Defensoría
Sin defensa no hay Justicia

MANUAL DE PROCEDIMIENTOS TECNOLÓGICOS

DEFENSORÍA PENAL PÚBLICA

DEPARTAMENTO DE INFORMÁTICA Y ESTADÍSTICA

Versión 1.0

Agosto de 2013

Elaborado por:	Revisado por:	Aprobado por:
Jefe Departamento de Informática y Estadísticas	Director Administrativo Nacional	Defensor Nacional
Fecha: 12/08/2013		

Defensoría
Sin defensa no hay Justicia

Contenido

I. 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
- RRHH : Recursos Humanos
- SPAM : Stupid Pointless Annoying Messages
- SSI : Sistema de Seguridad de la Información
- UAJ : Unidad de Asesoría Jurídica

II. 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, 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 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.

III. 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 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.

IV. 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 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 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.

V. Vigencia

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

VI. 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 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 aquellos que no se encuentren disponibles en Internet.

- **Alta Disponibilidad**: El funcionamiento de los sistemas informáticos del negocio 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 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 del servicio de defensa penal serán de carácter reservado.

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

VII. 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. **Directivos de Departamentos y Unidades de la Defensoría Penal Pública:** 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.

c. **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 de la Defensoría y que dicen relación con las actividades asociadas al uso de la tecnología a cargo del DIE.

d. **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.

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. **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.

g. **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.

h. **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.

i. **Personal 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. El Personal 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 los Servicios y Sistemas Informáticos:** Corresponden a todos aquellos que hacen uso total o parcial de los servicios y sistemas informáticos que se disponen en la Defensoría Penal Pública. Existirán 2 tipos de usuarios ; *Internos* correspondiente a todos aquellos que acceden a los sistemas y servicios en las dependencias físicas de la Defensoría Penal Pública, entre estos se consideran al personal de la Defensoría, al personal de proveedores externos (guardias, técnicos residentes) y estudiantes en práctica, *y Externos* correspondientes a todos aquellos 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.

VIII. Política Tecnológica

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 responda y solucionen las 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 y sistemas informáticos y presentar propuestas de mejora a ser evaluada 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 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.
- Mantener limpio y en óptimas condiciones el equipamiento asignado y su cuenta de correo electrónico.
- 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 a 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 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 del DAN. 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 password 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 Director 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 de su adecuado uso, mantenimiento y custodia 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 las DR, DL y Departamentos de la DN, de acuerdo a sus necesidades para el desempeño de sus funciones (equipos de videoconferencia, impresoras, relojes biométricos, UPS, WIFI, proyectores, telefonía, etc.).

Cada Defensoría o Departamento 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 DAF, 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 tener contratos de soporte y actualización.

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

- Base de datos : Oracle 11g
- Correo electrónico : Exchange 2010
- Productividad : MS Office Profesional
- Antivirus : McAfee
- Virtualización : WMWare Sphere V.5.1

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. Esto incluye las siguientes aplicaciones:

Sistema Operativo	Windows 7 Profesional.
Herramienta de Productividad	Microsoft Office Pro 2010, que incluye Word, Excel, Power Point, Outlook y One Note.
Lector de documentos PDF	Adobe Reader x (10.1.1 v)
Compresor de archivos	7–Zip, que posee más compatibilidad con formatos de compresión.
Antivirus Corporativo DPP	McAfee, que incluye antivirus (software maliciosos) y anti spyware (software de espionaje).
Complementos	Java versión 6 update 30, para uso de sistema SIGDP Flash Player 11.2v, para permitir la completa navegación en sitios web que lo exigen. Codec K-Lite Codec Pack 6.3v, 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.

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 DN.

- **Soporte Nivel 2:** Requerido sólo 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.	Telecomunicaciones Telefonía Videoconferencia Housing Plataforma Central Oracle Infraestructura Virtual Bases de Datos Correo Electrónico 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.	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 el servicio de housing que asegura las debidas condiciones de protección, monitoreo y continuidad del servicio y que cumple 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 Informáticos

Se deberá contar con un plan de contingencia que prevea fallas críticas en los servicios y/o sistemas principales, el que deberá contener una copia actualizada de los programas y sus ambientes operativos, respaldos de datos y equipamiento 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 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:

- **Esenciales**: Arica, Iquique, Antofagasta, Copiapó, La Serena, Valparaíso, Rancagua, Talca, Concepción, Temuco, Valdivia, Puerto Montt, Coyhaique, Punta Arenas, Centro Justicia, DN y Los Héroes.

- **Alto Impacto**: 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.

- **Mediano Impacto**: Vallenar, Chañaral, Ovalle, San Antonio, San Fernando, Rengo, Santa Cruz, Linares, Angol, Ancud, Castro y Curacaví.

- **Bajo Impacto**: Tocopilla, Tal-Tal, Illapel, Los Andes, La Ligua, Pichilemu, Cauquenes, Parral, San Javier, Constitución, Arauco, Cañete, Coronel, Villarrica y Puerto Natales.

- **Extremas**: Alto Hospicio, Isla de Pascua, Futaleufú, Puerto Cisnes, Cochrane, Chile Chico, Puerto Aysén y Porvenir.

Aspecto	Esenciales	Alto Impacto	Mediano Impacto	Bajo Impacto	Extremas
Velocidad Enlace	6 a 100 Mbps	1 a 2Mbps	1 a 2 Mbps	1 a 2 Mbps	512 Kbps a 2 Mbps
Punto de Conexión	Santiago	Santiago o Esencial si hay en la misma ciudad	Santiago o Esencial si hay en la misma ciudad	Santiago o Esencial si hay en la misma ciudad	Santiago o Esencial si hay en la misma ciudad
Enlace Respaldo	Si (algunos)	No	No	No	No
Wi-Fi	Si	Si	No	No	No
Videoconferencia	Si	No	No	No	No
Cantidad y tipo de teléfonos	Tipo A: Secretarias Tipo B: Jefatura	Tipo A: 1 Tipo B: 2 a 6	Tipo A: 0 Tipo B: 2 a 5	Tipo A: 0 Tipo B: 2 a 4	Tipo A: 0 Tipo B: 1 a 2
Consola Visualizador	Si	No	No	No	No
Troncales Planta Telefónica	8 máx.	2	2	2	2
Servidores	Si	No	No	No	No
Computadores	20 ó más	5 a 7	2 a 5	2 a 4	1 ó 2
Fax	2	1	1	1	1
Impresoras	Color + B/N multifuncional	B/N multifuncional	B/N multifuncional	B/N multifuncional	B/N multifuncional
Scanner	Si	No	No	No	No
Reloj Biométrico	Si	Si	No	No	No
Pistolas Lectoras	Si	Si	Si	Si	Si
Encargado Informático	Si	No	No	No	No
Data-Show	Si	Si (algunas)	No	No	No

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 con el negocio de la organización y se pueden definir como esenciales.
- **Impacto Medio:** considera los sistemas que relacionándose con el negocio, provocan un impacto medio o de carácter estacional en la organización.
- **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 de esta.

	Sistemas		
Criterios	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, a excepción de los 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 4 capas	A medida en 4 capas Licenciado	
Browser	IE 9.0 o posterior Firefox 21 o posterior	IE 9.0 o posterior Firefox 21 o posterior	IE 9.0 o posterior Firefox 21 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: al que sólo tendrá acceso personal del área de Operaciones del DIE.
- Ambiente de Prueba: al que tendrán acceso los usuarios del grupo de pruebas.
- Ambiente de Desarrollo: al que tendrán acceso personal del área de Desarrollo del DIE y programadores externos.

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 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 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 DS 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/IEC 27.001:2005 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 respaldo 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 (seguros, redundancia de equipamiento, alertas y monitoreo, mantención preventiva y correctiva) 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 del servicio y la calidad en la prestación.

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. 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 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 Informático

Los contratos de provisión de servicios informáticos 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 se deberá exigir 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 permita 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, etc.; pero fuera de los horarios de trabajo, el horario de trabajo corresponderá al determinado por la jefatura correspondiente y el estatuto administrativo.

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, publicitados y notificados a todos los funcionarios de la institución, y se entenderá y dará por "conocido" por los funcionarios de la institución.

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 sistemas y servicios informáticos que se requiere para prestar sus servicios a la Defensoría. Todo documento publicado por este medio se entenderá y dará por "conocido" por los funcionarios de la institución.

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.

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 y sistemas informáticos. En otras palabras, un nombre de usuario y una clave cifrada, personal y confidencial. Para ello, cada incorporación de nuevas personas se integren a la Defensoría deberá ser informada por el Departamento de RRHH 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 RRHH, deberá 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, 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, 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 contratado 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 dos 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 funcionario y se podrán utilizar para intercambio de información de todo orden entre funcionarios de la institución y entre éstos y terceros ajenos de la organización. Su mantención estará a cargo del correspondiente usuario. No se asignarán cuentas de correo electrónico a asistentes de las empresas de defensa licitada, ni tampoco a las personas que efectúen prácticas profesionales en la institución.

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 destruya 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 áreas 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.