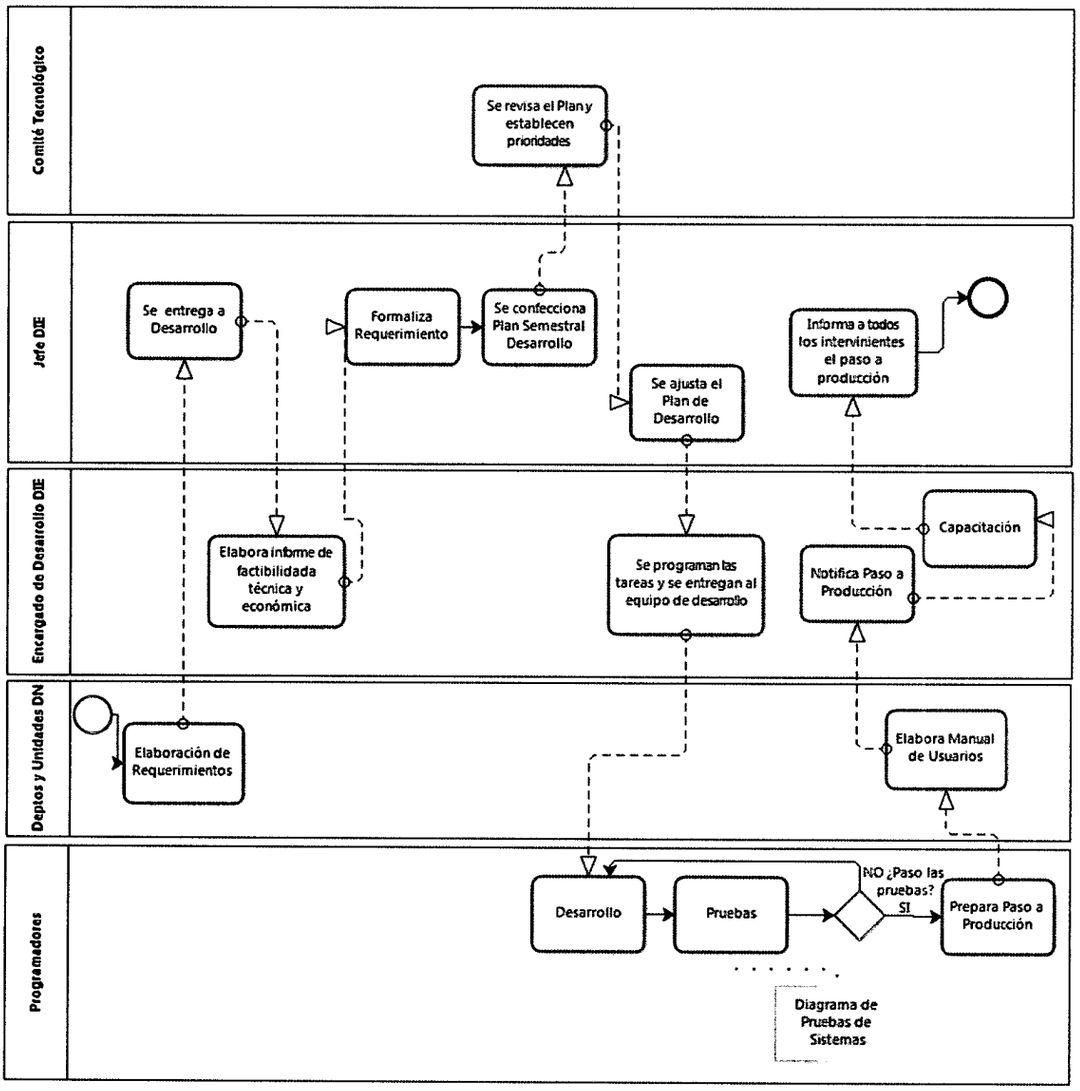
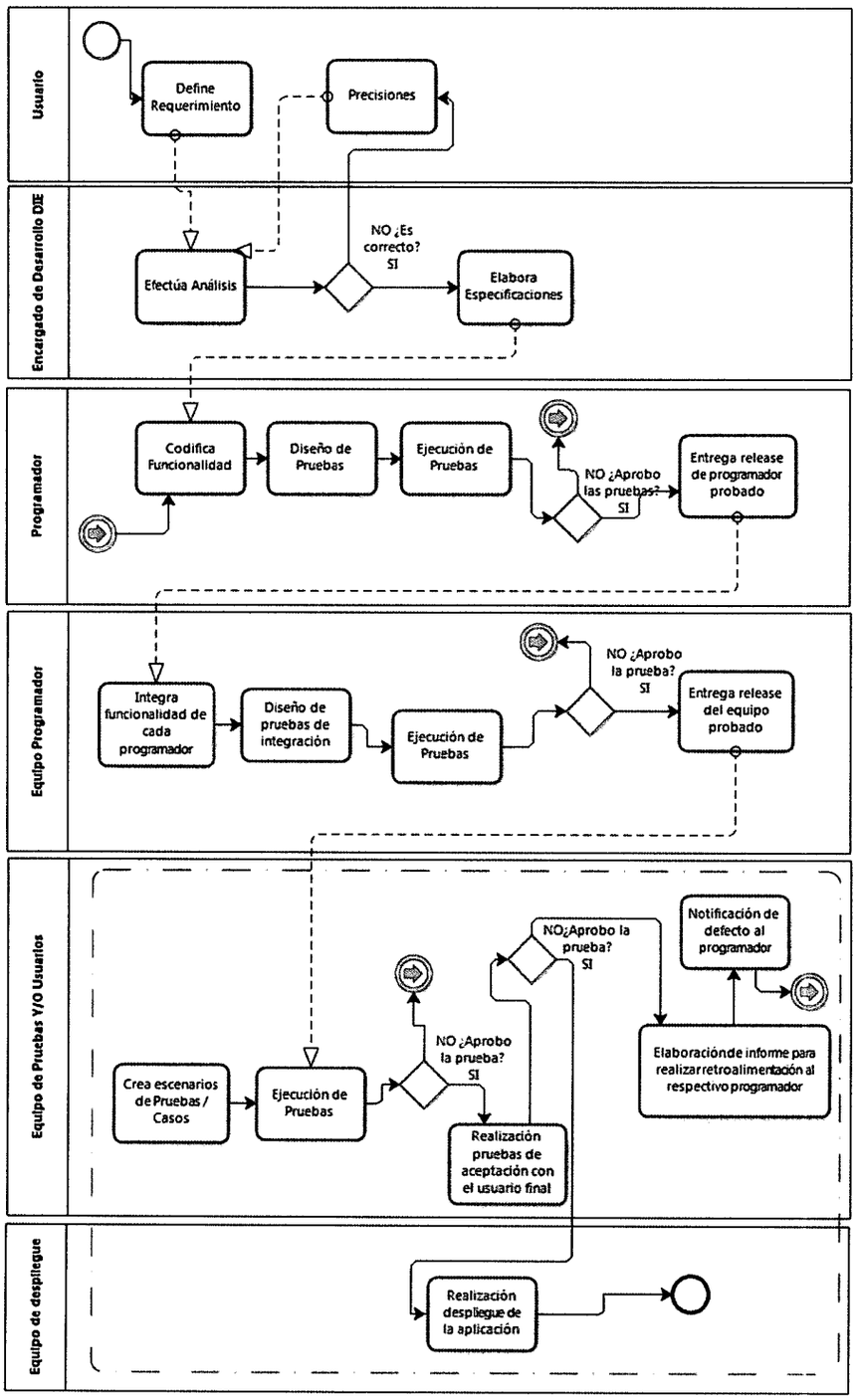
## h. Diagrama de Flujo

### Diagrama de Proceso de Desarrollo de un Requerimiento



## Diagrama de Pruebas de Sistemas




## i. Anexos

- No hay

# 5. Procedimiento de Contrataciones

## 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 DS 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.
- **Encargado de la Gestión de los Contratos del 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 contrata 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 Catalogo Electrónico del Convenio Marco, donde el documento que compromete la compra es la solicitud de compra del DIE dirigida a la DAF. Si la contrata se efectúa mediante el procedimiento de trato directo, está será realizada a través de resolución 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 licitación 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**

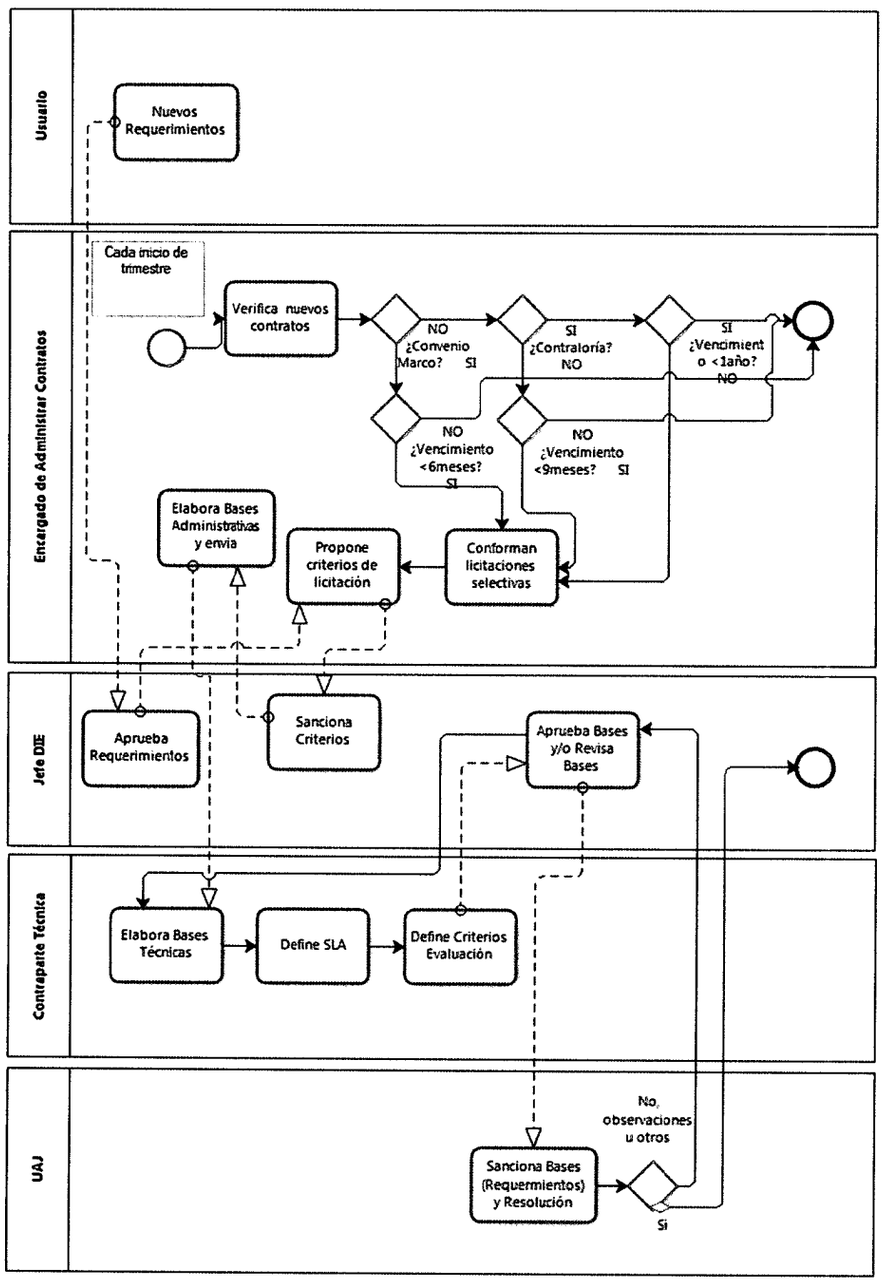
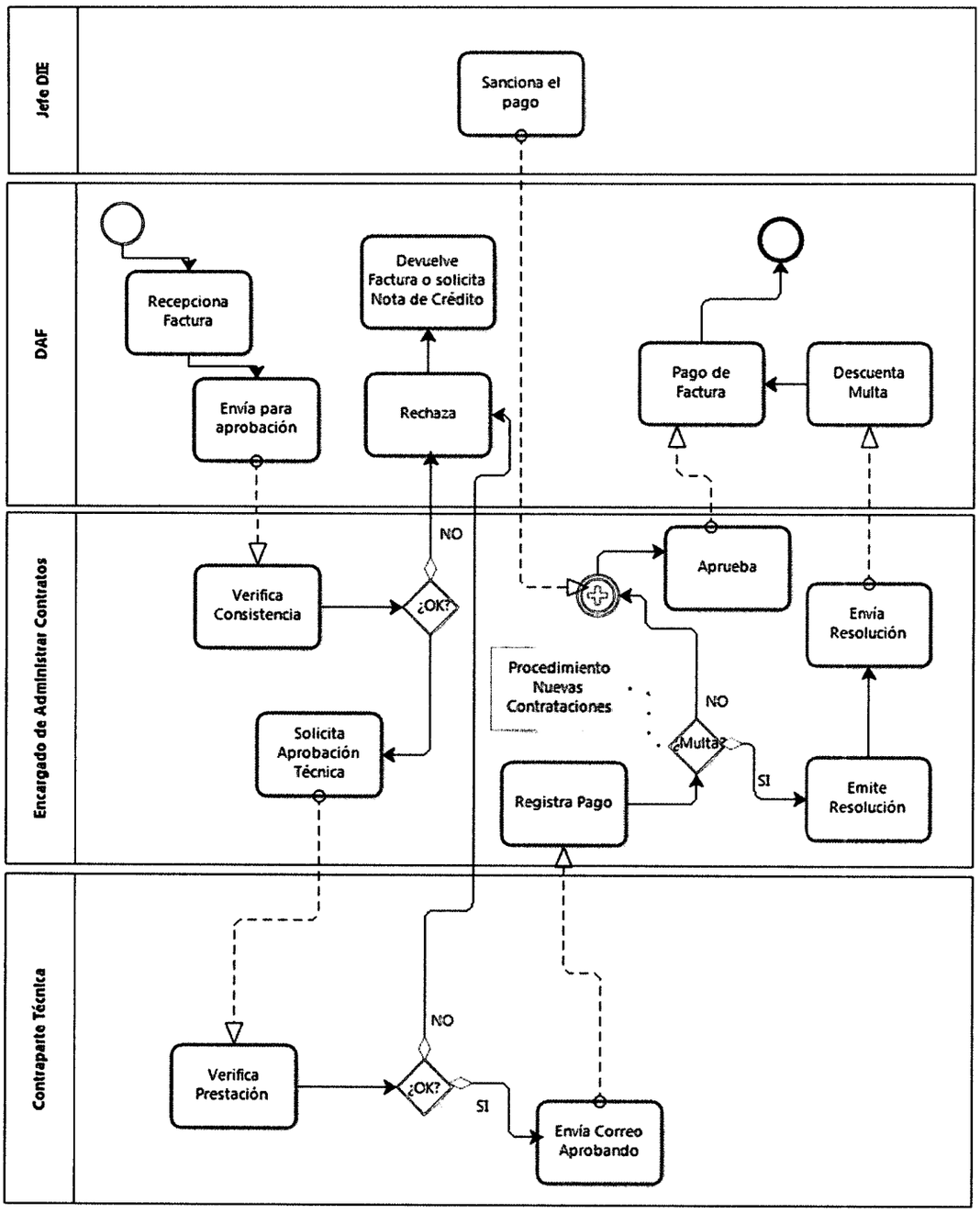


**Diagrama de Proceso de Pago**




## j. Anexos

- No hay

# 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 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 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 password. 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

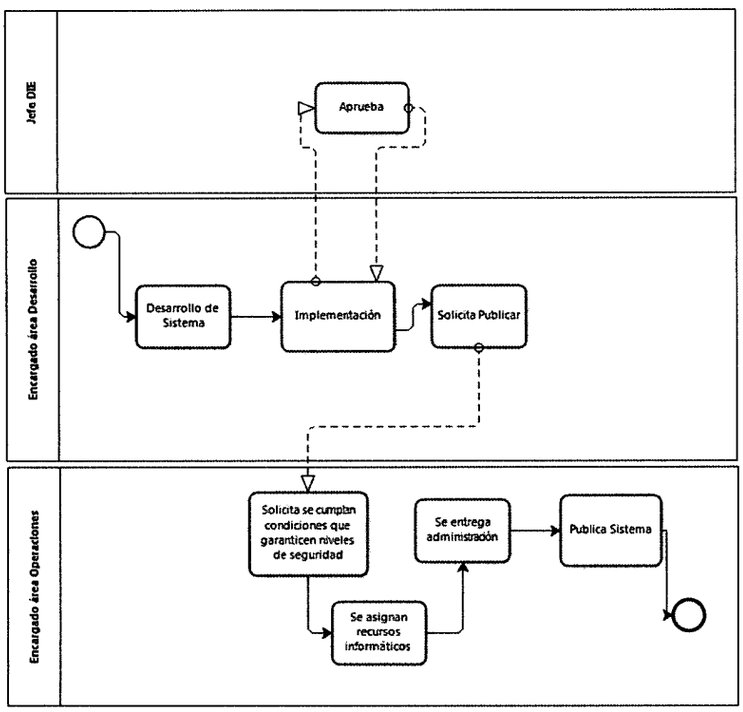
- Políticas de privacidad, disponibles en la página Intranet.
- Ley N°20.285 sobre acceso a la Información Pública.

## g. Indicadores

- No hay

## h. Diagrama de Flujo

**Diagrama de Publicación de Sistemas**




## i. Anexos

- No hay

# 7. Procedimiento de Seguridad de la Información

## 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.
- **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.

# 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.

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**

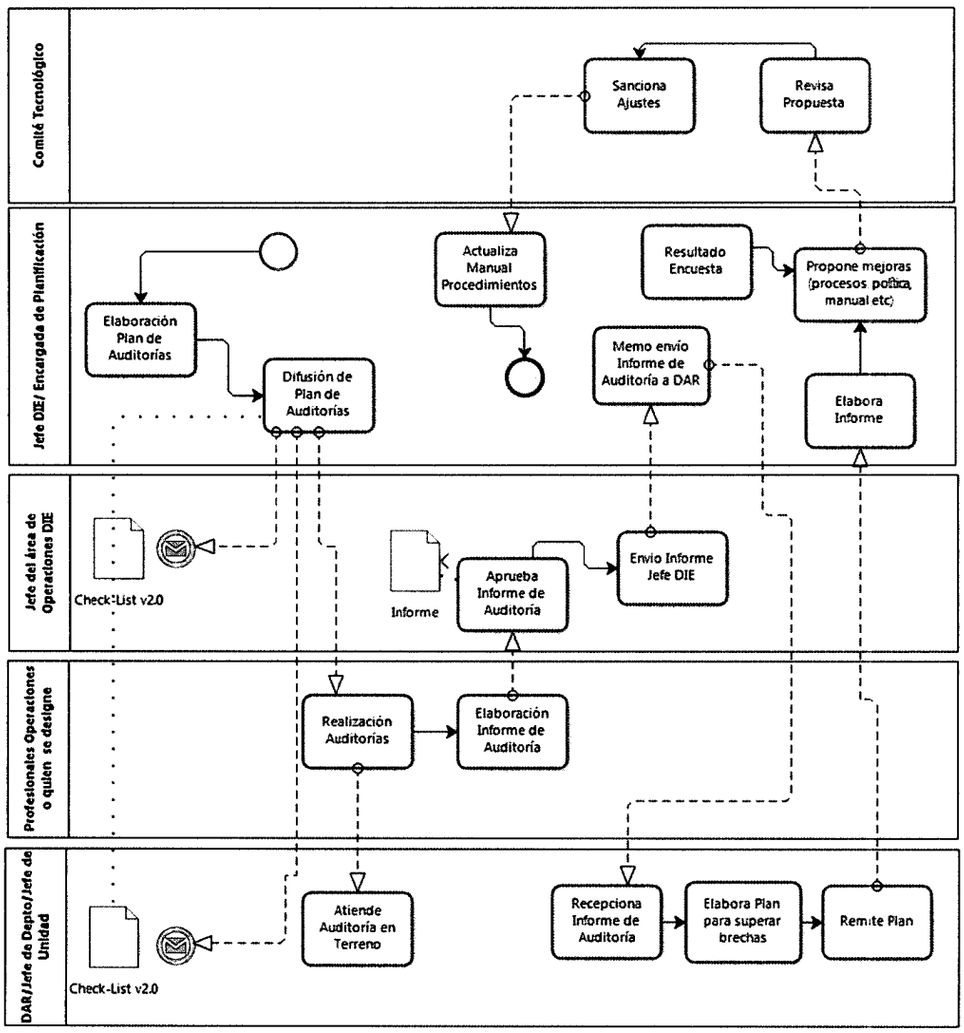
- No aplica.

**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<br>Sin defensa no hay Justicia | **Auditoría**<br>**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 ultima mantencion 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 | Encargado de Informática Regional |
| Fecha: / / | Nombre: |
| 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 | |

# XI. Anexos

## 1. 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/IEC 27.000:2005 es un conjunto de estándares desarrollados -o en fase de desarrollo- por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), 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°1921 de fecha 16 de Junio de 2011 de la Defensoría Nacional, que aprueba la Política de Seguridad de la Información.
- Resolución Exenta N°1598 de fecha 19 de Mayo de 2011 de la Defensoría Nacional, que conforma el Comité de Seguridad de la Información.
- Resolución Exenta N°595 de fecha 14 de Febrero de 2012 de la Defensoría Nacional, Procedimientos Administrativos de Activo Fijo.
- Ley N°20.285, sobre Acceso a la Información Pública.
- Ley N°10.039, 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.

## 2. 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:** Esta 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 una microcomputadora 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 una PC conectada a una red.
- **Extensiones:** En informática, la extensión de archivo es una cadena de caracteres anexados al final de un nombre de archivo separados por un punto. Las extensiones suelen determinar el tipo de formato del archivo al que pertenecen y así poder ser reconocido por el sistema operativo o por el programa que lo ejecuta
- **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:** Consiste en una área dedicada al almacenamiento de equipamiento destinado al procesamiento y almacenaje 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: entre otros la red telefónica. Esta interconexión de redes heterogéneas ha sido posible gracias a la familia de protocolos TCP/IP.
- **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.
- **Nuevas tecnologías de información y comunicación:** Término que agrupa al conjunto de herramientas y medios que permiten el intercambio y el procesamiento de la información.
- **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
- **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 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 Informáticos:** Conjunto de partes que funcionan relacionándose entre sí con un objetivo preciso. Sus partes son hardware y software.

- **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:** Porcentaje de tiempo que se asegura que un servicio o plataforma informática está disponible sin interrupciones.
- **Software:** Se conoce como software al equipamiento lógico o 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 medido en horas, para que un proveedor solucione un incidente, desde que el personal técnico se hace presente en la Defensoría.
- **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.