REPÚBLICA DE CHILE
Ministerio de Justicia
Defensoría Penal Pública

APRUEBA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA DEFENSORÍA PENAL PÚBLICA Y DEJA SIN EFECTO RESOLUCIÓN EXENTA N°1921 DE FECHA 16 DE JUNIO DE 2011.

Santiago, 28 DIC. 2012

Resolución Exenta N° 4280 /

VISTOS:

1. El D.F.L. N° 1/19.653 de 2000, del Ministerio Secretaría General de la Presidencia, que fija texto refundido, coordinado y sistematizado de la Ley N° 18.575, Orgánica Constitucional de las Bases Generales de la Administración del Estado;

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

3. La Ley N° 19.880, que fija las Bases de los Procedimientos Administrativos que rigen los Actos de los Órganos de la Administración del Estado;

4. Decreto Supremo N°83, de 2005, 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;

5. La NCh-ISO 27001. Of2009, sobre Tecnología de la Información, Técnicas de Seguridad, Sistemas de Gestión de la Seguridad de la Información.

6. La NCh-ISO 27002. Of2009, sobre Tecnología de la Información, Código de prácticas para la Gestión de la Seguridad de la Información.

7. El Decreto Supremo N° 616, de fecha 15 de septiembre de 2011, del Ministerio de Justicia, que nombra al suscrito Defensor Nacional;

8. La Resolución Exenta N° 1921, de fecha 16 de junio de 2011, que aprueba Política de Seguridad de la Información de la Defensoría Penal Publica.

9. La Resolución Exenta N° 1598 del 19 de Mayo de 2011, que crea el Comité de Seguridad de la Información.

10. La Resolución N° 1600, de fecha 30 de octubre de 2008, de la Contraloría General de la República, que fija normas sobre exención del trámite de Toma de Razón; y

CONSIDERANDO:

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

2. Que se han oficializado normas tendientes a proteger la seguridad de la información con que cuente la Institución, estableciéndose la política de seguridad institucional, hecho que se produjo durante el año 2011 a través de la Resolución Exenta N°1921.

3. Que dicha Política está sujeta a la evaluación periódica, que permita incorporar mejoras a través de actualizaciones de la misma.

4. Que en ese contexto, el Comité de Seguridad de la Información acordó incluir las recomendaciones recibidas desde la Red de Expertos del PMG-SSSI, en el sentido de establecer la periodicidad en la revisión del cumplimiento de la Política de Seguridad de la Información, todo lo cual quedo registrado en Acta de dicho Comité suscrita por los integrantes del mismo con fecha 12 de Diciembre de 2012.

5. Que en este sentido, revisada por el Departamento de Informática y Estadística de la Institución, se ha sugerido al suscrito dictar el presente acto administrativo tendiente a aprobar la versión 2.0 de la Política de Seguridad de la Información de la Defensoría Penal Pública. Por tanto;

RESUELVO:

1.- APRUÉBESE La actualización del documento Política de seguridad de la información de la Defensoría Penal Pública, cuyo texto es el siguiente:

POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN DEFENSORÍA PENAL PÚBLICA Versión 2.0

I. CONTROL DE VERSIONES

Nº Revisión	Fecha Elaboración	Motivo de la revisión	Páginas Modificadas	Autor
1	16.06.2011	Creación de Política General de Seguridad de la Información	Todas	JCGS
2	12.12.2012	Actualización e incorporación de mejoras en el texto		AESDC

II. DECLARACIÓN INSTITUCIONAL

Con el objeto de asegurar los niveles adecuados de seguridad, de la información que se genere, maneje, gestione, procese, intercambie y almacene, en los procesos declarados en el alcance del Sistema de Seguridad de la Información, la Defensoría Penal Pública declara su compromiso de adoptar 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, estas medidas incluyen la definición de políticas y procedimientos, que todo funcionario debe 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.-, así como, los equipos y sistemas que soportan esta información; y las personas que la utilizan y que tienen el conocimiento de los procesos institucionales.

Para los efectos de la presente política; se considera que las acciones, en el ámbito de la seguridad de información, van dirigidas a la preservación de las dimensiones o propiedades que se indican a continuación:

Integridad, propiedad relacionada con el mantenimiento de la exactitud y completitud de la información y los demás activos;

Confidencialidad, propiedad que determina que la información solo esté disponible o se revele a usuarios (individuos, entidades o procesos) autorizados;

Disponibilidad, propiedad que determina que la información sea accesible y utilizable por solicitud de una entidad autorizada, cuando se le necesite, minimizando interrupciones de servicio debido a diversas situaciones (cortes de energía, fallas de hardware, actualizaciones del sistema o cambio de hardware).

Esta Política General de Seguridad de la información 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 ha constituido 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 y Asesoría Jurídica.

III. OBJETIVOS DE LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

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

1. Clasificación e Inventario de Activos de Información

- Contar con un inventario detallado de los activos de información, según tipo, formato, ubicación, importancia, responsable y procedimiento de manipulación.
- Identificar y etiquetar los activos de información existentes, según la importancia que tienen para la institución.

2. Análisis de Riesgo

- Realizar el análisis de los riesgos asociados a los activos de información, en relación a su nivel de criticidad para la institución y el lugar físico o virtual donde se localizan.
- Identificar e implementar post controles adecuados, considerando los criterios para la aceptación de los riesgos y la disponibilidad de recurso de la Defensoría.
- Actualizar periódicamente los resultados del análisis de riesgos, para evaluar el impacto que los controles definidos han tenido sobre los niveles de riesgos
- Identificar aquellos activos de información de carácter secreto o reservado, que requieren de una protección adicional.

3. Capacitación del Personal

- Establecer responsables de los activos de información pertenecientes a cada proceso, departamento y unidad de la institución.
- Capacitar a los responsables, a través de talleres, cursos y seminarios, en temáticas relacionadas a la seguridad de la información y estrategias para 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.

4. 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, confidencialidad y disponibilidad de los activos de información.
- Definir mecanismos de revisión y evaluación de su aplicación.

IV. 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.

Esta Política se apoya en un conjunto de Políticas Específicas, las que se relacionan a continuación:

- Política de Uso de 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 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
- Política de Informática v2.11

Además, se considera un Plan de Emergencia y Evacuación de dependencias de la Defensoría Penal Pública, así como el Plan de Continuidad de las Operaciones de la Defensoría Penal Pública.

V. ROLES Y RESPONSABILIDADES

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

a) Encargado de Seguridad de la Información, quien lo preside y será el responsable de:

- Asesorar al Jefe Superior del Servicio en las materias relativas a seguridad de la Información, incluyendo, entre otros los aspectos relativos a 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 de seguridad de la información, ya sean estos computacionales, u otros relacionados con activos de la información, cualquiera sea su formato.
- Establecer vías y medios de comunicación e intercambio 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, evaluar y actualizar en caso necesario, un Plan de Continuidad de las Operaciones, 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.

b) Jefe del Departamento de Informática y Estadística, o un profesional designado por éste;

c) Jefe del Departamento de Administración y Finanzas, o un profesional designado por éste;

d) Jefe del Departamento de Recursos Humanos, o un profesional designado por éste;

e) Jefe del Departamento de Control de Gestión, o un profesional designado por éste;

f) Jefe del Departamento de Asesoría Jurídica, o un profesional designado por éste;

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.
- Realizar el seguimiento de los cambios significativos en la exposición de los activos de información a las diversas amenazas, así como de los niveles de riesgo asociados.
- 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.

VI. MARCO GENERAL PARA LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

1. 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.

2. Formato

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

3. Gestación

La formulación y ejecución de las políticas se debe realizar en base al trabajo periódico del Comité de Seguridad de la Información, el que debe sesionar 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 designan 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.

4. Aprobación

Las políticas contempladas deben ser 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, deben ser presentadas al Comité de Seguridad de la Información, que realizará observaciones y comentarios, para finalmente aprobar sus contenidos, y presentarlos al Jefe de Servicio.

5. Difusión

Esta Política General de Seguridad de la Información y las demás políticas específicas, se encuentran disponibles en la Intranet y, según corresponda, en el sitio Web institucional. Además se debe disponer de una copia impresa en cada unidad.

6. Actualización de la Política

Para la actualización de contenidos, el Encargado de Seguridad de la Información debe recibir comentarios y sugerencias realizados por los funcionarios y usuarios de la institución, y posteriormente debe presentar un informe, relativo a estas sugerencias y comentarios, al Comité de Seguridad, para su análisis y aprobación.

Frente a un hecho que requiera una decisión inmediata, el Encargado debe convocar a una sesión extraordinaria para resolver el tema en particular.

La Política General de Seguridad de la Información debe ser revisada al menos una vez al año.

7. Evaluación

El Departamento de Informática y Estadística debe incluir en sus evaluaciones periódicas, formalizadas mediante el documento *Procedimiento de Auditoría de Procedimientos Vigentes V 2.0,* la verificación del nivel de cumplimiento de la Política de Seguridad de la Información, la cual se realizará a lo menos una vez al año. Asimismo, la evaluación del presente documento, puede ser incluida en los procesos de auditoría, a través del sistema de evaluación selectiva de la Unidad de Auditoría Interna, según el nivel de riesgo que se defina para cada periodo y que sirve de insumo para la planificación anual de auditoría.

2.- **DÉJASE SIN EFECTO** Resolución Exenta N°1921 de 2011, a contar de la total tramitación de la presente.

3.- **PUBLÍQUESE** la presente Resolución en la Intranet Institucional totalmente tramitada.

ANÓTESE, NOTIFÍQUESE Y ARCHÍVESE,

DEFENSORÍA PENAL PÚBLICA
DEFENSOR NACIONAL

GEORGY SCHUBERT STUDER
DEFENSOR NACIONAL

mc
DAN/UAJ/DIE/aps

Distribución

- Director Administrativo Nacional (DAN)
- Unidad de Asesoría Jurídica (UAJ)
- Departamento de Estudios y Proyectos (DEP)
- Departamento de Evaluación, Control y Reclamaciones (DECR)
- Departamento de Administración y Finanzas (DAF)
- Departamento de Recursos Humanos (DRH)
- Departamento de Informática y Estadísticas (DIE)
- Unidad de Auditoria Interna (UAI)
- Unidad de Comunicaciones
- Gabinete
- Unidad de Control de Gestión (UCG)
- Defensorías Regionales
- Oficina de Partes

Defensoría Sin defensa no hay Justicia	COMITÉ DE SEGURIDAD DE LA INFORMACIÓN DEFENSORIA PENAL PUBLICA ACTA DE REUNION	Página 1 de 12

Identificación

Fecha	:	Santiago, 12 de diciembre de 2012.	**Participantes:** **Defensoría Penal Pública (DPP):** • Andrés Mahnke Malschafsky (DAN, Encargado de Seguridad) • Andres Santoro (Jefe del DIE) • Pablo García (jefe del DECR) • María Cristina Marchant (Jefa DAF) • Pablo García (Jefe DECR) • Pedro Guerra (Jefe RRHH) • Angélica Álvarez (Jefa UCG) • Pablo Jara (Jefe Unidad de Auditoría Interna) • Alvaro Paredes (Jefe UAJ) • Luis Felipe Troncoso (Profesional UCG) • José Luis Craig (Defensor Regional del Maule) • Triana Cortes (Profesional UCG) • Natacha Paredes (Profesional DIE) **Ausentes:** • Aaron Pinto, profesional Depto. Informática y Estadísticas, y encargado PMG Seguridad de la Información. (en Comisión de Servicio) Se adjunta lista de asistencia
Lugar	:	Sala de Consejo Piso 8.	

Objetivos de la reunión

1. Presentar los avances del Sistema de Seguridad de la Información
2. Revisar procedimientos del plan de implementación, para someterlos a aprobación
3. Analizar resultados de la Medición de gestión de incidentes
4. Revisar etapa de evaluación del Sistema de Seguridad de la información
   a) Revisión etapa Evaluación del Sistema de Seguridad de la información
   b) Revisión de los resultados de las actividades desarrolladas y la efectividad en la mitigación de riesgos.
   c) Identificación de riesgos persistentes y otras debilidades, y su análisis de causa.
   d) Recomendaciones de mejora, que consideren medidas correctivas y preventivas

Desarrollo de la reunión:

I.- Avance del Sistema de Seguridad y actividades desarrolladas.

1. El Jefe del Depto. de Informática Andrés Santoro, informa los avances del Sistema de gestión de seguridad de la información, y da cuenta de las gestiones realizadas para el cierre del Levantamiento del Inventario de Activos de Información y la Revisión y Análisis de los riesgos asociados a los Activos de media y alta criticidad.

   - Se hizo entrega de documentación conforme se establecía en el calendario al 31 de Octubre pasado.
   - Se recibieron observaciones a la documentación entregada por parte de la Red de Expertos (Subsecretaría del Interior y DIPRES).
   - Se sostuvo reunión de trabajo el día 04 de diciembre de 2012, con expertos de la RED, Sr. Marcos Terreros de Interior y Sra. Carmen Contreras de DIPRES. Por la DPP participaron Sras. Angelica Alvarez, Triana Cortes de la Unidad de Control de Gestión y Srs. Andrés Santoro y Aaron Pinto, del Depto. de Informática y Estadísticas.
   - Se solicita por parte de la red de expertos correcciones a la Matriz, principalmente de consistencia de los contenidos.
   - Se informan estas acciones al Encargado de Seguridad y se acuerda Plan de Trabajo de cierre y citación del Comité de Seguridad para el día 12 de Diciembre.

2. Se culminó la elaboración de los procedimientos y del Plan de Continuidad comprometidos en el Plan General.

3. Se informó los hitos de revisión que vienen en relación al PMG. Se adjunta presentación.

II.- Revisión de la documentación final a entregar:

Mencionar y resumir objetivo de cada procedimiento que será revisado.

- **Política General de Seguridad de la Información** (actualización), inclusión de las recomendaciones recibidas desde la Red de Expertos, respecto a la periodicidad en la revisión del cumplimiento de la Política. En etapa de solicitud de **FIRMA** de aprobación.

- **Plan de Continuidad**, define actividades y responsabilidades tendientes a dar continuidad a los servicios definidos en el alcance del sistema de seguridad de la información de la Defensoría, el cual permite enfrentar de forma correcta la continuidad operacional para los procesos institucionales relevantes, la contingencia tecnológica, especificando escenarios de catástrofe y fallas a enfrentar, y el manejo de crisis, estableciendo la estrategia de gestión en situaciones de contingencia de los activos de información instalados y servicios críticos existentes en el Housing de la DPP. En etapa de solicitud de **FIRMA** de aprobación.

Recursos Humanos

- *Procedimiento de Roles y responsabilidades para los funcionarios, honorarios y terceros respecto de la seguridad de la información.* **Aprobado.**

Sistemas de Información

- *Procedimiento de Planificación y Aceptación de Sistemas.* Establece mecanismo para fijar criterios de aceptación a los requerimientos de desarrollo para los sistemas SIGDP y SIGO. En etapa de solicitud de **FIRMA** de aprobación.
- *Procedimiento de Procesamiento Correcto de las Aplicaciones.* Establece mecanismo a aplicar para efectuar el proceso de pruebas de los sistemas, previo a su paso a producción. En etapa de solicitud de **FIRMA** de aprobación.

Asociados a Nivel de Usuario

- *Procedimiento de Seguimiento de Actividades de contratos con servicios externalizados de procesamiento de Información.* **Aprobado**
- *Procedimiento de Seguridad de Carpetas de Causas.* Establece medidas que permitan proteger la documentación y equipamiento de accesos no autorizados y de peligros ambientales. Está elaborado en concordancia con lo definido en MOE respecto de la materia. En etapa de solicitud de **FIRMA** de aprobación.

Asociados al Servicios de Nivel Central

- *Procedimiento de Respaldo y Recuperación de Bases de Datos SIGDP (actualización).* **Aprobado**
- *Procedimiento de Plataforma Antivirus.* **Aprobado**

- ***Procedimiento sobre Operaciones y Responsabilidades.*** Define criterios y responsabilidades respecto de las acciones a efectuar para materializar la entrada en producción de una nueva versión de los sistemas SIGDP ó SIGO. En etapa de solicitud de **FIRMA** de aprobación.
- ***Procedimiento de Seguridad de los Archivos del Sistema.*** Establece criterios de seguridad respecto de los archivos de sistemas para evitar errores en los procesos de instalación de nuevas versiones de los sistemas. En etapa de solicitud de **FIRMA** de aprobación.
- ***Procedimiento de Seguimiento de Actividades de Procesamiento de Información.*** Consolida lo definido individualmente por los procedimientos de Plataforma de Antivirus, seguridad de los archivos y aceptación de sistemas. En etapa de solicitud de **FIRMA** de aprobación.

III.- Resultados de la Medición de gestión de incidentes

Se mantiene el reporte de 5 incidentes de seguridad. En el periodo se establecieron acciones de difusión del procedimiento entre los usuarios, participando en actividad con los asistentes administrativos, el pasado 22 de Noviembre en la localidad de Rapel.

Mencionar los 5 incidentes reportados.

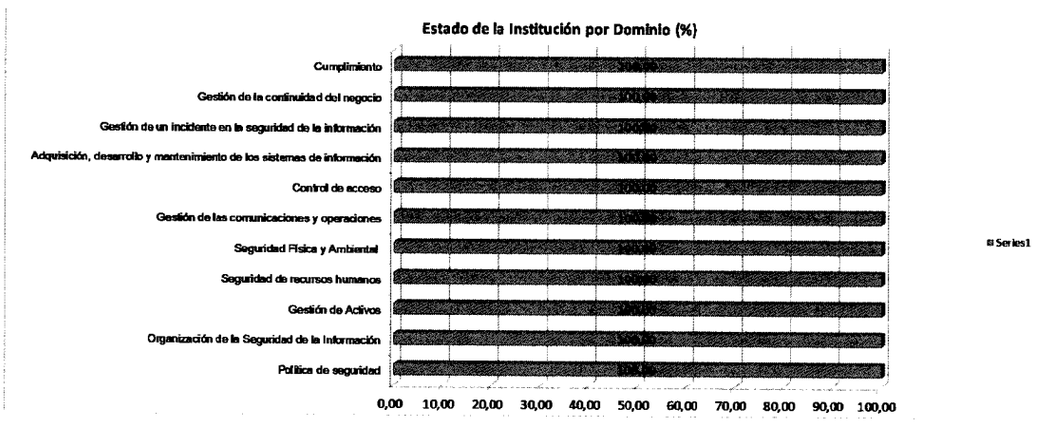
N° incidente	Fecha	Defensoría	Clasificación Incidente	Descripción Incidente
1	14-05-2012	Defensoria Regional De Concepción	Posible acceso no autorizado	Pagina de sistema queda publicada en Internet sin control de acceso.
2	17-05-2012	Defensoria Nacional	Acceso a base de datos no autorizado	Vulnerabilidad de acceso a base de datos de producción de SIGDP
3	27-09-2012	Defensoria Nacional	Disponibilidad del servicio de correo	Correos externos no están llegando a casillas de usuarios DPP
4	09-10-2012	Defensoria Nacional	Disponibilidad de servicio de correo	Casilla de correo con capacidad máxima
5	22-10-2012	Defensoria Nacional	Disponibilidad de servicio Internet	Problemas con enlace de respaldo GTD

IV.- Revisión etapa Evaluación del Sistema de Seguridad de la información

PMG/MEI - SSI: RESUMEN - IMPLEMENTACIÓN

Red de Expertos
Subsecretaría del Interior - División Informática
Dirección de Presupuestos - División Tecnologías de Información

Política de seguridad	100,00	100,00
Organización de la Seguridad de la Información	100,00	50,00
Gestión de Activos	100,00	42,42
Seguridad de recursos humanos	100,00	41,67
Seguridad Física y Ambiental	100,00	70,00
Gestión de las comunicaciones y operaciones	100,00	41,80
Control de acceso	100,00	50,00
Adquisición, desarrollo y mantenimiento de los sistemas de información	100,00	31,58
Gestión de un incidente en la seguridad de la información	100,00	100,00
Gestión de la continuidad del negocio	100,00	33,33
Cumplimiento	100,00	20,00



1. Revisión del 100,00 % de cumplimiento logrado, por parte del CSI

1.1 <u>Análisis simplificado por Dominio</u>.

a) **Política de Seguridad:** actualmente se encuentra en proceso de aprobación la actualización de la política, la cual incluirá el período de revisión del estado de cumplimiento de ésta.
Se mantiene acceso permanente a este documento a través de la intranet institucional.

b) **Organización de la Seguridad de la Información:** El comité de seguridad se mantiene en un trabajo activo y permanente dentro del año, realizando los análisis de información entregada por el encargado de PMG de SII y el Jefe del Depto. de Informática y Estadísticas.

c) **Gestión de Activos:** Se realizaron avances sustantivos durante el año 2011, y este control se encuentran plenamente aplicados en la gestión institucional de la Defensoría.

d) **Seguridad de recursos humanos:** Se elaboró de acuerdo al plan, Procedimiento de roles y responsabilidades para los funcionarios, honorarios y terceros respecto de la seguridad de la información.

Se han realizado activas capacitaciones a un total de 100 funcionarios de la institución, principalmente a los encargados de informática y asistentes, quienes se encargarán de replicar los principales aspectos del sistema de seguridad de la información en las defensorías regionales.

e) **Seguridad física y ambiental:** de acuerdo al estado declarado en el diagnóstico de riesgos, se comprometió en el plan general, el Procedimiento de Seguridad del Equipamiento, el cual fue cumplido durante el mes de noviembre del presente mes.

f) **Gestión de las comunicaciones y operaciones:** Se realizó, de acuerdo al plan, procedimiento de Respaldo y recuperación de base de datos, 'Procedimiento de Planificación y Aceptación de Sistemas, 'Procedimiento de Seguimiento de Actividades de contratos con servicios externalizados de procesamiento de Información, Procedimiento de Seguimiento de Actividades de Procesamiento de Información, Procedimiento sobre Operaciones y Responsabilidades, 'Procedimiento de Plataforma Antivirus. Estos documentos se encuentran disponibles en la intranet institucional, para revisión y sugerencias de mejora por parte de los usuarios y encargados informáticos regionales.

g) **Control de acceso:** los requisitos de este control se encuentran plenamente cubiertos por documentación pertinente, los cuales fueron identificados y respaldados en el diagnóstico de inventario y de riesgos.

h) **Adquisición, desarrollo y mantenimiento de los sistemas de información.** Se realizó de acuerdo al plan Procedimiento de Procesamiento Correcto de las Aplicaciones, Procedimiento de Seguridad de los Archivos del Sistema. Este documento se encuentra disponible en la intranet institucional, para revisión y sugerencias de mejora por parte de los usuarios y encargados informáticos regionales.

i) **Gestión de un incidente en la seguridad de la información:** los requisitos de este control se encuentran plenamente cubiertos por documentación pertinente, los cuales fueron identificados y respaldados en el diagnóstico de inventario y de riesgos.

j) **Gestión de la continuidad del negocio:** Se realizó un plan de continuidad del negocio, como primera experiencia de trabajo, que permitirá reconocer claramente los principales riesgos que podrían afectar los procesos de negocio de la Defensoría y como realizar su respectivo tratamiento. A partir de este documento se realizarán las evaluaciones en terreno, a través de las auditorias internas, las cuales permitirán detectar aspectos de mejora.

k) **Cumplimiento:** los requisitos de este control se encuentran plenamente cubiertos por documentación pertinente, los cuales fueron identificados y respaldados en el diagnóstico de inventario y de riesgos.

1.2 Revisión medición de indicadores y metas de gestión, incluidos los requeridos por la Dirección de Presupuestos

Dominio al que se vincula	Nombre del indicador	Fórmula de cálculo	Fecha de inicio de la medición	Frecuencia de la medición	Efectiva a Agosto de 2012	Efectiva a Octubre de 2012	Efectiva a Diciembre de 2012	Medios de verificación	Supuestos	Notas
Organización de la seguridad de la Informaci ón (A.6.1.3)	Porcentaje de incidentes de seguridad que reciben tratamiento de acuerdo al Plan de Continuidad de Negocios establecido en el Sistema de Seguridad de la Información en el año t	(N° total de incidentes de seguridad de la información reportados que reciben tratamiento de acuerdo al Plan de Continuidad de Negocios / N° total de incidentes de seguridad de la información reportados) * 100	01-01-2013	Mensual	n/a	n/a	n/a	1.Registros de Incidentes. 2.Solución del Incidente.		
Todos	Porcentaje de riesgos de seguridad de la información a los que se les han aplicado los controles de seguridad en forma completa y satisfactoria	(N° total de riesgos identificados como no cubiertos por la Institución en etapa 1 de 2012 a los cuales se ha aplicado control de seguridad en forma completa y satisfactoria / N° total de riesgos identificados como no cubiertos por la Institución en etapa 1 de 2012) * 100	01-09-2012	Mensual	n/a	72.1%	100%	1. Procedimiento asociado a la cobertura del riesgo.		
Gestión de Operaciones y Comunicaciones (10.1 al 10.10)	Porcentaje de respaldo realizados respecto de las programaciones	(N° de respaldos realizados en plazo / N° de Respaldos programados) x 100	01-09-2012	Mensual	n/a	100% (60 / 60)	100% (60 / 60)	Reporte de respaldos ejecutados	Causas externas que afecten funcionamiento normal. El equipamiento de respaldo no presenta fallas inesperadas.	
Organización de la seguridad de la Informaci ón (6.1 y 6.2)	Porcentaje de contratos Tecnológicos con incorporación de clausulas de confidencialidad	(Número de Contratos Tecnológicos con incorporación de clausulas de confidencialidad suscritos en periodo / Total de Contratos Tecnológicos con Terceros suscritos en el periodo) X 100	01-07-2012	Trimestral	100% (1/1)	100% (1 / 1)	100% (1/ 1)	Nómina de contratos tecnológica con clausula de confidencialidad emitidos por la unidad correspondiente	No se consideran contrataciones menores a 100 UTM. Se exceptúan contratos por adhesión.	aplicable c las contratos suscritos a partir de licitaciones del 2012 en adelante
Seguridad de RRHH (8.1, 8.2 y 8.3)	Personal con inducción en SSI	(N° de total de personas que recibe inducción inicial en seguridad de la información en el año 2012/ N° Total de personal programado a capacitar en SSI en el año 2012) X 100	01-10-2012	Mensual	n/a	25% (25 / 100)	100% (100 / 100)	Informe de capacitación	Disponibilidad del funcionario	Personal a capacitar: Informáticos Regionales Informáticos DN y Asistentes

2. Revisión de los resultados de las actividades desarrolladas y la efectividad en la mitigación de riesgos.

Dado que es necesario realizar verificaciones al funcionamiento del Sistema de Seguridad de la información, la Defensoría ha optado por efectuar auditorias internas. Éstas han estado dirigidas a revisar la aplicación de los procedimientos vigentes.

Durante el año 2012 se han realizado auditorias en las Defensorías Regionales, la cual incluye la aplicación de los procedimientos asociados a Seguridad de la Información. Se esta en proceso de elaborar los Informes de los resultados y remitirlos a las Direcciones Administrativas Regionales para la aplicación de acciones de mejora.

No obstante, en esta reunión se informa en forma general los siguientes resultados.

N°	Hallazgo	Control vulnerado	Defensoría
1	El ambiente donde se ubican las UPS presenta un nivel alto de temperatura, provocando riesgos de funcionamiento de este dispositivo, dejando desprotegidos los equipos instalados en la Defensoría.	A.9.2.2 ¿el equipamiento está protegido de fallas de energía y otras interrupciones causadas por fallas en los servicios básicos de soporte?	Regional de Aysén
2	El ambiente donde se ubican las UPS presenta un nivel alto de temperatura, provocando riesgos de funcionamiento de este dispositivo, dejando desprotegidos los equipos instalados en la Defensoría.	A.9.2.2 ¿el equipamiento está protegido de fallas de energía y otras interrupciones causadas por fallas en los servicios básicos de soporte?	Regional de Los Lagos

3. Identificación de riesgos persistentes y otras debilidades, y su análisis de causa.

Persiste falta de sensibilización del personal respecto de la importancia de informar los incidentes presentados en las áreas de informática, funcionamiento de sistemas, entre otros, de acuerdo al procedimiento vigente. Ello, se mantiene pese a las capacitaciones realizadas al personal de la DPP.

La causa radica en la reciente implementación del SSI en la Defensoría y la complejidad que ha significado la comprensión de la norma ISO 27001, para el personal encargado de implementar y controlar el sistema de seguridad, hecho que se hace más difícil de internalizar en aquellos funcionarios que son usuarios del sistema y que deben cumplir con los requisitos de la norma, e informar de los incidentes que surjan en la institución.

4. Recomendaciones de mejora, que consideren medidas correctivas y preventivas

De acuerdo a los resultados obtenidos de los puntos anteriores, se planifican las medidas correctivas y preventivas necesarias, a fin de corregir los problemas y sus causas. Estas recomendaciones han sido aprobadas por el Comité de Seguridad de la Información, dado que son parte de la evaluación del sistema.

- **Acción correctiva 1**: realizar capacitaciones presenciales del Sistema de seguridad de la información, específicamente registro de incidentes y principales riesgos que pueden afectar la continuidad operacional de la Defensoría. Esto se realizará a cada depto. y unidad de la Defensoría Nacional. En el caso de las Defensorías Regionales se realizarán por videoconferencia y presenciales.
  Responsable: encargado de PMG y encargados informáticos regionales.
  Plazo: 2do y 3er trimestre año 2013.

- **Acción correctiva 2:** Realizar difusión permanente del Sistema de Seguridad de la Información, a través de la publicación de documentación en la intranet institucional, dejando disponibles los antecedentes para revisión de los usuarios.
  Responsable: encargado PMG SSI
  Plazo: continuo durante el año 2013.

- **Acción correctiva 3:** realizar auditorias internas de verificación del funcionamiento del sistema de seguridad, priorizando en aquellos incidentes registrados y en los controles que han sido vulnerados.
  Responsable: Departamento Informática y Estadísticas.
  Plazo: 2do trimestre 2013

- **Acción Preventiva** 1: difundir en intranet recomendaciones para evitar los principales riesgos que pueden afectar el funcionamiento de los procesos del alcance del sistema de seguridad. Ello con un sentido más general y práctico que permita mayor cercanía con los usuarios.
  Responsable: Unidad de Comunicaciones
  Plazo: 3er trimestre 2013

- **Acción Preventiva 2:** Solicitar a la Unidad de Auditoria Interna, incorporar en su plan de auditorias aspectos de la norma ISO 27001, en cuanto a desempeño de controles, procedimiento y estrategias de mitigación de riesgos. Ello, para reforzar la internalización del sistema de seguridad incorporándolo en forma transversal a los compromisos institucionales del Defensor Nacional.
  Responsable: Encargado de Seguridad (Director Administrativo Nacional) y Jefe Depto. Informática y Estadísticas.
  Plazo: 1er trimestre de 2013

5. Difusión de los resultados de la implementación / Medios de verificación:

Difusión en intranet durante el año 2012:

- **12/10/2012 : Informática lanza encuesta para evaluar sus servicios**

A contar de hoy el Departamento de Informática y Estadística habilitará encuesta.

La Encuesta tiene por finalidad generar información que permita evaluar el funcionamiento, eficiencia y eficacia de los servicios que provee el Departamento de Informática y Estadística y elaborar un informe de análisis de resultados y propuestas de mejora, éste documento se encuentra inserto dentro de los compromisos que tiene dicho Departamento como parte del Convenio de Desempeño Colectivo del año 2012. Para estos efectos, se consideró obtener la opinión de todos los funcionarios de la Defensoría.

- **05/10/2012 : Informática aprobó dos nuevos manuales de procedimientos críticos**

Uno regula el control de ingreso y egreso de equipamiento computacional y el otro el aseguramiento de calidad de los software con que trabaja la Defensoría.

El Departamento de Informática y Estadísticas (DIE) aprobó recientemente dos manuales de procedimientos críticos. Sobre este tema, durante este año esa unidad institucional efectuó un levantamiento de información, que permitió actualizar el catastro de procedimientos vigentes e identificar aquellas actividades que requerían de una regulación. El procedimiento para gestionar listas de correo en la DPP, que informa y entrega directrices que permiten gestionar los grupos de correo electrónico en la institución. Se elaboró una normativa interna para regular el control de ingreso y egreso de equipamiento computacional, con el objetivo de sistematizar las gestiones que se realizan en la entrada y salida de todos los equipos computacionales, para así evitar la falta de registro, las pérdidas y hasta los hurtos de equipamiento.

El otro procedimiento, denominado 'Procedimiento de aseguramiento de la calidad de software de la Defensoría', tiene como fin establecer y describir las actividades que deben realizar los encargados de revisar los sistemas informáticos desarrollados al interior de la Defensoría, con la finalidad de obtener un mejor producto o con un nivel mínimo de errores.

- **31/07/2012 : Iniciativa se enmarca dentro de PMG Sistema Seguridad de la Información**

Informática crea mecanismo para reportar eventos contra la seguridad
Con ello se pretende contar con un medio único, formal y conocido por todos los funcionarios para reportar los posibles eventos y debilidades que se puedan observar en la seguridad de la información.

Informática creó un correo electrónico para reportar los eventos que puedan poner en peligro la seguridad de la información. Con el fin de minimizar los posibles riegos de seguridad al interior de la institución, se ha implementado un mecanismo especial para reportar eventos que afecten la seguridad de la información. Esta iniciativa se enmarca dentro del Programa de Mejoramiento de Gestión (PMG) del Sistema

Seguridad de la Información 2012, que busca difundir las políticas, procedimientos y uso correcto de las instalaciones del proceso de la información.

Para ello, se elaboraron instrucciones para que los funcionarios, personal a honorarios y externos que prestan servicios en la DPP, puedan reportar los diversos incidentes que se registren al interior del organismo, ya sea que involucren la confidencialidad, integridad o disponibilidad de los instrumentos de trabajo o la información disponible.

- **17/07/2012 : Es el primero de tres manuales críticos de Informática, que busca gestionar listas de correo en la DPP**

A través de distintas normas, el documento entrega información y directrices que permitirán gestionar los correos electrónicos, un canal de información considerado crítico en la Defensoría Nacional.

- **27/06/2012 : La DPP informó a la DIPRES el avance de su Sistema de Seguridad de la Información 2012**

Ahora queda pendiente que la Red de Expertos de la Dipres entregue sus observaciones para sancionar el plan de acción definitivo.

En el marco de las actividades comprometidas en el Programa de Mejoramiento de Gestión (PMG) "Sistema de Seguridad de la Información 2012", el Departamento de Informática y Estadísticas de la Defensoría informó sobre los avances logrados en la materia hasta el 31 de mayo pasado, con el objetivo de lograr su aprobación este año.

Compromisos de difusión:

Se efectuará una acción de difusión de las políticas y procedimientos aprobados recientemente a las distintas áreas responsables.

Se elaborará nota para ser publicada como noticia en la Intranet, dando cuenta del estado de avance del Sistema de Seguridad de la Información.

Todas las acciones son aprobadas por los miembros del Comité.

Para constancia se registra acta revisada por asistentes y lista de asistentes.

Defensoría Sin defensa no hay Justicia	COMITÉ DE SEGURIDAD DE LA INFORMACIÓN DEFENSORIA PENAL PUBLICA	Página 1 de 1
	ACTA DE REUNION	

REUNION COMITÉ SEGURIDAD DE LA INFORMACIÓN
SALA DE CONSEJO – 8° PISO DEFENSORIA NACIONAL
Miércoles 12 de diciembre del 2012 14:00 hrs.

N°	NOMBRE	CARGO	FIRMA
1	Alvaro Paredes	Jefe UAJ	
2	M. Cristina Matcham	DAF	
3	Pedro Guerra L.	RRHH	
4	Andrés Mahnke	D.J.N.	
5	Pablo Jara M.	UAJ	
6	Eriana Cortés G	UCG	
7	Angélica Alvarez M.	Jefe UCG	
8	Pablo García	DECN	
9	José Luis Craig	DR VII	
10	Andres Santoro	DIE	
11			
12			
13			
14			
15			

REPÚBLICA DE CHILE
Ministerio de Justicia
Defensoría Penal Pública

DEJA SIN EFECTO RESOLUCIÓN EXENTA N°3066 DE FECHA 29 DE SEPTIEMBRE DE 2011 Y DESIGNA ENCARGADO DE SEGURIDAD DE LA INFORMACIÓN EN LA DEFENSORIA PENAL PÚBLICA Y FIJA FUNCIONES.

Santiago, 14 AGO. 2012

Resolución Exenta N° 2419 /

VISTOS:

1. El D.F.L. N° 1/19.653 de 2000, del Ministerio Secretaría General de la Presidencia, que fija texto refundido, coordinado y sistematizado de la Ley N° 18.575, Orgánica Constitucional de las Bases Generales de la Administración del Estado;

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

3. La Ley N° 19.880, que fija las Bases de los Procedimientos Administrativos que rigen los Actos de los Órganos de la Administración del Estado;

4. Decreto Supremo N°83, de 2005, 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;

5. La NCh-ISO 27001. Of2009, sobre Tecnología de la Información, Técnicas de Seguridad, Sistemas de Gestión de la Seguridad de la Información.

6. La NCh-ISO 27002. Of2009, sobre Tecnología de la Información, Código de prácticas para la Gestión de la Seguridad de la Información.

7. La Resolución Exenta N° 2744 de fecha 01 de septiembre de 2011, que establece el orden de subrogancia del Defensor Nacional ;

8. La Resolución N° 152 de fecha 01 de julio de 2008, que nombra al suscrito Defensor Regional de la Defensoría Regional Metropolitana Sur.

9. La Resolución Exenta N°3066, de fecha 29 de septiembre de 2011, que designa Encargado de la Información en la Defensoría Penal Pública, fija funciones que indica y deja sin efecto Resolución Exenta N°1599 de 2011.

10. La Resolución N° 1600, de fecha 30 de octubre de 2008, de la Contraloría General de la República, que fija normas sobre exención del trámite de Toma de Razón; y

CONSIDERANDO:

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

2. Que se han oficializado normas tendientes a proteger la seguridad de la información con que cuente la Institución, determinándose una Encargado de Seguridad de la Información, hecho que se produjo durante el año 2011 a través de la Resolución Exenta N°3066, recayendo dicha designación en el Director

Administrativo Nacional.

3. Que se ha estimado necesario realizar ciertos ajustes al acto administrativo mencionado en el considerando anterior, que en concordancia con el principio de celeridad, no formalización y economía procedimental, que rigen los Órganos de la Administración del Estado, se ha estimado procedente refundir en la presente, por tanto;

RESUELVO:

1.- DÉJASE SIN EFECTO Resolución Exenta N°3066 de 2011, a contar de la total tramitación de la presente.

2.-DESÍGNASE Encargado de la Seguridad de la Información a **don Andrés Mahnke Malschafsky**, Cédula Nacional de Identidad 7.889.445-8, Director Administrativo Nacional, o quien se encuentre ejerciendo dicho cargo en razón de la subrogancia del mismo, establecidas por el Defensor Nacional.

3.- FÍJASE como funciones específicas del Encargado de Seguridad de la Información, las siguientes:

a) Asesorar al Jefe Superior del Servicio en las materias relativas a seguridad y definición de las políticas sobre la materia;

b) Tener a su cargo el desarrollo inicial de las políticas de seguridad al interior de la Defensoría Penal Pública y velar por su correcta aplicación;

c) Coordinar la realización de programas de concientización al personal de manera periódica, asegurar el mantenimiento y mejora de las competencias en este campo de acción;

d) Informar al Comité de Seguridad de la Información, creado mediante Resolución Exenta N°1921 de 2011, los riesgos vigentes y proponer los controles necesarios para su mitigación;

e) Coordinar y supervisar la respuesta, y las acciones que se generen para el tratamiento de incidentes que afecten los activos de información;

f) Establecer puntos de enlace con encargados de seguridad de la información de otros organismos públicos y especialistas externos que le permitan estar al tanto de las tendencias, normas y métodos de seguridad pertinentes;

g) Asegurar la evaluación de exposiciones a amenazas de seguridad de la información y situaciones de no cumplimiento en términos de afectar la disponibilidad, confidencialidad e integridad de los activos de información;

h) Asegurar la evaluación del riesgo en la incorporación de activos, dentro del alcance del sistema de gestión de la seguridad de la información.

i) Asegurar que todas las áreas internas y externas (incluyendo los proveedores y aquellos que actúan a su nombre) cumplan con las políticas e instrucciones de seguridad definidas por la Defensoría Penal Pública y en general por las disposiciones legales atingentes.

j) Asegurar el análisis y seguimiento, por parte de los especialistas pertinentes, de la información proveniente de fuentes reconocidas sobre alertas de seguridad de la información y sus mecanismos de solución.

k) Planificar y mantener las acciones de recuperación de los sistemas de información ante la ocurrencia de un desastre, asegurando la formulación de un Plan de Continuidad del Servicio para garantizar se mantengan las operaciones críticas para la institución.

l) Todas aquellas que encomiende el Jefe Superior del Servicio, en el marco de la seguridad de la información.

Para el desarrollo de sus funciones el Encargado de Seguridad, contará con la asesoría especializada en materias relacionadas con la seguridad de la información de dos Oficiales de Seguridad, uno de la Unidad de Recursos Humanos, y otro de la Unidad de Informática, los cuales serán nombrados por los Jefes de las respectivas unidades.

4.- PUBLÍQUESE la presente Resolución en la Intranet Institucional.

ANÓTESE, NOTIFÍQUESE Y ARCHÍVESE,

CLAUDIO PAVLIC VÉLIZ
DEFENSOR NACIONAL (S)

DAN/UAJ/UCG/UIE/cvm

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 (UGDP)
- Unidad de Informática (UIE)
- Oficina de Partes

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 :

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.

- 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,

DEFENSORÍA PENAL PÚBLICA
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