JUNJI
Ministerio de Educación

Gobierno de Chile

DEPARTAMENTO DE FISCALIA

REF.: APRUEBA POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN.

RESOLUCIÓN EXENTA N° 015/ 2492

SANTIAGO, 13 OCT 2011

VISTOS:

La Ley Nº 17.301, que crea la Junta Nacional de Jardines Infantiles; el Decreto Supremo Nº 1.574 de 1971, del Ministerio de Educación; el Decreto Supremo N° 83 de 2004, del Ministerio Secretaria General de la Presidencia, que aprueba norma técnica para los órganos de la Administración del Estado sobre seguridad y confidencialidad de los documentos electronicos; la Resolución Nº 1.600 de 2008, de la Contraloria General de la República, y demás normas pertinentes.

CONSIDERANDO:

1.- Que, mediante Resolución Exenta Nº 015/803 de 23 de marzo de 2011, se aprueba Política General de Seguridad de la Información para la Junta Nacional de Jardines Infantiles.

2.- Que, tal política requiere el señalamiento de normas particulares relativas, entre otras, a la seguridad organizativa, a la seguridad lógica, a la seguridad física y a los aspectos jurídicos, en manejo de información.

3.- Que, el Comité de Seguridad de la Información en reunión de 9 de septiembre de 2011, dio su aprobación al texto denominado Manual de Políticas Específicas de Seguridad de la Información, elaborado por el Encargado de Seguridad de la Información, y revisado por el Departamento Fiscalía y por los integrantes del citado Comité.

RESUELVO:

APRUEBASE el siguiente Manual de Políticas Específicas de Seguridad de la Información:

DIFÚNDASE entre los funcionarios y funcionarias de la Junta Nacional de Jardines Infantiles.

ANÓTESE, COMUNÍQUESE Y ARCHÍVESE.

JUNTA NACIONAL DE JARDINES INFANTILES
VICEPRESIDENTA EJECUTIVA

MARÍA FRANCISCA CORREA ESCOBAR
VICEPRESIDENTA EJECUTIVA
JUNTA NACIONAL DE JARDINES INFANTILES

JUNTA NACIONAL DE JARDINES INFANTILES
FISCALIA

MFCE/MXGA/AHM/AAT/PRM/IAD/iad
DISTRIBUCIÓN
- Vicepresidencia Ejecutiva
- Comité de Seguridad de la Información
- Directores Departamentos
- Directoras/es Regionales
- Jefes y Encargados de Unidades
- Of. de Partes.

MANUAL DE POLÍTICAS ESPECIFICAS

DE SEGURIDAD DE LA INFORMACIÓN PARA

JUNTA NACIONAL DE JARDINES INFANTILES

Índice

FISCALIA

FISCALIA

INTRODUCCIÓN

En una organización la gestión de seguridad puede tornarse compleja y difícil de realizar, esto no por razones técnicas, más bien por razones organizativas. Por ello es necesario coordinar todos los esfuerzos para propender un entorno informático institucional seguro. Mediante la simple administración del recurso humano y tecnológico, sin un adecuado control que integre los esfuerzos y conocimiento humano con las técnicas depuradas de mecanismos automatizados, tal desafío se encontrará, en la mayoría de los casos, con un ambiente complicado y difícil. Para facilitar esta labor es necesario emplear mecanismos reguladores de las funciones y actividades desarrolladas por cada uno de los funcionarios y funcionarias de la institución. El documento que se presenta como "Políticas Específicas de Seguridad de la Información", integra estos esfuerzos de una manera conjunta. Éste pretende, ser el medio de comunicación en el cual se establecen las directrices específicas que regulen la forma en que la Institución, prevenga, proteja y maneje los riesgos de seguridad de la información en diversas circunstancias. Las políticas expuestas en este documento están sujetas a cambios realizables en cualquier momento, siempre y cuando se tengan presentes los objetivos de seguridad. Toda persona que utilice los servicios que ofrece la red, deberá conocer y aceptar el reglamento vigente sobre su uso, el desconocimiento del mismo, no exonera de responsabilidad al usuario, ante cualquier eventualidad que involucre la seguridad de la información o de la red institucional.

En términos generales este documento de "Políticas Específicas de Seguridad de la Información", engloba los procedimientos que a la fecha se estiman más adecuados, tomando como lineamientos principales cuatro criterios, que se detallan a continuación:

Seguridad Organizacional: Dentro de éste, se establece el marco formal de seguridad de la información en que se debe sustentar el actuar de la Institución, incluyendo servicios o contrataciones externas a la infraestructura de seguridad, definida al efecto, integrando el recurso humano con la tecnología, estableciendo responsabilidades y actividades complementarias como respuesta ante situaciones anómalas a la citada seguridad.

Seguridad Lógica: Trata de establecer e integrar los mecanismos y procedimientos, que permitan monitorear el acceso a los activos de información, que incluyen los procedimientos de administración de usuarios, definición de responsabilidades, perfiles de seguridad, control de acceso a las aplicaciones y documentación sobre sistemas, que van desde el control de cambios en la configuración de los equipos, manejo de incidentes, selección y aceptación de sistemas, hasta el control de software malicioso.

FISCALIA

Seguridad Física: Identifica los límites mínimos que se deben cumplir en cuanto a perímetros de seguridad, de forma que se puedan establecer controles en el manejo de equipos, transferencia de información y control de los accesos a las distintas áreas con base en la importancia de los activos de información.

Seguridad Legal: Integra los requerimientos de seguridad que deben cumplir todos los funcionarios y usuarios de la red institucional bajo la reglamentación de la normativa interna de políticas y manuales de procedimientos de la JUNJI en cuanto al recurso humano, medidas o sanciones aplicables ante faltas o infracciones cometidas, así como también en aspectos relacionados con la legislación chilena en materias de seguridad de la información.

Cada uno de los criterios anteriores, sustenta un entorno de administración de suma importancia, para la seguridad de la información dentro de la red institucional de la Junta Nacional de Jardines Infantiles.

FISCALIA
4

1 GENERALIDADES

La información presentada en este documento ha sido organizada de manera que pueda ser interpretada por cualquier funcionario/a o por terceros con contrato de prestación de servicios en la Junta Nacional de Jardines Infantiles, con conocimientos informáticos o sin ellos. Las políticas fueron creadas según el contexto de aplicación, organizadas por niveles de seguridad de la información y siguiendo un entorno de desarrollo, sobre la problemática de la institución o previniendo futuras rupturas en la seguridad, aplicada sobre los diferentes recursos o activos de Información de la institución. El esquema de presentación del documento trata de las "Políticas específicas de Seguridad de la Información". En síntesis se presentara de la siguiente manera:

A. Nivel de Seguridad de la Información Organizativa:
   - ✓ Seguridad organizacional.
   - ✓ Políticas de Seguridad de la Información.
   - ✓ Excepciones de responsabilidad.
   - ✓ Clasificación y control de activos de información.
     - Responsabilidad por los activos de información.
     - Clasificación de la Información.
   - ✓ Seguridad ligada al personal (funcionarios/as y servidores externos)
     - Capacitación de usuarios.
     - Respuestas a incidentes y anomalías de Seguridad de la Información.

B. Nivel de seguridad lógico:
   - ✓ Control de accesos a Sistemas de Información.
   - ✓ Administración del acceso de usuarios.
     - Responsabilidad del usuario.
     - Uso de correo electrónico.
     - Uso de Internet.
   - ✓ Seguridad en acceso de terceros.
   - ✓ Control de acceso a la red.
   - ✓ Control de acceso al dominio.
   - ✓ Control de acceso a las aplicaciones.
   - ✓ Monitoreo del acceso y uso de Sistema.
   - ✓ Procedimientos operativos.
   - ✓ Planificación y recepción de Sistemas.
   - ✓ Protección contra Software malicioso.
   - ✓ Mantención de Sistemas.
   - ✓ Seguridad de medios de almacenamiento.

C. Nivel de Seguridad Física:
   - ✓ Seguridad de los equipos.
   - ✓ Controles generales.

D. Nivel de Seguridad legal:
   - ✓ Cumplimiento de requisitos legales.
   - ✓ Revisión de Políticas de Seguridad y cumplimiento técnico.
   - ✓ Consideraciones sobre Auditorias de Sistemas.

El lector de las políticas deberá enmarcar sus esfuerzos, sin importar el nivel organizacional en el que se encuentre dentro de la Institución, por cumplir todas las políticas pertinentes a su entorno de trabajo, utilización de los activos o recursos informáticos en los que éste se desenvuelve.

1.1 DEFINICIÓN DE POLÍTICAS DE SEGURIDAD INFORMÁTICA

1.1.1 ¿Que son las Políticas de Seguridad de la Información?

Son una forma de comunicación con el personal, ya que las mismas constituyen un canal formal de actuación, en relación con los recursos y servicios informáticos de la organización. Estas a su vez establecen las reglas y procedimientos que regulan la forma en que una organización previene, protege y maneja los riesgos de diferentes daños, sin importar el origen de éstos.

1.1.2 IMPORTANCIA DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Como parte integral de un Sistema de Seguridad de la Información (SSI), un manual de "Políticas de Seguridad de la Información", trata de definir : ¿Qué?, ¿Por qué?, ¿De qué? y ¿Cómo? se debe proteger la información. Estos engloban una serie de objetivos, estableciendo los mecanismos necesarios para lograr un nivel de seguridad adecuado a las necesidades establecidas dentro de la Institución. Estos documentos tratan a su vez de ser el medio de interpretación de la seguridad para toda la organización.

1.1.3 ORGANIZACIÓN DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

La Junta Nacional de Jardines Infantiles para dar cumplimiento a las políticas y normas deberá tener y contar con roles específicos y funciones dentro del Comité de Seguridad de la Información, representados por profesionales de las siguientes áreas y algunas de sus funciones son:

- *Vicepresidente/a Ejecutivo/a:* Autoridad de nivel superior que integra el Comité de Seguridad. Bajo su administración están la aceptación y seguimiento de las políticas y normativa de seguridad en concordancia con la normativa legal vigente y lo resuelto por el citado Comité.

FISCALIA

- *Encargado de Seguridad de la Información:* Funcionario/a con formación profesional idónea, encargado/a de velar por la seguridad de la información, realizar auditorías sobre este aspecto, proponer documentos de seguridad de la información relativos a políticas y normas; y de llevar un estricto control, con la ayuda del Departamento Informática, referente a los servicios informáticos prestados y niveles de seguridad aceptados para tales servicios.
- *Director/a del Departamento Informática:* Autoridad técnica especializada en el área, que vela por todo lo relacionado con la utilización de servidores, computadores de escritorio, sistemas de información, redes informáticas, procesamiento de datos e información y la comunicación en sí, a través de medios electrónicos.
- Director/a del Departamento Fiscalía: Autoridad institucional, que brinda la asesoría jurídica pertinente en el ámbito de la seguridad de la información.

El Comité de Seguridad de la Información, tendrá la facultad de citar a funcionarios de los cuales se necesite su conocimiento técnico, para dar respuesta a situaciones que involucren temas relacionados con la seguridad de la información.

Responsables de Activos de Información: Funcionarios (Directores de Departamento) dentro de los diferentes áreas de la Institución, que velarán por la seguridad y correcto funcionamiento de los activos informáticos, así como de la información procesada en éstos, dentro de sus respectivas áreas o niveles de mando.

2 BASE JURÍDICA.

La elaboración del manual de políticas de específicas de seguridad de la información, está fundamentado en el PMG de Seguridad de la Información de la Junta Nacional de Jardines Infantiles.

3 VIGENCIA

La documentación presentada como normativa de seguridad entrará en vigencia desde el momento en que ésta sea aprobada como documento técnico de seguridad de la información por las autoridades correspondientes de la Junta Nacional de Jardines Infantiles. Esta normativa deberá ser revisada y actualizada conforme a las exigencias de la Institución, o en el momento en que haya la necesidad de realizar cambios sustanciales en la infraestructura tecnológica de la Institución.

FISCALIA

4 VISIÓN

Constituir un nivel de seguridad de la información, altamente aceptable, mediante el empleo y correcto funcionamiento de la normativa y políticas de seguridad informática, basado en el sistema de seguridad de la información, a través de la utilización de técnicas y herramientas que contribuyan a optimizar la administración de los recursos informáticos de la Junta Nacional de Jardines Infantiles.

5 MISIÓN

Establecer las directrices necesarias para el correcto funcionamiento de un sistema de gestión para la seguridad de la información, enmarcando su aplicabilidad en un proceso de desarrollo continuo y actualizable, apegado a los estándares internacionales desarrollados para tal fin.

6 ALCANCES Y ÁREA DE APLICACIÓN

El ámbito de aplicación del manual de políticas específicas de seguridad de la información, es la infraestructura tecnológica y el entorno informático de la red institucional de la Junta Nacional de Jardines Infantiles. El órgano que garantizará la ejecución y puesta en marcha de la normativa y políticas de seguridad de la información es el Departamento Informática. Asimismo el responsable de la supervisión y cumplimiento de las normas sobre seguridad de la información es el Encargado de Seguridad de la Información, quien ejercerá su función en virtud de los acuerdos adoptados por el Comité de Seguridad de la Información.

7 GLOSARIO DE TERMINOS

- *Activo de información:* Es el conjunto de los bienes y derechos tangibles e intangibles de propiedad de una persona natural o jurídica que por lo general son generadores de renta o fuente de beneficios, en el ambiente informático llámese activo a los bienes de información y procesamiento, que posee la Institución. Recurso del sistema de información o relacionado con éste, necesario para que la organización funcione correctamente y alcance los objetivos propuestos.
- *Confidencialidad:* Característica de la información en virtud de la cual su revelación está autorizada sólo en la forma que se prevé para ello. Esto significa que la información debe estar protegida de ser copiada por cualquiera que no esté explícitamente autorizado por el propietario de dicha información.
- *Cuenta:* Mecanismo de identificación de un usuario; llámese de otra manera, al método de acreditación o autenticación del usuario mediante procesos lógicos dentro de un sistema informático.

- *Desastre o Contingencia:* interrupción de la capacidad de acceso a la información y al procesamiento de la misma a través de computadoras necesarias para la operación normal de un negocio.
- *Integridad:* Proteger la información de alteraciones no autorizadas por la organización.
- *Impacto:* consecuencia de la materialización de una amenaza o riesgo relativo a la vulneración de la seguridad de la información.
- *Responsabilidad:* En términos de seguridad de la información, significa determinar qué funcionario o servidor externo en la Institución, es responsable directo de mantener seguros los activos de cómputo e información.
- *Servicio:* Conjunto de aplicativos o programas informáticos, que apoyan la labor institucional y administrativa, sobre los procesos diarios que demanden información o comunicación de la Institución.
- *SSI:* Sistema de Seguridad de la Información.
- *Soporte Técnico:* Funcionario/a designado/a o encargado/a de velar por el correcto funcionamiento de las estaciones de trabajo, servidores, o equipo de oficina dentro de la Institución.
- *Riesgo:* posibilidad de que se produzca un impacto determinado en un activo, en un dominio o en toda la organización.
- *Usuario:* Defínase a cualquier persona jurídica o natural, que utilice los servicios informáticos de la red institucional y tenga una especie de vinculación laboral con la Institución.
- *Vulnerabilidad:* posibilidad de ocurrencia de la materialización de una amenaza sobre un activo de información.

8 *POLÍTICAS ESP*ECIFICAS DE SEGURIDAD DE LA INFORMACIÓN

8.1 OBJETIVO

Proporcionar la información necesaria, con el más amplio nivel de detalle posible, a los usuarios/as y funcionarios/as de la Junta Nacional de Jardines Infantiles, relativas a las normas y mecanismos que deben cumplir y utilizar para proteger el hardware y software de la red institucional de la Junta Nacional de Jardines Infantiles, así como la información que es procesada y almacenada en éstos.

8.2 NIVEL 1: DE LA SEGURIDAD ORGANIZATIVA

8.2.1 POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN:

Artículo I. Administradores de Servicios: Se definen dos tipos de administradores de servicios según las distintas plataformas tecnológicas institucionales. Estos son: Administrador de Sistemas y Administrador de Comunicación y Redes.

Artículo II. Cumplimiento de normativas y directrices: El usuario acatará las disposiciones expresas sobre la utilización de los servicios informáticos de la red institucional.

Uso de los servicios de la red institucional. Los servicios de la red institucional son de exclusivo uso institucional y para dar respuesta a los distintos procesos administrativos de las distintas áreas de negocio de la JUNJI, cualquier cambio en la normativa de uso de los mismos, se incorporará como política específica de seguridad de la Información.

Artículo III. Comité de Seguridad de la Información: La Junta Nacional de Jardines Infantiles creó un Comité de Seguridad de la Información, que vela por el cumplimiento de la normativa sobre seguridad de la información órgano que debe propiciar el entorno necesario para cumplir con el Sistema de Seguridad de la Información, SSI, el cual tendrá entre sus funciones:

a) Velar por la seguridad de los activos informáticos.
b) Gestión y procesamiento de información.
c) Cumplimiento de políticas de seguridad de la información.
d) Elaboración de planes de seguridad de la información.
e) Capacitación de usuarios en temas de seguridad de la información.
f) Proponer la aplicación de medidas o sanciones, según corresponda.
g) Gestionar y coordinar esfuerzos, por crear un plan de contingencia, que dé sustento o solución, a problemas de seguridad de la información dentro de la Institución. El mismo orientará y guiará a los funcionarios, la forma o métodos necesarios para salir avante ante cualquier eventualidad que se presente.
h) Informar sobre problemas de seguridad a la Alta Dirección de la Institución.
i) Poner especial atención a los usuarios de la red institucional sobre sugerencias o quejas con respecto al funcionamiento de los activos de información.
j) El Comité de Seguridad de la Información estará integrado por los siguientes miembros o quienes ellos designen en su representación:
   - El/La Vicepresidente/a Ejecutivo/a.
   - El/La Encargado/a de Seguridad de la Información.
   - El/La Director Departamento Informática.
   - El/La Director/a del Departamento Fiscalía
   - Los/Las Funcionarios/as de la JUNJI que por su conocimiento técnico ayudarán a dar respuestas a temas de seguridad de la información.

Artículo IV. El administrador de sistemas es el/la funcionario/a encargado/a de mantener en funcionamiento los servicios necesarios para la correcta explotación de los sistemas dentro de la red institucional.

Artículo V. El administrador de la red de datos y comunicaciones es el/la funcionario/a encargado de mantener los servicios de comunicaciones con el fin de brindar a los usuarios una red de datos segura para sus distintas funciones.

Artículo VI. Todo usuario de la red institucional de la Junta Nacional de Jardines Infantiles, gozará de absoluta privacidad sobre su información, o la información que provenga de sus acciones, salvo en casos, en que se vea involucrado en actos ilícitos o contraproducentes para la seguridad de la red institucional, de sus servicios o de cualquier otra red ajena a la Institución, previa aprobación de autoridad competente.

Artículo VII. Los usuarios tendrán el acceso a Internet, correo electrónico y acceso a sistemas informáticos, siempre y cuando se cumplan los requisitos mínimos de seguridad para acceder a este servicio y se acaten las disposiciones de conectividad del Departamento Informática.

8.2.2 EXCEPCIONES DE RESPONSABILIDAD

Artículo I. Los usuarios que por orden escrita de sus superiores realicen acciones que perjudiquen a otros usuarios o la información que estos procesan.

Artículo II. Algunos usuarios pueden estar exentos de responsabilidad, o de seguir algunas de las políticas específicas enumeradas en este documento, debido a la responsabilidad de su cargo, o a situaciones no programadas. Estas excepciones deberán ser solicitadas formalmente y aprobadas por el Comité de Seguridad de la Información, CSI, con la documentación necesaria para el caso, siendo el/la Vicepresidente/a Ejecutivo/a quien dé la aprobación final mediante el correspondiente acto administrativo.

8.2.3 CLASIFICACIÓN Y CONTROL DE ACTIVOS

8.2.3.1 RESPONSABILIDAD POR LOS ACTIVOS

Artículo I. Cada departamento o unidad, tendrá un responsable por el/los activo/s de información crítico/s o de mayor importancia para la Institución, el Departamento, la Sección y/o Unidad.

Artículo II. El funcionario/a o Unidad responsable de los activos de cada dependencia administrativa o área de trabajo, velará por el correcto uso y confidencialidad de los activos físicos (hardware y medios magnéticos), activos de información (Bases de Datos, Archivos, documentación de sistemas, procedimientos operativos, configuraciones, etc.), activos de software (aplicaciones, software de sistemas, herramientas y programas de desarrollo).

FISCALIA

Artículo III. Los responsables de los activos de información son los encargados de la seguridad y confidencialidad de la información almacenada y buen uso de estos recursos.

8.2.3.2 CLASIFICACIÓN DE LA INFORMACIÓN

Artículo I. Los Departamentos de la Junta Nacional de Jardines Infantiles, de forma individual, son responsables, de clasificar de acuerdo al nivel de importancia, la información que en ellos se procese.

Artículo II. Se tomarán como base, los siguientes criterios, como niveles de importancia, para clasificar la información:

a) Pública: Aquella financiada con fondos públicos y que reviste tal carácter en virtud de la Ley Nº 20.285, de Acceso a la Información Pública.
b) Interna: Aquella que corresponde a comunicaciones que tienen lugar al interior de la JUNJI.
c) Confidencial: Aquella cuya revelación está autorizada sólo en la forma que se prevé para ello.

Artículo III. Los activos de información de mayor importancia para la Institución deberán clasificarse por su nivel de exposición o vulnerabilidad.

8.2.4 SEGURIDAD DE LA INFORMACIÓN LIGADA A LOS/LAS FUNCIONARIOS/AS DE LA JUNI Y AL PERSONAL DE EMPRESAS CONTRATISTAS DE LA JUNJI QUE PRESTEN SERVICIO EN ELLA.

Artículo I. Se entregará a todos los/las funcionarios/as de la JUNJI que cumplan labores administrativas que ameriten tener acceso a la red informática institucional, una cuenta de acceso a dicha red, además de toda la documentación técnica necesaria relativa a los derechos y deberes para ejercer sus labores dentro de esta Institución, en el momento en que se inicie la prestación de servicios.

Artículo II. La información institucional procesada, manipulada o almacenada por el/la funcionario/a es propiedad exclusiva de la Junta Nacional de Jardines Infantiles.

Artículo III. La Junta Nacional de Jardines Infantiles no se hace responsable por daños causados provenientes del hecho de sus funcionarios a la información o activos de procesamiento, propiedad de la Institución, ni tampoco de los daños causados desde sus instalaciones de red a equipos informáticos externos.

8.2.4.1 CAPACITACIÓN DE USUARIOS

Artículo I. Los usuarios de la red institucional, serán capacitados en materias y problemáticas de seguridad de la información, según sea el área operativa y en función de las actividades que se desarrollan.

Artículo II. Se deben tomar todas las medidas de seguridad necesarias, antes de realizar una capacitación a personal ajeno o propio de la Institución, siempre y cuando

se vea implicada la utilización de los servicios de red o se exponga material de importancia considerable para la Institución.

8.2.4.2 RESPUESTAS A INCIDENTES Y ANOMALÍAS DE SEGURIDAD

Artículo I. 1. De los respaldos diarios de información: Se realizarán respaldos de la información, diariamente, para los activos de mayor importancia o críticos, un respaldo semanal que se utilizará en caso de fallas y un tercer respaldo efectuado mensualmente, el cual deberá ser guardado y evitar su utilización a menos que sea estrictamente necesaria. Estos respaldos son de responsabilidad del Administrador de Sistemas.

2.- De los respaldos semanales de información: Se realizarán respaldos semanales sobre la plataforma de servicios a los usuarios (correo, internet, web). Estos respaldos son de responsabilidad del Administrador de Comunicación y Redes.

Artículo II. De la responsabilidad por la tenencia y manejo de información: La información alojada en los equipos y en los servidores institucionales y manipulada por los usuarios en los equipos asignados para sus funciones, son de su exclusiva responsabilidad, por lo cual cada usuario debe solicitar al Depto. Informática se realicen respaldos periódicos de información.

Artículo III. Del procedimiento ante fallas: Las solicitudes de soporte, efectuados por funcionarios/as que se desempeñen en áreas de proceso o gestión, relativas a problemas en sus estaciones de trabajo, se canalizaran a través de los funcionarios/as del Depto. Informática designados para este propósito.

Artículo IV. El Encargado de Seguridad de la Información elaborará un documento donde se expliquen los pasos o procedimientos que se deberán seguir en caso de situaciones anómalas atentatorias a la seguridad de la información.

Artículo V. Del registro de eventos anómalo: Cualquier situación anómala y contraria a la seguridad deberá ser documentada, para la posterior revisión de los registros de sistemas con el objetivo de verificar la situación y dar una respuesta congruente y acorde al problema, ya sea esta en el ámbito jurídico o administrativo.

8.3 NIVEL 2: DE LA SEGURIDAD LÓGICA

8.3.1 CONTROL DE ACCESOS A SISTEMAS DE INFORMACIÓN

Artículo I. De los Sistemas de Información. Se entenderán como Sistemas de Información todo el software y/o aplicaciones que se encuentren alojados en los servidores centrales y que den respuesta al tratamiento y administración de datos e información, generados a nivel nacional para dar respuesta a las necesidades institucionales.

Artículo II. De la difusión del uso de los Sistemas Informáticos: El Departamento Informática o la unidad a cargo de la administración y servicios de los sistemas proporcionará toda la documentación necesaria para agilizar la utilización de los

FISCALIA

sistemas referente a modificaciones, guías, controles, auditorias y la administración de base de datos correspondiente por cada sistema.

Artículo III. De los requerimientos de información: Cualquier petición de información, servicio o acción proveniente de un determinado usuario o Departamento, se deberá efectuar siguiendo los canales de gestión formalmente establecidos por la Institución, para realizar dicha acción, los que requieren, necesariamente la visación del respectivo/a Director de Departamento. No dar seguimiento a esta política implica:

a) No dar respuesta o no ejecutar la acción o servicio requerido.
b) Enviar informe completo dirigido al Comité de Seguridad de la Información, el mismo será realizado por la persona o el Departamento al cual le es solicitado el servicio, a fin de que dicho Comité requiera la información faltante y proponga las medidas o sanciones a aplicar por la infracción al procedimiento.
c) Exponerse a eventuales medidas o sanciones aplicadas por el / la Vicepresidente/a Ejecutivo/a.

8.3.2 ADMINISTRACIÓN DEL ACCESO DE USUARIOS

Artículo I. Serán usuarios de la red institucional los funcionarios/as o personal que se desempeñe a honorarios en la Junta Nacional de Jardines Infantiles, respecto de los cuales se determine por su jefatura, se les considere como usuarios de red. Ello siempre que cumplan funciones administrativas en la Institución, identificándose previamente el objetivo de uso o permisos explícitos que se autorizarán a su respecto, y entregándose al Depto. Informática la información personal del usuario.

Artículo II. Los/as funcionarios/as y personal a honorarios que se definan como usuarios de la red, tendrán el carácter de usuarios limitados, toda vez que tendrán acceso únicamente a los servicios de Internet, recursos compartidos de la red institucional y correo institucional. Cualquier cambio sobre los servicios a los que estos tengan acceso, deberá ser revisado y autorizado previamente por el Depto. Informática, adecuándose a las nuevas especificaciones o condiciones de uso que le resulten aplicables con el cambio efectuado.

Artículo III. Se consideran usuarios externos o terceros, cualquier entidad o persona natural, que tenga una relación con la Institución fuera del ámbito de funcionario o del desempeño a honorarios, siempre que tenga una vinculación relativa a la prestación servicios tecnológicos con la Institución.

Artículo IV. El acceso a la red por parte de terceros es estrictamente restrictivo y permisible únicamente mediante firma impresa y documentación de aceptación de confidencialidad hacia la Institución y comprometido con el uso exclusivo del servicio para el que le fue provisto el acceso.

Artículo V. No se proporcionará el servicio solicitado por un usuario, Departamento o Unidad, sin antes haberse completado todos los procedimientos de autorización necesarios para su ejecución establecidos en la Norma Específica de usuarios de la red.

Artículo VI. La longitud mínima de caracteres permisibles en una contraseña se establece en 6 caracteres, los cuales tendrán una combinación alfanumérica, incluida en estos caracteres especiales.

8.3.2.1 DE LAS RESPONSABILIDADES DE LOS USUARIOS.

Artículo I. El usuario es responsable exclusivo de mantener en reserva su contraseña.

Artículo II. El usuario será responsable del uso que haga de su cuenta de acceso a los sistemas o servicios a que esté autorizado a emplear.

Artículo III. Se debe evitar el guardar o escribir las contraseñas en cualquier papel o superficie o dejar constancia de ellas, a menos que ésta sea guardada en un lugar seguro.

Artículo IV. El usuario es responsable de eliminar cualquier rastro de documentos proporcionados por la unidad de informática, que contenga información que pueda facilitar a un tercero la obtención de la información de su cuenta de usuario.

Artículo V. El usuario es responsable de evitar la práctica de establecer contraseñas relacionadas con alguna característica de su persona o relacionado con su vida o la de parientes, como fechas de cumpleaños o alguna otra fecha importante.

Artículo VI. El usuario deberá proteger su equipo de trabajo, evitando que personas ajenas a su cargo puedan acceder a la información almacenada en él, mediante una herramienta de bloqueo temporal (protector de pantalla), protegida por una contraseña, el cual deberá activarse en el preciso momento en que el usuario deba ausentarse.

Artículo VII. Cualquier usuario que encuentre una falla de seguridad en los sistemas informáticos de la Institución, está obligado a reportarlo al Administrador del Sistema, al Administrador de Redes, al Encargado de Informática o al Encargado de Seguridad de la Información.

Artículo VIII. Los usuarios, son los responsables de la información electrónica trabajada y almacenada en el equipo a su disposición. Para evitar perdida de información valiosa, la Institución destinara, a quien lo solicite, un espacio de almacenamiento en los servidores centrales para su almacenamiento y respaldo correspondiente.

8.3.2.2 Uso de correo electrónico

Artículo I. El servicio de correo electrónico de la Junta Nacional de Jardines Infantiles es un servicio institucional, el cual se presta a los funcionarios/as y servidores a honorarios creados como usuarios de la red. Se debe hacer uso de él, acatando todas las disposiciones de seguridad diseñadas para su utilización y evitar el uso o introducción de software malicioso a la red institucional.

FISCALIA

Artículo II. No se crearán cuentas de correo genéricas, sin previa consulta y resolución del Comité de Seguridad de la Información.

Artículo III. El correo electrónico es de uso exclusivo, para los funcionarios/as y servidores a honorarios de la Junta Nacional de Jardines Infantiles y sólo para fines institucionales.

Artículo IV. Todo uso indebido de este servicio, será motivo de suspensión temporal de su cuenta de correo o, según sea necesario, de la eliminación total de la cuenta dentro del sistema, considerando la magnitud de la infracción cometida.

Artículo V. El usuario será responsable de la información que sea enviada a través de su cuenta de correo institucional.

Artículo VI. El Comité de Seguridad de la Información, se reserva el derecho de monitorear las cuentas de usuarios, que presenten un comportamiento que, eventualmente, afecte la seguridad de la red institucional.

Artículo VII. Los usuarios de correos electrónicos institucionales son responsables de respetar las Leyes Nº 17.336, sobre Propiedad Intelectual y Nº 19.039, sobre Propiedad Industrial, y sus Reglamentos, en particular en lo relativo al Derecho de Autor, quedando impedidos de emplear este medio para distribuir de forma ilegal licencias de software o reproducir información sin autorización del autor.

8.3.2.3 Uso de Internet

Artículo I. El servicio de Internet es un servicio institucional, el cual se presta a los usuarios de la red institucional, quienes deben hacer uso de él, acatando todas las disposiciones de seguridad de la información diseñadas para su utilización, contenidas en las normas específicas sobre uso de Internet.

Artículo II. Se prestará el servicio de Internet, siempre que existan los requisitos de seguridad de la información mínimos definidos en las normas específicas sobre uso de Internet.

Artículo III. Todo uso indebido de este servicio, en términos de navegación prolongada o que exceda a la normativa institucional, será motivo de investigación de los sitios visitados por el usuario y de una suspensión temporal de este servicio respecto de ese usuario.

Artículo IV. El usuario será responsable de la navegación por sitios de Internet y de la información que de estos sitios pueda emanar.

Artículo V. El Comité de Seguridad de la Información, se reserva el derecho de monitorear las cuentas de usuarios, que presenten un comportamiento que, eventualmente, incida negativamente en la seguridad de la red institucional.

FISCALIA

8.3.2.4 Del uso de la telefonía IP

Artículo I. El servicio de telefonía IP es un servicio institucional, el cual se presta a los funcionarios/as y servidores a honorarios que cumplen funciones administrativas (oficinas) en dependencias institucionales.

Artículo II. Los dispositivos IP, deben ser distribuidos según necesidad institucional y su descripción se realizará por unidad o función asignada.

8.3.3 SEGURIDAD EN ACCESO DE TERCEROS

Artículo I. El acceso de terceros será concedido siempre y cuando se cumplan con los requisitos de seguridad de la información establecidos en el contrato de prestación de servicios suscrito entre la Junta Nacional de Jardines Infantiles y el tercero.

Artículo II. Todo usuario externo, estará facultado a utilizar única y exclusivamente el servicio que le fue asignado, y quedará sujeto a las normas internas especificas y a las responsabilidades que devengan de la utilización del mismo.

Artículo III. Los servicios accedidos por terceros acatarán las disposiciones generales de acceso a servicios por el personal interno de la Institución, además de los requisitos expuestos en su contrato con la Institución, estableciéndose al efecto cláusulas de confidencialidad.

8.3.4 CONTROL DE ACCESO A LA RED

Artículo I. El acceso a la red interna, se permitirá siempre y cuando se cumpla con los requisitos de seguridad definidos al efecto en la normas específicas sobre uso de Internet, relativa a la configuración de navegación, y éste será permitido mediante un mecanismo de autenticación.

Artículo II. Se debe eliminar cualquier acceso a la red sin previa autenticación o validación del usuario o el equipo empleado para ello.

Artículo III. Cualquier alteración del tráfico entrante o saliente a través de los dispositivos de acceso a la red, será motivo de verificación por la Unidad de Comunicación y Redes y tendrá como resultado directo la realización de una auditoria de seguridad a cargo de dicha Unidad.

Artículo IV. El Departamento informática deberá emplear dispositivos de red para el bloqueo, enrutamiento, o el filtrado de tráfico evitando el acceso o flujo de información, no autorizada hacia la red interna o desde la red interna hacia el exterior.

Artículo V. Se registrará todo acceso a los dispositivos de red, mediante archivos de registro o Log, de los dispositivos que provean estos accesos.

8.3.5 CONTROL DE ACCESO AL DOMINIO JUNJI

Artículo I. Las cuentas de usuarios no podrán tener privilegios de administrador del equipo asignado. Esta facultad sólo estará disponible para los encargados de informática.

Artículo II. Al terminar una sesión de trabajo en las estaciones, los administradores, los operadores de sistemas o cualquier otro usuario, evitará dejar encendido el equipo, a fin de precaver la utilización de la estación de trabajo por otra persona.

Artículo III. El acceso a la configuración del sistema operativo de los servidores, es únicamente permitido a los usuarios con el perfil de administrador.

Artículo IV. Los administradores de servicios, tendrán acceso único a los módulos de configuración de las respectivas aplicaciones que tienen bajo su responsabilidad.

Artículo V. Todo servicio provisto o instalado en los servidores, será ejecutado bajo cuentas restrictivas, en ningún momento se obviarán situaciones de servicios corriendo con cuentas administrativas, estos privilegios tendrán que ser eliminados o configurados correctamente.

8.3.6 CONTROL DE ACCESO A LAS APLICACIONES

Artículo I. Las aplicaciones deberán estar correctamente diseñadas, con funciones de acceso específicas y roles para cada usuario del entorno operativo de la aplicación.

Artículo II. Se deberá definir y estructurar el nivel de permisos sobre las aplicaciones, de acuerdo al nivel de ejecución o criticidad de las aplicaciones o archivos, y haciendo especial énfasis en los derechos (accesos) de escritura, lectura, modificación, ejecución o borrado de información.

Artículo III. Se deberán efectuar revisiones o pruebas minuciosas sobre las aplicaciones, de forma aleatoria, sobre distintas fases, antes de ponerlas en un entorno operativo real, con el objetivo de evitar redundancias en las salidas de información u otras anomalías.

Artículo IV. Las salidas de información, de las aplicaciones, en un entorno de red, deberán ser documentadas, y especificar el usuario que deberá ejecutar exclusivamente la salida de información.

Artículo V. Se deberá llevar un registro mediante Log de aplicaciones, sobre las actividades de los usuarios en cuanto a accesos, errores de conexión, horas de conexión, intentos fallidos, terminal desde donde conecta, entre otros, de manera que proporcionen información relevante y revisable posteriormente.

8.3.7 MONITOREO DEL ACCESO Y USO DEL SISTEMA

Artículo I. Se registrará y archivará toda actividad, procedente del uso de las aplicaciones, sistemas de información y uso de la red, mediante archivos de Log o bitácoras de sistemas.

Artículo II. Los archivos de Log, almacenarán nombres de usuarios, nivel de privilegios, IP de conexión, fecha y hora de acceso o utilización, actividad desarrollada, aplicación implicada en el proceso, intentos de conexión fallidos o acertados, archivos a los que se tuvo acceso, entre otros.

Artículo III. Se efectuará una copia automática de los archivos de Log, y se conducirá o enviara hacia otra terminal o servidor, evitando se guarde la copia localmente donde se produce.

8.3.8 PROCEDIMIENTOS OPERATIVOS

Artículo I. El Departamento Informática, será el único administrador de los distintos servicios informáticos y sistemas de información y será el responsable absoluto por mantener en óptimo funcionamiento estos servicios.

Artículo II. Las configuraciones y puesta en marcha de servicios, serán normadas por el Departamento Informática, y el Comité de Seguridad de la Información.

Artículo III. El personal responsable de los servicios, llevará archivos de registro de fallas de seguridad del sistema, revisará estos archivos de forma frecuente y en especial después de ocurrida una falla.

8.3.9 PLANIFICACIÓN Y ACEPTACIÓN DE SISTEMAS

Artículo I. El Departamento Informática, o personal del mismo dedicado o asignado en el área del desarrollo de aplicaciones, realizará todo el proceso de programación, análisis y desarrollo de sistemas, y puesta en marcha del software necesario para la Junta Nacional de Jardines Infantiles.

Artículo II. La aceptación del software se hará efectiva por las unidades solicitantes de la Institución, previo análisis y pruebas efectuadas por el personal de informática.

Artículo III. Únicamente se utilizará software certificado o en su defecto software previamente revisado y aprobado, por personal calificado en el área de seguridad de la información.

Artículo IV. La aceptación y uso de los sistemas faculta al Encargado de Seguridad de la Información, para efectuar pruebas o diagnósticos a la seguridad de los mismos.

Artículo V. El software diseñado para dar respuesta a procesos institucionales, deberán ser analizados y aprobados, tanto por el Departamento de Informática como por el Encargado de Seguridad de la Información, antes de su implementación.

Artículo VI. Es tarea de programadores el realizar pruebas de validación de entradas, en cuanto a:

- Valores fuera de rango.
- Caracteres inválidos, en los campos de datos.
- Datos incompletos.
- Datos con longitud excedente o valor fuera de rango.
- Datos no autorizados o inconsistentes.
- Procedimientos operativos de validación de errores.
- Procedimientos operativos para validación de caracteres.
- Procedimientos operativos para validación de la integridad de los datos.
- Procedimientos operativos para validación e integridad de las salidas.

FISCALIA

Artículo VII. Toda prueba de las aplicaciones o sistemas, se deberá hacer teniendo en cuenta las medidas de protección de los archivos de producción reales.

8.3.10 PROTECCIÓN CONTRA SOFTWARE MALICIOSO

Artículo I. Se adquirirá y utilizará software únicamente de fuentes confiables.

Artículo II. Los servidores, al igual que las estaciones de trabajo, tendrán instalado y configurado correctamente software antivirus actualizable y activada la protección en tiempo real.

8.3.11 MANTENCION DE SISTEMAS

Artículo I. El mantenimiento de las aplicaciones y software de sistemas es de exclusiva responsabilidad del personal del Departamento Informática, o del personal de soporte técnico de dicho Departamento o del prestador externo contratado al efecto.

Artículo II. El cambio de archivos de sistema, no es permitido, sin una justificación aceptable y verificable por el Encargado de Seguridad de la Información.

Artículo III. Se llevará un registro global del mantenimiento efectuado sobre los equipos y cambios realizados desde su instalación.

8.3.12 SEGURIDAD DE MEDIOS DE ALMACENAMIENTO

Articulo I. Los medios de almacenamiento o copias de seguridad de los sistemas de información, o información de la Institución, serán etiquetados de acuerdo a la información que almacenan u objetivo que suponga su uso, detallando o haciendo alusión a su contenido.

Artículo II. Los medios de almacenamiento con información crítica o copias de respaldo deberán ser manipulados única y exclusivamente por el personal encargado de hacer los respaldos y el personal encargado de su resguardo.

Artículo III. Todo medio de almacenamiento con información crítica será guardado bajo llave en un compartimento especial al cual tendrá acceso únicamente, el Encargado de Seguridad de la Información o el Director del Departamento Informática

Artículo IV. Se llevará un control, en el que se especifiquen los medios de almacenamiento en los que se debe guardar información y su uso.

8.3.13 INSCRIPCIÓN DE DOMINIOS PÚBLICOS (INTERNET)

Artículo I. Toda inscripción de dominios (www.nic.cl) con carácter institucional debe ser realizada por el Encargado de Seguridad de la Información.

Artículo II. Las inscripciones de dominios que tengan relación con Departamentos, Unidades, Secciones, Jardines Infantiles y cualquiera otra oficina administrativa o técnica que dependa de la Junta Nacional de Jardines Infantiles deberán contar con la aprobación del Comité de Seguridad de la Información.

Artículo III. La publicación de los dominios institucionales y sitios web se realizarán en servidores institucionales bajo la administración del Departamento Informática de la Institución.

8.4 NIVEL 3: DE LA SEGURIDAD FÍSICA

8.4.1 SEGURIDAD DE LOS EQUIPOS

Artículo I. El cableado de red, se instalará físicamente separado de cualquier otro tipo de cables y debidamente protegido e individualizado, llámese a estos de corriente o energía eléctrica, para evitar interferencias.

Artículo II. Los servidores, sin importar la plataforma a la cual brinda servicios, con problemas de hardware, deberán ser reparados localmente, de no cumplirse lo anterior, deberán ser retirados sus medios de almacenamiento o tomar las medidas necesarias para no afectar los servicios que se entregan.

Artículo III. Los equipos o activos críticos de información y proceso, deberán ubicarse en áreas aisladas y seguras, protegidas con un nivel de seguridad verificable y manejable por el Encargado de Seguridad de la Información y las personas responsables por esos activos, quienes deberán estar claramente identificados.

Artículo IV. Deberá llevarse un control exhaustivo del mantenimiento preventivo y otro para el mantenimiento correctivo que se les haga a los servidores, con el registro correspondiente.

8.4.2 CONTROLES GENERALES

Artículo I. Las estaciones de trabajo en las cuales se procese información crítica, deberán evitar el uso de medios de almacenamientos extraíbles, que puedan facilitar el robo o manipulación de la información por terceros o personal que no deba tener acceso a esta información.

Artículo II. En ningún momento se deberá dejar información sensible de robo, manipulación o acceso visual, sin importar el medio en el que ésta se encuentre, de forma que pueda ser alcanzada por terceros o personas que no deban tener acceso a esta información.

Artículo III. Toda oficina o área de trabajo debe poseer entre sus inventarios, herramientas auxiliares (extintores adecuados, alarmas contra incendios, lámpara de emergencia), necesarias para resguardar los recursos tecnológicos y la información, como asimismo, deberá capacitarse a los usuarios en el uso de estas herramientas auxiliares.

Artículo IV. Toda visita a las oficinas de tratamiento de datos críticos e información (unidad de informática, sala de servidores, entre otros) deberá ser registrada mediante el formulario de accesos a las salas de procesamiento crítico, para posteriores análisis del mismo.

Artículo V. La sala de servidores, deberá estar separada de las oficinas administrativas del Departamento Informática o cualquier otra unidad, dependencia o sala de recepción del personal, mediante una división en la unidad de informática, recubierta de material aislante o protegido contra el fuego y exceso de ruido, esta sala deberá ser utilizada únicamente por las estaciones prestadoras de servicios y/o dispositivos afines.

Artículo VI. El suministro de energía eléctrica debe hacerse a través de un circuito exclusivo para los equipos de cómputo, o en su defecto el circuito que se utilice no debe tener conectados equipos que demandan grandes cantidades de energía.

Artículo VII. El suministro de energía eléctrica debe estar debidamente polarizado, no siendo conveniente la utilización de polarizaciones locales de tomas de corriente, sino que debe existir una red de polarización.

Artículo VIII. Las instalaciones o sala de servidores deberá contar con una adecuada instalación eléctrica, y proveer del suministro de energía mediante una estación de alimentación ininterrumpida o UPS para poder proteger la información.

8.5 NIVEL 4: DE LOS ASPECTOS JURÍDICOS EN LA SEGURIDAD DE LA INFORMACIÓN

8.5.1 CUMPLIMIENTO DE REQUISITOS LEGALES

Artículo I. La Junta Nacional de Jardines Infantiles, se reserva el derecho de defensa, a cualquier usuario, ante cualquier asunto contencioso o no relacionado con infracciones a las leyes de copyright o piratería de software.

Artículo II. Todo el software comercial que utilice la Junta Nacional de Jardines Infantiles, deberá estar legalmente registrado, en los contratos de compra de licencias de software.

Artículo III. La adquisición de software deberá realizarse a través del Departamento Informática, previa justificación de las unidades requirentes y evaluación de compra por el citado Departamento.

Artículo IV. La instalación de software no licenciado es y será exclusiva responsabilidad del usuario, sin perjuicio de las responsabilidades de las jefaturas directas y del Departamento Informática por ausencia de los controles que les corresponde ejercer.

Artículo V. Tanto el software comercial como el software libre son propiedad intelectual exclusiva de sus desarrolladores, la Institución respeta la propiedad intelectual y se rige por el contrato de licencia de sus autores.

Artículo VI. El software comercial licenciado a la Junta Nacional de Jardines Infantiles, es propiedad exclusiva de la Institución, la misma se reserva el derecho de reproducción de éste, sin el permiso de sus autores, respetando el esquema de cero piratería y/o distribución a terceros.

FISCALIA

Artículo VII. En caso de transferencia de software comercial a terceros, se harán las gestiones necesarias para tal efecto y se acatarán las medidas de licenciamiento relacionadas con la propiedad intelectual.

Artículo VIII. Cualquier cambio en la política de utilización de software comercial o software libre, se hará documentado y en base a las disposiciones de la respectiva licencia.

Artículo IX. El software desarrollado internamente, por el personal que labora en la Institución es propiedad exclusiva de la Junta Nacional de Jardines Infantiles.

Artículo X. La adquisición del software libre o comercial deberá ser gestionado con las empresas creadoras o distribuidoras de ellos y acatando las disposiciones legales, en ningún momento se obtendrá software de forma fraudulenta.

Artículo XI. Los contratos con terceros, en la gestión o prestación de un servicio, deberán especificar, las medidas necesarias de seguridad, nivel de prestación del servicio, y/o el personal involucrado en tal proceso.

8.5.2 REVISIÓN DE POLÍTICAS DE SEGURIDAD Y CUMPLIMIENTO TÉCNICO

Artículo I. Toda violación a las políticas de licenciamiento de software, será motivo de sanciones aplicables al personal que incurra en la violación.

Artículo II. El documento de seguridad será elaborado y actualizado por el Encargado de Seguridad de la Información, junto al Comité de Seguridad de la Información, su aprobación y puesta en ejecución será responsabilidad del / la Vicepresidente/a Ejecutivo/a.

8.5.3 CONSIDERACIONES SOBRE AUDITORIAS DE SISTEMAS

Artículo I. Se debe efectuar una auditoria de seguridad a los sistemas de acceso a la red, semestralmente, enmarcada en pruebas de acceso tanto internas como externas, desarrolladas por personal técnico especializado o en su defecto por personal capacitado en el área de seguridad de la información.

Articulo II. El Encargado de Seguridad de la Información, junto al Administrador de la red, realizarán auditorias periódicas al sistema, con el fin de localizar intrusos o usuarios que estén haciendo mal uso de los recursos de un servidor.

Artículo III. Toda auditoria a los sistemas, estará debidamente aprobada por Auditoría Interna, y tendrá el sello y firma del Comité de Seguridad.

Artículo IV. Cualquier acción que amerite la ejecución de una auditoria a los sistemas informáticos deberá ser documentada y establecida su aplicabilidad y objetivos de la misma, así como razones para su ejecución, personal involucrado en la misma y sistemas implicados.

Artículo V. La auditoría no deberá modificar en ningún momento el sistema de archivos de los sistemas implicados, en caso de haber necesidad de modificar algunos, se deberá hacer un respaldo formal del sistema o sus archivos.

Artículo VI. Las herramientas utilizadas para la auditoria deberán estar separadas de los sistemas de producción y en ningún momento estas quedarán al alcance de personal ajeno a la elaboración de la auditoría.

9 CONTROL DE CAMBIOS

Nº Revisión	Fecha Aprobación	Motivo de la revisión	Páginas Modificadas	Autor
1	31/05/2011	Aprobación y revisión del documento	Todas	PRM
2	09/09/2011	Autorización y revisión del documento por el Comité de Seguridad de la Información.	Todas	AAT, IAD, CRC.