GOBIERNO DE CHILE
JUNTA NACIONAL DE AUXILIO
ESCOLAR Y BECAS

JUNTA NACIONAL DE AUXILIO ESCOLAR Y BECAS
OFICINA DE PARTES

JUNAEB
16 NOV 2011
OFICINA DE PARTES

APRUEBA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y PLAN DE DIFUSIÓN Y REVISIÓN DE LA POLITICA DE SEGURIDAD.

RESOLUCIÓN EXENTA Nº 066353

SANTIAGO, 03 NOV 2011

VISTO:

Lo dispuesto en la Ley Nº 15.720 que crea la Junta Nacional de Auxilio Escolar y Becas; Decreto Supremo de Educación Nº 5311 de 1968 que Reglamenta la Junta Nacional de Auxilio Escolar y Becas, , en el Decreto Ley Nº180 de 1973, en el Decreto con Fuerza de Ley Nº 29 del Ministerio de Hacienda del año 2004 que fija el texto refundido coordinado y sistematizado de la Ley Nº 18.834, sobre Estatuto Administrativo, el Decreto con Fuerza de Ley Nº 1/19.653 del Ministerio Secretaría General de la Presidencia, que fija el texto refundido, coordinado y sistematizado de la Ley Nº 18.575, Orgánica Constitucional de Bases Generales de Administración del Estado; la Ley Nº 19.799, sobre Documentos Electrónicos, Firma Electrónica y los Servicios de Certificación de dicha Firma; el Decreto Nº 181/2002 del Ministerio de Economía Fomento y Reconstrucción que aprueba el Reglamento de la Ley Nº19.799 sobre Documentos Electrónicos, Firma Electrónica y los Servicios de Certificación de dicha Firma; el Decreto Nº 83-2004 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; y la Resolución Nº1.600, de la Contraloría general de la República, que fija normas sobre exención del trámite de Toma de Razón, y

CONSIDERANDO:

a) Que, las entidades regidas por el Decreto Nº 83/2004 del Ministerio Secretaría General de la Presidencia, entre los cuales se encuentra comprendida la Junta Nacional de Auxilio Escolar y Becas "JUNAEB", deben adoptar políticas de seguridad permanente, que incluyan planes de contingencia frente a fenómenos de toda índole que pudieran poner en riesgo la continuidad operacional de los sistemas de información;

b) Que de acuerdo a la normativa aplicable, las exigencias y recomendaciones de éstas para los Órganos de la Administración del Estado tienen por finalidad garantizar estándares mínimos de seguridad en el uso, almacenamiento, acceso y distribución del documento electrónico, entre otros; y salvaguardar el uso del documento electrónico de manera segura, confiable y en pleno respeto a la normativa vigente sobre confidencialidad de la información intercambiada.

c) Que, de acuerdo a lo establecido en el artículo 11 del Decreto Nº 83/2004 del Ministerio Secretaría General de la Presidencia, la Junta Nacional de Auxilio Escolar y Becas "JUNAEB", debe establecer una política de seguridad que fije las directrices

generales que orienten la materia de seguridad dentro de cada Institución, que refleje claramente el compromiso, apoyo e interés en el fomento y desarrollo de una cultura de seguridad institucional.

d) Que, la política de seguridad deberá incluir como mínimo, una definición de seguridad del documento electrónico, sus objetivos globales, alcance e importancia; la difusión de sus contenidos al interior de la organización; su reevaluación en forma periódica al menos cada tres años.

e) Que, a la fecha JUNAEB no cuenta con una Política de Seguridad, ni la difusión de sus contenidos al interior de la organización.

f) Que, considerando las normas técnicas vistas que establecen las características mínimas obligatorias de seguridad y confidencialidad que deben cumplir los documentos electrónicos de los Órganos de la Administración del Estado, y JUNAEB, con el propósito de mejorar su administración y gestión acorde a los requerimientos tecnológicos, tomando en consideración los principios de neutralidad tecnológica, libertad de prestación de servicios y equivalencia del soporte electrónico al soporte papel, es necesario establecer una Política de Seguridad de la Información y un Plan de Difusión y Revisión de la misma.

RESUELVO,

ARTÍCULO ÚNICO: Apruébese documento Política de Seguridad de la Información código D-DI-PI001 con fecha 03/08/2011 y documento Plan de difusión y revisión de la Política de Seguridad código D-DI-PI002 con fecha 25/07/2011, cuyos textos se insertan a continuación:

POLITICA GENERAL DE SEGURIDAD DE LA INFORMACION

1. DECLARACIÓN INSTITUCIONAL

Desde el año 1996, la Junta Nacional de Auxilio Escolar y Becas, se constituye como la institución que registra, almacena y procesa la información acerca de las diferentes dimensiones que configuran la condición de vulnerabilidad. Toda esta información es necesaria para la asignación y racionalización de las prestaciones que otorga el Estado en el área de la Educación.

Para apoyar su misión, la JUNAEB ha desarrollado una plataforma tecnológica a través de la cual se registra, procesa, transmite y almacena información, mediante diferentes activos de la información, que permite la gestión propia de sus programas, la interacción con la comunidad escolar, ciudadanía en general y los integrantes de la JUNAEB en todo el país.

La JUNAEB reconoce que la información es un bien estratégico que, como otros bienes de la organización, tiene gran valor y necesita ser protegida tanto en su obtención, procesamiento, transmisión y almacenamiento en forma apropiada. La seguridad de la información la protege de una gran gama de amenazas con el fin de asegurar la continuidad de las operaciones, minimizar el daño de la institución y maximizar la eficiencia y las oportunidades de mejora.

Cualquier forma que tome la información, ya sea impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o medios electrónicos o mostrados en películas o en una conversación, los dispositivos a través de los cuales es compartida y almacenada, siempre debe estar protegida en forma adecuada.

Para la JUNAEB, es de alta importancia la protección de la información y de los procesos de apoyo, representados por la infraestructura tecnológica de información y comunicaciones (TIC), que deben asegurar la confidencialidad, integridad y disponibilidad de la información.

Por lo tanto, todo el personal que integra la JUNAEB, será responsable de la confidencialidad, integridad y disponibilidad de la información, que por cargo y función, le corresponde.

2. Objetivos

Establecer normas que regulen el correcto uso de los activos de información, en las distintas actividades que el personal de la JUNAEB realiza para el desempeño de sus funciones, con el fin de asegurar la confidencialidad, integridad y disponibilidad de los servicios e información.

Garantizar estándares mínimos de seguridad en el uso, almacenamiento, acceso y distribución de información

Establecer los requisitos y condiciones generales de seguridad a las que se encuentra sujeto la JUNAEB, de acuerdo a las normas legales y reglamentarias pertinentes, así como los riesgos a que están expuestos sus Activos de Información y los principios y objetivos internos para el resguardo de sus operaciones.

3. Alcance

La presente Política de Seguridad de la información de la JUNAEB expresa, en forma clara y breve, los lineamientos generales, respecto al buen uso de los Activos de información, tanto compartidos como de cada uno de los usuarios internos o externos. Fija las directrices y soporte para la seguridad de la información en concordancia con los requerimientos institucionales y las leyes y regulaciones pertinentes.

Estos lineamientos, están destinados a servir de guía para la definición de normas específicas, que serán parte de las disposiciones complementarias de carácter administrativo y técnico que se dicten para el cumplimiento de lo dispuesto en la presente Política.

La seguridad de la información es de responsabilidad de todos los usuarios que se relacionan con la Institución, ya sean usuarios externos, que sean identificables, que presten servicios o asesorías y que por sus funciones deban acceder a la Red de Área Extendida (WAN), o usuarios internos en la Red de Área Local (LAN,) con acceso a los Activos de Información de la JUNAEB. Por tal razón, las políticas establecidas en este documento son de conocimiento y cumplimiento obligatorio para todos los usuarios a los que se les otorgue acceso a estos activos. En el caso de los usuarios externos, dicha obligación deberá expresarse en los contratos y/o acuerdos respectivos.

4. POLÍTICA DE SEGURIDAD

4.1 Seguridad organizacional

Con el objeto de mejorar y optimizar la seguridad de la información en la institución, y darle la transversalidad a nivel organizacional, se creará una vez que la Política de seguridad de la información sea aprobada y entre en vigencia, un Comité de Seguridad, presidido por el Encargado de Seguridad y conformado por:

- Encargado de Departamento de Informática
- Encargado de Departamento Gestión de Personas
- Encargado de Planificación y Control de Gestión
- Asesor Jurídico

La misión del Comité de Seguridad de la Información será velar por la confidencialidad, integridad y disponibilidad de la información y los medios que la soporta, ya sea tecnológicos o no, para lo cual elaborará políticas, procedimientos, acciones y medidas administrativas. Además de promover la seguridad dentro de la organización a través de compromisos apropiados y recursos adecuados, asegurando una orientación clara y apoyo a las iniciativas de seguridad.

El Comité de Seguridad de la Información, sesionará una vez al mes o cuando sea necesario de acuerdo a las necesidades de la JUNAEB.

Las funciones que desarrollará el jefe de seguridad de la información, las que serán establecidas en la resolución que lo designe, serán a lo menos las siguientes:

a) Tener a su cargo el desarrollo inicial de las políticas de seguridad y el control de su implementación, y velar por su correcta aplicación.

b) Coordinar la respuesta a incidentes de seguridad.

c) 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 pertinentes.

Por su parte, el Departamento de Informática, tomará las medidas necesarias para resguardar los Activos de Información y mantener su disponibilidad, confiabilidad e Integridad, de acuerdo a las directrices establecidas por el Comité de Seguridad de la Información. En el ámbito de la seguridad de la información, desarrollará las siguientes funciones:

a) Propondrá disposiciones generales para el uso de Activos de Información;

b) Propondrá capacitaciones pertinentes para el personal de la JUNAEB;

c) Realizará capacitaciones a dicho personal referida a la política de seguridad informática y de procedimientos del área TIC, en las competencias requeridas conforme al perfil de cada cargo;

d) Gestionará el procedimiento que se inicie en virtud de la denuncia de un incidente de seguridad.

e) Realizará procesos internos de auditoría de acuerdo a las necesidades establecidas por el jefe del Departamento de Informática.

f) Adoptará las medidas necesarias para resguardar los Activos de Información en conformidad a las instrucciones impartidas por el Comité de Seguridad de la Información.

Cada usuario interno o externo, será responsable de sus activos de información y de implementar los controles de seguridad respectivos, así como respetar las políticas y normas de seguridad establecidas.

4.2 Clasificación, control y etiquetado de bienes

El Departamento de Informática, mantendrá un registro de los Activos de Información de la JUNAEB, sus configuraciones e inventarios y personal responsable de cada uno de ellos.

De igual forma, propondrá las disposiciones necesarias para la correcta administración y uso de los equipos de procesamiento de datos por parte de los usuarios internos y/o externos, para el soporte por parte de la unidad de mantenimiento y para los cambios de configuraciones que se realicen a estos equipos.

Respecto al derecho de acceso a la información de los órganos de la Administración del Estado, deberán respetarse los principios establecidos en el artículo 11 de la Ley N° 20.285, de 2008, del Ministerio Secretaría General de la Presidencia.

4.3 Seguridad del personal

Con el objeto de reducir los riesgos de error humano o mal uso de los recursos informáticos, el Departamento de Informática, propondrá anualmente al Comité de Seguridad de la Información, los requerimientos de actualización de competencias para el personal de administradores de los sistemas informáticos, redes y seguridad, que les permita cumplir adecuadamente las misiones de su responsabilidad.

El Departamento de Gestión de Personas dispondrá de un proceso de inducción para el personal contratado por la JUNAEB, en materias correspondientes a la confidencialidad de la información y sistemas informáticos, que sean puestos a disposición de los integrantes de la institución, para el desempeño de sus funciones.

De igual forma se considerará, dentro del proceso de inducción al personal que se incorpora anualmente a la JUNAEB, una capacitación por parte del Departamento de Informática, referida a la política de seguridad informática y de procedimientos del área TIC, en las competencias requeridas conforme al perfil de cada cargo.

Todo el personal que tenga conocimiento de incidentes de seguridad, entendiendo por tales a todo evento que impida el normal funcionamiento de los Activos de Información y que afecte la seguridad informática, deberá informarlo en la forma más rápida y expedita posible a la ***Mesa de Ayuda*** del Departamento de Informática, la que deberá disponer de un procedimiento de gestión de incidentes, que deberá ser coordinado por el Encargado de Seguridad de la Información.

En caso que el personal de la JUNAEB infrinja las normas de seguridad de la información, deberá instruirse un procedimiento sumario en conformidad a lo dispuesto en el Estatuto Administrativo a fin de aplicar la medida disciplinaria que corresponda, sin perjuicio de la responsabilidad civil o penal que pudiera existir. Para el caso de que las infracciones sean realizadas por personal externo, se procederá de acuerdo a lo establecido en los respectivos contratos y/o acuerdos vigentes a fin de determinar las sanciones pertinentes, sin perjuicio de las responsabilidades civiles o penales que puedan corresponder.

4.4 Seguridad física y del ambiente

Se considerará dentro de las áreas de acceso restringido, las instalaciones en las que se encuentren equipos de procesamiento o comunicaciones de datos. Dentro de estas áreas restringidas, se encuentran: sala de servidores, dependencias donde se encuentran equipos de comunicaciones pertenecientes al cableado estructurado de la red LAN, oficina de administradores y monitoreo, oficinas de desarrolladores, taller de soporte, estaciones de trabajo de los usuarios y todas las instalaciones que el Comité de Seguridad de la Información determine que deban ser de acceso restringido.

4.5 Gestión de operaciones y comunicaciones

El Departamento de Informática deberá gestionar los procedimientos de apoyo, servicios informáticos y de seguridad de la información, de acuerdo a las normas establecidas por el Comité de Seguridad de la Información.

Con el fin de reducir el riesgo en el uso de los Activos de Información, en el Departamento de Informática se separarán los roles de las áreas de desarrollo, prueba y administración.

A su vez, el Comité de Seguridad de la Información definirá los procedimientos a seguir en la gestión de incidentes de seguridad, los que deberán ser implementados por el Departamento de Informática, bajo la coordinación del Encargado de Seguridad de la Información.

Por su parte, el Departamento de Informática realizará procesos internos de auditoría de acuerdo a las necesidades establecidas por el Jefe del Departamento, sin perjuicio del rol de auditoría que le corresponde al Departamento de Auditoría de la JUNAEB.

El Departamento de Informática deberá implementar los mecanismos de protección preventiva y activa contra software maliciosos, que puedan llegar en forma física o lógica a la red o estaciones de trabajo.
La información de los sistemas y configuraciones de los servidores de servicios importantes para las funciones de la institución, deberán ser respaldados periódicamente por el Departamento de Informática, conforme a los procedimientos definidos por el Comité de Seguridad de la Información.

A fin de asegurar el buen uso de los servicios informáticos por parte de los usuarios internos o externos, el Departamento de Informática, propondrá las normas de uso de los servicios TIC que estén a disposición del personal o de otras instituciones que hacen uso de los Activos de la Información, de comunicaciones e información de la JUNAEB, las que deberán ser aprobadas por el Comité de Seguridad de la Información.

4.6 Control de accesos

Cada usuario de los Activos de Información, tendrá acceso a la información de las aplicaciones informáticas, conforme al rol de su cargo y de acuerdo al nivel de acceso definido por el Comité de Seguridad de la Información. Es decir, se asignarán los privilegios de acceso a los usuarios internos o externos, basados en su necesidad de uso, con un criterio de información mínima, conforme a su rol y funciones.

La información de los sistemas que, bajo las condiciones anteriores, tenga acceso el personal, es para el uso exclusivo de las tareas que por rol le corresponde y no podrá ser entregada o divulgada en forma integral o parcial a terceros que no sean sus respectivos jefes y sólo para fines del trabajo productivo.

El acceso a la información será conforme a un Plan de Cuentas, propuesto por el Departamento de Informática en conjunto con los Jefes de Departamento y aprobado por el Comité de Seguridad de la Información. Los privilegios de acceso que se asignen a los respectivos mandos, se otorgarán de acuerdo a su ámbito de acción y responsabilidades.

4.7 Desarrollo y mantenimiento de sistemas de información

Todo Activo de Información que se requiera incorporar a la JUNAEB, deberá ser evaluado por el Departamento de Informática desde el punto de vista de un análisis de riesgos, antes de su compra, a fin de considerar en el proceso de adquisición, los requerimientos de seguridad que involucren los nuevos Activos.

Los software operacionales, deberán ser controlados, administrados y mantenidos en una biblioteca técnica, junto a todas sus actualizaciones.

Los software computacionales, compilaciones de datos, adaptaciones y cualquier documento relacionado con ello, son de propiedad de la JUNAEB, por cuanto han sido realizados por personal de la institución, en el desempeño de sus funciones, sea que éstos hayan sido realizados individualmente o de manera colectiva.
Los Activos de Información identificados como importantes para la continuidad del accionar de la JUNAEB, deberán contar con contrato de mantenimiento y/o soporte con los proveedores, a fin de asegurar su funcionamiento o reemplazo conforme a los niveles de servicio requeridos y su actualización.

4.8 Gestión de la continuidad del negocio

El Departamento de Informática deberá aplicar una estrategia, aprobada por el Comité de Seguridad de la Información, que asegure la continuidad operacional de los procesos críticos de la institución. A su vez, deberá gestionar los planes de contingencia, conforme a la estrategia definida.

El Encargado de Seguridad de la Información, asumirá la responsabilidad de ejecución de la planificación de contingencia que permita asegurar la continuidad de los procesos críticos en la JUNAEB.

5. REVISIONES

El Comité de Seguridad de la Información efectuará una revisión de esta Política al menos una vez al año, sin perjuicio de que pueda ser evaluada en cualquier momento, dependiendo de la necesidad de la organización.

6. DIFUSIÓN

Todo el personal de la JUNAEB deberá tomar conocimiento de la presente política y ésta quedará disponible para futuras consultas en la plataforma Intranet.

7. GLOSARIO DE TERMINOS

Para los propósitos de esta Política, las siguientes palabras se entenderán en el sentido que a continuación se indica:

Activo: Cualquier elemento que tenga valor para la organización. Para el ámbito de seguridad de la información, se puede clasificar en:

a) **Activos de Información**: Se entenderá por Activo de Información todo elemento en que se registre, en que se almacene y/o procese datos e información, sea a través de medios tecnológicos o no, tales como: bases de datos y archivos, contratos y acuerdos, documentación del sistema, manuales de usuario, material de entrenamiento, procedimientos operacionales o de soporte, plan de continuidad de negocio, información de auditorías, información archivada, activos de software, activos físicos y servicios.

b) **Activos de Software**: Constituidos por las aplicaciones de software, Software de sistemas y Herramientas de desarrollo y utilidades.

c) **Activos Físicos**: Constituidos por el equipamiento computacional, Equipamiento de comunicaciones, Medios móviles y otros equipamientos.

d) **Servicios**: Servicios de computación y comunicaciones. Utilidades generales (ej. electricidad, luz, aire acondicionado, etc.)

e) **Personas**: Constituidos por los usuarios, que utilizan la estructura tecnológica, el área de comunicaciones y que gestionan la información.

f) **Intangibles**: Constituidos por los activos referidos a la reputación e imagen de la institución.

Amenaza: Una causa potencial de un incidente no-deseado, el cual puede derivar en daño a un sistema u organización.

Análisis de Riesgos: Uso sistemático de la información para identificar las fuentes y calcular el riesgo.

Auditoria de Seguridad informática: Proceso sistemático, independiente y documentado que permite realizar una evaluación detallada de la Arquitectura de Seguridad mediante un análisis a nivel técnico (servidores, networking, firewalls, routers) y a nivel de procedimientos (procesos de revisiones y actualizaciones, políticas de accesos, contraseñas, planes de contingencia, etc.)

Confidencialidad: Garantía de que accedan a la información sólo aquellas personas autorizadas a hacerlo.

Integridad: Mantenimiento de la exactitud y totalidad de la información y los métodos de procesamiento.

LAN: Constituido por Redes de Área Local que interconectan distintos dispositivos entre sí, en el ámbito de un edificio.

Disponibilidad: Garantía de que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Mesa de Ayuda: Unidad del Área de Soporte, que atiende y da solución a los requerimientos técnicos de los usuarios.

Política: Intención y dirección general expresada formalmente por la autoridad máxima en la institución.

Riesgo: Combinación de la probabilidad de un evento y su ocurrencia.

Seguridad de la Información: Preservación de confidencialidad, integridad y disponibilidad de la información; además, también puede involucrar otras propiedades como autenticidad, responsabilidad, no-repudio y confiabilidad.

Sistema Informático: Constituido por el conjunto de computadores, software asociado, periféricos, terminales, procesos físicos, medios de transferencia de información y otros, que forman un todo autónomo capaz de realizar procesamiento de información y/o transferencia de información.

Software malicioso: También conocido como **Malware** (del inglés "malicious software") entendiéndose por tal todo software que tiene como objetivo infiltrarse en un sistema informático y dañar la (o las) computadora(s) que lo sustenta(n) sin el conocimiento de su dueño, con finalidades muy diversas. En esta categoría, encontramos desde Virus informáticos hasta Troyanos y Spyware.

El Malware hace referencia a una variedad de software o programas de códigos hostiles e intrusivos. Se debe considerar que el ataque a la vulnerabilidad por malware, puede ser a una aplicación, una computadora, un sistema operativo o una red completa.

Tecnología de la Información y de las Comunicaciones (TIC): Constituida por la agrupación de los elementos y las técnicas utilizadas en el tratamiento y la transmisión de la información, principalmente de informática, internet y telecomunicaciones.

WAN: Redes de área extendida, que constituyen la interconexión de distintos tipos de redes, en un ámbito global.

PLAN DE DIFUSIÓN Y REVISIÓN

DE LA

POLITICA DE SEGURIDAD

1. OBJETIVO GENERAL DIFUSIÓN DE LA POLÍTICA DE SEGURIDAD

La Política de Seguridad de la Información de JUNAEB, tiene por objetivo:

- Establecer normas que regulen el correcto uso de los activos de información,
- Garantizar estándares mínimos de seguridad en el uso, almacenamiento, acceso y distribución de información
- Establecer requisitos y condiciones generales de seguridad a la que se encuentre sujeto la JUNAEB de acuerdo a las normas legales y reglamentarias vigentes (1), así como los riesgos a que están expuestos sus activos de información.

El objetivo general del Plan de Difusión es que el personal, los nuevos funcionarios y los agentes externos relevantes, conozcan los temas relacionados a la seguridad de los activos de información y los beneficios y obligaciones asociadas. Así mismo socializar la Política, indicando que la Institución está incorporando de manera paulatina el Sistema de Seguridad de la Información.

2. ALCANCE DE LA DIFUSIÓN

Internos:

Dirección Nacional de JUNAEB: Departamento Informática, SIIAC, Departamento de Comunicaciones, Departamento de Recursos, Servicios Generales, Departamento de Jurídica, Departamento de Gestión de Personas, Departamento de Alimentación Escolar, Departamento de Salud, Departamento de Becas, Departamento de Logística, Departamento de Planificación y Control de Gestión, Unidad de Auditoría.

Externos:

Usuarios que realizarán una determinada actividad, así como los principales Proveedores autorizados por JUNAEB.

3. CONTENIDOS Y CANALES DE DIFUSIÓN

Internos: Personal activo y nuevos funcionarios.

- Sistema de Seguridad de la Información: (objetivo, clasificación de activos, responsabilidades)
- Política de Seguridad de la Información Institucional (objetivos, ámbitos involucrados)
- Plan de trabajo del Sistema de Seguridad en la Institución.

CANALES DE DIFUSIÓN INTERNOS:

- Publicación de la Política en la Intranet Institucional.
- Inducción a nuevos Funcionarios.
- Charlas y Reuniones.
- Oficios Informativos.

Externos: Proveedores, Personal externo

- Requerimientos de Seguridad Relevantes, en base al tipo de actividad que realizará al interior de la institución.

CANALES DE DIFUSIÓN EXTERNOS:

- Base de Licitación de bienes y servicios.
- Contratos de prestación de bienes o servicios.
- Documento de Instrucciones de Seguridad.

4. PLAN DE TRABAJO DE DIFUSIÓN

Medio de Difusión	Contenido	Fecha de Implementación	Responsable	Medio de Verificación
Publicación de la Política en la Intranet Institucional	Política de Seguridad de la Información JUNAEB	05/08/2011	Comité de Seguridad de la Información	Pantallazo de la política en la Intranet.
Oficio Informativo	Contexto de Implementación del Sistema de Seguridad de la Información	30/08/2011	Encargado Seguridad de la Información	Oficio
Inducción a nuevos Funcionarios	Sistema de Seguridad de la Información: (objetivo, clasificación de activos, responsabilidades) Política de Seguridad de la Información Institucional (objetivos, ámbitos involucrados) Plan de trabajo del Sistema de Seguridad en la Institución.	Se entregará un set de Información en temas relativos a la seguridad al momento de la contratación. Y Posteriormente se entrevistará con el Encargado de seguridad.	Gestión de Personas	Acta de Asistencia a Inducción.
Charlas y Reuniones con Departamentos	Sistema de Seguridad de la Información: (objetivo, clasificación de activos, responsabilidades) Política de Seguridad de la Información Institucional (objetivos, ámbitos involucrados) Plan de trabajo del Sistema de Seguridad en la Institución. Principales recomendaciones a	26-30 Septiembre del 2011	Comité de Seguridad de la Información	Acta de Asistencia.

	considerar en temas de seguridad de la Información			
Publicación en la Intranet Institucional del Plan de difusión y revisión de la PSI.	Documento de Plan de Difusión y Revisión de la PSI	30/09/2011	Coordinadora PMG SSI	Pantallazo publicación en la Intranet.

5. INDICADORES DE EVALUACIÓN DEL PLAN DE DIFUSIÓN.

Nombre Indicador	Formula Indicador	Unidad de medida	Valor Esperado	Medio de Verificación
Porcentaje de funcionarios socializados	(Número total de funcionarios de la DN socializados)*100/ (Número total de funcionarios de la DN)	Porcentaje	80%	-Lista de asistencia -Encuesta de Asimilación concepto Seguridad de la Información

6. REVISIÓN DE LA POLÍTICA (OBJETIVO GENERAL).

La política de Seguridad de la Información deberá ser revisada en un periodo específico con el objeto de asegurar la continua idoneidad, eficiencia y efectividad de la Política de Seguridad de la Información.
Esta revisión deberá considerar los siguientes aspectos:

- Retroalimentación de partes involucradas
- Cambios en los procesos Institucionales, directiva, nueva legislación, tecnología, incidentes de seguridad recientes.
- Alertas ante amenazas y vulnerabilidades
- Recomendaciones Provistas por autoridades relevantes.

7. CONTENIDOS A CONSIDERAR EN LA REVISIÓN:

Los contenidos de la Política de Seguridad que serán sometidos a revisión tiene relación con los ámbitos abordados en ésta.

- Seguridad Organizacional
- Clasificación , control y etiquetado de bienes
- Seguridad del Personal
- Seguridad Física y del ambiente
- Gestión de Operaciones y Comunicaciones
- Control de Accesos
- Desarrollo y mantenimiento de sistemas de información
- Gestión de la continuidad del negocio

8. PLAZO DE REVISIÓN DE LA POLITICA

La revisión de la Política de Seguridad de la Información se realizará anualmente, sin perjuicio de que pueda ser evaluada en cualquier momento, dependiendo de la necesidad de la organización.

ANÓTESE Y COMUNIQUESE, la presente resolución al Coordinador del Subcomité de Gestión de Seguridad y Confidencialidad del Documento Electrónico y Activos de Información, del Ministerio del Interior y al personal de JUNAEB.

JUNTA NACIONAL DE AUXILIO ESCOLAR Y BECAS
SECRETARIO GENERAL

CONSTANZO SCARELLA GUTIERREZ
SECRETARIO GENERAL
JUNTA NACIONAL DE AUXILIO ESCOLAR Y BECAS

JDLF/LHC/MJRS/HFO/pfm
Distribución:

1-. Gabinete
2-. Unidad de Control de Gestión
3-. Unidad de Asesoría Jurídica
4-. Oficina de Partes
5-. Departamento de Informática
6-. Departamento de Gestión de Personas