f. 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.

IX. Comité Tecnológico

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

a. Objetivo

Revisar las políticas y procedimientos 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 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, y los Jefes de los Departamentos de Estudios y Proyectos (DEP), Evaluación Control y Reclamaciones (DECR), Administración y Finanzas (DAF) y Recursos Humanos (RRHH).

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 Presidente, debiendo sesionar con la asistencia de sus titulares y al menos 4 de sus miembros. Anualmente, deberán revisarse los siguientes temas:

- Modificaciones al Manual de Procedimientos Tecnológicos.
- Seguimiento al Plan Tecnológico.
- Resultado de Auditorías.

X. Procedimientos

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, art. N°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 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:** 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 la asignación de correos electrónicos se determino crear dos tipos de casillas que tienen capacidades diferentes, en cuanto a; cantidad de espacio utilizado, tamaño de los correos, cantidad de remitentes, entre otros, los que fueron dimensionados, de acuerdo, a los recursos tecnológicos disponibles, los tipos de casillas disponibles se encuentra en el *Anexo C* Casillas Electrónicas.

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*.
- *Casillas Electrónica*, incluido *anexo C.*
- *Perfiles de Usuarios*, incluido anexo D.

g. Referencias

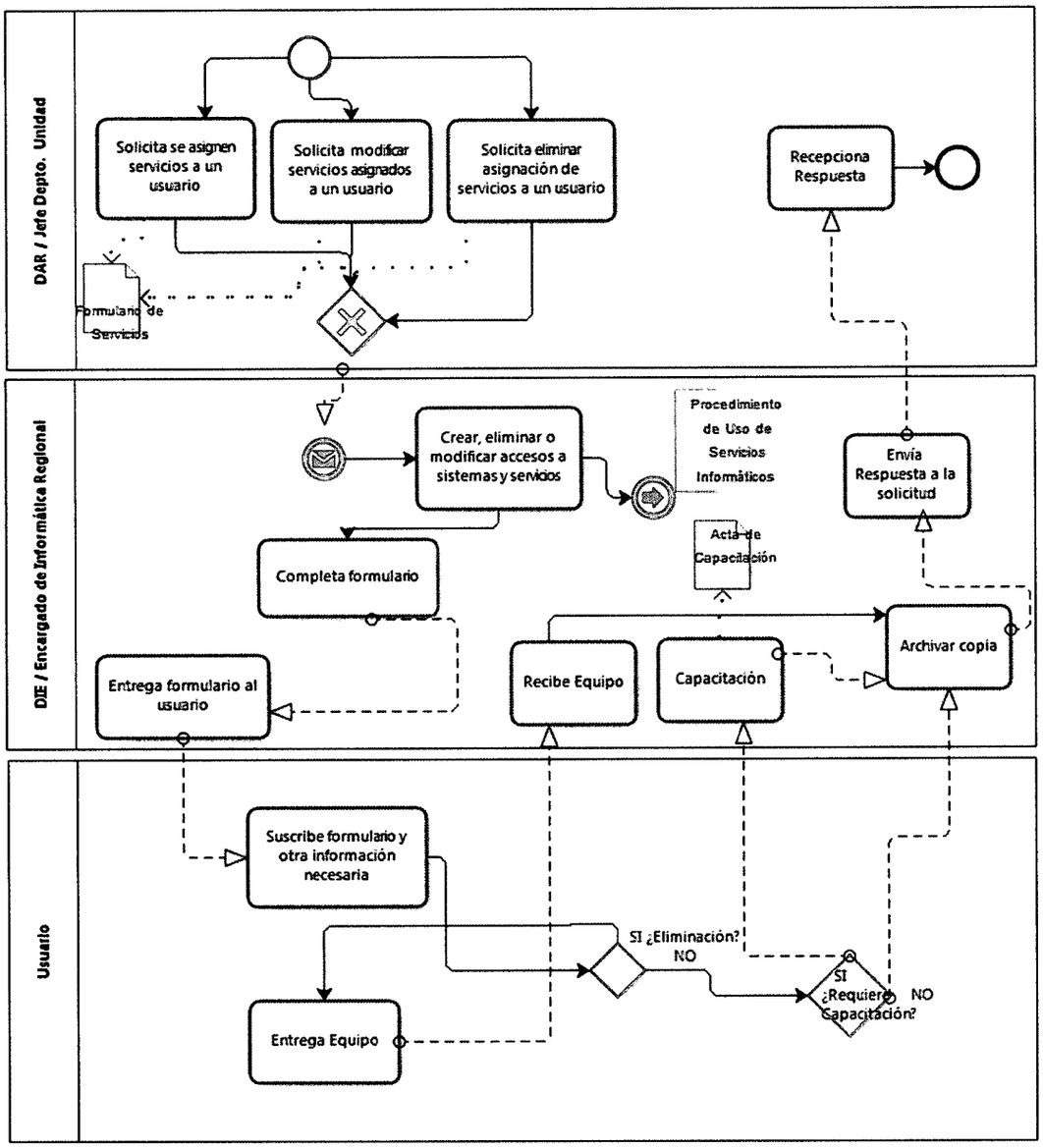
- Política Tecnológica, Política de Asignación de los Servicios Informáticos.
- Ley 18.334 sobre Estatuto Administrativo.
- DFL N° 1/19.653.

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)

Fecha			Uso DIE **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

Casillas Electrónicas

Funcionarios	Directivo
• Tamaño de la casilla electrónica 1 GB • Cantidad máxima de destinatarios 50 • Tamaño máximo de mensaje y adjunto 10 MB • Tamaño máximo de mensaje entrante 10 MB	• Tamaño de la casilla electrónica 3 GB • Cantidad máxima de destinatarios 50 • Tamaño máximo de mensaje y adjunto 10 MB • Tamaño máximo de mensaje entrante 10 MB

Anexo D

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. Procedimiento de Uso de Servicios Informáticos

a. Objetivo

Describir las acciones necesarias para el uso, custodia, seguridad y resguardo del equipamiento institucional que se encuentra asignado a los usuarios y los sistemas informáticos a los cuales se les brinda acceso.

b. Alcance

Se entenderá por equipamiento los siguientes: Computadores de Escritorio, Teléfonos, Celulares y Equipamiento en General. Además en este procedimiento se incorpora el uso de los servicios de Correo Electrónico, Licenciamiento y Sistemas Informáticos. También 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, 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, 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 hrs. 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 y sistemas.

- **Fallas:** En el *anexo B* se incluye un formato tipo para el reporte de fallas del usuario al encargado de soporte 1er nivel. Para que el soporte de 1er nivel realice los reportes de falla ya sea sobre los sistemas o servicios, debe utilizar el Sistema REDMINE, dicho sistema entrega una orden de trabajo que es gestionada por el soporte de 2do nivel. Todos los encargados de soporte de 1er y 2do nivel deben tenerlo instalado y utilizarlo al momento de efectuar los reportes de falla tanto de operaciones como de desarrollo.

3. Uso de Correo Electrónico

- **Uso**: Cada usuario será el responsable del uso de su correo electrónico, el que tendrá asignado una casilla con un espacio máximo y condiciones de uso, las que deberán ser informadas por el soporte de 1er nivel, al momento de ser creada la casilla o en capacitaciones posteriores.

- **Incidentes:** Los incidentes que ocurran al usuario durante el uso del correo deberán ser reportados al soporte de 1er nivel, sobre todo en los casos en que el usuario tenga dudas sobre la fuente de los correos o los adjuntos que incorporan.

- **Escalabilidad:** EL usuario reportará todos los incidentes al soporte de 1er nivel, quien deberá reportar los incidentes al soporte de 2do nivel o Encargado de Operaciones del DIE. Este servicio tiene incorporado en su contrato el servicio de soporte en caso de fallas u otros incidentes.

- **Soporte y plazos:** Los tipos de soporte para este servicio son los determinados en la *Política de Soporte a Usuarios*. Y los plazos de respuesta estarán determinados por el contrato de servicios vigente.

4. Uso de Licencias de Software

Como lo indica las políticas tecnológicas el uso de licenciamiento para el software que se utiliza en los computadores personales, notebook y otros, es obligatorio. Asimismo respecto de las plataformas de servicios donde se establece el tipo de software que utilizará la Defensoría para el motor de base de datos, virtualización y otros.

5. Uso de Sistemas Informáticos

El uso de los sistemas de la Defensoría va a estar determinado por el perfil del usuario, todos los sistemas deben tener niveles de autenticación para los usuarios, donde las claves corresponderán al RUT y la contraseña a los 6 primeros dígitos del mismo, las claves deberán ser cambiadas por el usuario la primera vez que utilicen los sistemas y remplazarlas por lo menos cada 3 meses.

Al momento de entregar a los usuarios las claves y contraseñas de entrada a los sistemas deberá efectuarse una capacitación sobre su uso por parte del soporte de 1er nivel.

Las cuentas de usuario que permanezcan sin actividad durante un mes calendario serán automáticamente bloqueadas.

f. Registros

- Pruebas para verificar el funcionamiento de los servicios de telefonía fija, telefonía móvil y computadores de escritorio, incluido *anexo A*.
- Para los reportes de falla o solicitud de soporte, deberá quedar un registro, de parte del usuario y este deberá ser vía correo electrónico, con la información necesaria para el reporte, los que se detallan en el *Formulario Reporte de Falla del Usuario al Soporte de 1er Nivel,* incluido en el *anexo B*.
- Constancia en carabineros, en caso de Robo o Hurto, emitido por Carabineros de Chile.
- REDMINE para el reporte de 2do nivel.

g. Referencias

- Política Tecnológica, Política Uso de los Servicios Informáticos
- Ley 18.334 sobre Estatuto Administrativo.
- DFL N° 1/19.653.

h. Indicadores

- I_{01}= Cantidad de fallas reportadas en el año t / Cantidad de fallas resueltas en el año t.
  Nota: Los valores de este indicador se van a extraer del sistema REDMINE.

i. Diagrama de Flujo

Diagrama de Flujo Reporte de Fallas

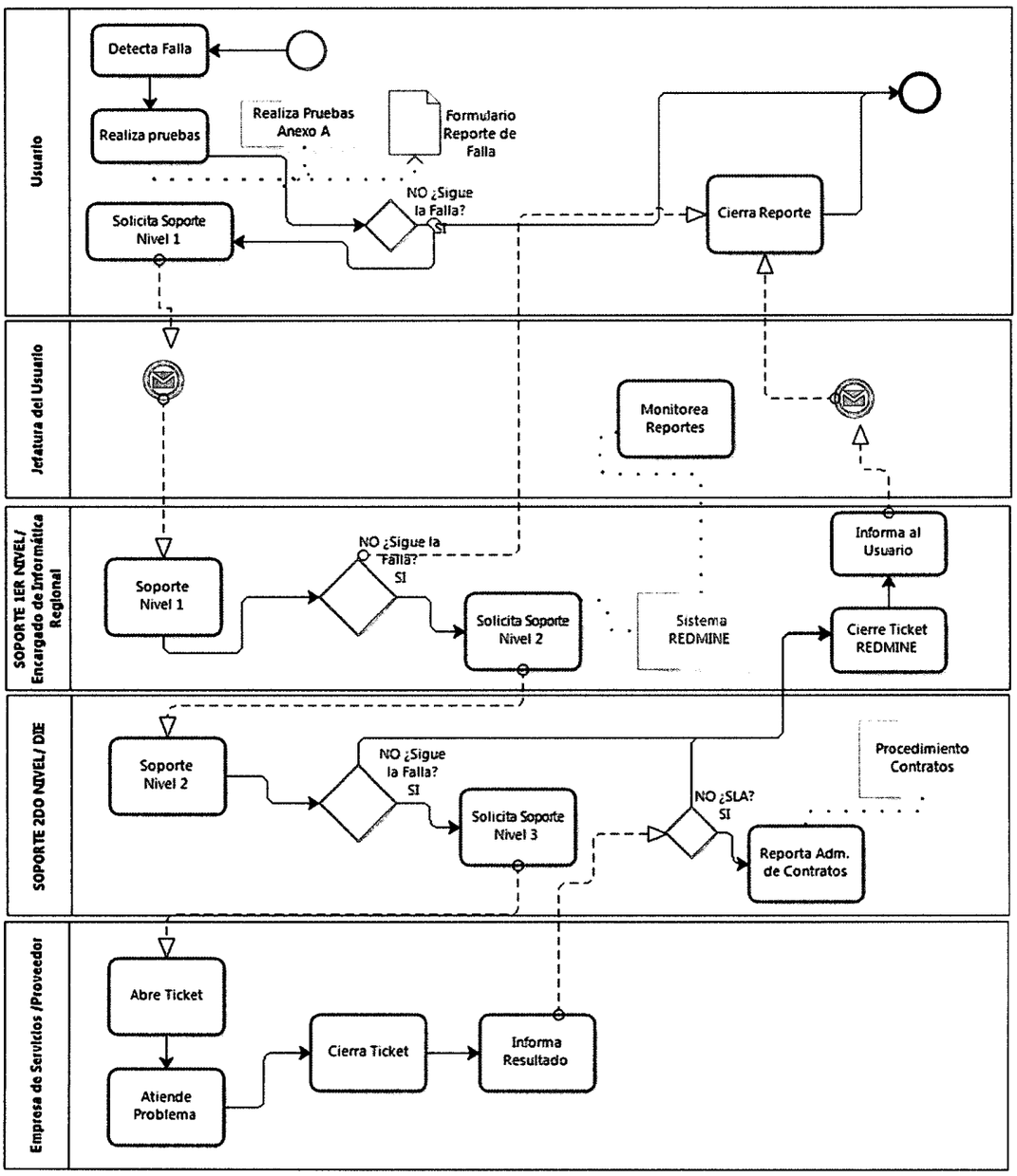
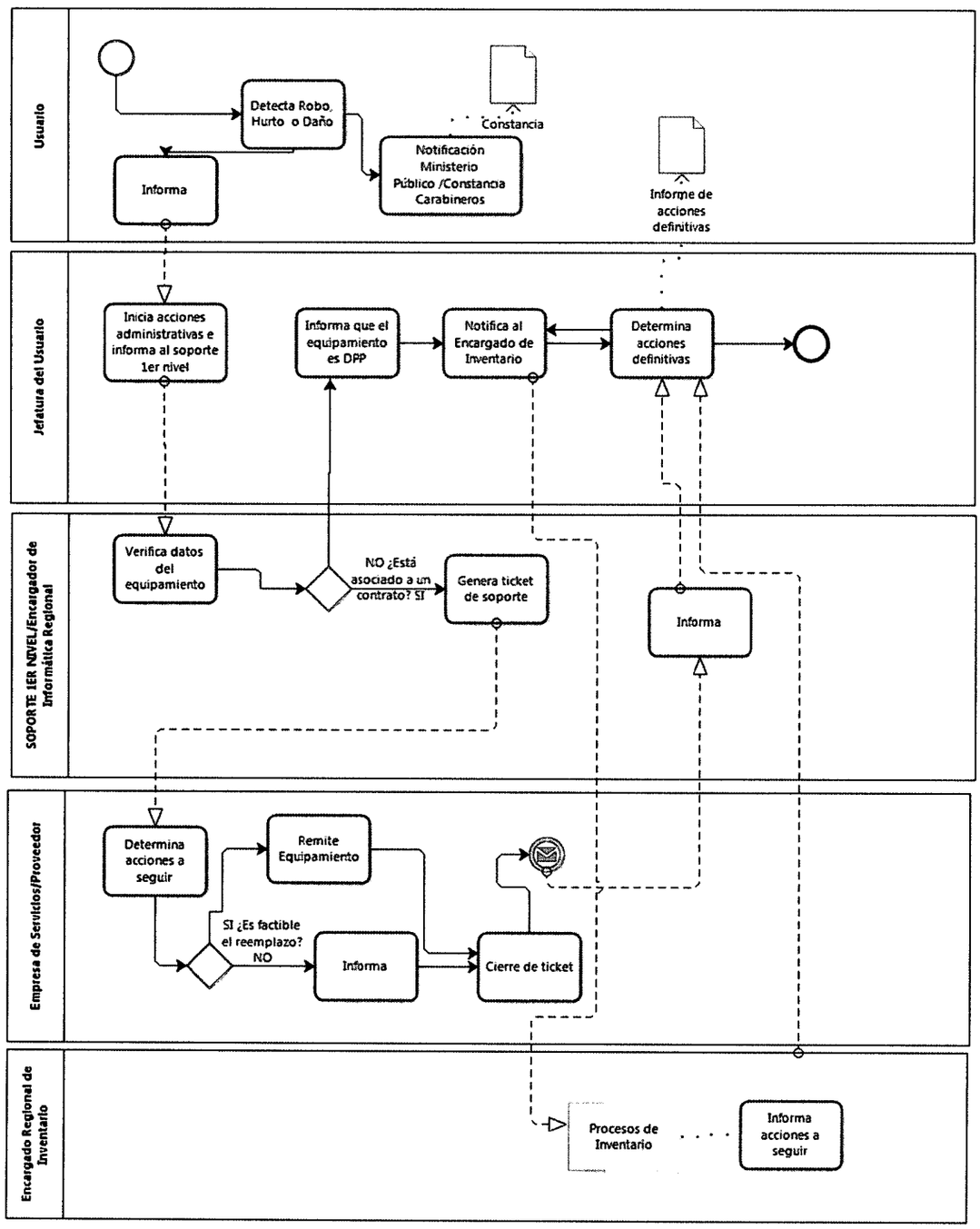


Diagrama de Flujo Robos, Hurtos o Daños del Equipamiento



j. 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 esta 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		

Anexo B
Formulario Reporte de Falla del Usuario al Soporte de 1er Nivel

Formulario Reporte de Fallas	Defensoría Sin defensa no hay Justicia
Uso USUARIO	
Región	
Oficina	
Defensoría	
Nombre del Usuario Responsable	
Tipo Equipamiento	
Serie del equipamiento	
Etiqueta (si corresponde)	
Descripción del evento o falla	
Fecha del Reporte	
Uso Encargado de Informática/DIE	
Acciones realizadas	
Ticket de atención	
Fecha de atención	
Observaciones	

Cierre de Reporte

Acta de entrega:

Fecha

Día	Mes	Año

Usuario

Encargado DIE/Regional

Nombre:

3. Procedimiento de Servicios Informáticos

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 esta 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:** Mensualmente 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

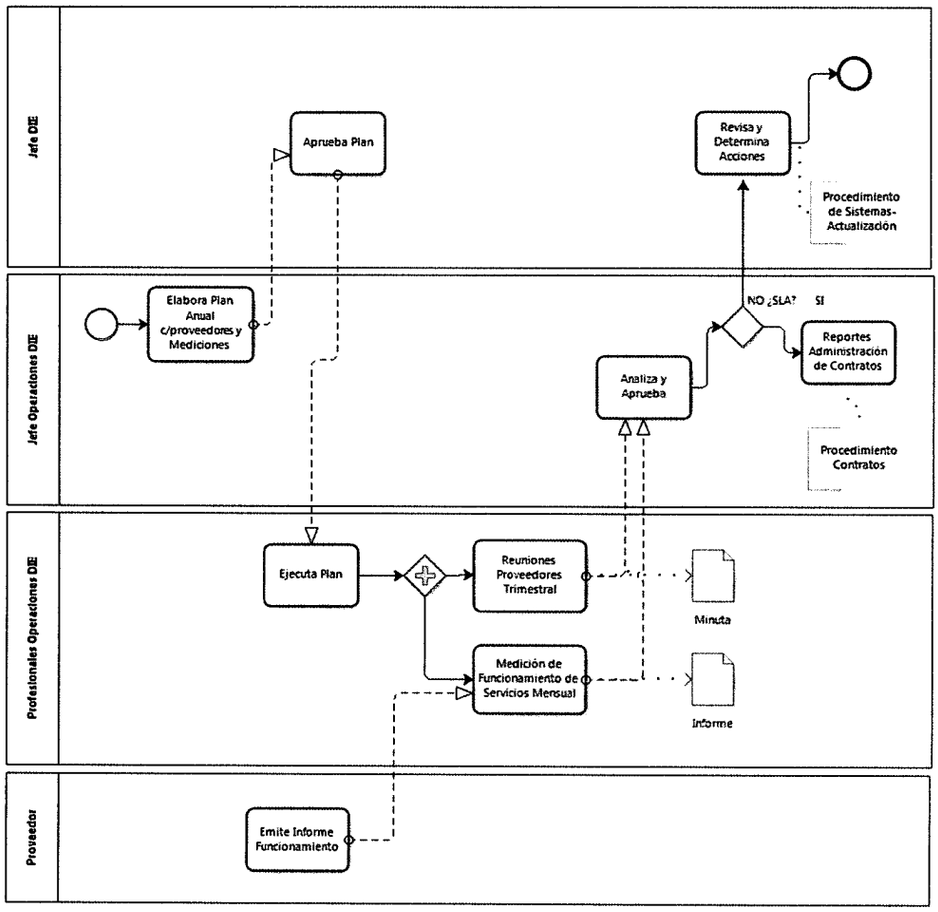
- Contrato de Servicios con los proveedores.

g. Indicadores

- I_{03}= Cantidad de informes emitidos por Operaciones en el año t / Cantidad de informes que corresponden en el año t (10).
  Nota: Para la emisión de los informes de exceptúan los meses de (enero-febrero).
- 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 Administración (cumple/no cumple)												
2. Medición Mantención Preventiva (cumple/no cumple)												
3. Medición Mantención Correctiva (cumple/no cumple)												
4. Medición disponibilidad (eventos y tpo)												
5. Multas												
Reuniones (Marcar fecha)												
Servicio de Telecomunicaciones												
1. Medición Servicio de Administración (cumple/no cumple)												
2. Medición Mantención Preventiva (cumple/no cumple)												
3. Medición Mantención Correctiva (cumple/no cumple)												
4. Medición 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			

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 Semestral*, 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 Semestral*.
- **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, SCD y SIGO.

    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: Carpetas, Inspectoría, ARGEDO, 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 25 sistemas restantes identificados.

2. **Levantamiento de Requerimientos:** El Comité Tecnológico tiene una participación relevante en esta etapa cuyo fin es establecer la prioridad a los requerimientos que se van a llevar a desarrollar. Este proceso se inicia con el informe de requerimientos de las unidades, que deberán efectuarse en forma semestral. 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.

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 esta compuesto por un grupo de usuarios designados para este propósito.

5. Respaldo de Sistemas

a. Base de Datos Oracle: Para respaldar una base de datos ORACLE versión 10g se debe utilizar el utilitario Recovery para lo cual se deberá acceder la máquina donde se encuentra la base de datos instalada con una cuenta con privilegios de SYSDBA a través de ORACLE Enterprise Manager o directamente por medio de la herramienta SQL Plus. Se pueden hacer dos tipos de respaldo online y offline. Se podrá hacer un backup online solo si la base de datos está en modo ARCHIVELOG. Los backup offline obligan a que las bases de datos no pueda ser utilizada mientras se desarrolle el respaldo. Para poner la base de datos en modo ARCHIVELOG/NOARCHIVELOG se puede hacer de Enterprise manager también se puede hacer desde SQL Plus.

   Se deberá efectuar un backup full una vez a la semana que guarde todos los archivos que forman parte de la base de datos, es decir, Datafiles, Archivos de Redo Log, ControlFiles, archivo de parámetros y Undo Segments y diariamente un respaldo incremental para respaldar las modificaciones o creación de nuevos registros.

b. Base de Datos Exchange: Para realizar el respaldo de las bases de datos mailbox Exchange se utilizará NTBACKUP. Esta es una herramienta de respaldo incluida en el sistema operativo Windows en todas sus versiones.

c. Base de Datos SQL SERVER: Para respaldar una base de datos SQL SERVER se debe utilizar el Agente SQL SERVER. Se deben considerar respaldos permanentes y backup completo o full una vez a la semana y diariamente incremental. Para programar la ejecución de tareas se debe crear un JOB a través del SQL Agent, orientado al árbol SQL Server donde se encuentra las bases de datos y demás funciones, la carpeta Management > SQL Agent. El script para generar el backup debe identificar el nombre de la base de datos y la ubicación del respaldo.

d. Base de Datos SIAR: Para realizar el respaldo de una base de datos MySQL se utiliza "mysqldump". Se deben considerar respaldos permanentes backup completo o full una vez a la semana. Para automatizar la ejecución del proceso de respaldo, se debe utilizar un mecanismo que ofrece el sistema operativo para este efecto. Para el caso de los sistemas LINUX se debe utilizar cron.

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 clausulas 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.