REPÚBLICA DE CHILE
Ministerio de Justicia
Defensoría Penal Pública

APRUEBA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA DEFENSORÍA PENAL PÚBLICA.

Santiago, 16 JUN. 2011

Resolución Exenta N° 1921

VISTOS:

1. Lo dispuesto en la Ley N°19.718, que crea la Defensoría Penal Pública;

2. Lo dispuesto en Decreto Supremo N° 83 del Ministerio Secretaría 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;

3. Lo dispuesto en la norma chilena NCh N° 27.002 del Instituto Nacional de Normalización, de 2009, sobre códigos de práctica para la gestión de seguridad de la información;

4. El oficio DN N° 793, de 2008, que aprueba, publica y difunde la Política Informática de la Defensoría Penal Pública, actualizada en el año 2010;

5. El Decreto Supremo N°503 del 04 de julio de 2008, del Ministerio de Justicia, que nombra a la suscrita Defensora Nacional.

6. Guía Metodológica 2011 Programa de Mejoramiento de la Gestión del Sistema de Seguridad de la Información. Subsecretaría del Interior – Dirección de Presupuestos del Ministerio de Hacienda.

7. La Resolución Exenta N° 1.600, de la Contraloría General de la República, de 2008, que fija normas sobre exención del trámite de toma de razón.

CONSIDERANDO:

1. Que las políticas del gobierno están orientadas a la incorporación de Tecnologías de la Información y Comunicaciones en los órganos de la Administración del Estado, con el fin de mejorar los servicios e información ofrecidos a los usuarios, de generar una gestión pública más eficaz y eficiente e incrementar sustantivamente la transparencia del sector público y la participación ciudadana;

2. Que en el marco del Programa de Mejoramiento de la Gestión "Sistema de Seguridad de la Información", mediante Resolución Exenta N°1598 de fecha 19 de mayo de 2011, se creó el Comité de Seguridad de la Información y se fijaron sus funciones.

3. Que dicho Comité se constituyó con fecha 19 de mayo de 2011, según consta en acta suscrita por la totalidad de sus integrantes y asistentes a la sesión.

4. Que dentro de las funciones del Comité referido está proponer la Política de Seguridad de la Información a la Jefa de Servicio. En este sentido el Encargo de Seguridad de la Institución y Presidente del Comité ya referido, remitió propuesta a la suscrita, a través memorándum Comité SSI N°001 con fecha 14 de junio del 2011.

RESUELVO:

1. **APRUÉBESE** la Política de General de Seguridad de la Información de la Defensoría Penal Pública, cuyo texto es el siguiente :

DEFENSORÍA PENAL PÚBLICA ASESOR JURÍDICO

POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN
DEFENSORÍA PENAL PÚBLICA
Versión 1 - 27.05.2011

CONTROL DE VERSIONES

Nº Revisión	Fecha Elaboración	Fecha Aprobación	Motivo de la revisión	Páginas Modificadas	Autor
1	27.05.2011		Creación de Política General de Seguridad de la Información	Todas	JCGS

I.- DECLARACIÓN INSTITUCIONAL

Con el objeto de asegurar los niveles mínimos de seguridad de la información que se maneje, genere, procese, intercambie y almacene, la Defensoría Penal Pública adoptará las medidas necesarias y disponibles para lograr niveles adecuados de integridad, confidencialidad y disponibilidad para todos los activos de información institucional considerados relevantes, de manera tal que se asegure la continuidad operacional de los procesos institucionales y la entrega de servicios a los usuarios/ clientes/ beneficiarios, a través de políticas y procedimientos que todo funcionario deberá conocer, aplicar, cumplir y difundir.

Según la normativa vigente, decreto supremo N° 83, de 2004, del Ministerio Secretaría General de la Presidencia; los activos de información corresponden a "todos aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la institución", es decir, la información propiamente tal, en sus múltiples formatos -papel o digital, texto, imagen, audio, video, etc.-, los equipos y sistemas que soportan esta información; y las personas que la utilizan y que tienen el conocimiento de los procesos institucionales.

Por integridad de la información se entiende que estará disponible tal y como se almacenó por un usuario autorizado; por confidencialidad, que estará disponible sólo para usuarios autorizados para acceder a la información; y por disponibilidad, que estará disponible cuando se le necesite, minimizando interrupciones de servicio debido a situaciones tales como cortes de energía, fallas de hardware, actualizaciones del sistema o cambio de hardware.

Esta política general de seguridad considera aspectos relacionados a seguridad informática, ambiental y de las personas, además de la protección de los bienes, equipos e instalaciones donde se almacenan o administran activos de información.

Para el perfeccionamiento de este documento se conformó un Comité de Seguridad de la Información, compuesto por el Encargado de Seguridad de la Información institucional, quien lo presidirá, y los Jefes, o un representante de ellos, de las siguientes unidades: Informática y Estadísticas, Administración y Finanzas, Recursos Humanos, Control de Gestión, Gestión de Defensa Penal y Asesoría Jurídica.

II.- OBJETIVOS DE LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Los objetivos de la gestión de seguridad de la información son los siguientes:

CLASIFICACIÓN Y CATASTRO DE ACTIVOS DE INFORMACIÓN

- Contar con un inventario detallado de los activos de información, según tipo, formato, ubicación, importancia, responsable y procedimiento de manipulación.

DEFENSORÍA PENAL PÚBLICA ASESOR JURÍDICO

- Identificar y etiquetar los activos de información existentes, según la importancia que tienen para la institución.

ANÁLISIS DE RIESGO

- Elaborar un análisis del riesgo en que se encuentran actualmente los activos de información, en relación a su importancia para la institución y el lugar físico o virtual donde se localizan.
- Identificar aquellos activos de información de carácter secreto o reservado, que requieren de una protección adicional.

CAPACITACIÓN DEL PERSONAL

- Establecer un equipo de responsables de los activos de información pertenecientes a cada departamento y unidad de la institución.
- Capacitar al equipo de responsables, a través de talleres, cursos y seminarios, en temáticas relacionadas a la generación, manejo y resguardo de los activos de información relevantes para la institución.
- Proporcionar a este equipo el material de apoyo (manuales y textos de referencia) relacionado a la seguridad de los activos de información.
- Realizar instancias de difusión y sensibilización masiva de la importancia de la seguridad de la información en la institución.
- Publicar toda la documentación relativa a la seguridad de la información, a través de la Intranet y el sitio Web institucional.

POLÍTICAS, ESTÁNDARES Y PROCEDIMIENTOS

- Articular las diferentes políticas incluidas dentro de la política general, con el objeto que permitan una lectura integral entre ellas.
- Definir mecanismos de actualización periódica.
- Diseñar pautas de procedimientos frente a situaciones críticas que afecten la integridad de los activos de información.

III.- ALCANCE DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La presente política de seguridad de la información debe ser conocida y practicada por todos los funcionarios de la DPP incluidos el personal que presta servicio de defensa penal en la modalidad de licitados. Asimismo, estarán obligados los terceros que independiente del vínculo con la Defensoría, tengan acceso a activos de información.

A continuación, se enuncian las políticas específicas que conforman la política informática institucional:

- Política de Uso del Correo Electrónico
- Política de Uso de Accesos a Internet y Control de Contenidos
- Política de Uso de Accesos a Intranet (Red Interna)
- Política de Autenticación de Usuarios
- Política de Licenciamiento de Software
- Política de Arriendo del Equipamiento Informático
- Política de Mantención y Soporte del Equipamiento Informático
- Política de Contratación de Housing
- Política de Respaldos
- Política de Protección de Estaciones de Trabajo
- Política de Protección de Servidores
- Política de Desarrollo de Sistemas de Información
- Política de Mantención y Soporte de Sistemas de Información

Además, se considera un Plan de Emergencia y Evacuación de dependencias de la Defensoría Penal Pública.

IV.- ROLES Y RESPONSABILIDADES

Para el desarrollo de esta Política General de Seguridad de la Información, se ha establecido un Comité compuesto por las siguientes personas:

1. Encargado de Seguridad de la Información, quien lo presidirá;

Las funciones de este profesional serán las siguientes:

- Asesorar al Jefe Superior del Servicio en las materias relativas a seguridad de los documentos electrónicos y definición de las políticas sobre la materia.
- Tener a su cargo el desarrollo inicial de las políticas de seguridad al interior de la Defensoría Penal y velar por su correcta aplicación.
- Coordinar la respuesta a incidentes computacionales y otros relacionados con activos de la información, cualquiera sea su formato.
- Establecer puntos de enlace con encargados de seguridad de otros organismos públicos y especialistas externos que le permitan estar al tanto de las tendencias, normas y métodos de seguridad pertinente.
- Formular un Plan de Contingencia para asegurar la continuidad de operaciones críticas para la institución.
- Y todas aquellas que encomiende el Jefe Superior del Servicio, en el marco de la seguridad de la información.

2. Jefe de la Unidad de Informática y Estadísticas, o un profesional de dicha unidad en su representación;
3. Jefe de la Unidad de Administración y Finanzas, o un profesional de dicha unidad en su representación;
4. Jefe de la Unidad de Recursos Humanos, o un profesional de dicha unidad en su representación;
5. Jefe de la Unidad de Control de Gestión, o un profesional de dicha unidad en su representación;
6. Jefe de la Unidad de Gestión de Defensa Penal, o un profesional de dicha unidad en su representación; y
7. Jefe de la Unidad de Asesoría Jurídica Gestión, o un profesional de dicha unidad en su representación.

Las funciones de este Comité serán las siguientes:

- Proponer la Política de Seguridad de la Información y las responsabilidades generales y específicas de gestión de seguridad de la información.
- Monitorear los cambios significativos en la exposición de los activos de información a amenazas mayores.
- Revisar y monitorear los incidentes de seguridad de la información que afectan la gestión del Servicio, a fin de establecer acciones preventivas y correctivas.
- Proponer iniciativas para mejorar la seguridad de la información crítica para la gestión del Servicio.
- Las que encomiende el Jefe Superior del Servicio, en el marco de la seguridad de la información.

V.- MARCO GENERAL PARA LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

- **Objetivos**

Contar con un sistema de gestión de seguridad de la información que permita lograr niveles adecuados de **integridad**, **confidencialidad** y **disponibilidad** para todos los activos de información institucional considerados relevantes, de manera tal que se asegure la continuidad operacional de los procesos institucionales y la entrega de servicios a usuarios/ clientes/ beneficiarios.

- **Formato**

Se utilizará un formato adaptado y aprobado por el Comité de Seguridad de la Información, según los requerimientos y necesidades propios de la institución.

- **Gestación**

La formulación y ejecución de las políticas se realizará en base al trabajo periódico del Comité de Seguridad de la Información, el que sesionará al menos dos veces al año y será dirigido por el Encargado de Seguridad de la Información, quien podrá convocar a sesiones extraordinarias para resolver situaciones que lo requieran.

Para el desarrollo de los procedimientos y acciones específicas se designarán Comités Operativos, realizando reuniones extraordinarias con los responsables de los distintos procesos institucionales, para analizar las principales amenazas que enfrentan los activos de información relacionados a su trabajo.

- **Aprobación**

Las políticas contempladas serán presentadas, discutidas y aprobadas en primera instancia en los Comités Operativos, luego de lo cual serán remitidas a la Unidad de Asesoría Jurídica, para certificar que son coherentes con el marco legal vigente.

Posteriormente, serán presentadas al Comité de Seguridad de la Información, que realizará observaciones y comentarios, para finalmente aprobar sus contenidos.

- **Difusión**

Las políticas se encontrarán disponibles en la Intranet y, según corresponda, en el sitio Web institucional. Además se dispondrá de una copia impresa en cada unidad.

- **Revisión**

Para la actualización de contenidos, el Encargado de Seguridad de la Información recibirá los comentarios y sugerencias realizados por los usuarios de la institución, quien a su vez presentará un informe al Comité para su análisis y aprobación. Frente a un hecho que requiera una decisión inmediata, el Encargado convocará a una sesión extraordinaria para resolver el tema en particular.

La Política General de Seguridad de la Información será revisada integralmente al menos una vez al año.

2.- PUBLÍQUESE la presente Resolución en la intranet Institucional para su difusión.

Anótese, Notifíquese y Archívese,

DEFENSORIA PENAL PUBLICA
DEFENSORA NACIONAL

PAULA VIAL REYNAL
DEFENSORA NACIONAL

DAN / UAJ / UIE /
Distribución:
- Director Administrativo Nacional (DAN)
- Unidad de Asesoría Jurídica (UAJ)
- Unidad de Administración y Finanzas (UAF)
- Unidad de Recursos Humanos (URH)
- Unidad de Control de Gestión (UCG)
- Unidad de Gestión de Defensa Penal (UGDP)
- Unidad de Informática y Estadísticas (UIE)
- Archivo Oficina de Partes