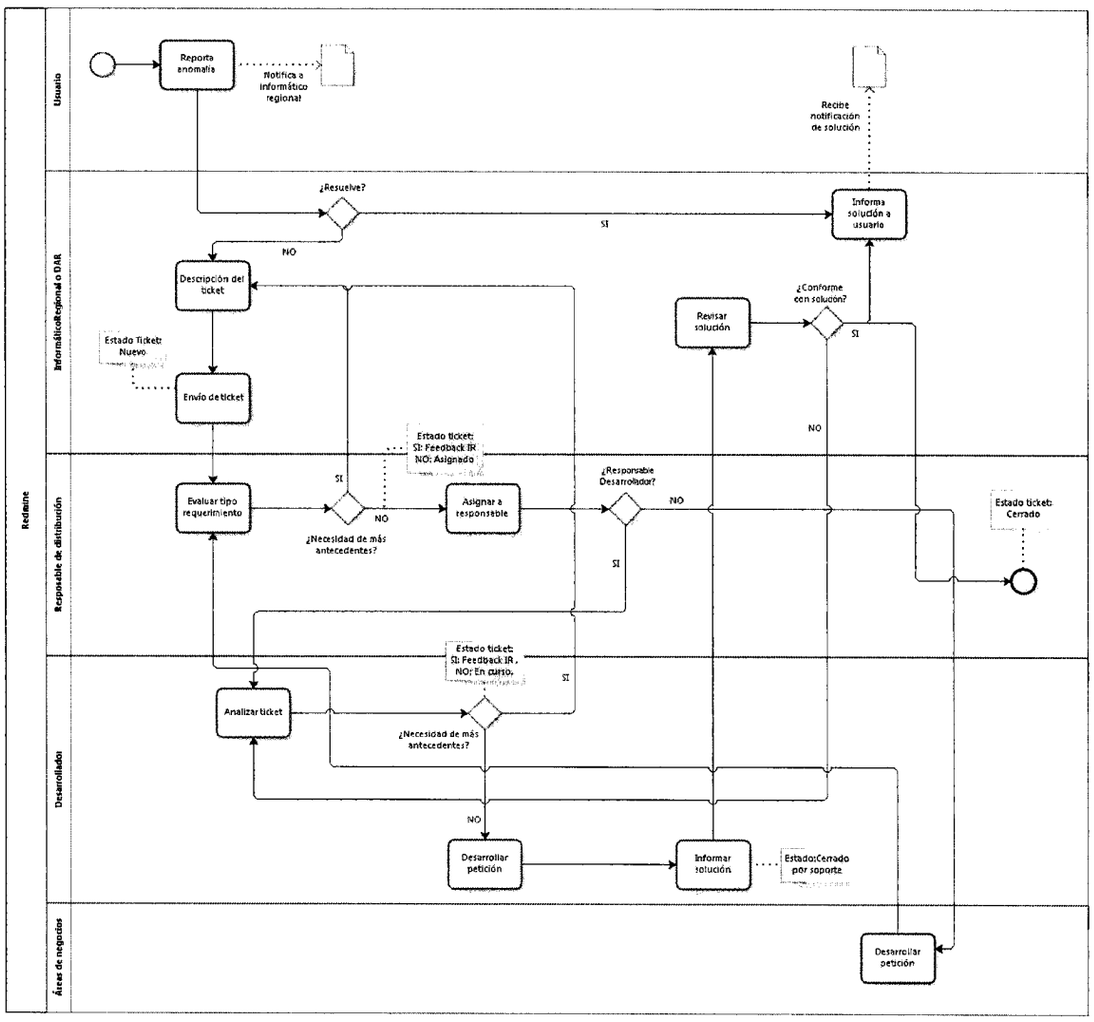
g. Indicador

I = Cantidad de ticket cerrados en el periodo t / Cantidad de ticket ingresados en el periodo t

Se considerará como un buen desempeño un porcentaje de cumplimiento igual o superior al 70% y el cumplimiento parcial menor al 70% y sobre el 60%.

h. Anexos

Anexo A: Flujo de Información



3. Procedimientos de Servicios Informáticos

3.1 Procedimiento de Seguimiento a los Servicios

a. Objetivo

Este procedimiento describe y establece las actividades que se deben ejecutar con el propósito de efectuar un seguimiento a los servicios, en cuanto a disponibilidad, respuesta ante fallas o incidentes y funcionamiento.

b. Alcance

El documento está referido a los servicios de que dispone la Defensoría y se enfoca en determinar si los servicios entregados cumplen los criterios de funcionamiento, es decir, los establecidos en los contratos de prestación del servicio. Además permite obtener una evaluación de los prestadores.

c. Responsabilidades

- **Jefe Departamento de Informática y Estadísticas:** Controlar que se cumpla lo establecido en los contratos de servicios, y establecer los criterios de evaluación de los mismos.
- **Profesionales del área de Operaciones del DIE:** Entregar la retroalimentación necesaria para evaluar los servicios contratados. Efectuar las mediciones de los servicios e informar los resultados de las mediciones y realizar reuniones trimestrales con los proveedores.
- **Encargados de Informática Regional:** Reportar problemas o fallas en los servicios que no se resuelvan a nivel local y en los plazos acordados, entregar información sobre tickets de atención al Encargado del área de Operaciones del DIE y de mantener un registro actualizado de los códigos de atención de los servicios.

d. Descripción de Actividades

1. **Medición Resultado de Funcionamiento:** Trimestralmente deberá efectuarse una medición sobre el funcionamiento de los servicios entregados por el proveedor, este análisis deberá quedar consignado en un informe que contenga lo siguiente:
   - Identificación del Servicio.
   - Especificaciones del Contrato. (Velocidades, SLA, etc.)
   - Tipo de prueba realizada.
   - Resultado de la prueba realizada.
   - Conclusión. (se cumple los especificado en el contrato)
   - Observaciones o recomendaciones.

   Este informe deberá ser validado por el Encargado del área de Operaciones del DIE y remitido al Jefe DIE.

2. **Reunión Trimestral con el Proveedor:** De los Informes de Medición de Funcionamiento de Servicios, será posible obtener información relevante sobre la calidad de servicio y exponerse al proveedor sus resultados. Esta reunión deberá permitir lograr una mayor y mejor coordinación con el proveedor en cuestiones técnicas y administrativas. Una vez realizada la reunión deberá elaborarse una minuta de trabajo, que consigne fecha, participantes, temas tratados y acuerdos (con fecha), la confección de la minuta será de responsabilidad del Encargado de Operaciones del DIE y deberá ser remitida al Jefe DIE.

e. Registros

- Plan de Reuniones Anual, *Anexo A.*
- Informe Medición de Funcionamiento de Servicios, *Anexo A.*
- Minuta Reunión Trimestral con Proveedores, *Anexo B.*

f. Referencias

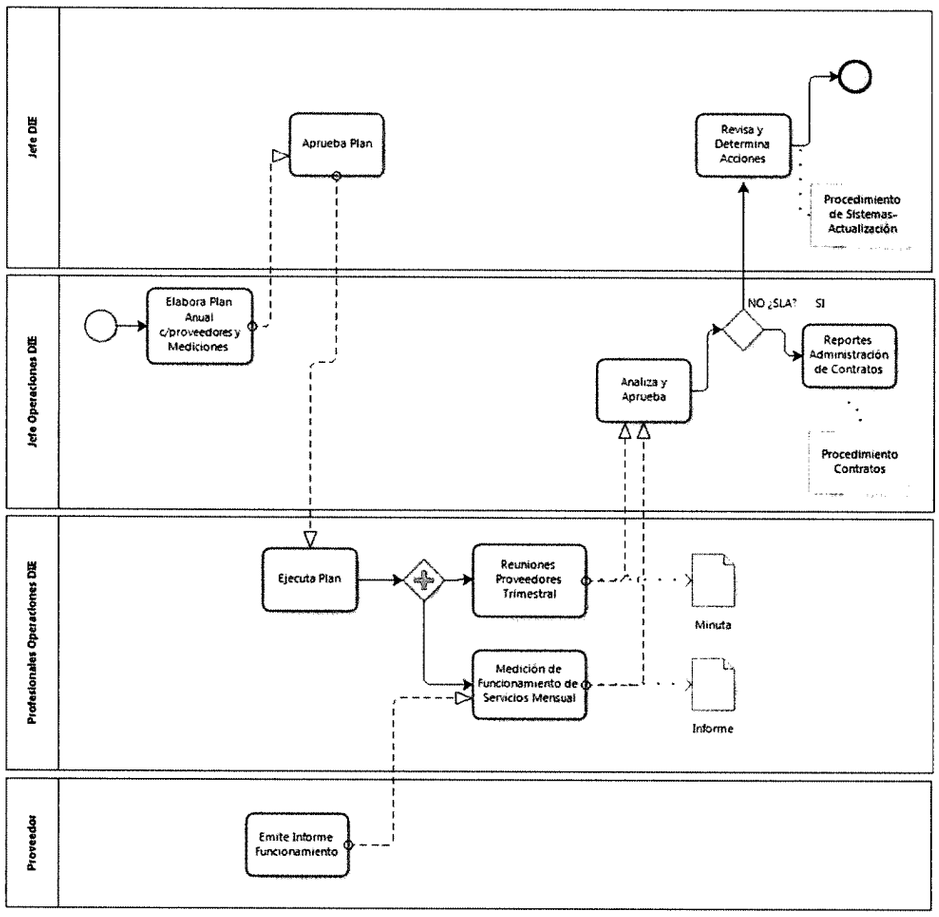
- Contrato de Servicios con los proveedores.

g. Indicadores

- I_{03}= Cantidad de informes emitidos por Operaciones en el año t / Cantidad de informes que corresponden en el año t (4).
- I_{04}= Cantidad de reuniones con los proveedores año t / Cantidad de reuniones con los proveedores que corresponden en el año t (4).
  Nota: Las 4 reuniones son por proveedor.

h. Diagrama de Flujo

Diagrama de Servicios



i. Anexos

Anexo A
Plan de Reuniones y Mediciones

Plan de Reuniones y Mediciones Mensuales

	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre
Servicio de Videconferencia												
1. Medición Servicio de Administracion (cumple/no cumple)												
2. Medicion Mantención Preventiva (cumple/no cumple)												
3. Medición Mantencion Correctiva (cumple/no cumple)												
4. Medicion disponibilidad (eventos y tpo)												
5. Multas												
Reuniones (Marcar fecha)												
Servicio de Telecomunicaciones												
1. Medicion Servicio de Administracion (cumple/no cumple)												
2. Medición Mantencion Preventiva (cumple/no cumple)												
3. Medición Mantención Correctiva (cumple/no cumple)												
4. Medicion disponibilidad (eventos y tpo)												
5. Multas												
Reuniones (Marcar fecha)												
Servicio de Impresoras												
Servicio de Computadores												
Servicio de Plataforma Oracle												
Servicios de Plataforma Virtual												
Servicios MCafee												

Anexo B
Minuta de Reuniones

Defensoría
Sin defensa no hay Justicia

ACTA REUNIÓN DE COORDINACIÓN SOPORTE SIGDP	
Unidad	Departamento de Informática y Estadística.
Tema	Reunión de coordinación para temas .....
Objetivo	

Fecha	Hora Inicio	Hora Término	Lugar
			Videoconferencia

PARTICIPANTES				
N°	**Nombre**	**Inicial**	**Asist.**	**Organización – Área**
1				
2				
3				
4				

TEMAS TRATADOS	
N°	Tema
1	
2	
3	
4	

ACUERDOS DE LA REUNIÓN			
N°	Acuerdo	Responsable	Fecha
1			
2			
3			

3.2 Procedimiento Plan de Contingencia

a. Objetivo

Hacer frente a fallas críticas en los servicios tecnológicos y/o sistemas informáticos principales, disponiendo una copia actualizada de los programas, ambientes operativos y datos, siendo revisado y probado anualmente.

b. Alcance

Esta versión del plan se aplica exclusivamente al servicio de Correo Electrónico[1], clasificado en primer lugar en los rankings de criticidad[2] y de relevancia[3] de los servicios informáticos de la Defensoría Penal Pública, conforme lo informado en el Plan Tecnológico DPP 2012-2016, aprobado mediante RE DN 463 de fecha 26-09-2013; y permite recuperar dicho servicio en condiciones de contingencia ante la ocurrencia de un conjunto de fallas que imposibilite su operación normal en el ambiente contratado al efecto.

c. Responsabilidades

- **Comité Tecnológico:** revisar y dar seguimiento al Plan, con las siguientes responsabilidades:
  1. Revisar y analizar escenarios ante un reporte de falla no resuelta en la prestación del servicio de Correo Electrónico.
  2. Instruir al Jefe del Departamento de Estudios y Proyectos para que informe y coordine a los funcionarios de la Defensoría Penal Pública el paso a un escenario de contingencia.
  3. Instruir al Jefe del Departamento de Informática y Estadística para que active ejecución del Plan de contingencia.
  4. Instruir acciones posteriores de acuerdo al estado de situación reportado.
- **Jefe del Departamento de Informática y Estadística (DIE):** coordinar la aplicación de este plan de contingencia, con las siguientes responsabilidades:
  1. Convocar al Comité Tecnológico.
  2. Liderar el equipo de personas involucrados en la ejecución de las actividades de este procedimiento.
  3. Monitorear la ejecución de las actividades programadas y asegurar que el cronograma y las prioridades establecidas se cumplen.
  4. Informar estado de situación y participar en el Comité Tecnológico.
  5. Emitir informe de resultados de funcionamiento del servicio de Correo Electrónico en condiciones de contingencia.

[1] Contrato aprobado por RE DN 2222 de fecha 26-07-2012, por un plazo de 36 meses o hasta agotar presupuesto de 4200 UTM IVA incluido.
[2] La criticidad de los servicios informáticos se estableció a través de 7 criterios y las siguientes ponderaciones: Necesidad en el funcionamiento diario (20%), Cobertura geográfica (10%), Tipos de usuarios que lo utilizan (15%), Vinculación con la prestación de defensa (10%), Tipo de proceso que apoya (20%), Número de usuarios (10%) y Tiempo máximo de indisponibilidad (15%).
[3] La relevancia de los servicios informáticos se midió mediante una encuesta aplicada a todos los funcionarios, en carácter de voluntaria, entre el 12 y 22 de Octubre 2012.

- **Profesionales de Operaciones del DIE:** con las siguientes responsabilidades:
  1. Ejecutar las actividades de este procedimiento.
  2. Mantener actualizada y almacenada en un ambiente seguro toda la documentación relacionada al servicio de Correo Electrónico.
  3. Mantener informado al Jefe del Departamento.
- **Jefe del Departamento de Estudios y Proyectos de la Defensoría Nacional(DEP):** con las siguientes responsabilidades:
  1. Informar y coordinar a los funcionarios de la Defensoría Penal Pública el paso a un escenario de contingencia.
  2. Participar en el Comité Tecnológico.

e. Descripción de Actividades

- En caso de una contingencia real, tras cumplirse 8 horas sin servicio y desconocer aún las causas que lo provocan:
  1. Convocar al Comité Tecnológico.
  2. Revisar y analizar escenarios ante un reporte de falla no resuelta en la prestación del servicio de Correo Electrónico.
  3. Activar plan de contingencia e informar a los funcionarios de la Defensoría Penal Pública el paso a un escenario de contingencia.
  4. Habilitar ambiente de contingencia y reportar estado de situación de cada una de las actividades que se señalan a continuación al Comité Tecnológico.
  5. Disponer de los respaldos[4] de recuperación.
  6. Crear máquina virtual[5] para ocuparla como servidor de contingencia.
  7. Restaurar la configuración del ambiente operativo del servicio desde los respaldos.
  8. Restaurar la configuración del ambiente de datos del servicio desde los respaldos.
  9. Habilitar servicio de Correo Electrónico en condiciones de contingencia.
  10. Probar correcto funcionamiento.
  11. Publicar el servicio de Correo Electrónico.

- En caso de un ejercicio del plan de contingencia, periodicidad anual:
  1. Fijar fecha para realizar ejercicio.
  2. Notificar al proveedor del servicio de Correo Electrónico.

[4] De acuerdo a lo definido en TTRR del Convenio Marco Grandes Compras N° 13219 publicado con fecha 10-09-2013 y posterior aprobación del contrato por el servicio de Infraestructura Virtual mediante RE DN 630 de fecha 27-12-2013; la Defensoría contará con 22,5 TB en discos de alta capacidad que estarán destinados al almacenamiento de información para sistemas de consulta y la realización de los respaldos primarios de recuperación e históricos, ubicados en el Datacenter. Además, contará con al menos 8 TB en discos para respaldos secundarios de recuperación que formarán parte de un Storage instalado en Sala de Servidores ubicada en dependencias del DIE en Defensoría Nacional; dando cumplimiento a lo señalado en el Manual de Procedimientos Tecnológicos de la Defensoría Penal Pública, capítulo VIII. Política Tecnológica, punto 3. Políticas de Servicios Informáticos, letra f) Política de Respaldo de Sistemas de Información.

[5] De acuerdo a lo definido en TTRR del Convenio Marco Grandes Compras N° 13219 publicado con fecha 10-09-2013 y posterior aprobación del contrato por el servicio de Infraestructura Virtual mediante RE DN 630 de fecha 27-12-2013; la Defensoría contará con 4 (cuatro) servidores para virtualización instalados en el Datacenter, en los que se podrá definir y configurar servidor virtual para la recuperación de los procesos en condiciones de contingencia.

3. Habilitar ambiente de contingencia y reportar estado de situación de cada una de las actividades que se señalan a continuación al Jefe del Departamento de Informática y Estadística.
4. Disponer de los respaldos de recuperación.
5. Crear máquina virtual para ocuparla como servidor de contingencia.
6. Restaurar la configuración del ambiente operativo del servicio desde los respaldos.
7. Restaurar la configuración del ambiente de datos del servicio desde los respaldos.
8. Habilitar servicio de Correo Electrónico en condiciones de contingencia.
9. Probar correcto funcionamiento.
10. Emitir informe de resultados de ejercicio del servicio en condiciones de contingencia, una semana después de efectuado el ejercicio.

j. Registros

- Informe de resultados de ejercicio del servicio de Correo Electrónico en condiciones de contingencia.

k. Referencias

- Manual de Procedimientos DPP, RE DN 439 de fecha 29-08-2013.
- Contrato Servicio de Housing, RA DN 61 de fecha 16-04-2012.
- Contrato del Servicio de Infraestructura Virtual, RE DN 630 de fecha 27-12-2013.
- Contrato de Servicio de Correo Electrónico, RE DN 2222 de fecha 26-07-2012.

l. Indicadores

- No hay.

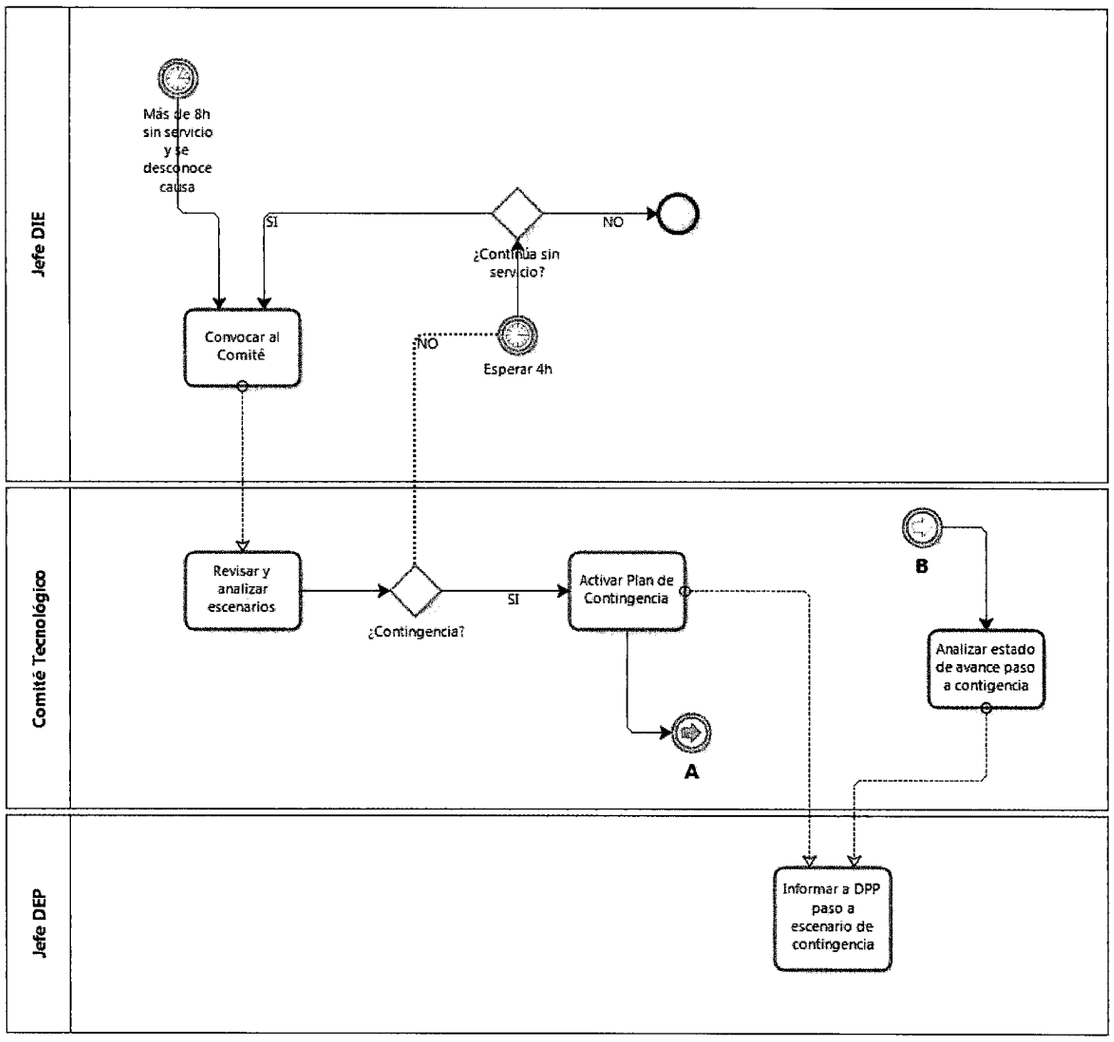
m. Diagrama de Flujo

- Ver anexos A y B.

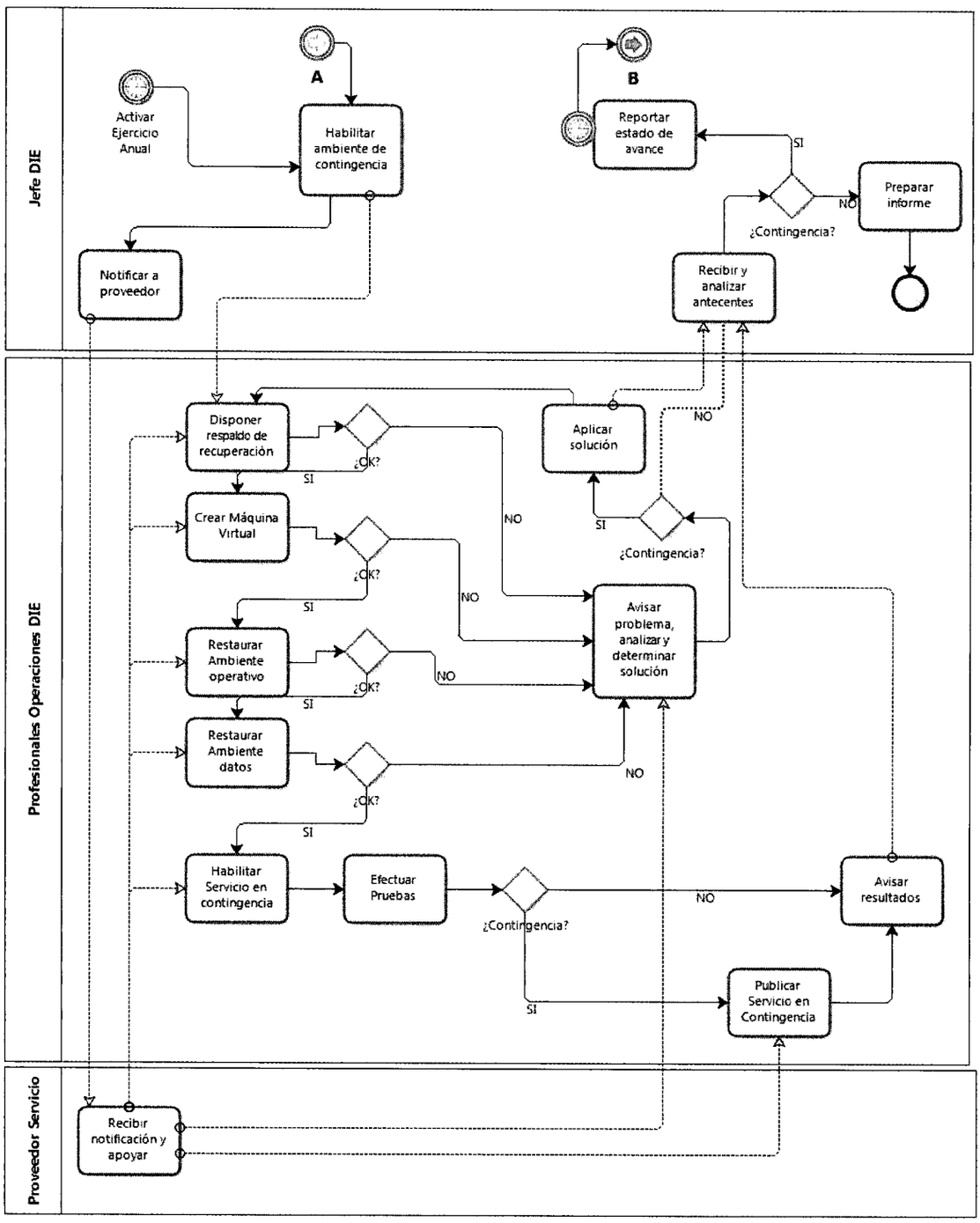
n. Anexos

- Activación del Plan de Contingencia del servicio de Correo Electrónico.
- Habilitación de ambiente de contingencia del servicio de Correo Electrónico.

Anexo A: Activación del Plan de Contingencia del servicio de Correo Electrónico



Anexo B: Habilitación de ambiente de contingencia del servicio de Correo Electrónico



4. Procedimiento de Sistemas de Información

a. Objetivo

Describir las acciones que deberán ser efectuadas por el DIE de manera de garantizar el desarrollo de sistemas bajo los estándares definidos por la Institución y de acuerdo al Plan Tecnológico.

b. Alcance

Este documento describe desde la clasificación de los sistemas, que permite determina su nivel de relevancia para la asignación de recursos que podrá ser un insumo para la elaboración de Planes de Continuidad Operacional hasta el desarrollo y mantención de sistemas, que describe la metodología para el desarrollo de aplicaciones, pruebas necesarias a la entrada en operaciones y el respaldo. Y Finalmente la instalación de versiones nuevas y actualizaciones de software.

c. Responsabilidades

- **Comité Tecnológico:** Sancionar el *Plan de Desarrollo*, determinar prioridad y recursos disponibles.
- **Jefe Departamento de Informática y Estadísticas:** Entregar los requerimientos y su factibilidad al Comité Tecnológico para que sean sancionados. Revisar y aprobar el *Plan anual de Mantención y Actualización de Software* y el *Plan de Desarrollo*.
- **Profesionales del área de Desarrollo del DIE:** Analizar la factibilidad de los requerimientos, hacer una ficha de los proyectos y ejecutar el proceso de desarrollo.
- **Profesionales del área de Operaciones del DIE:** Apoyar la instalación de nuevas versiones o actualizaciones de software.

d. Descripción de Actividades

1. **Clasificación de Sistemas:** Para establecer la relevancia en los sistemas de la institución y poder definir políticas y planes de continuidad, se determinaron criterios de medición, estos criterios se encuentran descritos en la Política de Categorización de Sistemas Informáticos.

    a. Sistemas Alto Impacto: Considera los sistemas que se relacionan con el negocio de la organización. En esta categoría quedan los sistemas: SIGDP, SIGMOE, SIAR y SIACD.

    b. Sistemas Impacto Medio: Considera los sistemas que relacionándose con el negocio, provocan un impacto medio o de carácter estacional en la organización. En esta categoría quedan: SEGFAC, Experiencia Profesional, SIG, Centro de Contactos Defensores, Preinscripción, Carga de Trabajo, Reporte Inconsistencias y Simulador de Ofertas.

c. Sistemas de Bajo Impacto: Considera los sistemas que provocan un bajo nivel de impacto a nivel de la organización, o su impacto es altamente focalizados solo en alguna unidad. En esta categoría quedan los 21 sistemas restantes identificados.

2. **Levantamiento de Requerimientos:** El Comité Tecnológico establece la prioridad a los requerimientos que se van a llevar a desarrollar. Este proceso se inicia con el informe de requerimientos conforme el Procedimiento de Uso de Servicios Informáticos vía REDMINE. Para dar un ordenamiento a las solicitudes y priorizar se efectuará una evaluación de la factibilidad técnica y económica que será de responsabilidad del DIE, la que será presentada al Comité, una vez formalizada la prioridad del requerimiento se deberá notificar a los involucrados por un medio formal de la decisión del Comité.

3. **Desarrollo de Sistemas:** El Encargado del área de Desarrollo del DIE deberá coordinar y gestionar la ejecución de las actividades programadas. Las cuales se efectuarán en un ambiente de desarrollo y testing, según corresponda.

4. **Prueba de Sistemas:** Esta etapa del proceso de desarrollo de software permitirá asegurar que el software cumpla con las especificaciones requeridas y eliminar los errores. El Encargado del área de desarrollo deberá entregar al grupo QA (Quality Assurance; aseguramiento de calidad) el software o nueva funcionalidad para su revisión, los casos de prueba y el Plan de Pruebas.

   a. Casos de Prueba: Se deberá disponer de distintos tipos de casos, bajo diferentes condiciones o variables, y que sean requisito para el funcionamiento de la aplicación, los casos deberán cubrir todas las funcionalidades solicitadas, mínimo deberá existir un caso por funcionalidad. Los casos deberán ser definidos en la etapa anterior a la prueba, para no producir retrasos en la etapa de prueba. Para ello el grupo QA debe interiorizarse en las funcionalidades con los usuarios requirentes.

   b. Plan de Pruebas: Corresponde a la planificación que debe realizar el grupo QA durante la cual se efectuarán los casos de prueba y otras pruebas funcionales que se consideren necesarias. El Plan deberá contener plazos e identificar a los usuarios que formarán parte de esta actividad. El resultado deberá quedar documentado, indicando nombre del proyecto, alcance, participantes, resultado de los casos de prueba y cualquier otra información relevante. Y se deberá indicar claramente los errores detectados así como las variables utilizadas. Esta información es valiosa para los desarrolladores. En caso de no existir errores, el Encargado de Desarrollo realizará las gestiones con los usuarios requirentes del sistema para las pruebas finales y su posterior paso a producción.

   c. Equipo de Pruebas: Este equipo está compuesto por un grupo de usuarios designados para este propósito.

5. **Respaldo de Sistemas**

a. Se contempla el respaldo de las aplicaciones, configuraciones de aplicaciones, bases de datos operacionales y bases de datos del correo electrónico.

b. Software de respaldo: NetVault Backup, solución de respaldo y recuperación que permite proteger los datos en diversos entornos, desde una consola intuitiva; escalable y soporta múltiples plataformas de servidores y aplicaciones.

c. Políticas de respaldo
Los tipos de respaldos a efectuar en el servicio son:
- Respaldos de recuperación
  - Primarios: Deben garantizar la continuidad operacional, escritos a disco.
  - Secundarios: Réplica del respaldo primario, efectuado en un medio de almacenamiento ubicado fuera de las dependencias del Housing.
  - Respaldos Históricos: Orientado a guardar información para consultas que puedan requerirse en el futuro.

- Periodicidad de los respaldos y ejercicios de restauración:
  - Bases de datos: diario.
  - Aplicaciones y configuraciones: mensual.
  - Ejercicios de restauración; semestral.
  - Tiempo de retención de los respaldos: para las bases de datos, 1 mes; para programas y configuraciones, 3 meses; históricos, 10 años.

6. **Nuevas Versiones o actualizaciones de software:** El software utilizado por la Defensoría deberá ser revisado al menos una vez al año, de manera de garantizar la utilización de versiones actualizadas.

7. **Mantención y actualización de Sistemas:** Los sistemas que requieran de mantenimiento deberán ser incorporados en la planificación anual, se deberá incorporar en alguna de las cláusulas de los contratos la mantención y actualización.

8. **Instalación software público:** La instalación deberá efectuarla el Encargado de Informática Regional o personal del DIE, según corresponda.

e. Registros

- Plan anual de Mantención y Actualización de Software, carta Gantt.
- Plan de Pruebas, formato libre.
- Plan de Desarrollo Semestral, Carta Gantt.
- Plan de Continuidad, formato vigente.
- Plan Tecnológico, formato vigente.

f. Referencias

- No hay.

g. Indicadores

- No hay.

h. Diagrama de Flujo

Diagrama de Proceso de Desarrollo de un Requerimiento

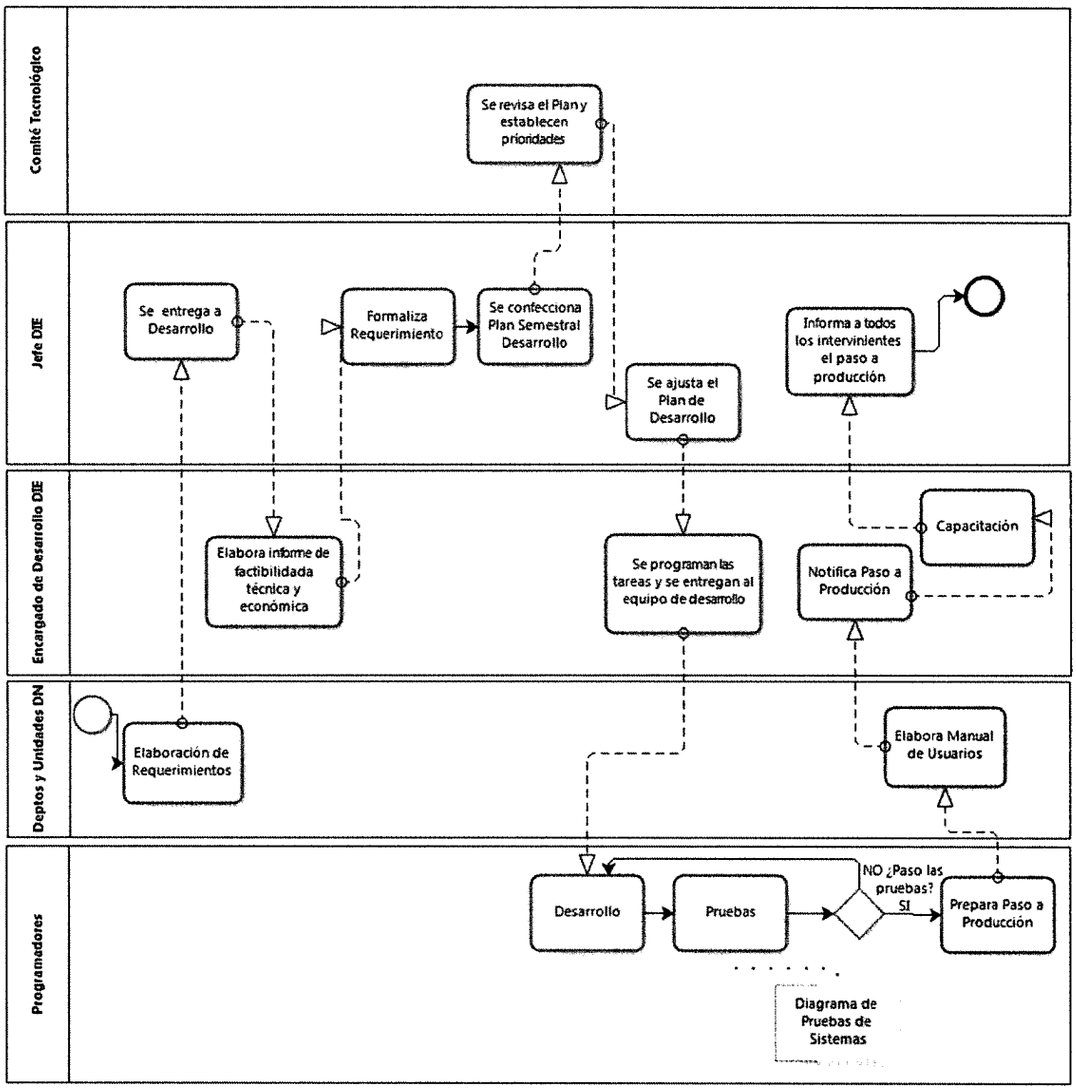
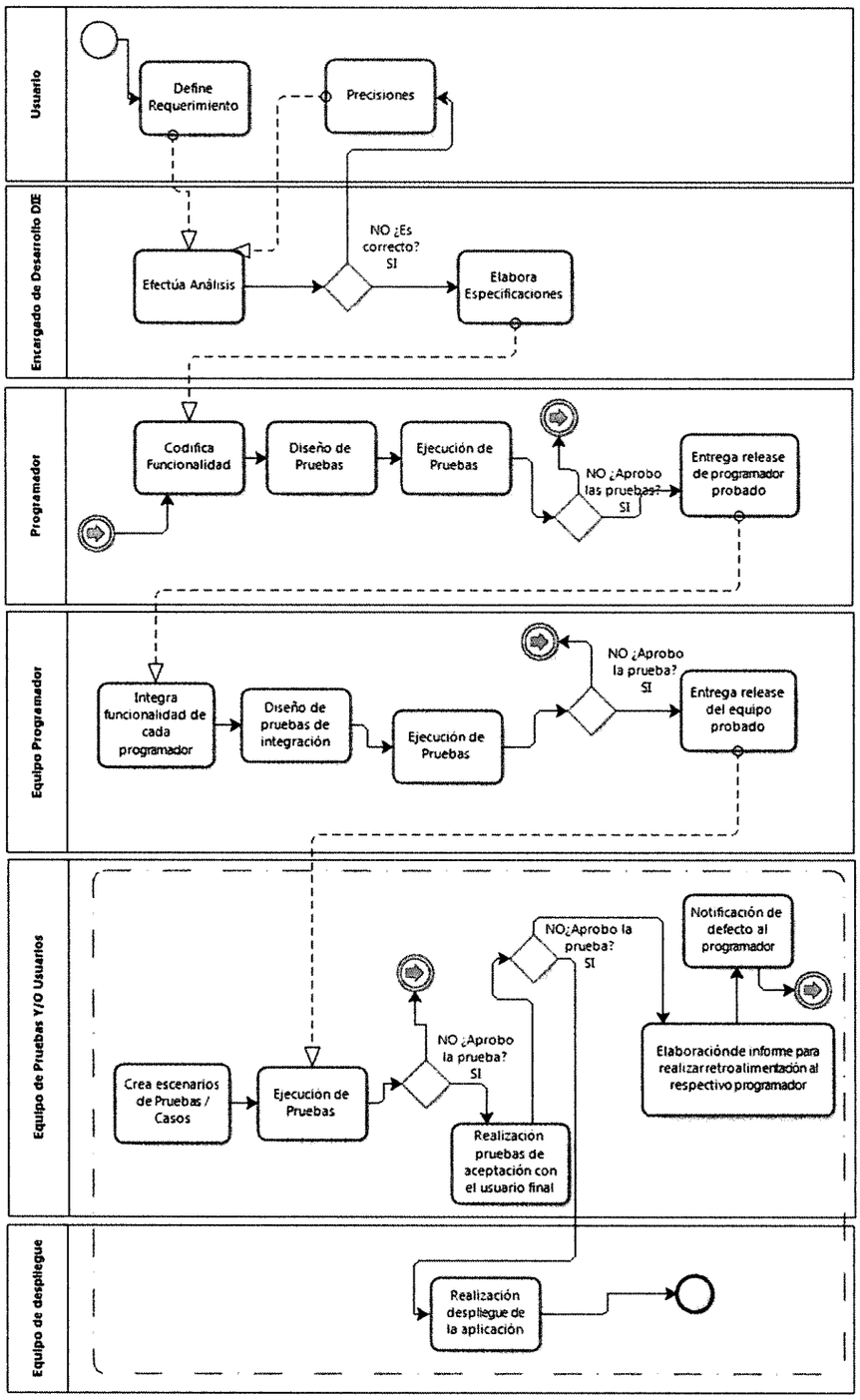


Diagrama de Pruebas de Sistemas



i. Anexos

- No hay

5. Procedimientos de Contrataciones

5.1 Procedimiento de Gestión de Contratos

a. Objetivo

Describir las actividades necesarias para una adecuada gestión de contratos de servicios, recepción oportuna y efectiva de los bienes y servicios, y seguimiento de los servicios adicionales contratados.

b. Alcance

Este procedimiento abarca la gestión de contratos nuevos y vigentes, la evaluación presupuestaria de los contratos, el seguimiento de los plazos, pagos y cumplimiento. Donde intervienen principalmente el DIE y la DAF.

c. Base Legal

- Ley 19.886 de Compras Públicas y su reglamento aprobado por el Decreto Supremo N°250, de 2004, del Ministerio de Hacienda.

d. Responsabilidades

- **Jefe Departamento de Informática y Estadísticas:** Velar por el cumplimiento de las leyes que regulan las compras públicas. Controlar el cumplimiento de los contratos de servicios. Gestionar la elaboración de las bases de licitación para la provisión o mantención de los servicios que requiere la institución en materia tecnológica.
- **Administrador de Contratos DIE:** Elaboración de los contratos de servicios y control de los pagos de los contratos vigentes. Control del gasto presupuestario del DIE. Y Contraparte de la Defensoría con los Proveedores de bienes o servicios.
- **Departamento de Administración y Finanzas:** Proveer de los recursos financieros necesarios que aseguren la continuidad de los servicios. Remitir facturas para autorizar el pago.
- **Unidad de Asesoría Jurídica:** Velar por el cumplimiento de la normativa vigente relativa a los contratos que suscriba la Defensoría.

e. Descripción de Actividades

La gestión de los contratos es una actividad permanente, y tiene actividades que son claves para el proceso de compra, que son:

- Elaboración de contratos.
- Definición de roles y responsabilidades.
- Gestión con el proveedor.
- Entrega del servicio.
- Gestión de pago.
- Modificaciones de los contratos
- Registrar y evaluar el contrato.

1. **Gestión de contratos nuevos**: Esta etapa del proceso permite evaluar la pertinencia de la contratación de un bien o servicio, los recursos disponibles y necesarios, y las condiciones. Se hace una diferenciación entre una contratación compleja de una simple, donde la primera involucra una importancia estratégica y el monto que involucra es alto.

   En el caso de contrataciones simples, el procedimiento de la adquisición será a través del Catálogo Electrónico del Convenio Marco, donde el documento que compromete la compra es la solicitud de compra del DIE dirigida a la DAF. Si la contratación se efectúa mediante el procedimiento de trato directo, está será realizada a través de resolución fundada que la autoriza y con la respectiva orden de compra.

   Las contrataciones complejas deberán materializarse a través de un contrato que permita un control adecuado sobre los bienes o servicios adquiridos, para lo cual se utilizará el sistema de convenio marco, licitación pública o privada y excepcionalmente se podrá efectuar un trato directo conforme lo establece la normativa de Compras Públicas. La licitación de un proceso se efectuará una vez identificados los requerimientos y confeccionadas las bases de licitación, en este proceso intervienen el DIE, DAF y la Unidad de Asesoría Jurídica.

   - Presupuesto: Una vez al año el DIE solicitará a la DAF el presupuesto para mantener en funcionamiento la plataforma tecnológica de la Defensoría y los servicios de que dispone, además de incorporar recursos para los proyectos que deban ser implementados.

   - Plazos y Pagos: El plazo para el inicio del proceso de contratación de nuevos servicios, será de 6 meses antes del término del contrato vigente.

2. **Gestión de Contratos Vigentes**: Para el control de la gestión los contratos vigentes será necesario tener un registro de los pagos, plazos. La mantención y actualización estará a cargo del Encargado de Administrar los Contratos.

f. Registros

- Registro de los contratos vigentes, planilla Excel.

g. Referencias

- Ley de Compras Públicas y Reglamento.
- Procedimientos de Compra de la DAF.

h. Indicadores

- I_{05}= Cantidad de procesos de contratación iniciados 6 meses antes / Cantidad de procesos efectuados en el año t.

i. Diagrama de Flujo

Diagrama de Proceso Nuevas Contrataciones y Vencimiento de Contratos

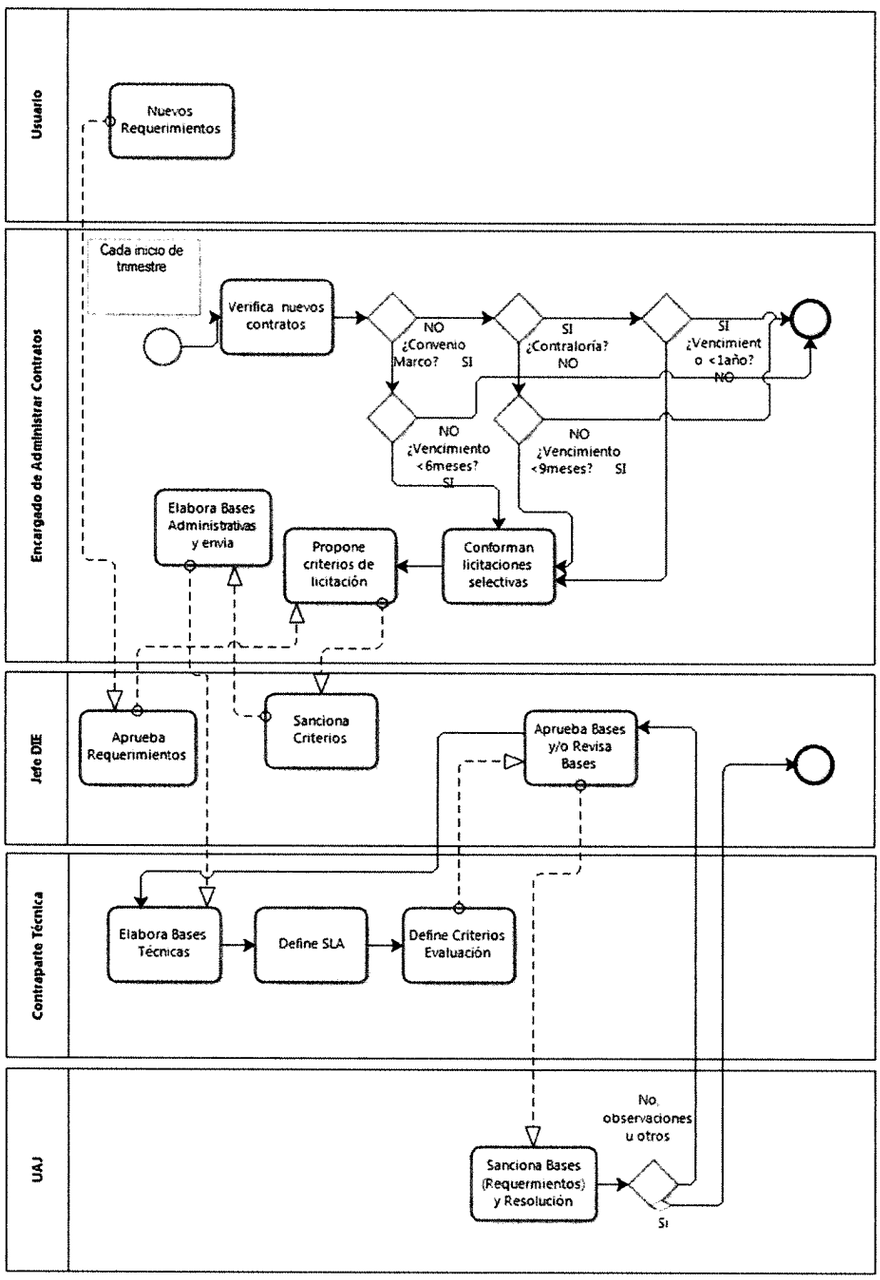
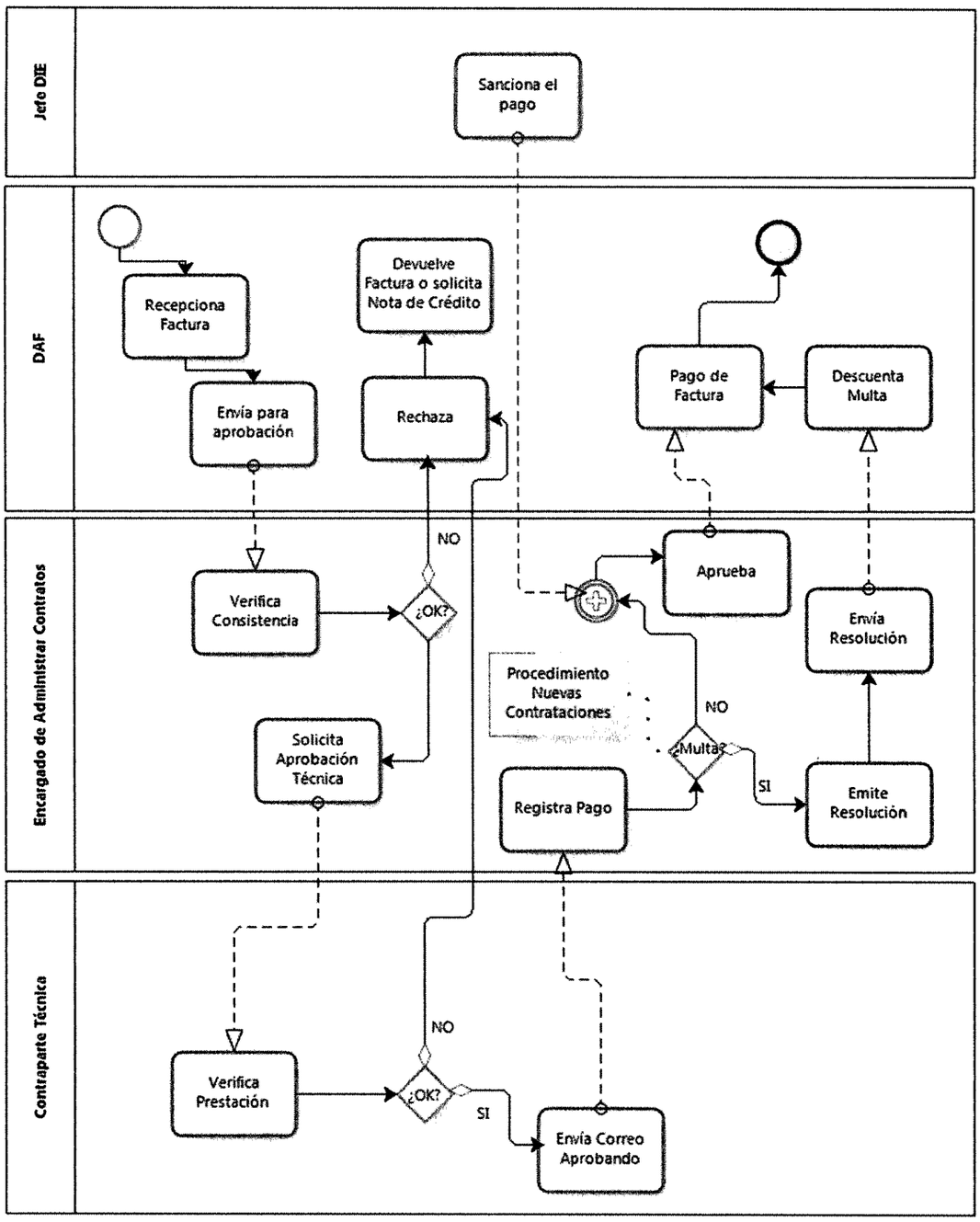


Diagrama de Proceso de Pago



j. Anexos

- No hay

5.2 Procedimiento Validación de Gastos Variables Telefonía Móvil

a. Objetivo

Describir las actividades necesarias para una adecuada revisión y validación de facturas de gastos variables en contratos administrados por el Departamento de Informática y Estadísticas, en adelante "DIE", que permitan certificar con elementos concretos si deben autorizarse para pago, buscando mitigar situaciones de riesgo que pudieran presentarse.

b. Alcance

Este procedimiento se aplica al siguiente contrato de servicio:

- Telefonía Móvil y Servicios Asociados, con la empresa ENTEL PCS Telecomunicaciones S.A. -en adelante "ENTEL PCS"-, aprobado mediante Resolución Exenta N° 396, de fecha 4 de Julio de 2014.

c. Base Legal

- Ley N° 19.886 de Bases sobre Contratos Administrativos de Suministro y Prestación de Servicios y su Reglamento.
- "Procedimiento de Pago a Proveedores y Control para su Seguimiento", aprobado mediante Resolución Exenta N° 2559, de fecha 27 de Agosto de 2010.
- Bases Administrativas y Técnicas y Anexos de Licitación Pública ID 1876-4-LP14 para la contratación del Servicio de Telefonía Móvil y Servicios Asociados, aprobadas mediante Resolución Exenta N° 161, de fecha 14 de Marzo de 2014.
- Ofertas Técnica y Económica de la empresa ENTEL PCS de fecha 15 de Abril de 2014, incluyendo todos los anexos y documentación presentada.
- Resolución Exenta N° 239, de fecha 7 de Mayo de 2014, que adjudica contratación del Servicio de Telefonía Móvil y Servicios Asociados a la empresa ENTEL PCS.
- Resolución Exenta N° 396, de fecha 4 de Julio de 2014, que aprueba contrato por el Servicio de Telefonía Móvil y Servicios Asociados a la empresa ENTEL PCS.

d. Responsabilidades

- **Jefe DIE**: Autorizar el pago de facturas en contratos administrados por el DIE.
- **Contraparte Técnica DIE**: Informar la existencia / inexistencia de inconvenientes que incidan en el pago y que permitan autorizar el pago de la factura.
- **Contraparte Administrativa DAF**: Coordinar el pago de las respectivas facturas.
- **Administrador de Contratos DIE**: Gestionar, administrar y velar por el fiel cumplimiento de los contratos y facturaciones, correspondientes a servicios administrados por el DIE.
- **DARES y Jefes de la Defensoría Nacional**: Autorizar los traspasos de dinero asociados a los gastos que deben ser cubiertos por sus centros de costo.

e. Descripción de Actividades

La revisión y validación de facturas de gastos variables es una actividad permanente durante toda la etapa de operación del contrato hasta su término completo y conforme, y consta de las siguientes actividades para el contrato referido en el alcance:

- Recibir detalle de llamadas.
  - Proveedor genera planilla Excel con detalle de facturación y lo deja disponible a través del Sistema de Gestión Online (SGO).
- Recibir factura de gastos variables.
  - Proveedor prepara y envía factura a Defensoría.
  - Contraparte Administrativa DAF valida aspectos formales, pago al día de cotizaciones previsionales de sus trabajadores dependientes y estado hábil en Chileproveedores; comunicando al proveedor en caso de problemas, para que éste los resuelva.
  - Si no hay problemas, Contraparte Administrativa DAF envía correo electrónico a Administrador de Contratos DIE con copia escaneada de factura para su validación.
- Validar factura de gastos variables.
  - Administrador de Contratos DIE valida aspectos formales: periodo de prestación de servicios, fecha de facturación y glosa de factura.
  - Contraparte Técnica DIE informa la existencia / inexistencia de inconvenientes que incidan en el pago y que permitan autorizar el pago de la factura.
  - Administrador de Contratos DIE valida detalle de facturación rescatado desde SGO y compara con valor total facturado. Con todo lo demás OK, se darán por aprobadas facturas con diferencias menores a 100 pesos.
  - Administrador de Contratos DIE analiza detalle de facturación y determina los gastos que deben ser cubiertos por Defensorías Regionales y Departamentos y Unidades de la Defensoría Nacional por tratarse de servicios especiales: consumo en exceso de Mensajes de Texto, servicios de Roaming solicitados y servicios de Telefonía Satelital solicitados.
- Aprobar o rechazar factura de gastos variables.
  - Administrador de Contratos DIE informa propuesta de resultado al Jefe DIE y solicita confirmación, informa por correo electrónico a Contraparte Administrativa DAF -avisando aprobación, detallando servicios normales y especiales, y recordando Notas de Crédito y Multas pendientes de aplicar-, y registra en planilla Excel la validación del gasto variable y el posterior pago de la factura.
  - En caso de aprobación, Contraparte Administrativa DAF gestiona su pago e informa a los Directores Administrativos Regionales y Jefes Defensoría Nacional traspasos de dinero a efectuar para cubrir servicios especiales.
  - En caso de rechazo, Contraparte Administrativa DAF avisa al proveedor para que corrija lo que sea necesario y envíe nuevamente la factura y/o nota de crédito si corresponde.

f. Registros

- Detalle de facturación, planilla Excel.
- Validación y pago de facturas de gastos variables, planilla Excel.

g. Referencias

- Ley de Compras Públicas y Reglamento.
- Procedimiento de Pago a Proveedores y Control para su Seguimiento (DAF).

h. Indicadores

- No hay.

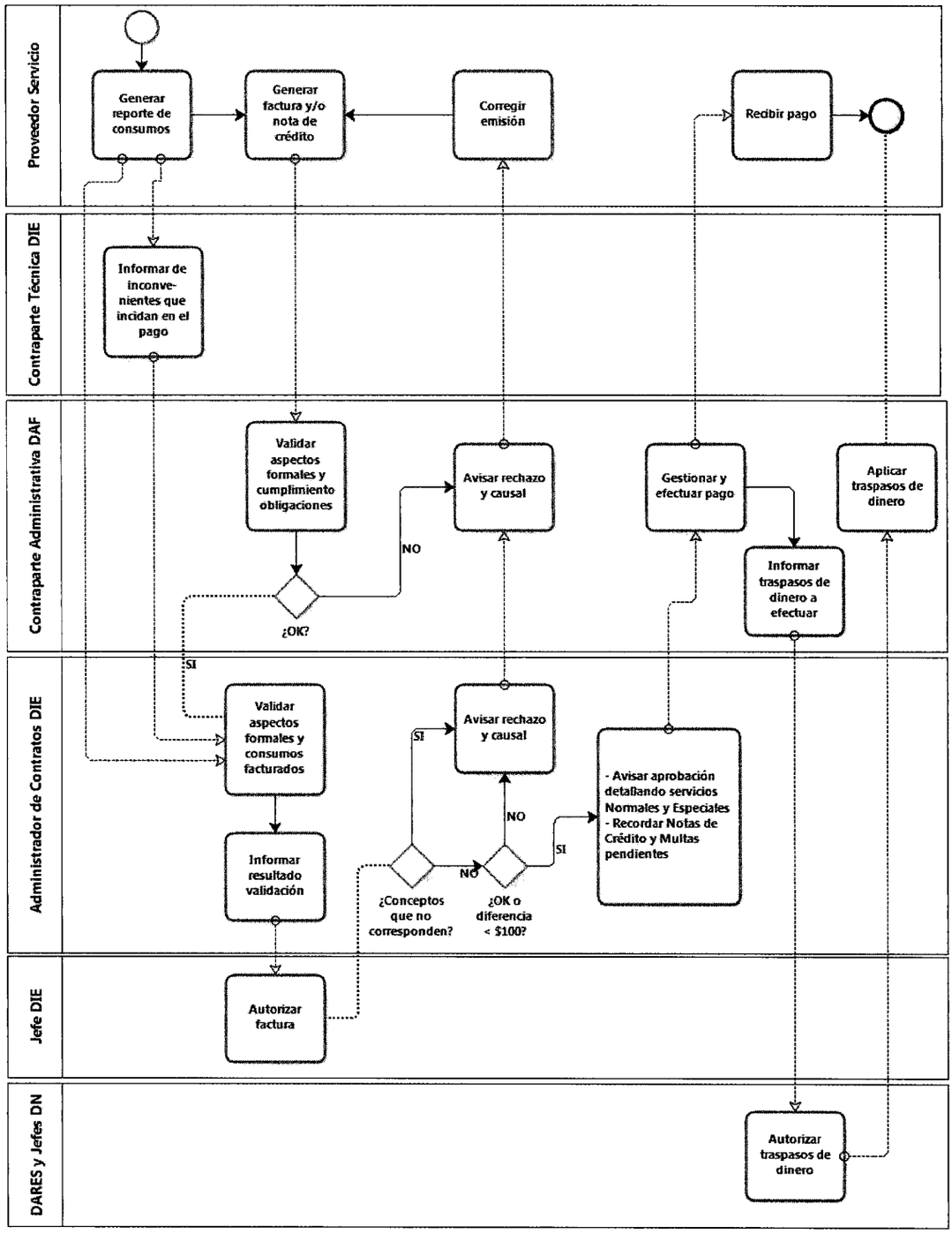
i. Diagrama de Flujo

- Ver Anexo A.

j. Anexos

- Anexo A: Diagrama Validación de Gastos Variables Telefonía Móvil.

Anexo A
Diagrama Validación de Gastos Variables Telefonía Móvil



5.3 Procedimiento Validación de Gastos Variables Impresión

a. Objetivo

Describir las actividades necesarias para una adecuada revisión y validación de facturas de gastos variables en contratos administrados por el Departamento de Informática y Estadísticas, en adelante "DIE", que permitan certificar con elementos concretos si deben autorizarse para pago, buscando mitigar situaciones de riesgo que pudieran presentarse.

b. Alcance

Este procedimiento se aplica al siguiente contrato de servicio:

- Arriendo de Máquinas Multifuncionales e Impresoras, con la empresa STUEDEMANN S.A. -en adelante "OFIMUNDO"-, aprobado mediante Resolución Exenta N° 97 de fecha 31 de Enero de 2014.

c. Base Legal

- Ley N° 19.886 de Bases sobre Contratos Administrativos de Suministro y Prestación de Servicios y su Reglamento.
- "Procedimiento de Pago a Proveedores y Control para su Seguimiento", aprobado mediante Resolución Exenta N° 2559 de fecha 27 de Agosto de 2010.
- Bases de Licitación ID 2239-9-LP11 del Convenio Marco "Impresoras y Arriendo de Impresoras", suscrito por la Dirección de Compras y Contratación Pública.
- Términos de Referencia para el Servicio de Arriendo de Máquinas Multifuncionales e Impresoras, a través de Publicación N° 14501 de fecha 2 de Diciembre de 2013, bajo la modalidad de Grandes Compras.
- Ofertas Técnica y Económica de la empresa OFIMUNDO de fecha 12 de Diciembre de 2013, incluyendo todos los anexos y documentación presentada.
- Resolución Exenta N° 01, de fecha 2 de Enero de 2014, que adjudica contratación del Servicio de Arriendo de Máquinas Multifuncionales e Impresoras a la empresa OFIMUNDO.
- Resolución Exenta N° 97, de fecha 31 de Enero de 2014, que adjudica contratación del Servicio de Arriendo de Máquinas Multifuncionales e Impresoras a la empresa OFIMUNDO.

d. Responsabilidades

- **Jefe DIE**: Autorizar el pago de facturas en contratos administrados por el DIE.
- **Contraparte Técnica DIE**: Informar la existencia / inexistencia de inconvenientes que incidan en el pago y que permitan autorizar el pago de la factura.
- **Contraparte Administrativa DAF**: Coordinar el pago de las respectivas facturas.
- **Administrador de Contratos DIE**: Gestionar, administrar y velar por el fiel cumplimiento de los contratos y facturaciones, correspondientes a servicios administrados por el DIE.

e. Descripción de Actividades

La revisión y validación de facturas de gastos variables es una actividad permanente durante toda la etapa de operación del contrato hasta su término completo y conforme, y consta de las siguientes actividades para el contrato referido en el alcance:

- Recibir reporte de consumos.
  - Proveedor genera planilla Excel con reporte de consumos y lo envía por correo electrónico a Contraparte Técnica DIE.
- Validar reporte de consumos.
  - Contraparte Técnica DIE valida reporte de consumos: en sí mismo, comparando con meses anteriores, comparando con información que entrega el Sistema de Gestión de Equipos y comparando -cada 3 meses- con una muestra al azar de contadores obtenidos en terreno.
- Aprobar o rechazar reporte de consumos.
  - Contraparte Técnica DIE avisa al proveedor su aprobación o rechazo.
  - Si aprueba, proveedor debe preparar y enviar factura.
  - Si rechaza, proveedor debe corregir y enviar nuevamente reporte de consumos.
- Recibir factura de gastos variables.
  - Proveedor prepara y envía factura a Defensoría.
  - Contraparte Administrativa DAF valida aspectos formales, pago al día de cotizaciones previsionales de sus trabajadores dependientes y estado hábil en Chileproveedores; comunicando al proveedor en caso de problemas, para que éste los resuelva.
  - Si no hay problemas, Contraparte Administrativa DAF envía correo electrónico a Administrador de Contratos DIE con copia escaneada de factura para su validación.
- Validar factura de gastos variables.
  - Administrador de Contratos DIE valida aspectos formales: periodo de prestación de servicios, fecha de facturación, valor de UF utilizado y glosa de factura.
  - Administrador de Contratos DIE valida consumos informados, valores unitarios y valor total facturado. Con todo lo demás OK, se darán por aprobadas facturas con diferencias menores a 100 pesos.
- Aprobar o rechazar factura de gastos variables.
  - Administrador de Contratos DIE informa propuesta de resultado al Jefe DIE y solicita confirmación, informa por correo electrónico a Contraparte Administrativa DAF (recordando Notas de Crédito y Multas pendientes de aplicar) y registra en planilla Excel la validación del gasto variable y el posterior pago de la factura.
  - En caso de aprobación, Contraparte Administrativa DAF gestiona su pago.
  - En caso de rechazo, Contraparte Administrativa DAF avisa al proveedor para que corrija lo que sea necesario y envíe nuevamente la factura.

f. Registros

- Reporte de consumos, planilla Excel.
- Validación y pago de facturas de gastos variables, planilla Excel.

g. Referencias

- Ley de Compras Públicas y Reglamento.
- Procedimiento de Pago a Proveedores y Control para su Seguimiento (DAF).

h. Indicadores

- No hay.

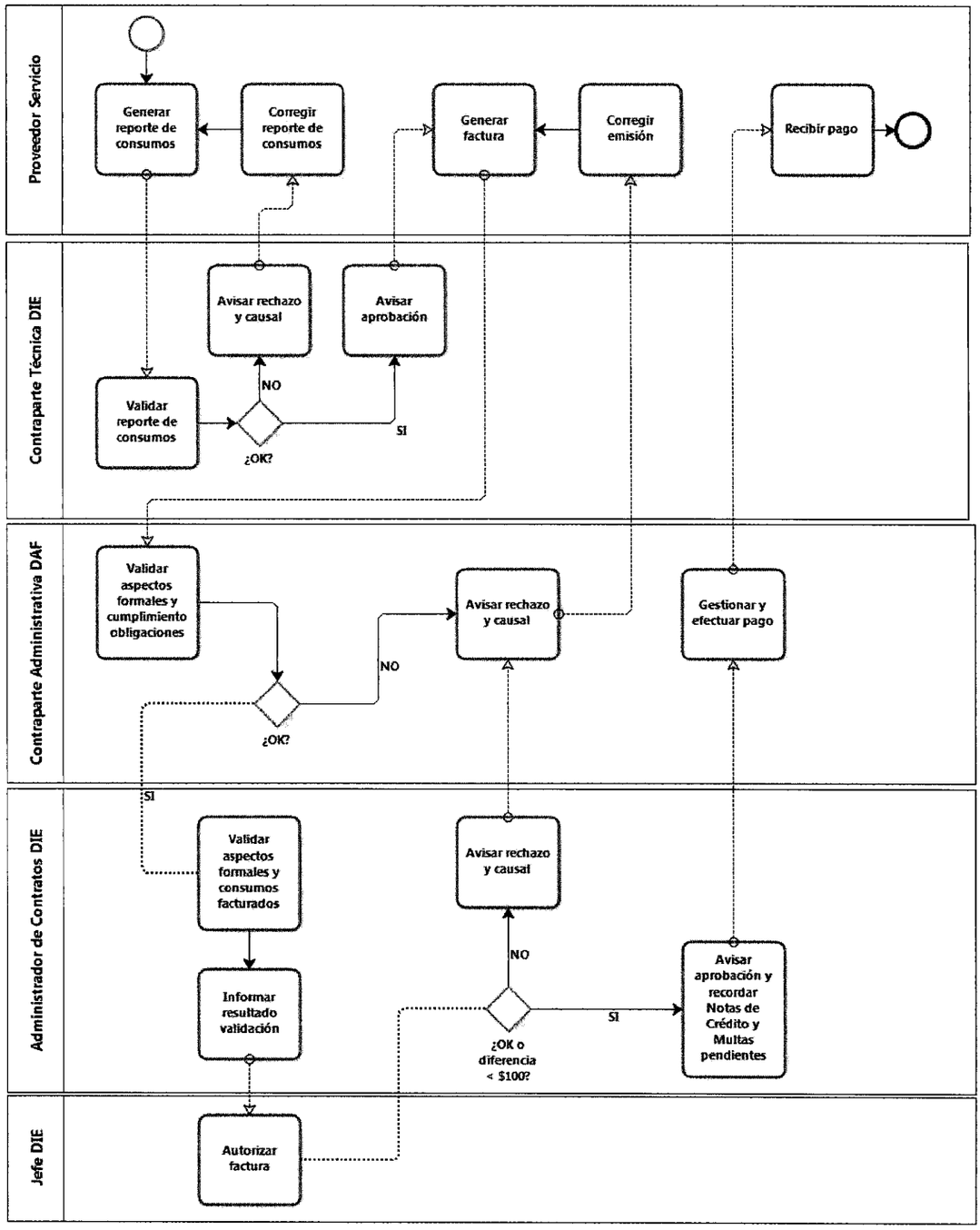
i. Diagrama de Flujo

- Ver Anexo A.

j. Anexos

- Anexo A: Diagrama Validación de Gastos Variables Impresión.

Anexo A
Diagrama Validación de Gastos Variables Impresión



6. Procedimiento de Acceso de Internet

a. Objetivo

Delimitar los permisos de acceso de los usuarios a los contenidos de páginas web y el entorno web, de forma de garantizar un adecuado uso de los recursos de comunicaciones y enlaces.

b. Alcance

Este documento se aplica a todos los usuarios, por cuanto describe los niveles de acceso a páginas web, define restricciones y permisos.

c. Responsabilidades

- **Jefe Departamento de Informática y Estadísticas:** Entregar los lineamientos y criterios para el acceso de los usuarios al entorno WEB.
- **Encargado del área de Desarrollo del DIE:** Implementar las medidas de seguridad necesarias en los sistemas informáticos que se publiquen en el entorno WEB.
- **Encargado del área de Operaciones del DIE:** Implementar y configurar el entorno WEB utilizado por los usuarios y garantizar que cuente con los recursos necesarios para su funcionamiento.

d. Descripción de Actividades

- **Limitaciones, restricciones y permisos de acceso:** Las restricciones que se impongan al acceso de los usuarios a páginas web van a estar determinadas por la capacidad del enlace y el nivel de confiabilidad que se tenga del contenido. Se dará privilegio al acceso a páginas WEB de contenido seguro y cuya materia esté relacionada con el quehacer de la Defensoría.

- **Alta de servicios y sistemas (publicación):** Los sistemas informáticos que deban ser publicados en el ambiente WEB de la Defensoría deberán tener los resguardos necesarios que proporcionen un ambiente seguro y confiable. Para lo cual se establecerá un sistema de autenticación de usuarios, es decir, los sistemas deberán utilizar usuario y contraseña. En el caso de las páginas WEB Intranet, Extranet e Internet se deberá proporcionar el registro adecuado para la imagen de la institución, publicaciones e información, el diseño podrá ser contratados con terceros de forma de garantizar originalidad en el diseño. Además en temas de interconexión se establecerán convenios escritos con otras instituciones relacionadas al ámbito penal, de forma de mejorar y simplificar procesos.

e. Registros

- Listado de Dominios Inscritos por la Defensoría.
- Convenios de Interconexión.

f. Referencias

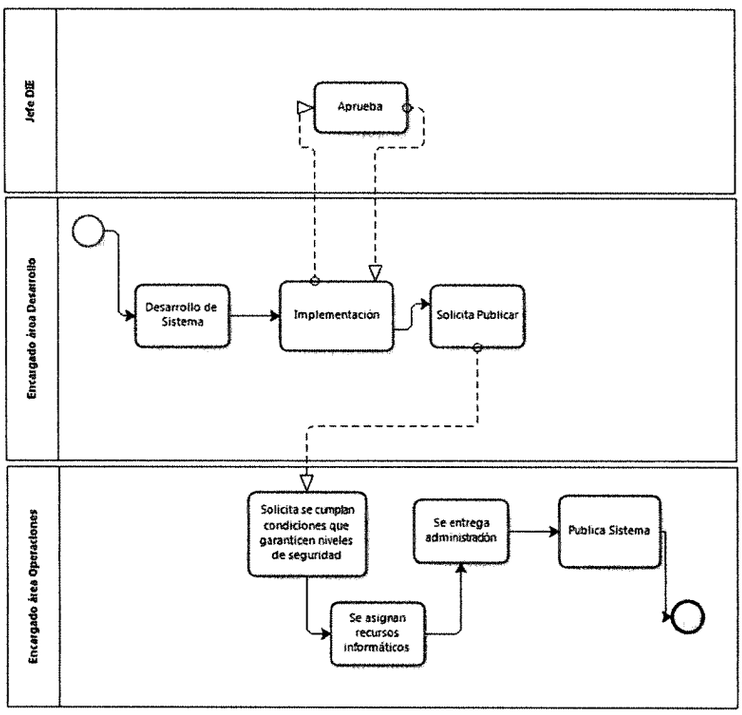
- Políticas de privacidad, disponibles en la página Intranet.
- Ley N°20.285 sobre acceso a la Información Pública.

g. Indicadores

- No hay

h. Diagrama de Flujo

Diagrama de Publicación de Sistemas



i. Anexos

- No hay

7. Procedimientos de Seguridad de la Información

7.1 Procedimiento de Administración de Usuarios y Accesos

a. Objetivo

Establecer las directrices que permitan asegurar niveles adecuados de seguridad de la información que se genere, gestione, procese, intercambie y almacene, en los procesos de la Defensoría.

b. Alcance

Este procedimiento considera aspectos relacionados a la seguridad informática, ambiental, y de las personas, además de la protección de los bienes, equipos e instalaciones donde se almacena o administran activos de información.

c. Base Legal

- Decreto Supremo N°83, de 2004, del Ministerio Secretaría General de la Presidencia, que aprueba norma técnica para los órganos de la Administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos.
- Decreto Supremo N°29, de 2004, del Ministerio de Hacienda, que fija texto refundido coordinado y sistematizado de la Ley 18.834, sobre Estatuto Administrativo, en su Párrafo 5 denominado "*De las Prohibiciones*", señala en su artículo 84 El funcionario estará afecto a las siguientes prohibiciones: g) Ejecutar actividades, ocupar tiempo de la jornada de trabajo o utilizar personal, material o información reservada o confidencial del organismo para fines ajenos a los institucionales; en caso de haber incumplimiento de ello, se deberán aplicar las sanciones correspondientes conforme lo establece el mismo Estatuto en sus artículos 119 y 120, previa investigación o sumario administrativo.
- Ley N°19.223 que tipifica figuras penales relativas a la informática.

d. Responsabilidades

- **Comité Tecnológico:** Sancionar los procedimientos tecnológicos y velar por su correcta aplicación en las actividades establecidas. Su Presidente actuará como Encargado de Seguridad de la Información de la Institución.
- **Jefe Departamento de Informática y Estadísticas:** Velar por el cumplimiento del Manual de Procedimientos Tecnológicos y sancionar sus actualizaciones
- **Profesionales del DIE y Encargados de Informática Regionales:** Asegurar la protección de los sistemas, a través de la aplicación de las actividades que se formalizan en el presente manual.
- **Usuarios:** Cumplir lo establecido en el presente manual y asegurar en sus actividades el cumplimiento de lo establecido en el mismo.

e. Descripción de Actividades

1. **Administración de usuarios y grupos:** Se debe dar cumplimiento a lo indicado en el *Procedimiento de Asignación de Servicios Informáticos*, y adicionalmente para la administración adecuada y organizada de los grupos de correo se debe tener en cuenta lo siguiente para la solicitud de grupos:

    - Nombre: Nombre descriptivo del grupo de distribución y ojala incluir información referente a la Defensoría a la que pertenece o tiene dependencia.
    - RXX: Prefijo utilizado para los grupos de regiones, donde las XX identifican la región, ejemplo R11, RMS, etc.
    - DN: Prefijo que identifica la Defensoría Nacional.
    - DPP: Prefijo utilizado para los grupos que tengan carácter oficial o de cobertura nacional.

    La administración estará a cargo del DIE y de los Encargados de Informática Regionales, quienes deberán mantener actualizado las cuentas de usuarios y los grupos de distribución de correo con sus respectivas listas de integrantes.

    En el caso que la Defensoría requiera cambiar el administrador de las cuentas, deberá solicitarlo al Jefe DIE, a través de un medio formal, quien deberá sancionar la solicitud y enviarla al Encargado de Operaciones del DIE, este último tiene un plazo de 48 horas para ejecutar la acción.

    Se definen los siguientes grupos permanentes:

    - Grupos de funcionarios cuya lista de integrantes corresponde a la totalidad de los funcionarios, debe ser administrada por el DIE y el listado solo incluye funcionarios de la Defensoría.
    - Grupos de funcionarios por departamento o unidad corresponde a la totalidad de los funcionarios de un depto. o unidad, este grupo debe ser administrado por las secretarías respectivas.
    - Grupos por región, corresponde a los funcionarios de las DR.
    - Grupos empresas licitadas, estos grupos deben crearse fuera del grupo de funcionarios y debe ser administrado por los Encargados de Informática Regionales.
    - Grupos Inspectorías, corresponde a los funcionarios de las inspectorías y deben ser incluidos en el grupo regional y administrador por los Encargados de Informática Regionales.

La nomenclatura general será:

- RXX Funcionarios Defensoría: donde xx corresponde al número de la región. Este grupo debe tener como integrantes a todos los funcionarios de la Defensoría en la región.
- RXX Defensores Defensoría: donde xx corresponde al número de la región. Grupo que debe tener el listado de todos los defensores institucionales de la región.
- RXX Defensores Licitados: donde xx corresponde al número de la región. Grupo que debe tener el listado de todos los defensores licitados de la región.
- RXX Asistentes Defensoría: donde xx corresponde al número de la región. Grupo que debe contener a todos los asistentes de la región.
- RXX Todos Defensoría: donde xx corresponde al número de la región. Grupo que debe contener a todos los usuarios de la DPP y licitados de la región.
- DN Departamento o Unidad: grupo que debe contener a todos los integrantes del departamento o unidad.
- DN Todos Funcionarios: grupo compuesto por todos los grupos correspondientes a departamentos y unidades de la Defensoría Nacional.
- DPP Todos Funcionarios: grupo compuesto por todos los grupos de funcionarios de regiones y la defensoría nacional.
- DPP Todos Defensores Licitados: grupo compuesto por todos los grupos de defensores licitados de todas las regiones.
- DPP Todos Defensores Defensoría: grupo compuesto por todos los grupos de defensores institucionales de todas las regiones.
- DPP Todos Defensores: grupo compuesto por los grupos DPP Todos Defensores Licitados y DPP Todos Defensores Defensoría.
- DPP Todos Asistentes Defensoría: grupo compuesto por todos los grupos de asistentes licitados de todas las regiones.
- DPP Todos Asistentes: grupo compuesto por los grupos DPP Todos Asistentes Licitados y DPP Todos Asistentes Defensoría.
- DPP Todos Defensoría: grupo compuesto por todos los grupos tanto esenciales tanto de regiones como de la DN.

2. Acceso a los Archivos de Sistema: Todo Repositorio o contenedor de código fuente, base de datos o archivo perteneciente a un sistema deberá poseer un acceso restringido y solo las usuarios debidamente autorizados podrán copiar, cambiar o eliminar información y tendrán acceso controlado según sea su rol o responsabilidad. La definición de accesos será responsabilidad del Encargado del área de Desarrollo, quien será el encargado de emitir los perfiles de seguridad de acceso a los intervinientes del sistema.

3. Acceso a la Información: Se debe tener en consideración que para que se cumpla con el seguimiento de actividades de procesamiento de información al menos las actividades siguientes deben efectuarse y documentarse:

    - Instalación de Antivirus en todo el equipamiento de la Institución.
    - Efectuar revisiones periódicas sobre las instalaciones del Antivirus en el equipamiento de la Defensoría, incluirlas en las auditorías que efectúa el DIE al cumplimiento de los Procedimientos Vigentes.
    - Efectuar un control sobre la documentación, control de versiones, control de instalación de software, control de acceso a código fuente y control de cambios del software que se instala y utiliza en la Institución.
    - Establecer los criterios de aceptación de software, procurando evitar vulnerabilidades en los sistemas instalados en la Institución.

4. Acceso Físico al Housing: Las dependencias que sirven para el resguardo del equipamiento principal de la Defensoría deberá tener un acceso controlado, actualmente el housing es arrendado a una empresa externa la cual garantizas niveles de seguridad adecuados. En cuanto al control de ingreso a las salas de servidores ubicadas en la DN y DR será de responsabilidad del DIE y de los Encargados de Informática Regionales, proveer de un medio controlado para el acceso, los que serán sujetos de auditoría.

f. Registros

- Registro control de acceso a Housing y Salas de Servidores.
- Registro de actualización de versiones de software o fichas técnicas.

g. Referencias

- Sistema de Seguridad de la Información PMG SSI.

h. Indicadores

- No hay.

i. Diagrama de Flujo

- No hay.

j. Anexos

No hay.

7.2 Procedimiento de Solicitud de Información

a. Objetivos

El presente tiene por **objetivo general**, estandarizar el proceso de solicitud y entrega de información referente a causas atendidas por la Defensoría Penal Pública, a través de la Unidad de Estadísticas.

Dicha final, se materializa en los siguientes **objetivos específicos**:

- Establecer las etapas específicas involucradas en la solicitud y entrega de información estadística a nivel Institucional.
- Establecer requirentes de información válidos (usuarios internos).
- Generar un canal único de respuesta a requerimientos de información estadística.
- Sistematizar y documentar los procesos de extracción y análisis de información estadística.
- Indagar en mejoras a considerar en el proceso de registro de información vinculada al trabajo de cada servicio que presta la Institución.

b. Alcance

El alcance de esta iniciativa es transversal al proceso de trabajo de la Unidad de Estadísticas, así como del proceso de gestión de información estadística de la Institución en su conjunto. Se integra de modo directo al modelo de generación de información, estableciendo canales de ingreso de requerimientos y perfiles de demandas, facilitando el seguimiento al cumplimiento de respuesta a las solicitudes, permitiendo a su vez la sistematización de respuestas a requerimientos que posteriormente puedan ser de utilidad para otros usuarios.

c. Responsabilidades

La implementación del protocolo de solicitud de información, conlleva acciones y responsabilidades concretas de diferentes actores al interior de la Defensoría Penal Pública. En primer lugar es necesario diferenciar entre **proveedores** y **usuarios** de información estadística.

Por **proveedor**, se comprende al área responsable del diseño e implementación del presente protocolo, como organismo a cargo de dar respuesta a los requerimientos de información estadística que la Institución requiera, tanto para fortalecer su propio actuar, como para dar respuesta a requerimientos externos, respecto al accionar de la Defensoría Penal Pública.

Este rol recae en el Departamento de Informática y Estadísticas, a través de su Jefe de Departamento y de su Unidad de Estadísticas. El Jefe de Departamento tiene por misión la revisión y visación de la implementación del presente protocolo, así como la revisión y elaboración de respuestas ante requerimientos específicos. Por su parte, la Unidad de Estadísticas es la responsable de implementar y ejecutar el proceso establecido para efectos de dar respuesta a solicitudes de información estadística, lo cual se materializa en las siguientes actividades: 1. Ejecutar el protocolo de solicitud de información; 2. Mantener y documentar actualizaciones del protocolo; 3.Informar y capacitar en el uso adecuado del protocolo; 4. Sistematizar solicitudes y respuestas generadas a partir del protocolo.

Con el fin de clarificar las fases del proceso de solicitud de información, la figura del **usuario** se ha segmentado en:

- **Usuario inicial**: persona natural o jurídica, externa o interna a la organización, que requiere información estadística específica.
- **Usuario DPP**: funcionario de la Institución, designado por un departamento y/o unidad de la administración central o de defensorías regionales de la Institución, que solicita información estadística para su uso en la gestión de prestación de defensa y/o para dar respuesta a requerimientos externos de acceso a información estadística[6].

Con el fin de ejemplificar la diferenciación de usuarios expuesta, a continuación se presenta cuadro comparativo según principales requerimientos de información atendidos por la Unidad de Estadísticas:

Requerimiento de información	Usuario inicial	Usuario DPP
Solicitudes acogidas por Ley de transparencia.	Persona natural o jurídica.	Unidad de Asesoría Jurídica.
Solicitudes de información por parte de medios de comunicación.	Medio de comunicación.	Unidad de Comunicaciones y Prensa.
Solicitudes de información de personas naturales o jurídicas para fines de investigación.	Persona natural o jurídica.	Departamento de Estudios y Proyectos.

Las **responsabilidades** específicas definidas según actor, son las siguientes:

Usuario Inicial:

- Enviar la solicitud de información estadística, al departamento y/o unidad de la Defensoría Penal Pública que trabaje la información específica deseada.
- Redefinir la solicitud de información estadística, ante la eventualidad de que el requerimiento presente observaciones técnicas necesarias de clarificar para realizar una adecuada extracción y análisis de información.
- Recepcionar la respuesta final enviada.

Usuario DPP:

- Recepcionar y evaluar solicitud de información.
- En los casos que corresponda, solicitar aclaraciones adicionales al requerimiento emitido por usuario inicial.
- En los casos que corresponda, responder consultas de la Unidad de Estadísticas y/o Jefe de Departamento de Informática y Estadísticas, ante la necesidad de aclaraciones adicionales al requerimiento emitido por usuario inicial.

[6] Un caso particular se da ante solicitudes de un usuario DPP, que requiere información para realizar análisis, no comprendidos dentro del ejercicio habitual de sus funciones (por ejemplo, para la realización de investigaciones académicas). Ante esta situación, el requerimiento se comprende como externo y por lo tanto, será considerado como usuario inicial, para los fines del presente protocolo.

- En los casos que corresponda, suscribir convenio de confidencialidad entre la Institución y el usuario inicial[7]. Posteriormente, informar y enviar respaldo formal vía memorándum al Departamento de Informática y Estadísticas.
- Enviar solicitud vía REDMINE[8] a Unidad de Estadísticas.
- Elaborar y enviar respuesta a usuario inicial.

Unidad de Estadísticas:

- Recepcionar y evaluar solicitud de información.
- En los casos que corresponda, solicitar a usuario DPP depuraciones al requerimiento de información.
- En los casos que corresponda, diseñar query y generar extracción de datos, desde bases de datos de la Institución.
- Procesar, analizar e informar respecto a los hallazgos que la solicitud de información generase.
- En los casos que corresponda, emitir y enviar respuesta a usuario DPP.
- Generar proceso de cierre y respaldo de documentos asociados a la respuesta de la solicitud de información.

Jefe de Departamento de Informática y Estadísticas:

- En los casos que corresponda, validar análisis e informe emitido por Unidad de Estadísticas.
- En los casos que corresponda, solicitar revisión del requerimiento a la Unidad de Estadísticas y/o usuario DPP.
- En los casos que corresponda, dar respuesta a usuario DPP.

d. Descripción de actividades

Respecto a las etapas de trabajo comprendidas en el proceso de generación de información estadística, se distinguen las siguientes fases:

- Recepción y evaluación de la solicitud de información enviada por usuario inicial.
- En los casos que corresponda, solicitar aclaraciones a requerimiento.
- En los casos que corresponda, suscribir convenio de confidencialidad para el trabajo con información protegida.
- Realizar solicitud formal vía REDMINE, para su respaldo, seguimiento y ejecución.
- En los casos que corresponda, diseño de algoritmo de extracción de información.
- En los casos que corresponda, extracción de información desde sistemas informáticos.
- Procesamiento y validación de datos disponibles para dar respuesta a requerimiento.
- Confección de informe de análisis.
- Auditoría y retroalimentación interna.
- Envío de respuesta.

[7] Por ejemplo, información detallada a nivel de causa o causa-imputado y/o que permita la individualización de la persona atendida por Defensoría Penal Pública. La Unidad de Asesoría Jurídica es la encargada de definir los criterios jurídicos para la determinación de la necesidad de suscribir un convenio de confidencialidad entre usuario inicial y la Institución.

[8] Sistema web de gestión de solicitudes, habilitado por el Departamento de informática y Estadísticas de la Defensoría Penal Pública, para la recepción y seguimiento de requerimientos de atención, soporte y/o problemas varios que presenten los sistemas de información de la Institución. El link de acceso es http://10.17.5.186/redmine/login.

- Cierre requerimiento y respaldo de insumos asociados a respuesta a solicitud de información.

Las particularidades en cada uno de estos hitos, está mediada por los siguientes factores: canal de acceso de solicitud, producto requerido, perfil del usuario y prioridades propias del funcionamiento del Departamento de Informática y Estadísticas.

e. Diagrama de flujo de actividades

Ver Anexo.

f. Registros

- Solicitud de información vía REDMINE.
- En los casos que corresponda, memorándum informativo respecto de convenio de confidencialidad.
- En los casos que corresponda, convenio de confidencialidad firmado.
- Documentación de respaldo de análisis y notificación de entrega de respuesta por parte de Unidad de Estadísticas y/o Jefe de Departamento.

g. Referencias

- Formulario para la solicitud de información estadística.
- Definiciones técnicas para el adecuado llenado de formulario de solicitud de información estadística.
- Criterios jurídicos para la determinación de la necesidad de ejecutar un convenio de confidencialidad entre usuario inicial y la Institución.
- Criterios técnicos para la determinación de canal de respuesta del Departamento de Informática y Estadísticas a usuario DPP (Jefe del Departamento o Unidad de Estadísticas).
- Convenio de confidencialidad personas naturales y/o jurídicas.

h. Indicadores

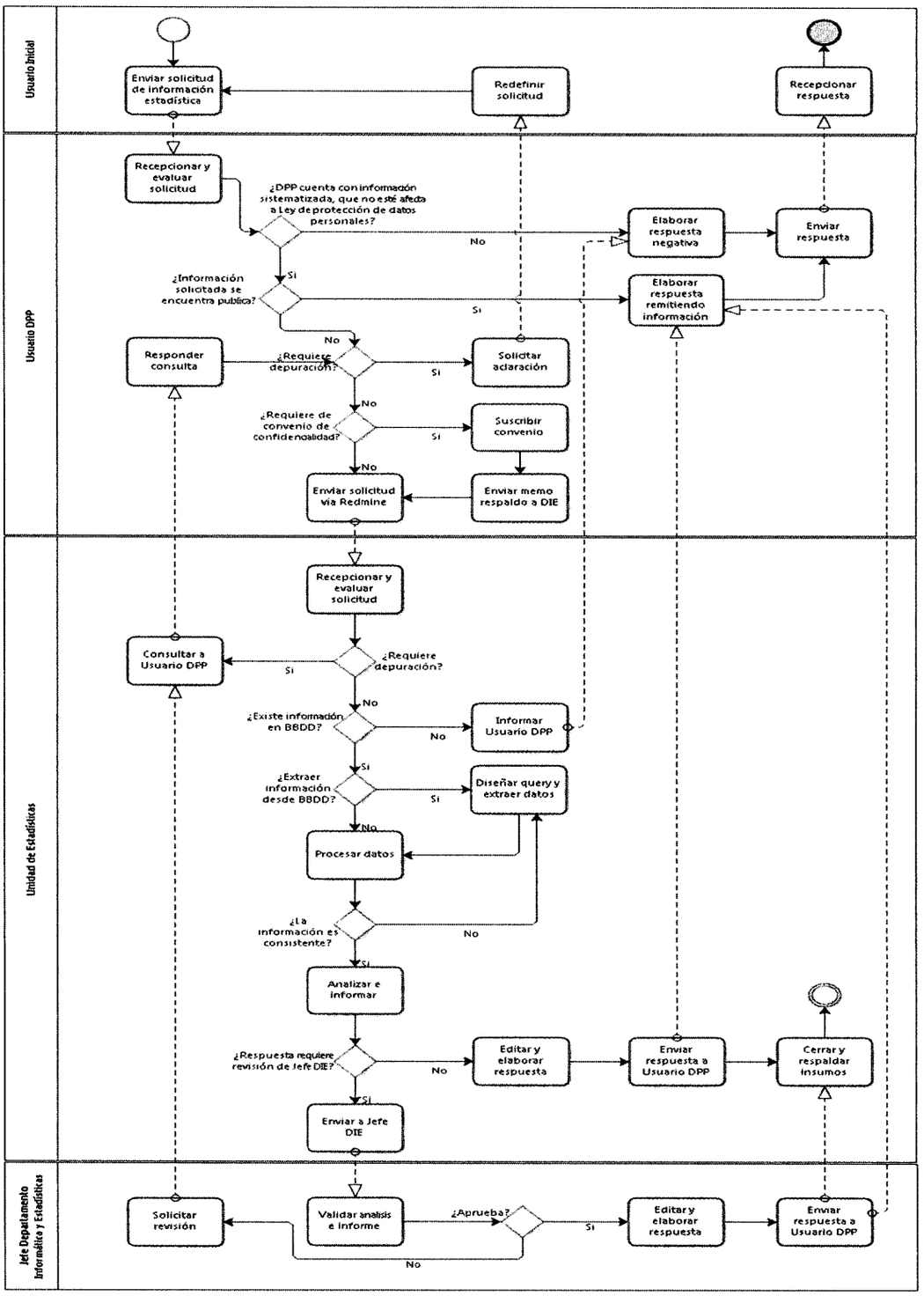
- Envío de respuesta a usuario inicial, respecto del total de solicitudes de información estadística realizadas a Defensoría Penal Pública.
- Envío de respuesta a usuario DPP, respecto del total de solicitudes de información estadística realizadas a Defensoría Penal Pública.
- En el caso de solicitudes acogidas a la Ley de transparencia, envío de respuesta a usuario DPP en un plazo inferior a 8 días, respecto del total de solicitudes de información estadísticas de esta naturaleza.

i. Anexos

- Diagrama de flujo de actividades.
- Formato convenio de confidencialidad para personas naturales[9].
- Formulario para la solicitud de información estadística.
- Manual de definiciones técnicas para el adecuado llenado de formulario de solicitud de información estadística.

[9] Aprobado por la Unidad de asesoría jurídica de la Defensoría Penal Pública.

A. Diagrama de flujo de actividades



B. Formato convenio de confidencialidad para personas naturales.

En Santiago de Chile, a 00 de MES del AÑO, entre don NOMBRE COMPLETO, PROFESIÓN, cédula nacional de identidad N° 00.000.000 - 0, domiciliado en CALLE N°, comuna de COMUNA, en adelante "el solicitante" y; la **DEFENSORÍA PENAL PUBLICA**, RUT N° 61.941.900-6, representada para estos efectos por don **ANDRÉS MAHNKE MALSCHAFSKY**, cédula nacional de identidad N° 7.889.445-8, domiciliado en Avenida Libertador Bernardo O'Higgins N°1449, 8° piso, comuna de Santiago, en adelante la "Defensoría"; se ha convenido el siguiente Acuerdo de Confidencialidad.

PRIMERO: Don NOMBRE COMPLETO, solicita a la Defensoría información respecto a DATOS GENERALES SOLICITADOS, como PERSONA CON FINES ACADÉMICOS/REPRESENTANTE INSTITUCIÓN PÚBLICA O DE ESTUDIOS/ REPRESENTANTE DE INSTITUCIÓN PRIVADA, al amparo de NOMBRE DE INST PUBLICA, PRIVADA o de CASA DE ESTUDIOS, cuyo representante legal es don NOMBRE COMPLETO, cédula nacional de identidad N° 00.000.000 - 0, domiciliado en CALLE N°, comuna de COMUNA.

SEGUNDO: Con el fin de respaldar la presente solicitud y Acuerdo de Confidencialidad, se adjunta a este documento:

- Copia de la cédula de identidad del solicitante.
- Carta de respaldo de la Institución pública, privada y/o académica que ampara la solicitud.
- (Sólo en el caso de Instituciones privadas) Copia de la cédula de identidad del representante legal y escritura de poderes.

TERCERO: El solicitante declara y reconoce que la información y/o documentos facilitados por la Defensoría, contienen información sensible conforme a lo dispuesto en el artículo 2°, letra g) de la Ley N°19.628, sobre Protección de la Vida Privada o de Datos de Carácter Personal. Por lo tanto, el presente Acuerdo se rige por las disposiciones de dicha Ley en su totalidad.

CUARTO: En consideración a la expuesto y dispuesto por la Ley 19.628, don NOMBRE COMPLETO, es el garante, guardador y responsable final del carácter confidencial de la información facilitada por la Defensoría, por lo cual no podrá por cualquier título y/o medio, revelar, difundir, publicar, vender, ceder, copiar, reproducir, interferir, interceptar, alterar, modificar, dañar, inutilizar, destruir, COMPARTIR, en todo o en parte esta información, ya sea durante su tratamiento para los fines señalados como después de su finalización.

Se exceptúan del presente Acuerdo y por lo tanto quedan excluidos todos aquellos documentos que contengan datos de los señalados en el artículo 21 de la mencionada Ley N°19.628.

QUINTO: La información y/o documentos facilitados sólo podrán ser objeto de análisis, para los fines con los cuales fueron solicitados en primera instancia a la Defensoría. En caso de que el solicitante, requiera utilizar la información para otros fines, deberá suscribir un nuevo acuerdo de confidencialidad, independientemente de que ya disponga de la información y/o documentos necesarios para los nuevos fines requeridos.

SEXTO: Con el fin de enriquecer el conocimiento público, en las materias asociadas a la información y/o documentos facilitados por la Defensoría, es que el solicitante hará entrega de una copia del

análisis y escrito final efectuado -en medio magnético- y la base de datos procesada para los fines de su solicitud –en medio magnético y formato de datos acordado con la Defensoría- como respaldo del tratamiento de la información descrita.

SEPTIMO: El presente Acuerdo se suscribe en tres ejemplares del mismo tenor y fecha, quedando uno en poder del solicitante y dos en poder de la Defensoría. La personería de don Andrés Mahnke Malschafsky para actuar en nombre y representación de la Defensoría, consta de Decreto Supremo N° 14, de fecha 8 de enero de 2015, del Ministerio de Justicia, que lo nombra Defensor Nacional.

Solicitante

ANDRÉS MAHNKE MALSCHAFSKY

Defensor Nacional

C. Formulario para la solicitud de información estadística.

Formulario solicitud de información estadística **FOLIO INTERNO** ____

Información general

Fecha solicitud: *día* *mes* *año* **Plazo estimado:** *día* *mes* *año*

Perfil Solicitud: ☐ 1. Interna. ☐ 2. Externa.

Requiere convenio: ☐ 1. Si. ☐ 2. No.

Producto solicitado: ☐ 1. Base de datos. ☐ 2. Tabla multivariable. ☐ 3. Información específica.

Finalidad solicitud: ☐ 1. Gestión interna. ☐ 2. Estadística. ☐ 3. Académica. ☐ 4. Medio de comunicación. ☐ 5. Otra. ¿Cuál?

Usuario DPP:

Departamento y/o Unidad

Nombre usuario *Cargo*

E-mail *Teléfono*

Usuario inicial:

Perfil usuario ☐ 1. Persona jurídica. ⟹ ☐ 1. Institución pública. ☐ 2. Institución privada. ☐ 2. Persona natural.

Institución, Departamento y/o Unidad

Nombre usuario *Cargo*

E-mail *Teléfono*

Solicitud de información estadística

Solicitud específica:

Universo:

Unidad ☐ 1. Causa. ☐ 2. Causa-imputado. ☐ 3. Individuo (Rut). ☐ 4. Delitos asociados a causa-imputado.

Medición según ☐ 1. Ingresos. ☐ 2. Términos. ☐ 3. Ingresos-términos período T. ☐ 4. En trámite al día Y.

Período:

Desde *día* *mes* *año* Hasta *día* *mes* *año*

Fragmentación:

Temporal ☐ 1. Total acumulado. ☐ 2. Por año. ☐ 3. Por mes.

Administrativa ☐ 1. País. ☐ 2. Región. ☐ 3. Tribunal. ☐ 4. Defensoría ☐ 5. Tipo defensor.

Variables descriptivas:

Sexo ☐ 1. Total indiferenciado. ☐ 2. Hombre/Mujer ☐ 3. Sólo hombre. ☐ 4. Sólo mujer.

Edad ☐ 1. Total indiferenciado. ☐ 2. Menor de 18 años/18 y más años. ☐ 3. Sólo menor de 18 años. ☐ 4. Sólo 18 y más años.

Etnia ☐ 1. Total indiferenciado. ☐ 2. Indígena/No indígena ☐ 3. Etnia específica. ¿Cuál(es)?.

Nacionalidad ☐ 1. Total indiferenciado. ☐ 2. Extranjero/No extranjero ☐ 3. Nacionalidad específica. ¿Cuál(es)?.

Segmentación de universo de datos, según:

☐ 1. No requiere segmentación adicional.
☐ 2. Delitos. ¿Cuál(es)?. ⟹
☐ 3. Formas de término. ¿Cuál(es)?. ⟹
☐ 4. Medidas cautelares. ¿Cuál(es)?. ⟹
☐ 5. Gestiones. ¿Cuál(es)?. ⟹
☐ 6. Audiencias. ¿Cuál(es)?. ⟹

¿Cuál(es)?

D. Manual de definiciones técnicas para el adecuado llenado de formulario de solicitud de información estadística.

Manual

Formulario solicitud de información estadística.

El presente manual, surge como referencia para orientar la solicitud de información estadística al interior de la Defensoría Penal Pública. Se enmarca dentro del proceso de estandarización de procedimientos de solicitud y entrega de información referente a las causas atendidas por la Institución.

Antecedentes preliminares, claves de tener en consideración ante cualquier tipo de solicitud de información estadística son los siguientes:

1. Los datos disponibles en el sistema informático de la Institución, sólo representan las causa-imputado ingresadas al sistema de defensa de la Defensoría Penal Pública. Por lo tanto, no evidencian la realidad País en estas materias.

2. El Departamento de Informática y Estadística (DIE), a través de su Unidad de Estadísticas, da cuenta del accionar de la Defensoría Penal Pública a través de los datos disponibles en los sistemas informáticos **con que al día de la solicitud cuenta la Institución**, mediando para ello el registro de los mismos por parte de usuarios de dichos sistemas.

3. Los datos se extraen desde sistemas informáticos específicos (generalmente, desde el Sistema Informático de Gestión de Defensa Penal-SIGDP), considerando causa-imputados ingresadas o terminadas en un período específico. Dada la naturaleza de la prestación de defensa y desfases probables en la actualización de registros en los sistemas informáticos, es factible observar variaciones en los datos estadísticos que se presentan ante actualizaciones de ciertos requerimientos.

4. En el caso de subconjuntos de datos inferiores a 10 casos, se procede a presentar información agrupada, considerando la misión institucional de velar por la protección y confidencialidad de los datos personales asociados a las personas atendidas por la Institución.

A continuación, se definen las variables necesarias de completar por parte del usuario (requirente de información) en el Formulario de solicitud de información estadística. Se segmentan en:

1. Información general del requerimiento y del usuario de la información, con el fin de contar con los antecedentes principales de la contraparte efectiva del requerimiento y situar la solicitud en un contexto específico.

2. Información de definición de la solicitud de información, con el fin de disponer del requerimiento textual, pero al mismo tiempo estableciendo parámetros específicos de medición para clarificar las expectativas del usuario final.

Información general:

Variable	Categorías de respuesta	Definición
Folio interno	Número	N° identificador de requerimiento. Uso interno. *No completar*.
Fecha solicitud	Día-Mes-Año	Fecha en que la solicitud fue recepcionada o generada por usuario DPP. No es la fecha de recepción por parte de Unidad de Estadísticas.
Plazo estimado	Día-Mes-Año	Fecha máxima estimada de requerir respuesta, ante solicitudes perentorias. No es fecha establecida como acuerdo de entrega, sino sólo una referencia para efectos de priorización de requerimientos.
Perfil solicitud	Interna	Solicitud de información generada por algún departamento y/o unidad nacional o regional, de la Institución.
	Externa	Solicitud de información generada por un usuario externo a la Institución (o para fines externos).
Requiere convenio	Si	Registro para establecer la obligatoriedad de adjuntar dicho convenio al formulario de solicitud de información.
	No	Registro para establecer que no se requiere adjuntar dicho convenio al formulario de solicitud de información.
Producto solicitado	Base de datos	Base de datos, que presenta información a nivel detalle por universo de datos solicitado.
	Tabla multivariable	Tabla bi o multivariada, que presenta información a nivel agregado, según la segmentación definida por el requirente.
	Información específica	Información específica respecto a causas y gestiones de defensa.
	Gestión interna	Perfil de demanda interna, como por ejemplo "N° de audiencias que se realizaron en el mes 1 del año T, respecto del total de audiencias realizadas en el año T".
Finalidad solicitud	Estadística	Perfil de demanda interna o externa, como por ejemplo "N° de causa-imputado ingresadas en región A, durante el mes 1 del año T".
	Académica	Perfil de demanda interna o externa, como por ejemplo "N° de causa-imputado atendidos por la Institución, por infracciones a la Ley 777, artículo 31".
	Medio de comunicación	Perfil de demanda externa, realizada expresamente por medios de comunicación o para ser publicada en ellos.
	Otra. ¿Cuál?	Especificar.
Usuario DPP	Departamento y/o Unidad	Diferenciar y explicitar, si corresponde a una solicitud regional y/o de defensor local o licitado.
	Nombre usuario	Especificar.
	Cargo	Especificar.
	E-mail y Teléfono	Sólo para efectos de contacto.
	Perfil usuario	Identificar si corresponde a una persona natural o jurídica. Ante esta última opción, explicitar si corresponde a una institución público o privada.
Usuario inicial	Institución, Departamento y/o Unidad	Especificar.
	Nombre usuario	Sólo para efectos de contacto.
	Cargo	Sólo para efectos de contacto.
	E-mail y Teléfono	Sólo para efectos de contacto.

Solicitud de información:

Variable	Sub Variable	Categorías de respuesta	Definición
Universo	Unidad	Causa	N° de procesos penales. El objetivo es retratar el número de PROCESOS o expedientes judiciales atendidos. La medición de causa es independiente de la cantidad de imputados que en ella estén involucrados, así como también de la cantidad de delitos por los cuales se les inicia un proceso específico.
		Causa-imputado	N° de imputado de delito asociado a una causa específica. El objetivo es retratar el número de ATENCIONES de defensa desarrolladas por parte de la Institución en un período de tiempo específico. La medición de causa-imputado es independiente de la cantidad de delitos por los cuales cada imputado está siendo (o fue) procesado en una causa específica.
		Individuo (Rut)	N° de imputado de delito, sin diferenciar las causas específicas por las cuales es (o fue) atendido. El objetivo es retratar el número de PERSONAS atendidas por parte de la Institución en un período de tiempo específico. La medición de individuos es independiente de la cantidad de delitos por los cuales cada imputado está siendo (o fue) procesado en una o más causas.
		Delitos asociados a causa-imputado	N° de delitos asociados a imputados. El objetivo es retratar la ocurrencia de ciertos DELITOS atendidos por parte de la Institución en un período de tiempo específico. La medición de delitos es independiente de la cantidad de causas o causa-imputados a los cuales fueron imputados, siendo una contabilización integradora de ellos.
	Medición según	Ingresos Términos Ingresos-términos período T En trámite al día Y	La contabilización de atenciones, puede ser respecto al registro de causas ingresadas en un período, terminadas en un período, ingresadas y terminadas en un período, o que se encuentran vigentes al momento de realizar la medición de datos. Esta característica es relevante, al considerar el período promedio de gestión de una causa y el impacto que ello tiene en los diferentes parámetros de medición.
Período	Desde	Día-Mes-Año	Fecha desde la cual se solicita extraer y analizar información.
	Hasta	Día-Mes-Año	Fecha hasta la cual se solicita extraer y analizar información.
Fragmentación	Temporal	Total acumulado	En el caso de solicitudes que abarquen un período de datos superior a 1 mes o 1 año, se solicita el N° acumulado y no diferenciado por período de tiempo.
		Por año	En el caso de solicitudes que abarquen un período de datos superior a 1 mes o 1 año, se solicita diferenciar por año la información.
		Por mes	En el caso de solicitudes que abarquen un período de datos superior a 1 mes o 1 año, se solicita diferenciar por mes (y año) la información.
	Administrativa	País Región Tribunal Defensoría Tipo defensor	La contabilización de atenciones, puede ser fragmentada o a nivel global (País). Las principales desagregaciones de información son respecto a región, tribunal, defensoría y tipo de defensor a cargo de cada causa-imputado (local o licitado).

Variable	Sub Variable	Categorías de respuesta	Definición
Variables descriptivas	Sexo	Total indiferenciado	N° acumulado, sin segmentar información por sexo.
		Hombre/Mujer	N° diferenciado por sexo.
		Sólo hombre	N° asociado solamente a imputados hombre.
		Sólo mujer	N° asociado solamente a imputadas mujeres.
	Edad	Total indiferenciado	N° acumulado, sin segmentar información por edad.
		Menor de 18 años/ 18 y más años	N° diferenciado por tramo de edad.
		Sólo menor de 18 años	N° asociado solamente a imputados menores de 18 años.
		Sólo 18 y más años	N° asociado solamente a imputados de 18 y más años.
	Etnia	Total indiferenciado	N° acumulado, sin segmentar información por etnia.
		Indígena/No indígena	N° diferenciado por auto-reporte de pertenecer a una etnia.
		Etnia específica	N° asociado solamente a imputados de etnias específicas.
	Nacionalidad	Total indiferenciado	N° acumulado, sin segmentar información por nacionalidad.
		Extranjero/No extranjero	N° diferenciado por condición de extranjero.
		Nacionalidad específica	N° asociado solamente a imputados de nacionalidades específicas.
Segmentación de universo de datos según	No requiere segmentación adicional		No requiere segmentación adicional a los parámetros ya consignados en las variables anteriores.
	Delitos		Especificar cuál(es), según listado disponible.
	Formas de término		Especificar cuál(es), según listado disponible.
	Medidas cautelares		Especificar cuál(es), según listado disponible.
	Gestiones		Especificar cuál(es), según listado disponible.
	Audiencias		Especificar cuál(es), según listado disponible.

8. Procedimiento de Cumplimiento, Actualización y Auditorías

a. Objetivo

El objetivo de este procedimiento es establecer un programa anual de auditorías a las DR, DL, Departamentos y Unidades de la DN, que permita al DIE mejorar procesos internos y hacer ajustes a las políticas y procedimientos contenidos en el Manual de Procedimientos Tecnológicos.

b. Alcance

Este documento está orientado a los profesionales de Operaciones del DIE y Encargados de Informática Regionales y a la actividad de auditoría que les corresponde. Y pretende brindar información valiosa para la toma de decisiones, detectar falencias, determinar medidas correctivas, ser fuente de información y medir la efectividad del presente documento.
Las auditorías serán efectuadas en las DR, DL, Departamentos y Unidades de la DN, para lo cual se establecerá un plan de auditorías anual el que será debidamente difundido. Y los resultados de las mismas serán un insumo que podrá ser utilizado por la Unidad de Auditoría.
Las auditorías serán realizadas por el DIE o los Encargados de Informática Regionales e incluso en forma cruzada.

c. Responsabilidades

- **Comité Tecnológico:** Sancionar las actualizaciones del presente documento. Conocer de las observaciones de las auditorías y las propuestas de mejora que plantea el DIE. Aprobar modificaciones a las políticas y procedimientos del *Manual de Procedimientos Tecnológicos*.
- **Jefe Departamento de Informática y Estadísticas:** Velar por el cumplimiento del presente instructivo, efectuar la planificación y difusión de las auditorías y proponer al Comité Tecnológico mejoras o ajustes que surjan como resultado de los hallazgos.
- **Profesionales del área de Operaciones del DIE y Encargados de Informática Regionales:** Realizar las auditorías que se planifiquen anualmente y elaborar un informe con los resultados. Efectuar el seguimiento o control a los compromisos de mejora que suscriban las áreas auditadas y ser sujetos de auditorías cruzadas.
- **Encargados de Informática Regional:** Entregar toda la información que se solicite durante la auditoría y posteriormente.
- **Directores Administrativos Regionales:** Comprometer acciones de mejora una vez recibido el informe de auditoría, a través de un *Plan de Mejoras*. Realizar seguimiento en forma independiente a las acciones de control que pueda efectuar el DIE o Auditoría Interna.
- **Unidad de Auditoría Interna:** Velar por el cumplimiento de los procedimientos descritos en este manual, específicamente en lo que concerniente al proceso de auditorías tecnológicas y promover actualizaciones y mejoras. Solicitar información sobre las auditorías, informes de compromisos y metas de los Departamentos y Unidades de la DN, DR o DL.

d. Descripción de Actividades

1. **Planificación:** Durante el primer trimestre del año, deberá prepararse el plan de auditorías, que considere los hallazgos realizados en auditorías anteriores, compromisos pendientes, diagnósticos o situaciones que ameriten efectuar el control. La cantidad de auditorías que se efectúen va a estar determinada por los recursos disponibles y otras actividades que puedan ser relevantes al momento de efectuar la selección. Este plan debe ser autorizado por el Jefe del DIE y difundido a las DR, DL, Departamentos y Unidades; y puede ajustarse en base a la aparición de problemas de funcionamiento en alguna oficina específica.

2. **Detalle de la Auditoría:** Las auditorías van a ser realizadas por los profesionales del área de operaciones o quienes el Encargado de Operaciones designe. Para el apoyo de esta actividad se dispondrá de un check-list que se encuentra incluido en el *anexo A* de este procedimiento, que contiene toda la información que es deseable obtener de la auditoría en terreno.

   La auditoría deberá hacerse cargo de los siguientes aspectos generales:

   - Cuentas del Active Directory
   - Estado de la sala de servidores
   - Estado de la UPS
   - Estado e Inventario de los Computadores de Escritorio y todo el equipamiento a cargo
   - Estado de los Access Point
   - Estado del Reloj Biométrico
   - Mediciones de la red de telecomunicaciones
   - Estado de las Impresoras
   - Estado de la telefonía fija y de celular
   - Altas y bajas de los usuarios en los sistemas
   - Cumplimiento de las normativas y procedimientos tecnológicos

3. **Informe de la Auditoría:** Una vez efectuada la auditoría, el encargado de efectuarla deberá confeccionar un informe ejecutivo que entregue los principales hallazgos y observaciones de la auditoría incorporando sugerencias que mejoren los procesos. Este informe deberá ser aprobado por el Jefe de Operaciones del DIE y remitido al jefe DIE a través de un medio formal, indicando las conclusiones del proceso. El Jefe DIE remitirá los informes a los DAR, Jefes de Unidad o Departamento, según corresponda, para que elaboren un *Plan de Mejoras*. Este plan deberá ser remitido al Jefe DIE quien presentará una propuesta general de perfeccionamiento a los procesos o acciones de mejora al *Comité Tecnológico*, que sancionará las actualizaciones necesarias a este manual y a las acciones que se lleven a cabo.

4. **Plazos y envío a las DR:** Una vez realizada la auditoría el encargado de efectuarla deberá remitir el informe dentro de los 10 días corridos siguientes al Jefe de Operaciones, quien lo remitirá al

Jefe DIE en un plazo no mayor a 5 días corridos. Una vez recibido el Jefe DIE tiene un plazo no mayor a 5 días para remitirlo al DAR, Jefe de Departamento o Unidad y el DAR, finalmente el Jefe de Departamento o Unidad tiene 10 días para remitir el Plan de Mejoras o compromisos al DIE.

5. **Unidad de Auditoría Interna**: La Unidad de Auditoría podrá solicitar estos informes de auditoría, informes de compromisos y de control que se hayan realizado, con el objeto de que puedan realizar un control sobre estas materias.

e. Registros

- Check-list v2.0, incluido *anexo A.*
- Informe de auditoría, incluido *anexo B.*
- Plan de Auditorías y cronograma, carta Gantt.
- Plan de Mejoras, carta Gantt que incluya recursos involucrados.

f. Referencias

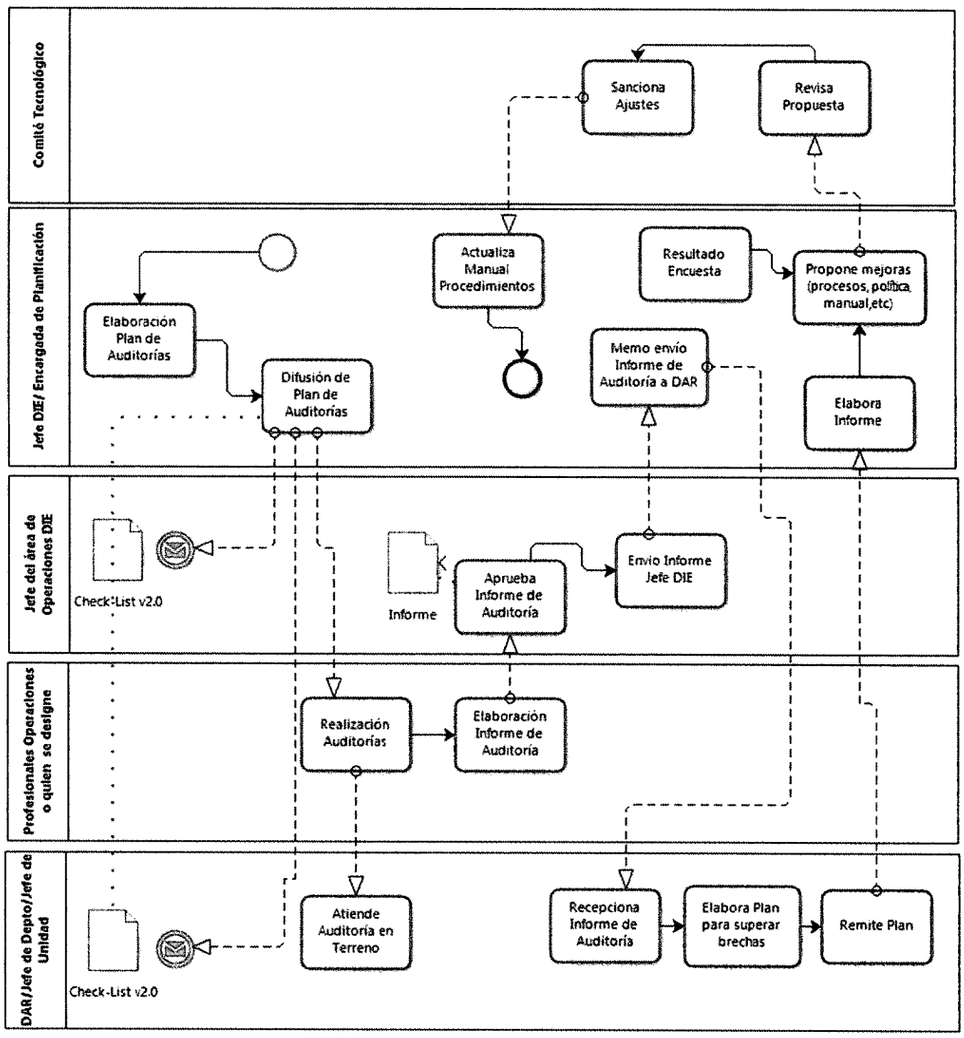
- No aplica.

g. Indicadores

- I_{02}= Cantidad auditorías comprometidas en el año t / Cantidad de auditorías realizadas en el año t.

h. Diagrama de Flujo

Diagrama de Cumplimiento, Actualización y Auditorías



i. Anexos

Anexo A
Check-List v2.0

Defensoría Sin defensa no hay Justicia	**Auditoría** **Departamento de Informática y Estadística**	**Versión:** 2.0

DEFENSORÍA : _____

1. Revisión de cuentas de correo en Active Directory

a. ¿Cuantos usuarios aparecen en el active directory? ☐

b.¿Cuantos usuarios aparecen en la lista entregada por RRHH? ☐

c. Diferencia. ☐

d. ¿Se actualizó la información? SI ☐ NO ☐

2. Estado de sala de servidores (sólo DR y DN)

a. Califique del 1 al 5 el orden general de la Sala de Servidores, donde 1 es muy ordenada y 5 muy desordenada. ☐

b. ¿Se incluye fotografía del Rack y de la Sala de Servidores? SI ☐ NO ☐

c. Califique del 1 al 5 el estado del equipamiento (servidores, routers, etc.), donde 1 es muy ordenado y 5 muy desordenado ☐

d. Fecha de la última mantención preventiva ☐

3. UPS

a. Consignar la fecha de la última mantención, con la orden de trabajo (fecha) ☐

b. ¿Se encuentra el cable By-Pass? SI ☐ NO ☐

c. ¿Está en buen estado? SI ☐ NO ☐

d. ¿El Encargado de Informática sabe ejecutar el By-Pass? SI ☐ NO ☐

4. Equipos de escritorio

a. ¿Se encuentra actualizado el inventario de computadores? SI ☐ NO ☐

b. ¿Cuantos equipos existen fuera del contrato? ☐

c. ¿Cuando fue la última vez que se actualizo Windows (fecha)? ☐

d. ¿Se encuentra el antivirus en todos los computadores? SI ☐ NO ☐

d.1 ¿En cuantos no se encuentra? ☐

e. Indique la fecha de la última mantención preventiva ☐

5. Access Point (WIFI)

a. Consigne la cantidad ☐

b. ¿Cuál es el estado? Bueno ☐ Regular ☐ Malo ☐

c. ¿Se han detectado problemas? SI ☐ NO ☐

d. Consigne la fecha de la última mantención preventiva ☐

6. Lector Biométrico

a. Consigne la cantidad ☐

b. ¿Cuál es el estado? Bueno ☐ Regular ☐ Malo ☐

c. ¿Se han detectado problemas? SI ☐ NO ☐

7. Redes

a. Consigne la cantidad de equipos en red

b. Estado de los equipos en red — Bueno ☐ Regular ☐ Malo ☐

c. Velocidad de enlace
Consignar los valores obtenidos
http://10.16.25.102/speedtest/

d. Puertas del SWITCH disponibles y ocupadas — Disponibles ☐ Ocupadas ☐

d.1 ¿Se detecto algún dispositivo no autorizado? SI ☐ NO ☐

e. ¿El Encargado de Informática tiene el listado de códigos de servicio? SI ☐ NO ☐

8. Impresoras

a. ¿Se detecto algún equipo en malas condiciones? SI ☐ NO ☐

b. ¿El Encargado de Informática tiene una planilla con el listado de códigos de servicio? SI ☐ NO ☐

c. Indique la fecha de la última mantención preventiva

9. Telefonía Fija

a. Consigne la cantidad de teléfonos y anexos — Teléfonos ☐ Anexos ☐

b. ¿Cuál es la cantidad de líneas disponibles?

c. Indique la fecha de la última mantención preventiva

10. Telefonía Celular

a. Consigne la cantidad de teléfonos — Teléfonos ☐ Anexos ☐

11. Procedimiento de Asignación de Servicios

a.¿Tiene los formularios de asignación? SI ☐ NO ☐

12. Procedimiento de Uso de los Servicios

a. ¿Utiliza el REDMINE?

13. Procedimiento de Uso de Sistemas Informáticos

a. Cuando fue la última vez que revizó las cuentas de usuarios de los sistemas SIGDP, SIAR y correo electrónico

14. Procedimiento de Seguridad de la Información

a. ¿Han existido incidentes de seguridad?

b.¿Han sido informados al Encargado de Seguridad?

15. Procedimiento de Licenciamiento

a. ¿Todo el software instalado en los pc's se encuentra licenciado?

Observaciones del Encargado de Informática Regional o del Auditor

Auditor Fecha: / / Nombre:	Encargado de Informática Regional Nombre: Defensoría:

Anexo B
Informe de Auditoría

Informe de Auditorías	Defensoría

Fecha (del informe de auditoría):

Localidades Auditadas (Identificación de la oficina auditada y el nombre del responsable de la oficina auditada).

Oficina	Responsable
1.	
2.	
3.	
4.	
5.	
6.	

1. **Hallazgos Principales (por oficina):**

2. **Detalle de los Hallazgos (por oficina):**

3. **Recomendaciones (por oficina):**

Nombre Auditor	
Firma	
Jefe del área de Operaciones	
Firma	

4 Anexos

1. Siglas

- DAF : Departamento de Administración y Finanzas
- DAN : Director Administrativo Nacional
- DECR : Departamento de Evaluación, Control y Reclamaciones
- Defensoría : Defensoría Penal Pública
- DEP : Departamento de Estudios y Proyectos
- DIE : Departamento de Informática y Estadísticas
- DL : Defensoría Local
- DN : Defensoría Nacional
- DR : Defensoría Regional
- IEC : International Electrotechnical Commission
- ISO : International Organization for Standardization
- IZC : Inspectoría Zonal Centro
- RRHH : Recursos Humanos
- SPAM : Stupid Pointless Annoying Messages
- SSI : Sistema de Seguridad de la Información
- UAJ : Unidad de Asesoría Jurídica

2. Referencias

- Ley N°19.718, que crea la Defensoría Penal Pública.
- Decreto Supremo N°77 del Ministerio Secretaría General de la Presidencia, de 2004, que aprueba norma técnica sobre eficiencia de las comunicaciones electrónicas entre órganos de la administración del Estado y entre estos y los ciudadanos.
- Decreto Supremo N°83 del Ministerio Secretaria General de la Presidencia, de 2004, que aprueba norma técnica para los órganos de la administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos.
- Decreto Supremo N°81 de 2004 del Ministerio Secretaría General de la Presidencia, que aprueba norma técnica para los órganos de la administración del Estado sobre interoperabilidad de documentos electrónicos.
- Norma ISO 27.001:2013 es un conjunto de estándares desarrollados por ISO (International Organization for Standardization), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.
- Resolución Exenta N°439, de fecha 29 de Agosto de 2013 de la Defensoría Nacional, que aprueba Manual de Procedimientos Tecnológicos de la Defensoría Penal Pública.
- Resolución Exenta N°463, de fecha 26 de Septiembre de 2013 de la Defensoría Nacional, que aprueba Plan Tecnológico Defensoría Penal Pública 2012-2016.
- Resolución Exenta N°595, de fecha 14 de Febrero de 2012, de la Defensoría Nacional, Procedimientos Administrativos de Activo Fijo y Oficio DAN N°828, de fecha 15 de septiembre de 2014, de actualización y formalización manual de "Procedimientos Administrativos Sistema de Activo Fijo", versión 03
- Ley N°20.285, sobre Acceso a la Información Pública.
- Ley N°19.039, De Propiedad Industrial.
- Ley N°17.336 sobre Propiedad Intelectual y sus modificaciones.
- Ley N°19.628 Sobre Protección de la Vida Privada o Protección de Datos de Carácter Personal.

3. Glosario de Términos

- **Activos de la Información:** Todos aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la institución.
- **Aplicaciones:** Programa informático que permite a un usuario utilizar un computador con un fin específico.
- **Confidencialidad:** Propiedad de la información mediante la cual se garantizará el acceso a la misma solo por parte de las personas que estén autorizadas y que ella no sea revelada a personas, ni entidades que no cuenten con autorización expresa.
- **Criticidad:** Nivel de impacto al funcionamiento de la Defensoría de la caída de un sistema o servicio.
- **Cumplimiento de los requisitos legales:** A los efectos de este manual, se entiende como el acatamiento de todas las leyes, obligaciones estatutarias, regulatorias o contractuales, así como de cualquier requisito de seguridad establecido por la Defensoría Penal Pública para materializar los controles asociados al Sistema de Seguridad de la Información.
- **Dirección IP:** Está referido al protocolo TCP-IP que consiste en un conjunto de convenciones de "diálogo", una secuencia de reglas a seguir en el intercambio de información. Un protocolo definirá, por ejemplo, la estructura y el orden a través de los cuales serán transmitidas las informaciones, las reglas de prioridad, la adaptación de flujos de datos a la capacidad de los enlaces, la forma en que serán detectados los errores de transmisión, etc. Internet descansa en una familia de protocolos de comunicación denominado TCP/IP (Transmisión Control Protocol/Internet Protocol).
- **Disponibilidad:** La propiedad de estar accesible y utilizable cuando lo requiera una entidad autorizada.
- **Dominio:** Un dominio o nombre de dominio es el nombre que identifica un sitio web.
- **E-mail (o correo electrónico):** Transmisión de mensajes a través de computadores. El destinatario del mensaje debe disponer de una casilla electrónica para recibir el mensaje.
- **Estación de Trabajo:** Es un microcomputador de alta gama diseñada para aplicaciones científicas y técnicas. En inglés son llamadas Workstation. El término "estación de trabajo" también ha sido usado para hacer referencia a un PC conectado a una red.
- **Firma Electrónica Avanzada:** Es aquella certificada por un prestador acreditado, que ha sido creada usando medios que el titular mantiene bajo su exclusivo control, de manera que se vincule únicamente al mismo y a los datos a los que se refiere, permitiendo la detección posterior de cualquier modificación, verificando la identidad del titular e impidiendo que desconozca la integridad del documento y su autoría.
- **Firma Electrónica Simple:** Es un conjunto de datos electrónicos unido a un documento y utilizado cuando un emisor envía un mensaje al receptor, y dicho mensaje va cifrado, de manera que nadie pueda modificarlo ni alterarlo. Además, la firma identifica al sujeto que la utiliza.
- **Hardware:** Corresponde a todas las partes tangibles de un sistema informático; sus componentes eléctricos, electrónicos, electromecánicos y mecánicos.

- **Horario de Trabajo:** Se entenderá como tal, el definido por la jefatura correspondiente.
- **Housing:** Área dedicada al almacenamiento de equipamiento destinado al procesamiento y almacenamiento de datos, con los respectivos sistemas que permiten un monitoreo constante del equipamiento y de las redes a las cuales están conectados.
- **Información:** Datos que poseen significado.
- **Integridad:** La propiedad de salvaguardar la exactitud y completitud de los activos.
- **Internet:** Es una federación de redes heterogéneas. Concretamente eso significa que cualquier computador del planeta puede comunicarse con cualquier otro computador, a través de cualquier medio de telecomunicaciones.
- **Intranet:** Red interna de empresas o administraciones que funciona con software y protocolos de Internet.
- **Lector Biométrico:** Es un dispositivo de identificación el cual utiliza la imagen tridimensional de la mano para verificar la identidad única de un sujeto.
- **Norma:** Acuerdos documentados que contienen especificaciones técnicas para ser usados como reglas, guías o definiciones características.
- **Política:** Actividad orientada a la toma de decisiones que conducen el accionar de la Defensoría.
- **Principios:** Reglas o normas, que orientan el presente documento.
- **Procedimiento:** Orden lógico de cómo debe efectuarse una actividad o proceso.
- **Protocolo:** Conjunto formal de instrucciones.
- **Repositorios:** Un repositorio, depósito o archivo es un sitio centralizado donde se almacena y mantiene información digital.
- **REDMINE:** Herramienta para la gestión de proyectos que incluye sistema de seguimiento de incidentes, calendario de actividades, diagramas de Gantt para la representación visual de la línea del tiempo de los proyectos, wiki, foro, visor del repositorio de control de versiones, control de flujo de trabajo basado en roles, integración con correo electrónico, entre otros.
- **Seguridad de la Información:** Preservación de la confidencialidad, integridad y disponibilidad de la información. Nota: Además, también pueden estar involucradas otras propiedades como la autenticidad, responsabilidad con obligación de informar, no-repudio y confiabilidad.
- **Servicios Tecnológicos:** Conjunto de partes que funcionan relacionándose entre sí con un objetivo preciso. Sus partes son hardware y software.
- **Sistemas Informáticos:** Conjunto de actividades (planeamiento, análisis, diseño, programación, operación, entrada de datos, autoedición, base de datos, etc.) asociados al manejo automatizado de la información que satisfacen las necesidades de los usuarios de este recurso.
- **Sistemas Operativos:** Un Sistema operativo (SO) es un software que actúa de interfaz entre los dispositivos de hardware y los programas usados por el usuario.
- **SLA:** Es una definición de los niveles de un servicio o plataforma informática en función de una serie de parámetros objetivos, establecidos de mutuo acuerdo entre cliente y proveedor, reflejando contractualmente nivel operativo de funcionamiento, multas por caída de servicio, limitación de responsabilidad por no servicio, etc.

- **Software:** Soporte lógico de un sistema informático, comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas, en contraposición a los componentes físicos, que son llamados hardware.
- **SPAM:** Envío de mensajes realizado en forma masiva, indiscriminada y no solicitada.
- **Tecnología WEB:** Conjunto de tecnologías de software que involucran una combinación de procesos de base de datos con el uso de un navegador en Internet a fin de realizar determinadas tareas o mostrar información.
- **Tecnologías de Información y Comunicaciones (Tics):** Término que agrupa al conjunto de herramientas y medios que permiten el intercambio y el procesamiento de la información.
- **Telecomunicaciones:** El conjunto de las técnicas de transmisión a distancia, cualquier sea el soporte.
- **Tiempo de respuesta:** Es el tiempo medido en horas, para que un proveedor tenga una respuesta o técnico en terreno, para solucionar un incidente, desde que se realiza el reporte a la mesa de ayuda del proveedor.
- **Tiempo de solución:** Es el tiempo para que un proveedor solucione un incidente, desde que el personal técnico se hace presente en dependencias de la Defensoría.
- **UPS:** Es un sistema de alimentación eléctrica ininterrumpida (por su nombre en inglés Uninterruptible Power Supply), consistente en una fuente de suministro eléctrico que posee una batería, permitiendo garantizar por un tiempo determinado el suministro de corriente a los dispositivos que tenga conectados y mantener la tensión de salida dentro de las tolerancias que se especifiquen, con independencia de las irregularidades y/o interrupciones que puedan producirse en la red de alimentación de la compañía eléctrica.
- **Web:** Presentación de una organización, de una empresa o de un particular en la www (modo de presentación gráfica en la Internet).
- **WIFI:** Mecanismo de conexión de dispositivos electrónicos de forma inalámbrica.