JJR/ FMM

CONSEJO NACIONAL DE LA CULTURA Y LAS ARTES
28 DIC. 2011
DOCUMENTO TOTALMENTE TRAMITADO

APRUEBA MARCO REGULATORIO DE LA SEGURIDAD DE LA INFORMACIÓN DEL CONSEJO NACIONAL DE LA CULTURA Y LAS ARTES.

RESOLUCION EXENTA Nº

VALPARAÍSO,

VISTOS: 28.12.2011 05963

Estos antecedentes; el Memorandum Interno N° 026/0971 del Jefe de la Sección de Planificación y Control de Gestión del Servicio ingresado al Departamento Jurídico con antecedentes completos con fecha 19 de Diciembre de 2011; la Resolución Nº 2492 que Aprueba Política General de Seguridad de la Información para el Consejo Nacional de la Cultura y las Artes; la Resolución N° 2493 que crea el Comité de Seguridad de la Información del Servicio; Acta de Reunión Extraordinaria N°6 del Comité de Seguridad de la Información de 14 de Diciembre de 2011; 10 Políticas de Seguridad, de Organización de la Seguridad de la Información, de Gestión de Activos; de Seguridad de los Recursos Humanos, de Seguridad Física y Ambiental, Gestión de las Comunicaciones y Operaciones, Control de Acceso, Adquisición, Desarrollo y Mantención de los Sistemas de Información, Gestión de Incidentes de la Seguridad de la Información, Gestión de la Continuidad del Negocio y Cumplimiento;

CONSIDERANDO:

Que, con el objetivo de apoyar el eficaz cumplimiento de las funciones que le competen, el Servicio ha desarrollado una plataforma tecnológica, la que permite interactuar de mejor manera con la ciudadanía y los integrantes del Consejo a lo largo del país, tomando en cuenta especialmente las funciones que le competen y que la información resguardada es propia de los sistemas del Servicio, por lo que resulta necesario establecer los requisitos y condiciones generales de seguridad a las que debe sujetarse el Consejo Nacional de la Cultura y las Artes, de acuerdo a las normas legales y reglamentarias que regulan esta materia.

Que, en este contexto, mediante la Resolución N° 2492, se aprobó la Política General de Seguridad de la Información para el Consejo Nacional de la Cultura y las Artes y la Resolución N° 2493 creó el Comité de Seguridad de la Información en el Consejo, ambas resoluciones de este Servicio y de fecha 27 de Mayo de 2011.

Que, el referido Comité en la Sesión Extraordinaria N°6 de 14 de Diciembre de 2011, dentro de sus facultades aprobó el Marco Regulatorio de la Seguridad de la Información, consistente en la definición de 10 Políticas de Seguridad de la Información basadas en los dominios de la Norma ISO 27001.

Que, asimismo dicho Comité aprobó 10 Políticas de Seguridad, que son de Organización de la Seguridad de la Información, de Gestión de Activos, de Seguridad de los Recursos Humanos, de Seguridad Física y Ambiental, de Gestión de las Comunicaciones y Operaciones, de Control de Acceso, de Adquisición, Desarrollo y Mantención de los Sistemas de Información, Gestión de Incidentes de la Seguridad de la Información, Gestión de la Continuidad del Negocio y Cumplimiento, las que constituyen el marco Regulatorio de la Seguridad de la Información del Consejo Nacional de la Cultura y las Artes.

Que, por su parte, el artículo segundo, numeral 42, de la Resolución N° 106, de 8 de Abril de 2011, del Consejo, cursada por la Contraloría General de la República con fecha 09 de Mayo de 2011, delega en el Subdirector Nacional del Consejo la facultad de impartir instrucciones y dictar los demás actos y resoluciones destinadas a implementar en el Servicio el Sistema de Gestión de la Seguridad de la Información,

establecido en el Decreto N° 83, de 2004, de Ministerio 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 las demás normas que lo complementan.

Que, en virtud de lo señalado y de lo dispuesto por la Ley Nº 19.880, que establece Bases de los Procedimientos Administrativos que rigen los Actos de los Órganos de la Administración del Estado, resulta necesario dictar el presente acto administrativo.

Y TENIENDO PRESENTE

Lo dispuesto en la Ley Nº19.891 que crea el Consejo Nacional de la Cultura y las Artes; en la Ley Nº19.880, que establece las Bases de los Procedimientos Administrativos que rigen los Actos de los órganos de la Administración del Estado; en el Decreto con Fuerza de Ley Nº 1/19.653 de 2000, 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 la Administración del Estado; en el Decreto 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; en la Resolución N° 106, de 2011, del Consejo Nacional de la Cultura y las Artes y en la Resolución Nº 1.600, de 2008 de la Contraloría General de la República, **vengo en dictar la siguiente:**

RESOLUCIÓN:

ARTÍCULO PRIMERO: Apruébase el Marco Regulatorio de la Seguridad de la Información del Consejo Nacional de la Cultura y las Artes, el que está constituido por 10 Políticas de la Seguridad de la Información, cuyo tenor es el siguiente:

POLÍTICA DE SEGURIDAD

ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

CONSEJO NACIONAL DE LA CULTURA Y LAS ARTES

AÑO 2011

CONTROL E HISTORIAL DE VERSIONES

N° Versión	Fecha	Descripción de las Modificaciones	Páginas Modificadas	Autor
1.0	15-07-2011	Elaboración de versión inicial	Todas	JGMV
1.1	17-10-2011	Correcciones de contenido, estilo, lenguaje, ordenamiento y presentación de temas	Todas	RAM
1.2	09-11-2011	Correcciones de contenido y de enfoque de género	Todas	RAM
1.3	15-11-2011	Retiro de registro de aprobación	Página 6	RAM

DECLARACIÓN CORPORATIVA

El Consejo Nacional de la Cultura y las Artes (CNCA) se compromete a administrar la seguridad de la información, a establecer un marco gerencial para iniciar y controlar su implementación, así como para la distribución de funciones y responsabilidades, y a garantizar la aplicación de medidas de seguridad adecuadas en los accesos de terceros a la información de la Institución.

ÁMBITO

- Esta Política se aplica a todos los recursos del CNCA y a todas sus relaciones con

terceros que impliquen el acceso a sus datos, recursos y/o a la administración y control de sus sistemas de información.

ROLES Y RESPONSABILIDADES

- **Encargado(a) de Seguridad de la Información**
  - Ser el responsable de impulsar la implementación de la presente Política.
  - Asistir al personal del CNCA en materia de seguridad de la información.
  - Analizar el riesgo de los accesos de terceros a la información de la Institución en conjunto con los(as) propietarios(as) de la información.
  - Verificar la aplicación de las medidas de seguridad necesarias para la protección de la misma.

- **Comité de Seguridad de la Información**
  - Tener a su cargo el mantenimiento, actualización y aprobación de las Políticas de Seguridad de la Información que deberán ser presentadas al Jefe de Servicio para su firma y distribución.

- **Subdirector(a) Nacional y Jefaturas de Departamento**
  - Autorizar la incorporación de nuevos recursos de procesamiento de información a las áreas y secciones de su incumbencia y dependencia.

REGLAS DE LA POLÍTICA

I. ORGANIZACIÓN INTERNA

Se deberá establecer una estructura de gestión para iniciar y controlar la implementación de la seguridad de la información dentro de la organización. En este sentido, el Comité deberá aprobar la política de seguridad de la información, asignar las funciones de seguridad, y coordinar y revisar la implementación de la seguridad en toda la organización.

1. **Compromiso de la Dirección con la Seguridad de la Información.**
   - 1.1. La seguridad de la información es responsabilidad de las Autoridades del CNCA, en tanto existe un compromiso explícito para su implementación, ejecución y cumplimiento.
   - 1.2. Se crea el Comité de Seguridad de la Información, integrado por representantes de todas las estructuras organizacionales del Servicio, destinadas a garantizar el apoyo manifiesto a las Autoridades y a las iniciativas de seguridad a implementar.
   - 1.3. El CNCA contará con un(a) Encargado(a) de Seguridad de la Información Institucional quien cumplirá la función de impulsar la implementación de la presente Política.

2. **Asignación de Responsabilidades de la Seguridad de la Información.**
   - 2.1. La máxima autoridad del CNCA, asigna las funciones relativas a la Seguridad de la Información de la institución en el(a) "Encargado(a) de Seguridad de la Información Institucional", quien tendrá a cargo las funciones relativas a la seguridad de los sistemas de información del CNCA, lo cual incluye la supervisión de todos los aspectos inherentes a la seguridad de la información tratados en la presente Política.
   - 2.2. El Comité de Seguridad de la Información propondrá y aprobará la definición y asignación de las responsabilidades que surjan del presente modelo.
3. **Autorización para Instalaciones de Procesamiento de Información.**
   - 3.1. Los recursos de procesamiento de información serán autorizados por el(a) Subdirector(a) Nacional y las Jefaturas de Departamentos involucrados, considerando su propósito y uso, conjuntamente con el(a) Encargado(a) de Seguridad de la Información Institucional, a fin de garantizar que se cumplan todas las políticas y requerimientos de seguridad pertinentes.
   - 3.2 El uso de recursos personales de procesamiento de información en el lugar de trabajo puede ocasionar nuevas vulnerabilidades. En consecuencia, su uso será evaluado en cada caso por el(a) Encargado(a) de Seguridad de la Información

Institucional y deberá ser autorizado por la jefatura de Sección de Tecnologías y por el(a) responsable del área al que se destinen los recursos.

4. Acuerdos de Confidencialidad.

4.1. Se deberán identificar y revisar con regularidad los requisitos de confidencialidad y/o los acuerdos de no-divulgación que reflejan las necesidades de la organización para la protección de la información, sin perjuicio de la aplicación general de la Ley N° 20.285 de Transparencia, la Ley N° 19.628 sobre Protección de Datos de carácter personal y su reglamento respecto de normas complementarias.

4.2. Para identificar los requisitos para los acuerdos de confidencialidad o de no-divulgación, se deberán considerar los siguientes elementos:

- **Asesoramiento Especializado en Materia de Seguridad de la Información**: El(a) Encargado(a) de Seguridad de la Información Institucional será el responsable de coordinar los conocimientos y las experiencias disponibles a fin de brindar ayuda en la toma de decisiones en materia de seguridad. Con el objeto de optimizar su gestión, se habilitará al(a) Encargado(a) de Seguridad de la Información Institucional el contacto con las Autoridades del Servicio, con los(as) responsables de las unidades organizativas de todas las áreas del CNCA, así como el contacto con grupos de interés especial.
- **Revisión Independiente de la Seguridad de la Información:** La Unidad de Auditoria Interna o en su defecto quien sea propuesto por el Comité de Seguridad de la Información realizará revisiones independientes sobre la vigencia e implementación de la Política de Seguridad de la Información, a efectos de garantizar que las prácticas del CNCA reflejan adecuadamente sus disposiciones.

II. ENTIDADES EXTERNAS

Se debe mantener la seguridad de la información y de los servicios de procesamiento de información de la organización a los cuales tienen acceso partes externas o que son procesados, comunicados o dirigidos por éstas.

5. Identificación de Riesgos del Acceso de Terceras Partes.

5.1. Cuando exista la necesidad de otorgar acceso a terceras partes a información del CNCA, el(a) Encargado(a) de Seguridad de la Información Institucional y el dueño(a) del proceso, propietario(a) de la Información de que se trate, llevarán a cabo y documentarán una evaluación de riesgos para identificar los requerimientos de controles específicos.

5.2. En ningún caso se otorgará acceso a terceros a la información, a las instalaciones de procesamiento u otras áreas de servicios críticos, hasta en tanto se hayan implementado los controles apropiados y se haya definido y establecido formalmente las condiciones para la conexión o el acceso.

6. Requerimientos de Seguridad en Contratos con Externos.

6.1. Se revisarán los contratos o acuerdos existentes, que se efectúen con terceros, para determinar y controlar que estos cumplan los mínimos estándares de seguridad y confidencialidad de la información.

CONTROL E HISTORIAL DE VERSIONES

N° Versión	Fecha	Descripción de las Modificaciones	Páginas Modificadas	Autor
1.0	15-07-2011	Elaboración de versión inicial	Todas	JGMV
1.1	19-10-2011	Correcciones de contenido, estilo, lenguaje, ordenamiento y presentación de temas	Todas	RAM
1.2	09-11-2011	Correcciones de contenido y de enfoque de género	Todas	RAM
1.3	15-11-2011	Retiro de registro de aprobación	Página 7	RAM

DECLARACIÓN CORPORATIVA

El Consejo Nacional de Cultura y las Artes, en adelante "CNCA", debe tener un profundo y detallado conocimiento sobre los activos que posee como parte importante de la administración de riesgos. Desde la perspectiva del Sistema de Gestión de Seguridad de la Información, la información que se maneja en el CNCA posee diferentes niveles de criticidad en cuanto al riesgo que representa su eventual divulgación, adulteración o indisponibilidad. Por lo anterior, se hace necesario diferenciar la información según el nivel de riesgo que genera su compromiso.

En este sentido, el CNCA se compromete a garantizar que los activos de información reciban un apropiado nivel de protección, clasificar la información para señalar su sensibilidad y criticidad, y definir los niveles de protección y medidas de tratamiento especial acordes a su clasificación.

ÁMBITO

- Esta Política se aplica a toda la información administrada en el CNCA, cualquiera sea el soporte en que se encuentre, define las categorías de clasificación de la información, y las reglas de manejo, copiado, almacenamiento, autorización de acceso y derecho a saber de la información.

ROLES Y RESPONSABILIDADES

Comité de Seguridad de la Información

- Designar a los propietarios(as) de la información.
- Asegurar que los lineamientos para la utilización de los recursos de las tecnologías de información contemplen los requerimientos de seguridad establecidos según la criticidad de la información que procesan.

- **Propietarios(as) de la Información**
  - Clasificar la información de acuerdo con su grado de sensibilidad, criticidad y esquema de clasificación definido por el Comité de Seguridad de la Información, de documentar y mantener actualizada la clasificación efectuada, y de definir las funciones que deberán tener permisos de acceso a la información.
  - Supervisar que el proceso de clasificación y rotulación de información de su área de competencia sea cumplida de acuerdo a lo establecido en la presente política.
  - Autorizar la divulgación de información, considerando los controles adecuados.

REGLAS DE LA POLÍTICA

1.Inventario y Propiedad de los Activos.

1.1. Se identificarán todos los activos importantes asociados a cada sistema de información, sus respectivos propietarios(as) y su ubicación, para luego elaborar un inventario con dicha información.

1.2. El mismo será actualizado ante cualquier modificación de la información registrada y revisada con una periodicidad de al menos cada un (1) año.

1.3. Los(as) encargados(as) y responsables de elaborar el inventario y mantenerlo actualizado son las Jefaturas de Departamento, Secciones y/o Unidades respectivas.

2. Uso Adecuado y Aceptable de los Activos.

2.1. La información, archivos físicos, los sistemas, los servicios, y los equipos (ejemplos: estaciones de trabajo, portátiles, impresoras, redes, Internet, correo electrónico, herramientas de acceso remoto, aplicaciones, teléfonos y faxes, entre otros) son activos del CNCA y se proporcionan a los(as) funcionarios(as) y terceros autorizados para cumplir con los propósitos del negocio.

2.2. Así mismo, el CNCA podrá monitorear, supervisar y utilizar su información, sistemas, servicios y equipos, de acuerdo con lo establecido en esta política y en cualquier proceso legal que se requiera.

2.3. El acceso a los documentos físicos y digitales estará determinado por las normas relacionadas con el acceso y las restricciones a los documentos públicos, a la competencia del área o dependencia específica, y a los permisos y niveles de acceso de los(as) funcionarios(as) y terceros determinados por las Jefaturas de Departamento, Secciones y/o Unidades.

2.4. **Internet**: La Internet es una herramienta de trabajo que permite navegar en muchos otros sitios relacionados o no con las actividades propias del negocio del CNCA, por lo cual, el uso adecuado de este recurso se debe controlar, verificar y monitorear, considerando para todos los casos.

2.5. **Correo Electrónico**: Los(as) funcionarios(as) y terceros autorizados a quienes el CNCA les asigne una cuenta de correo, deberán utilizarla de forma correcta y sólo para el uso específico de las tareas y actividades propias del cargo ejercido en el CNCA.

2.6. **Recursos Tecnológicos**: El uso adecuado de los recursos tecnológicos asignados por el CNCA a los(as) funcionarios(as) y/o terceros autorizados se reglamentará, controlará e informará.

3. Categorías de Clasificación de la Información.

3.1. La información del CNCA o de terceros confiados al CNCA, deben ser clasificados en una de las 3 siguientes categorías: RESERVADA, USO INTERNO O PÚBLICA, sin perjuicio de la aplicación general de la Ley N° 20.285 de Transparencia, la Ley N° 19.628 sobre Protección de Datos de carácter personal y su reglamento respecto de normas complementarias.

3.2. La definición de cada una es:

3.2.1. **RESERVADA**: El acceso a la información debe ser restringido severamente basado en el concepto de necesidad de conocer. Por su sensibilidad, esta información deberá ser resguardada con especial recelo, limitando su acceso sólo a aquellas personas que requieren de su conocimiento. En atención al impacto que puede ocasionar su divulgación o adulteración, se dispone que esta información deberá ser protegida, tanto en su almacenamiento como envío o transmisión, de manera tal que se asegure que sólo tenga acceso a ella el personal debidamente autorizado. Para su divulgación, se requiere del consentimiento formal del Propietario(a) de la Información.

3.2.2. **USO INTERNO**: Esta información es comunicada internamente sin restricciones y sólo puede ser divulgada a un tercero si, previamente, existe autorización del Propietario(a) para su entrega.

3.2.3. **PÚBLICA**: Esta información ha sido aprobada para la difusión pública. Quien entrega la autorización es el Propietario(a) de la Información.

4. Divulgación de Información

4.1. La desclasificación de la información, esto es, cambiar la categoría de RESERVADA a USO INTERNO o PÚBLICO; y de USO INTERNO a PÚBLICO, se efectuará de acuerdo a lo establecido en el procedimiento correspondiente.

4.2. Al efectuar dicha desclasificación, se deberá notificar a las personas relacionadas con la información que se desclasifica.

5. **Rotulación de Información.**

5.1. Toda información RESERVADA, USO INTERNO o PÚBLICA, debe ser rotulada de acuerdo al estándar definido por el Comité de Seguridad de la Información.

5.2. La información debe rotularse independientemente de estar almacenada en distintos medios: documentos electrónicos, documentos impresos, documentos manuscritos, cintas, disquetes, CD, etc.

5.3. El(a) Propietario(a) de la Información es el(a) responsable de asignarle la rotulación pertinente.

5.4. La asignación de propiedad de la información debe incluir la información que se recibe desde el exterior. En este caso, también el(a) Propietario(a) es el(a) responsable de asignar la clasificación y rotulación correspondiente.

5.5. Desde que la información es creada hasta que es eliminada o desclasificada, se debe mantener la rotulación definida en su clasificación original.

5.6. Cuando se consolida información clasificada en distintas categorías, la información resultante debe ser rotulada con la categoría más restrictiva.

6. **Copiado e Impresión de Información RESERVADA.**

6.1. La copia de información RESERVADA, debe ser autorizada por el(a) Propietario(a) de la Información, de acuerdo al procedimiento correspondiente.

7. **Almacenamiento de Información.**

7.1. Cuando no está en uso y especialmente en horario no-hábil, toda la información RESERVADA debe mantenerse almacenada, de modo de evitar que personas no-autorizadas tengan acceso a ella.

7.2. El almacenamiento de información RESERVADA no debe realizarse en el disco duro u otro componente del computador personal sin un sistema de control de acceso adecuado. La información RESERVADA y de USO INTERNO debe ser grabada en disco de red para garantizar su seguridad y respaldo.

7.3. Cuando no está en uso, la documentación escrita con información RESERVADA debe ser almacenada en gabinetes o escritorios con llave.

8. **Autorización de Acceso a Información Sensible (RESERVADA o de USO INTERNO).**

8.1 El acceso a información sensible debe ser autorizado explícitamente por el(a) Propietario(a) de la Información.

8.2 Los Acuerdos de No-Divulgación de Información que se firmen con terceros deben incluir cláusulas referentes al uso de la información y su eventual divulgación posterior.

8.3 Toda solicitud de información acerca de las Operaciones del CNCA y sus Sistemas, debe ser derivada al(a) Propietario(a) de la Información correspondiente. Esto no incluye la información de USO PÚBLICO.

8.4. Aunque la información no sea considerada sensible, para evitar ataques de Ingeniería Social[1], está prohibido que los(as) funcionarios(as) comenten con externos información acerca de otros(as) funcionarios(as).

8.5 Toda información que vaya a ser entregada al público, debe ser revisada de acuerdo a los procedimientos definidos.

8.6 Las actividades que requieran acceso a información sensible sólo las pueden realizar funcionarios(as) autorizados(as) por el Comité de Seguridad de la Información, a menos que se cumpla alguna de las siguientes condiciones:

- Un(a) funcionario(a) permanente no posee conocimiento o experiencia necesarios.
- Una emergencia o desastre requiere el uso de personal adicional.
- El(a) Propietario(a) de la información lo autorice.

9.Derecho a Saber.

9.1 Los(as) funcionarios(as) tienen derecho a conocer de antemano, los riesgos que corren en el lugar de trabajo respecto a la exposición a información restringida. La Jefatura de Departamento, Sección o Unidad respectiva debe informar de esos riesgos, tomar medidas para evitarlos y entrenar a los(as) funcionarios(as) sobre qué hacer ante esas situaciones.

9.2 Las políticas y procedimientos de seguridad deben ser conocidos por todos

los(as) funcionarios(as) del CNCA. Además, se podrá autorizar su conocimiento a consultores o auditores que lo requieran previa aprobación del(a) Encargado(a) de Seguridad de la Información.

[1] Ingeniería Social es un término utilizado en seguridad de la información para referirse a una táctica de usurpación de identidad.

POLÍTICA DE SEGURIDAD
SEGURIDAD DE LOS RECURSOS HUMANOS
CONSEJO NACIONAL DE LA CULTURA Y LAS ARTES

AÑO 2011

CONTROL E HISTORIAL DE VERSIONES

N° Versión	Fecha	Descripción de las Modificaciones	Páginas Modificadas	Autor
1.0	15-07-2011	Elaboración de versión inicial	Todas	JGMV
1.1	14-10-2011	Correcciones de contenido, estilo, lenguaje, ordenamiento y presentación de temas	Todas	RAM
1.2	04-11-2011	Correcciones de contenido y de enfoque de género	Todas	RAM
1.3	15-11-2011	Retiro de registro de aprobación	Página 6	RAM

DECLARACIÓN CORPORATIVA

La correcta gestión de los Recursos Humanos es parte integrante de la Administración de Seguridad, siendo los funcionarios(as) del Consejo Nacional de la Cultura y las Artes parte fundamental en el resguardo de la Seguridad de la Información.

ÁMBITO

- Esta política de Seguridad de Recursos Humanos se aplica a todos los funcionarios(as) del Consejo Nacional de la Cultura y las Artes, incluyendo el personal a planta, contrata, honorarios y código del trabajo.

ROLES Y RESPONSABILIDADES

- **Departamento de Recursos Humanos**
  - Verificar antecedentes de experiencia profesional y/o laboral, y antecedentes académicos, penales y requisitos legales del postulante.
  - Contratar nuevos funcionarios.
  - Entregar información objetiva en respuesta a solicitudes de referencias de ex-funcionarios(as) del Consejo Nacional de la Cultura y las Artes realizadas por entidades u organizaciones externas.
  - Proceso de Inducción a los nuevos funcionarios(as).

- **Funcionarios(as) del Consejo Nacional de la Cultura y las Artes**
  - Conocer y cumplir las políticas de seguridad de la información, asistir a charlas o entrenamientos en materias de seguridad.
  - Informar las vulnerabilidades detectadas y violaciones de seguridad de la información.

- **Jefaturas de Departamento**
  - Informar a las entidades y organizaciones externas con las que el funcionario(a) mantenía contacto a nombre del Servicio, que el ex-funcionario(a) ya no cuenta con la autorización para actuar en representación del Consejo Nacional de la Cultura y las Artes.

REGLAS DE LA POLÍTICA

1. **Verificación de Antecedentes Pre-contratación.**
   - 1.1. Todo proceso de Reclutamiento y Selección de personal debe ser canalizado sólo a través del Departamento de Recursos Humanos.
   - 1.2. El personal del Departamento de Recursos Humanos es el responsable de verificar los antecedentes de experiencia profesional y/o laboral, y antecedentes académicos, penales y requisitos legales del postulante, y en general, cualquier otro tipo de antecedente que pudiera afectar la seguridad de la información al interior de la Institución.

2. **Contratación.**
   - 2.1. La contratación de todo nuevo funcionario(a) del Consejo Nacional de la Cultura y las Artes, será canalizada por el personal del Departamento de Recursos Humanos según el procedimiento correspondiente.
   - 2.2. Los contratos de trabajo en la institución contarán con una cláusula en el que se detalle el tipo y características generales de la información a la que tendrá acceso o con la que trabajará directamente el funcionario(a).
   - 2.3. Los candidatos(as) deben de estar de acuerdo a firmar los términos y condiciones del empleo y de la organización, en el cual se les informará de las responsabilidades de la seguridad de la información.

3. **Inducción.**
   - 3.1. Todos los nuevos funcionarios(as) del Consejo Nacional de la Cultura y las Artes pasarán por un proceso de inducción a las Políticas, Procedimientos y Estándares de Seguridad de la Información, el cual será gestionado por el Encargado(a) de Seguridad de la Información, previa coordinación con el Departamento de Recursos Humanos y la Sección de Tecnologías.
   - 3.2. Todos los funcionarios(as) del Consejo Nacional de la Cultura y las Artes, deberán recibir información de las políticas y procedimientos de la organización para conocer sus funciones y desempeñarlas.

4. **No Divulgación de información**
   - 4.1. Todos los funcionarios(as) estarán sujetos a las claúsulas de confidencialidad dadas por la criticidad y sensibilidad de la información que éstos(as) manejen. En el caso del personal externo, y si el tipo de trabajo a realizar lo amerita, éstos(as) deberán firmar un contrato de no divulgación de la información.

5. **Propiedad Intelectual**
   - 5.1. Todos los productos, creaciones, desarrollos, campañas, trabajos, investigaciones, etc., logrados por un funcionario(a) durante la vigencia de su contrato en el Consejo Nacional de la Cultura y las Artes, serán de propiedad de la Institución.

6. **Políticas de Seguridad de la Información.**
   - 6.1. Es responsabilidad de cada funcionario(a) conocer y cumplir las políticas de seguridad de la información, asistir a charlas o entrenamientos en materias de seguridad.
   - 6.2. Es obligación de todo funcionario(a) el informar las vulnerabilidades detectadas y violaciones de seguridad de la información al superior directo y por su intermedio, al Comité de Incidentes.
   - 6.3. Ningún funcionario(a) puede violar los sistemas computacionales y redes de cualquier organización o individuo, ya sea dentro o fuera del horario de trabajo con recursos del Consejo Nacional de la Cultura y las Artes.
   - 6.4. Cualquier intento de violación de seguridad de la información o de vulnerabilidades de los sistemas internos o externos, ejecutada por funcionarios(as) no facultados(as) o autorizados(as) para ello, será considerado

como una falta a las políticas de seguridad de la información, independiente de la motivación, y podrá iniciar un proceso disciplinario, si procede, con las correspondientes sanciones de acuerdo al estatuto administrativo.

7. **Criterios de continuidad del empleo.**
   7.1. Periódicamente se realizará un análisis de la información relevante manejada por cada uno de los cargos de la Institución, con el objeto de establecer un mecanismo que permita que esos aspectos significativos sean conocidos por al mecanismo que permita que esos aspectos significativos sean conocidos por al menos otro funcionario(a), de manera de asegurar la continuidad de las operaciones del Consejo Nacional de la Cultura y las Artes.
8. **Finalización del Empleo.**
   8.1. Todo proceso de desvinculación debe realizarse conforme al Procedimiento de Desvinculación del Departamento de Recursos Humanos.
   8.2. Todos los funcionarios(as) deberán devolver los activos de información de la organización que estén en su poder a la terminación de su empleo.
   8.3. Los derechos de acceso de todos los funcionarios(as) a información e instalaciones de procesamiento de la información deben ser suspendidos a la terminación de su empleo.
   8.4. Se debe informar a las entidades y organizaciones externas con las que el funcionario(a) mantenía contacto a nombre del Servicio, que el ex-funcionario(a) ya no cuenta con la autorización para actuar en representación del Consejo Nacional de la Cultura y las Artes.

9. **Referencias de Ex Funcionarios**
   9.1. En respuesta a solicitudes de referencias de ex-funcionarios(as) del Consejo Nacional de la Cultura y las Artes realizadas por entidades u organizaciones externas, sólo la jefatura del Departamento de Recursos Humanos, o quien lo reemplace, entregará información objetiva.

POLÍTICA DE SEGURIDAD
SEGURIDAD FÍSICA Y AMBIENTAL
CONSEJO NACIONAL DE LA CULTURA Y LAS ARTES
AÑO 2011

CONTROL E HISTORIAL DE VERSIONES

N° Versión	Fecha	Descripción de las Modificaciones	Páginas Modificadas	Autor
1.0	15-07-2011	Elaboración de versión inicial	Todas	JGMV
1.1	15-11-2011	Correcciones de contenido, estilo, lenguaje, ordenamiento y presentación de temas	Todas	RAM

DECLARACIÓN CORPORATIVA

La seguridad física y ambiental brinda el marco para minimizar los riesgos de daños e interferencias a la información y a las operaciones del Consejo Nacional de Cultura y las Artes (CNCA). Asimismo, pretende evitar al máximo el riesgo de accesos físicos no autorizados, mediante el establecimiento de perímetros de seguridad. Se distinguen tres conceptos a tener en cuenta: la protección física de accesos, la protección ambiental y el transporte y protección. El control de los factores ambientales permite garantizar el correcto funcionamiento de los equipos de procesamiento y minimizar las interrupciones de servicio. Deben contemplarse tanto los riesgos en las instalaciones del CNCA como en instalaciones próximas a la sede del mismo que puedan interferir con las actividades.

ÁMBITO

- Esta Política se aplica a todos los recursos físicos relativos a los sistemas de información del CNCA, incluyendo: instalaciones, equipamiento, cableado, expedientes, medios de almacenamiento, entre otros.

ROLES Y RESPONSABILIDADES

- **Encargado(a) de Seguridad de la Información**
  - Definir junto con la Jefatura Sección de Servicios Tecnológicos y los Propietarios(as) de Información, según corresponda, las medidas de seguridad física y ambiental para el resguardo de los activos críticos.
  - Controlar su implementación.
  - Verificar el cumplimiento de las disposiciones sobre seguridad física y ambiental indicadas.

- **Jefatura Sección de Servicios Tecnológicos**
  - Definir junto con el Encargado(a) de Seguridad de la Información y los Propietarios(as) de Información, según corresponda, las medidas de seguridad física y ambiental para el resguardo de los activos críticos.
  - Controlar su implementación.
  - Verificar el cumplimiento de las disposiciones sobre seguridad física y ambiental indicadas.

- **Propietarios(as) de la Información**
  - Definir junto con el Encargado(a) de Seguridad de la Información y la Jefatura Sección de Servicios Tecnológicos, según corresponda, las medidas de seguridad física y ambiental para el resguardo de los activos críticos.

REGLAS DE LA POLÍTICA

1. Perímetro de Seguridad Física.

1.1. La protección física se llevará a cabo mediante la creación de diversas medidas de control físicas en las instalaciones de procesamiento de información del CNCA.

1.2. Se utilizarán perímetros de seguridad para proteger las áreas que contienen instalaciones de procesamiento de información, de suministro de energía eléctrica, de aire acondicionado, y cualquier otra área considerada crítica para el correcto funcionamiento de los sistemas de información.

1.3. Se deben definir y documentar claramente los perímetros de seguridad.

1.4. Las instalaciones de procesamiento de información se ubicarán dentro del perímetro de un edificio o área de construcción físicamente sólida.

1.5 Las paredes externas del área deben ser sólidas y todas las puertas que comunican con el exterior deben estar adecuadamente protegidas contra accesos no autorizados.

1.6 Se verificará la existencia de un área de recepción atendida por personal.

1.7 Se extenderán las barreras físicas necesarias desde el piso (real) hasta el techo (real), a fin de impedir el ingreso no autorizado y la contaminación ambiental.

1.8 Se debe identificar claramente todas las puertas de incendio de un perímetro de seguridad.

1.9 Se llevará un registro actualizado de los lugares y sitios protegidos.

2. Controles de Ingreso Físico.

2.1. Las áreas protegidas se resguardarán mediante el empleo de controles de acceso físico, los que serán determinados por el Encargado(a) de Seguridad de la Información junto con la Jefatura de Sección de Servicios Tecnológicos, a fin de permitir el acceso sólo al personal autorizado.

2.2. Se debe supervisar a los visitantes a áreas protegidas y registrar la fecha y horario de su ingreso y egreso.

2.3. Se debe controlar y limitar el acceso a la información clasificada y a las instalaciones de procesamiento de información, exclusivamente, a las personas autorizadas.

2.4. Se implementará el uso de una identificación unívoca visible para todo el personal del área protegida e instruirlo acerca de cuestionar la presencia de desconocidos no escoltados por personal autorizado y a cualquier persona que no exhiba una identificación visible.

3. <u>Ubicación y Seguridad del Equipamiento, Instalaciones y medios.</u>

3.1 El equipamiento será ubicado y protegido de tal manera que se reduzcan los riesgos ocasionados por amenazas y peligros ambientales, y las oportunidades de acceso no autorizado.

3.2. Se ubicará el equipamiento en un sitio donde se minimice el acceso innecesario y se provea de un control de acceso adecuado.

3.3. Se ubicarán las instalaciones de procesamiento y almacenamiento de información que manejan datos clasificados, en un sitio que permita la supervisión durante su uso.

3.4. Se aislarán los elementos que requieren protección especial para reducir el nivel general de protección requerida.

3.5. Se deben adoptar controles adecuados para minimizar el riesgo de amenazas potenciales, tanto internas como externas.

3.6. Se debe considerar, asimismo, el impacto de las amenazas citadas en el punto anterior que tengan lugar en zonas próximas a las sedes del CNCA.

4. <u>Suministro de Energía.</u>

4.1. El equipamiento estará protegido con respecto a las posibles fallas en el suministro de energía u otras anomalías eléctricas. El suministro de energía estará de acuerdo con las especificaciones del fabricante o proveedor de cada equipo.

4.2 Se dispondrá de múltiples enchufes o líneas de suministro para evitar un único punto de falla en el suministro de energía.

4.3. Se debe contar con un suministro de energía interrumpible (UPS) para asegurar el apagado regulado y sistemático o la ejecución continua del equipamiento que sustenta las operaciones críticas del CNCA.

4.4. Se debe montar un generador de respaldo para los casos en que el procesamiento deba continuar ante una falla prolongada en el suministro de energía.

5. <u>Seguridad del Cableado.</u>

5.1. El cableado de energía eléctrica y de comunicaciones que transporta datos o brinda apoyo a los servicios de información estará protegido contra intercepción o daño.

5.2 Se utilizará piso ducto o cableado embutido en la pared, siempre que sea posible, cuando corresponda a las instalaciones de procesamiento de información.

5.3. Se protegerá el cableado de red contra intercepción no autorizada o daño mediante el uso de conductos.

5.4. Se debe separar los cables de energía de los cables de comunicaciones para evitar interferencias.

5.5. Se debe proteger el tendido del cableado troncal (backbone) mediante la utilización de ductos blindados para los sistemas sensibles o críticos.

6. <u>Mantenimiento de Equipo.</u>

6.1. La mantención de los equipos tecnológicos deberá ser administrada y controlada por la sección de Servicios Tecnológicos y ejecutada por el área de Servicios de Atención Tecnológica (SAT), quienes serán los responsables de asegurar su continua disponibilidad e integridad.

6.2. El equipo se debe mantener en concordancia con los intervalos y especificaciones de servicio recomendados por el proveedor (Sección de Servicios Tecnológicos).

6.3. Sólo el personal de mantenimiento autorizado debe llevar a cabo las reparaciones y dar servicio al equipo.

6.4. Se deben mantener registros de todas las fallas sospechadas y reales, y todo mantenimiento preventivo y correctivo.

6.5. Se deben implementar los controles apropiados cuando se programa el equipo para mantenimiento, tomando en cuenta si su mantenimiento es realizado por el personal en el local o fuera de la organización.

7. Seguridad del Equipo fuera de las Instalaciones de la Organización.

7.1. La Sección de Servicios Tecnológicos deberá considerar los riesgos asociados a los equipos tecnológicos que se destinen para trabajar fuera de las dependencias del CNCA y para ello deberá implementar controles que aseguren la seguridad de los equipos institucionales.

7.2. El uso fuera de las dependencias de la institución de cualquier equipo de procesamiento de información debe ser autorizado por la Jefatura de Sección de Servicios Tecnológicos.

7.3. El equipo y medios sacados del local nunca deben ser dejados desatendidos en lugares públicos; durante un viaje, las computadoras portátiles deben ser llevadas como equipaje de mano y cuando sea posible, de manera disimulada.

7.4. Se deben observar en todo momento las instrucciones de los fabricantes para proteger el equipo; por ejemplo, protección contra la exposición a fuertes campos electromagnéticos.

7.5. Se deben determinar controles para el trabajo en casa a través de una evaluación del riesgo y los controles apropiados conforme sea apropiado; por ejemplo, archivos con llave, política de escritorio vacío, controles de acceso para las computadoras y una comunicación segura con la oficina.

7.6. Se debe contar con un seguro adecuado para proteger el equipo fuera del local.

7.7. Los riesgos de seguridad, por ejemplo, daño, robo o intercepción; puede variar considerablemente entre los locales y se debiera tomar esto en cuenta para determinar los controles más apropiados.

7.8. El equipo de almacenamiento y procesamiento de la información incluye todas las formas de computadoras personales, organizadores, teléfonos móviles, tarjetas inteligentes u otras formas que se utilicen para trabajar desde casa o se transporte fuera de local normal de trabajo.

8. Seguridad en la Eliminación o reutilización del Equipo.

8.1. La sección de Servicios Tecnológicos deberá considerar los riesgos asociados de eliminar equipos tecnológicos que posean la capacidad de almacenar información. Para ello el área de Servicios de Atención Tecnológica debe chequear los ítems del equipo que contiene medios de almacenaje para asegurar que se haya retirado o sobre-escrito cualquier data confidencial o licencia de software antes de su eliminación.

8.2. Los dispositivos que contienen información confidencial deben ser físicamente destruidos o se debe destruir, borrar o sobre-escribir la información utilizando técnicas que hagan imposible recuperar la información original, en lugar de simplemente utilizar la función estándar de borrar o formatear.

8.3. Los dispositivos que contienen data confidencial pueden requerir una evaluación del riesgo para determinar si los ítems deben ser físicamente destruidos en lugar de enviarlos a reparar o descartar.

8.4. La información puede verse comprometida a través de una eliminación descuidada o el re-uso del equipo.

9. Retiro de Bienes

9.1. El equipo, información o software no debe retirarse sin autorización de la jefatura directa, la cual deberá efectuarse con un periodo de tiempo definido con anticipación.

9.2. Los responsables de ejecutar el retiro de los equipos será el área de Servicios de Atención Tecnológica.

9.3. No se debe retirar el equipo, información o software sin autorización previa.

9.4. Los usuarios(as) empleados(as), contratistas y terceras personas que tienen la autoridad para permitir el retiro de los activos fuera del local deben estar claramente identificados.

9.5. se deben establecer límites de tiempo para el retiro del equipo y se debe realizar un chequeo de la devolución.

9.6. Cuando sea necesario y apropiado, el equipo debe ser registrado como retirado del local y se debe registrar su retorno.

9.7. También, se pueden realizar chequeos inesperados para detectar el retiro de propiedad, dispositivos de grabación no-autorizados, armas, etc., y evitar su ingreso al local. Estos chequeos inesperados deben ser llevados a cabo en concordancia con la legislación y regulaciones relevantes. El personal debe saber que se pueden llevar a cabo chequeos inesperados, y los chequeos se deben realizar con la debida autorización de los requerimientos legales y reguladores.

POLÍTICA DE SEGURIDAD

GESTIÓN DE LAS COMUNICACIONES Y OPERACIONES
CONSEJO NACIONAL DE LA CULTURA Y LAS ARTES
AÑO 2011

CONTROL E HISTORIAL DE VERSIONES

N° Versión	Fecha	Descripción de las Modificaciones	Páginas Modificadas	Autor
1.0	15-07-2011	Elaboración de versión inicial	Todas	JGMV
1.1	15-11-2011	Correcciones de contenido, estilo, lenguaje, ordenamiento y presentación de temas	Todas	RAM

DECLARACIÓN CORPORATIVA

La proliferación de software malicioso, como virus, troyanos, etc., hace necesario que se adopten medidas de prevención, a efectos de evitar la ocurrencia de tales amenazas. Es conveniente separar los ambientes de desarrollo, prueba y operaciones de los sistemas de la Institución, estableciendo procedimientos que aseguren la calidad de los procesos que se implementen en el ámbito operativo, a fin de minimizar los riesgos de incidentes producidos por la manipulación de información operativa. Los sistemas de información están comunicados entre sí, tanto dentro Consejo Nacional de la Cultura y las Artes (CNCA), como con terceros fuera de èl. Por lo tanto, es necesario establecer criterios de seguridad en las comunicaciones que se establezcan. Las comunicaciones establecidas permiten el intercambio de información, que deberá estar regulado para garantizar las condiciones de confidencialidad, integridad y disponibilidad de la información que se emite o recibe por los distintos canales.

ÁMBITO

- Esta Política se aplica a Todas las instalaciones de procesamiento y transmisión de información del CNCA.

ROLES Y RESPONSABILIDADES

- **Encargado(a) de Seguridad de la Información**
  - Definir procedimientos para el control de cambios a los procesos operativos documentados, los sistemas e instalaciones de procesamiento de información y verificar su cumplimiento, de manera que no afecten la seguridad de la información.
  - Establecer criterios de aprobación para nuevos sistemas de información, actualizaciones y nuevas versiones, contemplando la realización de las pruebas necesarias antes de su aprobación definitiva. Verificar que dichos procedimientos de aprobación de software incluyan aspectos de seguridad para las aplicaciones de Gobierno Electrónico.

- Definir procedimientos para el manejo de incidentes de seguridad y para la administración de los medios de almacenamiento.
- Definir y documentar una norma clara con respecto al uso del correo electrónico.
- Controlar los mecanismos de distribución y difusión de información dentro del CNCA.
- Definir y documentar controles para la detección y prevención del acceso no autorizado, la protección contra software malicioso y para garantizar la seguridad de los datos y los servicios conectados en las redes del CNCA.
- Desarrollar procedimientos adecuados de concientización de usuarios(as) en materia de seguridad, controles de acceso al sistema y administración de cambios.
- Verificar el cumplimiento de las normas, procedimientos y controles establecidos.
- En conjunto con la Jefatura del Departamento de Jurídico y la Jefatura de Sección de Servicios Tecnológicos, el(a) Encargado(a) de Seguridad de la Información evaluará los contratos y acuerdos con terceros para garantizar la incorporación de consideraciones relativas a la seguridad de la información involucrada en la gestión de los productos y/o servicios prestados.

- **Jefatura Sección de Servicios Tecnológicos**
  - Controlar la existencia de documentación actualizada relacionada con los procedimientos de comunicaciones y operaciones.
  - Evaluar el posible impacto operativo de los cambios previstos a sistemas y equipamiento y verificar su correcta implementación, asignando responsabilidades.
  - Administrar los medios técnicos necesarios para permitir la segregación de los ambientes de procesamiento.
  - Monitorear las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas de capacidad, a fin de evitar potenciales amenazas a la seguridad del sistema o a los servicios del usuario.
  - Controlar la realización de las copias de resguardo de información, así como la prueba periódica de su restauración.
  - Asegurar el registro de las actividades realizadas por el personal operativo, para su posterior revisión.
  - Desarrollar y verificar el cumplimiento de procedimientos para comunicar las fallas en el procesamiento de la información o los sistemas de comunicaciones, que permita tomar medidas correctivas.
  - Implementar los controles de seguridad definidos (software malicioso y accesos no autorizados).
  - Definir e implementar procedimientos para la administración de medios informáticos de almacenamiento, como cintas, discos e informes impresos, y para la eliminación segura de los mismos.
  - Participar en el tratamiento de los incidentes de seguridad, de acuerdo a los procedimientos establecidos.
  - En conjunto con el(a) Encargado(a) de Seguridad de la Información y la Jefatura del Departamento de Jurídico, la Jefatura de Sección de Servicios Tecnológicos evaluará los contratos y acuerdos con terceros para garantizar la incorporación de consideraciones relativas a la seguridad de la información involucrada en la gestión de los productos y/o servicios prestados.

- **Jefatura Departamento Jurídico**
  - En conjunto con el(a) Encargado(a) de Seguridad de la Información y la Jefatura de Sección de Servicios Tecnológicos, la Jefatura del Departamento de Jurídico evaluará los contratos y acuerdos con terceros para garantizar la incorporación de consideraciones relativas a la seguridad de la información involucrada en la gestión de los productos y/o servicios prestados.

- **Propietarios(as) de la Información**
  - En conjunto con el(a) Encargado(a) de Seguridad de la Información y la Jefatura de Sección de Servicios Tecnológicos, los(as) Propietarios(as) de la Información determinarán los requerimientos para resguardar la información por la cual son responsables.
  - Aprobarán los servicios de mensajería autorizados para transportar la información cuando sea requerido, de acuerdo a su nivel de criticidad.

REGLAS DE LA POLÍTICA

1. Procedimientos y Responsabilidades Operativas.

1.1. **Procedimientos de Operación Documentados.**

Se documentarán y mantendrán actualizados los procedimientos operativos identificados en esta Política y sus cambios serán autorizados por el(a) Encargado(a) de Seguridad de la Información. Los procedimientos especificarán instrucciones para la ejecución detallada de cada tarea, incluyendo:

- Procesamiento y manejo de la información.
- Requerimientos de programación de procesos, interdependencias con otros sistemas, tiempos de inicio de las primeras tareas y tiempos de terminación de las últimas tareas.
- Instrucciones para el manejo de errores u otras condiciones excepcionales que puedan surgir durante la ejecución de tareas.
- Restricciones en el uso de utilitarios del sistema.
- Personas de soporte a contactar en caso de dificultades operativas o técnicas imprevistas.
- Instrucciones especiales para el manejo de "salidas", como el uso de papelería especial o la administración de salidas confidenciales, incluyendo procedimientos para la eliminación segura de salidas fallidas de tareas.
- Reinicio del sistema y procedimientos de recuperación en caso de producirse fallas en el sistema.

1.2. **Gestión de Cambios.**

- Se definirán procedimientos para el control de los cambios en el ambiente operativo y de comunicaciones. Todo cambio deberá ser evaluado previamente en aspectos técnicos y de seguridad por la Sección de Servicios Tecnológicos.
- El(a) Encargado(a) de Seguridad de la Información controlará que los cambios en los componentes operativos y de comunicaciones no afecten la seguridad de los mismos ni de la información que soportan. La Jefatura de Sección de Servicios Tecnológicos evaluará el posible impacto operativo de los cambios previstos y verificará su correcta implementación.
- Se retendrá un registro de auditoría que contenga toda la información relevante de cada cambio implementado.

1.3. **Segregación de Deberes.**

- Se separará la gestión o ejecución de ciertas tareas o áreas de responsabilidad, a fin de reducir el riesgo de modificaciones no autorizadas, mal uso de la información o los servicios por falta de independencia en la ejecución de funciones críticas.
- Si el método de control anterior no se pudiera cumplir en algún caso, se implementarán controles como:
  - Monitoreo de las actividades.
  - Registros de auditoría y control periódico de los mismos.
  - Supervisión por parte de la Unidad de Auditoría Interna o en su defecto quien sea propuesto a tal efecto, siendo independiente al área que genera las actividades auditadas.
- Asimismo, se documentará la justificación formal por la cual no fue posible efectuar la segregación de funciones.
- Se asegurará la independencia de las funciones de auditoría de seguridad, tomando recaudos para que ninguna persona pueda realizar actividades en áreas de responsabilidad única sin ser monitoreada, y la independencia entre el inicio de un evento y su autorización, considerando los siguientes puntos:
  - Separar actividades que requieren connivencia para defraudar, por ejemplo efectuar una orden de compra y verificar que la mercadería fue recibida.
  - Diseñar controles, si existe peligro de connivencia de manera tal que dos o más personas estén involucradas.

1.4. **Separación de los Medios de Desarrollo, Prueba y Operación**.

- Los ambientes de desarrollo, prueba y operaciones, siempre que sea posible, estarán separados preferentemente en forma física, y se definirán y documentarán las reglas para la transferencia de software desde el estado de desarrollo hacia el estado operativo.

2. Gestión de la Entrega de Servicios de Terceros.

2.1. **Entrega del Servicio**.

- Se debe asegurar que los controles de seguridad, definiciones del servicio y niveles de entrega incluidos en el acuerdo de entrega del servicio de terceros se implementen, operen y mantengan.
- La entrega del servicio por un tercero debe incluir los acuerdos de seguridad pactados, definiciones del servicio y aspectos de la gestión del servicio.
- En caso de los acuerdos de abastecimiento externo, la institución debe planear las transiciones necesarias (de informaciones, medios de procesamiento de la información y cualquier otra cosa que necesite transferirse) y debiera asegurar que se mantenga la seguridad a través del periodo de transición.
- La institución debe asegurar que la tercera persona mantenga una capacidad de servicio suficiente junto con los planes de trabajo diseñados para asegurar que se mantengan los niveles de continuidad del servicio después de fallas importantes en el servicio o un desastre.

2.2. **Monitoreo y Revisión de los Servicios de Terceros**.

- Los servicios, reportes y registros provistos por terceros deben ser monitoreados y revisados regularmente, y se deben llevar a cabo auditorías regularmente.
- El monitoreo y revisión de los servicios de terceros debe asegurar que se cumplan los términos y condiciones de seguridad de los acuerdos, y que se manejen apropiadamente los incidentes y problemas de seguridad de la información. Esto debe involucrar una relación y proceso de gestión de servicio entre la Institución y la tercera persona.
- La responsabilidad de manejar la relación con terceros se debe asignar a una persona o equipo de gestión de servicios.
- La Institución debe asegurar que los terceros asignen responsabilidad para el chequeo del cumplimiento de los requerimientos de los acuerdos.
- Se deben poner a disposición las capacidades y recursos técnicos para monitorear los requerimientos del acuerdo, en particular si se cumplen los requerimientos de seguridad de la información.
- Se debe tomar la acción apropiada cuando se observan deficiencias en la entrega del servicio.
- La Institución debe mantener el control y la visibilidad general suficiente en todos los aspectos de seguridad con relación a la información confidencial o crítica o los medios de procesamiento de la información que la tercera persona ingresa, procesa o maneja.
- La Institución debe asegurarse de mantener visibilidad en las actividades de seguridad como la gestión del cambio, identificación de vulnerabilidades y reporte/respuesta de un incidente de seguridad, a través de un proceso, formato y estructura de reporte definidos.

2.3. **Manejo de Cambios en los Servicios de Terceros**.

Se debe manejar los cambios en la provisión de servicios, incluyendo el mantenimiento y mejoramiento de las políticas, procedimientos y controles de seguridad de la información existentes teniendo en cuenta el grado crítico de los sistemas y procesos del negocio involucrados y la re-evaluación de los riesgos.
El proceso de manejar los cambios en el servicio de terceros necesita tomar en cuenta:

- Los cambios realizados por la institución para implementar:
  - Aumentos los servicios ofrecidos actualmente.

- Desarrollo de cualquier aplicación y sistema nuevo.
- Modificaciones o actualizaciones de las políticas y procedimientos de la institución.
- Controles nuevos para solucionar incidentes de la seguridad de la información y para mejorar la seguridad.

- Cambios en los servicios de terceros para implementar:
  - Cambios y mejoras en las redes.
  - Uso de tecnologías nuevas.
  - Adopción de productos nuevos o versiones más modernas.
  - Desarrollo de herramientas y ambientes nuevos.
  - Cambios en la ubicación física de los medios del servicio.

3. Planificación y Aprobación de Sistemas.

3.1. Gestión de la Capacidad.

- La Jefatura de Sección de Servicios Tecnológicos, o el personal que éste designe, efectuará el monitoreo de las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas, a fin de garantizar un procesamiento y almacenamiento adecuados.
- Se tomará en cuenta, además, los nuevos requerimientos de los sistemas así como las tendencias actuales y proyectadas en el procesamiento de la información del CNCA para el periodo estipulado de vida útil de cada componente.
- Se informarán las necesidades detectadas a las autoridades competentes para que puedan identificar y evitar potenciales cuellos de botella, que podrían plantear una amenaza a la seguridad o a la continuidad del procesamiento y puedan planificar una adecuada acción correctiva.

3.2. Aceptación del Sistema.

- La Jefatura de Sección de Servicios Tecnológicos y el(a) Encargado(a) de Seguridad de la Información sugerirán criterios de aprobación para nuevos sistemas de información, actualizaciones y nuevas versiones, solicitando la realización de las pruebas necesarias antes de su aprobación definitiva.

4. Protección contra Software Malicioso.

4.1. Controles contra Software Malicioso.

- El(a) Encargado(a) de Seguridad de la Información definirá controles de detección y prevención para la protección contra software malicioso.
- La Jefatura de Sección de Servicios Tecnológicos, o el personal designado por éste, implementarán dichos controles.
- El(a) Encargado(a) de Seguridad de la Información desarrollará procedimientos adecuados de concientización de usuarios en materia de seguridad, controles de acceso al sistema y administración de cambios.

4.2. Controles contra Códigos Móviles.

- El(a) Encargado(a) de Seguridad de la Información definirá controles de detección y prevención para la protección contra códigos móviles.
- La Jefatura de Sección de Servicios Tecnológicos, o el personal designado por éste, implementarán dichos controles.
- El(a) Encargado(a) de Seguridad de la Información desarrollará procedimientos adecuados de concientización de usuarios en materia de seguridad, controles de acceso al sistema y administración de cambios.

5. Respaldos.

5.1. Back Up o Respaldos de Información.

- El(a) Encargado(a) de Seguridad de la Información definirá controles para la ejecución de tareas programadas para la generación de respaldos de la

información almacenada en software, la cual debe ser administrada y revisada constantemente.

6. Gestión de Seguridad de Redes.

6.1. Controles de Redes.

El(a) Encargado(a) de Seguridad de la Información definirá controles para garantizar la seguridad de los datos y los servicios conectados en las redes del CNCA contra el acceso no autorizado, considerando la ejecución de las siguientes acciones:

- Establecer los procedimientos para la administración del equipamiento remoto, incluyendo los equipos en las áreas usuarias, la que será llevada a cabo por el responsable establecido en el punto "Asignación de Responsabilidades en Materia de Seguridad de la Información".
- Establecer controles especiales para salvaguardar la confidencialidad e integridad del procesamiento de los datos que pasan a través de redes públicas y para proteger los sistemas conectados, implementar controles especiales para mantener la disponibilidad de los servicios de red y computadoras conectadas.
- Garantizar mediante actividades de supervisión, que los controles se aplican uniformemente en toda la infraestructura de procesamiento de información.
- La Jefatura de Sección de Servicios Tecnológicos deberá implementar dichos controles.

6.2. Seguridad de los Servicios de Red.

- El(a) Encargado(a) de Seguridad de la Información definirá controles para identificar los dispositivos de seguridad, niveles de servicio y requerimientos, e incluirlos en contratos de red estos sean internos o externos.

7. Gestión de Medios.

7.1. Gestión de los Medios Removibles.

La Jefatura de Sección de Servicios Tecnológicos, con la asistencia del(a) Encargado(a) de Seguridad de la Información, implementará procedimientos para la administración de medios informáticos removibles, como cintas, discos, casetes e informes impresos. Se deberán considerar las siguientes acciones para la implementación de los procedimientos:

- Eliminar de forma segura los contenidos, si ya no son requeridos, de cualquier medio reutilizable que ha de ser retirado o reutilizado por el CNCA.
- Requerir autorización para retirar cualquier medio del CNCA y realizar un control de todos los retiros a fin de mantener un registro de auditoria.
- Almacenar todos los medios en un ambiente seguro y protegido, de acuerdo con las especificaciones de los fabricantes o proveedores.

7.2. Eliminación de Medios.

- La Jefatura de Sección de Servicios Tecnológicos, junto con el(a) Encargado(a) de Seguridad de la Información, definirán los procedimientos para la eliminación segura de los medios de información respetando la normativa vigente.
- Los procedimientos deberán considerar que los siguientes elementos requerirán almacenamiento y eliminación segura.
- Se debe considerar que podría ser más eficiente disponer que todos los medios sean recolectados y eliminados de manera segura, antes que intentar separar el ítem sensible.

7.3. Procedimientos para el Manejo de la Información.

Se definirán procedimientos para el manejo y almacenamiento de la información de acuerdo a la clasificación establecida. En los procedimientos se contemplarán las siguientes acciones:

- Incluir en la protección a documentos, sistemas informáticos, redes, computación móvil, comunicaciones móviles, correo, correo de voz, comunicaciones de voz en general, multimedia, servicios e instalaciones postales, uso de máquinas de fax y cualquier otro ítem potencialmente sensible.
- Restringir el acceso solo al personal debidamente autorizado.
- Mantener un registro formal de los receptores autorizados de datos.
- Garantizar que los datos de entrada son completos, que el procesamiento se lleva a cabo correctamente y que se valida las salidas.
- Proteger los datos en espera ("colas").
- Conservar los medios de almacenamiento en un ambiente que concuerde con las especificaciones de los fabricantes o proveedores.

7.4. **Seguridad de la Documentación del Sistema**.

La documentación del sistema puede contener información sensible, por lo que se considerarán los siguientes recaudos para su protección:

- Almacenar la documentación del sistema en forma segura.
- Restringir el acceso a la documentación del sistema al personal estrictamente necesario.
- Dicho acceso será autorizado por el(a) Propietario(a) de la Información relativa al sistema.

8. Intercambios de Información.

8.1. **Políticas y Procedimientos de Intercambio de Información**.

- El(a) Encargado(a) de Seguridad de la Información deberá definir políticas y procedimientos que contemplen controles para mitigar el riesgo del intercambio formal de información mediante distintos medios de comunicación.

8.2. **Acuerdos de Intercambio**.

Cuando se realicen acuerdos entre organizaciones para el intercambio de información y software, se especificarán el grado de sensibilidad de la información del CNCA involucrada y las consideraciones de seguridad sobre la misma. Se tendrán en cuenta los siguientes aspectos:

- Responsabilidades gerenciales por el control y la notificación de transmisiones, envíos y recepciones.
- Procedimientos de notificación de emisión, transmisión, envío y recepción.
- Normas técnicas para el empaquetado y la transmisión.
- Pautas para la identificación del prestador del servicio de correo.
- Responsabilidades y obligaciones en caso de pérdida de datos.
- Uso de un sistema convenido para el rotulado de información clasificada, garantizando que el significado de los rótulos sea inmediatamente comprendido y que la información sea adecuadamente protegida.
- Términos y condiciones de la licencia bajo la cual se suministra el software.
- Información sobre la propiedad de la información suministrada y las condiciones de su uso.
- Normas técnicas para la grabación y lectura de la información y del software.
- Controles especiales que puedan requerirse para proteger ítems sensibles (claves criptográficas, etc.).

8.3. **Medios Físicos en Tránsito**.

Los procedimientos de transporte de medios informáticos entre diferentes puntos (envíos postales y mensajería) deberán contemplar:

- La utilización de medios de transporte o servicios de mensajería confiables. El(a) Propietario(a) de la Información a transportar determinará qué servicio de mensajería se utilizará conforme la criticidad de la información a transmitir.
- Suficiente embalaje para envío de medios a través de servicios postales o de mensajería, siguiendo las especificaciones de los fabricantes o proveedores.

- La adopción de controles especiales, cuando resulte necesario, a fin de proteger la información sensible contra divulgación o modificación no autorizadas. Entre los ejemplos se incluyen:
  - Uso de recipientes cerrados.
  - Entrega en mano.
  - Embalaje a prueba de apertura no autorizada (que revele cualquier intento de acceso).
  - En casos excepcionales, división de la mercadería a enviar en más de una entrega y envío por diferentes rutas.

8.4. Mensajes Electrónicos.

8.4.1. Riesgos de Seguridad.

Se implementarán controles para reducir los riesgos de incidentes de seguridad en el correo electrónico, contemplando:

- La vulnerabilidad de los mensajes al acceso o modificación no autorizados o a la negación de servicio.
- La posible intercepción y el consecuente acceso a los mensajes en los medios de transferencia que intervienen en la distribución de los mismos.
- Las posibles vulnerabilidades a errores, por ejemplo, consignación incorrecta de la dirección o dirección errónea, y la confiabilidad y disponibilidad general del servicio.
- La posible recepción de código malicioso en un mensaje de correo, el cual afecte la seguridad de la terminal receptora o de la red a la que se encuentra conectada.
- El impacto de un cambio en el medio de comunicación en los procesos del CNCA.
- Las consideraciones legales, como la necesidad potencial de contar con prueba de origen, envío, entrega y aceptación.
- Las implicancias de la publicación externa de listados de personal, accesibles al público.
- El acceso de usuarios remotos a las cuentas de correo electrónico.
- El uso inadecuado por parte del personal.

8.4.2. Política de Correo Electrónico.

El(a) Encargado(a) de Seguridad de la Información junto con la Jefatura de Sección de Servicios Tecnológicos definirán y documentarán normas y procedimientos claros ajustándose, además, a la normativa vigente con respecto al uso del correo electrónico, que incluya al menos los siguientes aspectos:

- Protección contra ataques al correo electrónico, por ejemplo, virus, intercepción, etc.
- Protección de archivos adjuntos de correo electrónico.
- Uso de técnicas criptográficas para proteger la confidencialidad e integridad de los mensajes electrónicos.
- Retención de mensajes que, si se almacenaran, pudieran ser usados en caso de litigio.
- Controles adicionales para examinar mensajes electrónicos que no pueden ser autenticados.
- Aspectos operativos para garantizar el correcto funcionamiento del servicio (ej.: tamaño máximo de información transmitida y recibida, cantidad de destinatarios, tamaño máximo del buzón del usuario, etc.).
- Definición de los alcances del uso del correo electrónico por parte del personal de la Institución.
- Potestad del CNCA para auditar los mensajes recibidos o emitidos por los servidores del CNCA, lo cual se incluirá en el "Compromiso de Confidencialidad".

Estos dos últimos puntos deben ser leídos a la luz de las normas vigentes que no sólo prohíben a los empleados a hacer uso indebido o con fines particulares del patrimonio estatal, sino que, también, imponen la obligación

de usar los bienes y recursos del Estado con los fines autorizados y de manera racional, evitando su abuso, derroche o desaprovechamiento.

Entender al correo electrónico como una herramienta más de trabajo provista al funcionario(a) a fin de ser utilizada conforme el uso al cual está destinada, faculta al empleador a implementar sistemas de controles destinados a velar por la protección y el buen uso de sus recursos.

Esta facultad, y de acuerdo a la normativa vigente, sin embargo, deberá ejercerse salvaguardando la dignidad del trabajador(a) y su derecho a la intimidad. Por tal motivo, el CNCA debe informar claramente a los funcionarios(as).

8.5. **Sistemas de Información**.
Se monitorearán los mecanismos de distribución y difusión tales como documentos, computadoras, computación móvil, comunicaciones móviles, correo, correo de voz, comunicaciones de voz en general, multimedia, servicios o instalaciones postales, equipos de fax, etc.

Al interconectar dichos medios, se considerarán las implicancias en lo que respecta a la seguridad y a las actividades propias del CNCA, incluyendo:

- Vulnerabilidades de la información en los sistemas de oficina, por ejemplo, la grabación de llamadas telefónicas o teleconferencias.
- Procedimientos y controles apropiados para administrar la distribución de información, por ejemplo el uso de boletines electrónicos institucionales.
- Exclusión de categorías de información sensible del CNCA si el sistema no brinda un adecuado nivel de protección.
- Limitación del acceso a la información de las actividades que desarrollan determinadas personas, por ejemplo, aquellas que trabajan en proyectos sensibles.
- La aptitud del sistema para dar soporte a las aplicaciones del CNCA, como la comunicación de órdenes o autorizaciones.
- Categorías de personal, contratistas y/o terceros a los que se permite el uso del sistema y las ubicaciones desde las cuales se puede acceder al mismo.
- Restricción de acceso a determinadas instalaciones a específicas categorías de usuarios(as).
- Identificación de la posición o categoría de los usuarios(as), por ejemplo, funcionarios(as) de la Institución, contratistas y/o terceros, en directorios accesibles por otros usuarios(as).
- Retención y resguardo de la información almacenada en el sistema.
- Requerimientos y disposiciones relativos a sistemas de soporte de reposición de información previa.

POLÍTICA DE SEGURIDAD
CONTROL DE ACCESO
CONSEJO NACIONAL DE LA CULTURA Y LAS ARTES

AÑO 2011

CONTROL E HISTORIAL DE VERSIONES

N° Versión	Fecha	Descripción de las Modificaciones	Páginas Modificadas	Autor
1.0	15-07-2011	Elaboración de versión inicial	Todas	JGMV
1.1	15-11-	Correcciones de contenido, estilo, lenguaje,	Todas	RAM

	2011	ordenamiento y presentación de temas		

DECLARACIÓN CORPORATIVA

El acceso por medio de un sistema de restricciones y excepciones a la información es la base de todo sistema de seguridad de la información. Para impedir el acceso no autorizado a los sistemas de información se deben implementar procedimientos formales para controlar la asignación de derechos de acceso a los sistemas de información, bases de datos y servicios de información y estos deben estar claramente documentados, comunicados y controlados en cuanto a su cumplimiento. Los procedimientos comprenden todas las etapas del ciclo de vida de los accesos de los usuarios de todos los niveles, desde el registro inicial de nuevos usuarios hasta la privación final de derechos de los usuarios que ya no requieren el acceso. La cooperación de los usuarios es esencial para la eficacia de la seguridad, por lo tanto es necesario concientizar a los mismos acerca de sus responsabilidades por el mantenimiento de controles de acceso eficaces, en particular aquellos relacionados con el uso de contraseñas y la seguridad del equipamiento.

ÁMBITO

- Esta Política se aplica a todas las formas de acceso de aquellos a quienes se les ha otorgado permisos sobre los sistemas de información, bases de datos o servicios de información del CNCA, cualquiera sea la función que desempeñen. Asimismo se aplica al personal técnico que define, instala, administra y mantiene los permisos de acceso, a las conexiones de red y a los que administran su seguridad.

ROLES Y RESPONSABILIDADES

- **Encargado(a) de Seguridad de la Información**
  - Definir junto con la Jefatura de Sección de Servicios Tecnológicos las normas y procedimientos para la gestión de accesos a todos los sistemas, bases de datos y servicios de información multiusuario.
  - Controlar la administración de las cuentas de usuarios y accesos a internet, y todos los controles asociados con el acceso a la información del CNCA.
  - Controlar la implementación y ejecución de esta política.

- **Jefatura Sección de Servicios Tecnológicos**
  - Definir junto con el(a) Encargado(a) de Seguridad de la Información las normas y procedimientos para la gestión de accesos a todos los sistemas, bases de datos y servicios de información multiusuario.
  - Controlar la administración de las cuentas de usuarios y accesos a internet, y todos los controles asociados con el acceso a la información del CNCA.
  - Monitorear el uso de las instalaciones de procesamiento de la información, la solicitud y aprobación de accesos a Internet, el uso de computación móvil, trabajo remoto y reportes de incidentes relacionados, la respuesta a la activación de alarmas silenciosas y la revisión de registros de actividades.
  - Controlar la implementación y ejecución de esta política.

REGLAS DE LA POLÍTICA

1. Requerimientos para el Control de Acceso.

1.1. **Política de Control de Acceso**.

En la aplicación de controles de acceso, se contemplarán los siguientes aspectos:

- Identificar los requerimientos de seguridad de cada una de las aplicaciones.
- Identificar toda la información relacionada con las aplicaciones.
- Establecer criterios coherentes entre esta Política de Control de Acceso y la Política de Clasificación de Información de los diferentes sistemas y redes.

- Identificar la legislación aplicable y las obligaciones contractuales con respecto a la protección del acceso a datos y servicios.
- Definir los perfiles de acceso de usuarios estándar, comunes a cada categoria de puestos de trabajo.
- Administrar los derechos de acceso en un ambiente distribuido y de red, que reconozcan todos los tipos de conexiones disponibles.

1.2. **Reglas de Control de Acceso**.

Las reglas de control de acceso especificadas, deberán:

- Indicar expresamente si las reglas son obligatorias u optativas
- Establecer reglas sobre la premisa "Todo debe estar prohibido a menos que se permita expresamente" y no sobre la premisa inversa de "Todo está permitido a menos que se prohiba expresamente".
- Controlar los cambios en los rótulos de información que son iniciados automáticamente por herramientas de procesamiento de información, de aquellos que son iniciados a discreción del usuario(a).
- Controlar los cambios en los permisos de usuario(a) que son iniciados automáticamente por el sistema de información y aquellos que son iniciados por el administrador(a).
- Controlar las reglas que requieren la aprobación del(a) administrador(a) o del Propietario(a) de la Información de que se trate, antes de entrar en vigencia, y aquellas que no requieren aprobación.

2. <u>Administración de Accesos de Usuarios(as).</u>

Con el objetivo de impedir el acceso no autorizado a la información se implementarán procedimientos formales para controlar la asignación de derechos de acceso a los sistemas, datos y servicios de información.

2.1. **Registro del Usuario(a)**.

- El(a) Encargado(a) de Seguridad de la Información definirá un procedimiento formal de registro de usuarios(as) para otorgar y revocar el acceso a todos los sistemas, bases de datos y servicios de información multiusuario(a).

2.2. **Gestión de Privilegios**.

- Se limitará y controlará la asignación y uso de privilegios, debido a que el uso inadecuado de los privilegios del sistema resulta frecuentemente en el factor más importante que contribuye a la falla de los sistemas a los que se ha accedido ilegalmente.
- Los sistemas multiusuario que requieren protección contra accesos no autorizados, deben prever una asignación de privilegios controlada mediante un proceso de autorización formal.
- Los(as) Propietarios(a) de Información serán los encargados de aprobar la asignación de privilegios a usuarios(as) y solicitar su implementación, lo cual será supervisado por el(a) Encargado(a) de Seguridad de la Información.

2.3. **Gestión de Contraseñas de los Usuarios(as)**.

La asignación de contraseñas se controlará a través de un proceso de administración formal, mediante el cual deben respetarse los siguientes pasos:

- Requerir que los usuarios(as) firmen una declaración por la cual se comprometen a mantener sus contraseñas personales en secreto y las contraseñas de los grupos de trabajo exclusivas entre los miembros del grupo.
- Garantizar que los usuarios(as) cambien las contraseñas iniciales que les han sido asignadas la primera vez que ingresan al sistema.
- Generar contraseñas provisorias seguras para otorgar a los usuarios(as).
- Almacenar las contraseñas sólo en sistemas informáticos protegidos.
- Utilizar otras tecnologías de autenticación y autorización de usuarios(as).
- Configurar los sistemas de tal manera que las contraseñas cumplan algunos parámetros de seguridad mínimos (duración, Longitud, Complejidad)

2.4. **Gestión de Contraseñas Críticas**.

- En los diferentes ambientes de procesamiento existen cuentas de usuarios(as) con las cuales es posible efectuar actividades críticas, como ser instalación de plataformas o sistemas, habilitación de servicios, actualización de software, configuración de componentes informáticos, etc. Dichas cuentas no serán de uso habitual (diario), sino que sólo serán utilizadas ante una necesidad específica de realizar alguna tarea que lo requiera y se encontrarán protegidas por contraseñas con un mayor nivel de complejidad que el habitual. El(a) Encargado(a) de Seguridad de la Información definirá procedimientos para la administración de dichas contraseñas.

2.5. **Revisión de los Derechos de Acceso del Usuario(a)**.

A fin de mantener un control eficaz del acceso a los datos y servicios de información, el Propietario(a) de la Información de que se trate llevará a cabo un proceso formal, a intervalos regulares definidos por el Encargado(a) de Seguridad de la Información, a fin de revisar los derechos de acceso de los usuarios(as). Se deberán contemplar los siguientes controles:

- Revisar los derechos de acceso de los usuarios(as) a intervalos definidos por el(a) Encargado(a) de Seguridad de la Información.
- Revisar las autorizaciones de privilegios especiales de derechos de acceso a intervalos definidos por el(a) Encargado(a) de Seguridad de la Información.
- Revisar las asignaciones de privilegios a intervalos definidos por el(a) Encargado(a) de Seguridad de la Información.

3. Responsabilidades del Usuario(a).

3.1. **Uso de Contraseñas**.

- Los usuarios(as) deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas.
- Las contraseñas constituyen un medio de validación y autenticación de la identidad de un usuario(a), y consecuentemente un medio para establecer derechos de acceso a las instalaciones o servicios de procesamiento de información.

3.2. **Equipo del Usuario(a) Desatendido**.

- Los usuarios(as) deberán garantizar que los equipos desatendidos sean protegidos adecuadamente.
- Los equipos instalados en áreas de usuarios(as), por ejemplo estaciones de trabajo o servidores de archivos, requieren una protección específica contra accesos no autorizados cuando se encuentran desatendidos.
- El(a) Encargado(a) de Seguridad de la Información debe coordinar con la Jefatura de Departamento de Recursos Humanos las tareas de concientización a todos los usuarios(as) y terceros, acerca de los requerimientos y procedimientos de seguridad, para la protección de equipos desatendidos, así como de sus funciones en relación a la implementación de dicha protección.

4. Control de Acceso a la Red.

4.1. **Política sobre Uso de los Servicios de Red**.

- Las conexiones no seguras a los servicios de red pueden afectar a todo CNCA, por lo tanto, se controlará el acceso a los servicios de red tanto internos como externos. Esto es necesario para garantizar que los usuarios(as) que tengan acceso a las redes y a sus servicios, no comprometan la seguridad de los mismos.
- La Jefatura de Sección de Servicios Tecnológicos tendrá a cargo el otorgamiento del acceso a los servicios y recursos de red, únicamente de acuerdo al pedido formal del titular de un departamento, sección o unidad que lo solicite para personal de su incumbencia. Este control es particularmente importante para las conexiones de red a aplicaciones que procesen información reservada o aplicaciones críticas, o a usuarios(as) que

utilicen el acceso desde sitios de alto riesgo, por ejemplo áreas públicas o externas que están fuera de la administración y del control de seguridad CNCA.

- Se desarrollarán procedimientos para la activación y desactivación de derechos de acceso a las redes.
- Se limitarán las opciones de elección de la ruta entre la terminal del usuario(a) y los servicios a los cuales el mismo se encuentra autorizado a acceder, mediante la implementación de controles en diferentes puntos de la misma.

4.2. **Autenticación del Usuario(a) para Conexiones Externas**.

- Las conexiones externas son de gran potencial para accesos no autorizados a la información del CNCA. Por consiguiente, el acceso de usuarios(as) remotos estará sujeto al cumplimiento de procedimientos de autenticación.
- Existen diferentes métodos de autenticación, algunos de los cuales brindan un mayor nivel de protección que otros. El(a) Encargado(a) de Seguridad de la Información, conjuntamente con el(a) Propietario(a) de la Información de que se trate, realizará una evaluación de riesgos a fin de determinar el mecanismo de autenticación que corresponda en cada caso.

4.3. **Identificación del Equipo en las Redes**.

- Una herramienta de conexión automática a una computadora remota podría brindar un medio para obtener acceso no autorizado a una aplicación del CNCA. Por consiguiente, las conexiones a sistemas informáticos remotos serán autenticadas. Esto es particularmente importante si la conexión utiliza una red que está fuera de control de la gestión de seguridad del CNCA. La autenticación de nodos puede servir como un medio alternativo de autenticación de grupos de usuarios(as) remotos, cuando éstos están conectados a un servicio informático seguro y compartido.

4.4. **Protección del Puerto de Diagnóstico y Configuración Remoto**.

- Muchas computadoras y sistemas de comunicación son instalados y administrados con una herramienta de diagnóstico remoto. Si no están protegidos, estos puertos de diagnóstico proporcionan un medio de acceso no autorizado. Por consiguiente, serán protegidos por un mecanismo de seguridad apropiado, con las mismas características del punto "Autenticación del Usuarios(as) para Conexiones Externas". También para este caso deberá tenerse en cuenta el punto "Identificación del Equipo en las Redes".

4.5. **Segregación en Redes**.

- Para controlar la seguridad en redes extensas, se podrán dividir en dominios lógicos separados. Para esto se definirán y documentarán los perímetros de seguridad que sean convenientes.
- Los perímetros se implementarán mediante la instalación de "gateways" con funcionalidades de "firewall" o redes privadas virtuales, para filtrar el tráfico entre los dominios.

4.6. **Control de Conexión a la Red**.

- El acceso a Internet será utilizado con propósitos autorizados o con el destino por el cual fue provisto.
- El(a) Encargado(a) de Seguridad de la Información definirá procedimientos para solicitar y aprobar accesos a Internet. Los accesos serán autorizados formalmente por la Jefatura de Departamento a cargo del personal que lo solicite. Asimismo, se definirán las pautas de utilización de Internet para todos los usuarios(a).
- Se evaluará la conveniencia de generar un registro de los accesos de los usuarios(as) a Internet, con el objeto de realizar revisiones de los accesos efectuados o analizar casos particulares.
- El control será comunicado a los usuarios(as) de acuerdo a lo establecido en el punto "Responsabilidades del Usuario". Para ello, el(a) Encargado(a) de Seguridad de la Información junto con la Jefatura de Sección de Servicios

Tecnológicos analizarán las medidas a ser implementadas para efectivizar dicho control, como ser la instalación de "firewalls", "proxies", etc.

- Sobre la base de lo definido en los requerimientos y procedimientos de seguridad, se implementarán controles para limitar la capacidad de conexión de los usuarios(as). Dichos controles se podrán implementar en los "gateways" que separen los diferentes dominios de la red.
- Algunos ejemplos de los entornos a las que deben implementarse restricciones son: correo electrónico, transferencia de archivos, acceso interactivo y acceso a la red fuera del horario laboral.

4.7. **Control de Routing de la Red**.

- En las redes compartidas, especialmente aquellas que se extienden fuera de los límites del Servicio, se incorporarán controles de ruteo, para asegurar que las conexiones informáticas y los flujos de información no violen la Política de Control de Accesos.
- Los controles contemplarán mínimamente la verificación positiva de direcciones de origen y destino. Adicionalmente, para este objetivo pueden utilizarse diversos métodos incluyendo, entre otros, la autenticación de protocolos de ruteo, ruteo estático, traducción de direcciones y listas de control de acceso.
- El(a) Encargado(a) de Seguridad de la Información junto con la Jefatura de Sección de Servicios Tecnológicos definirán las pautas para garantizar la seguridad de los servicios de red del CNCA, tanto públicos como privados.

5. Control de Acceso al Sistema Operativo.

5.1. **Procedimiento para un Registro Seguro**.

- El(a) Encargado(a) de Seguridad de la Información junto con la Jefatura de Sección de Servicios Tecnológicos realizarán una evaluación de riesgos a fin de determinar el método de protección adecuado para el acceso al sistema operativo.
- El acceso a los servicios de información sólo será posible a través de un proceso de conexión seguro. El procedimiento de conexión en un sistema informático será diseñado para minimizar la oportunidad de acceso no autorizado. Este procedimiento, por lo tanto, debe divulgar la mínima información posible acerca del sistema, a fin de evitar proveer de asistencia innecesaria a un usuario(a) no autorizado.

5.2. **Identificación y Autenticación del Usuario(a)**.

- Todos los funcionarios(as) del CNCA tendrán un identificador único (ID de usuario(a)) solamente para su uso personal exclusivo, de manera que las actividades puedan rastrearse con posterioridad hasta llegar al individuo responsable.
- Los identificadores de usuario(a) no darán ningún indicio del nivel de privilegio otorgado.
- En circunstancias excepcionales, cuando existe un claro beneficio para el CNCA, podrá utilizarse un identificador compartido para un grupo de usuarios(as) o una tarea específica. Para casos de esta índole, se documentará la justificación y aprobación del Propietario(a) de la Información de que se trate.

5.3. **Sistema de Gestión de Contraseñas**.

- Las contraseñas constituyen uno de los principales medios de validación de la autoridad de un usuario(a) para acceder a un servicio informático. Los sistemas de administración de contraseñas deben constituir una herramienta eficaz e interactiva que garantice contraseñas de calidad.

5.4. **Uso de las Utilidades del sistema**.

- La mayoría de las instalaciones informáticas tienen uno o más programas utilitarios que podrían tener la capacidad de pasar por alto los controles de

sistemas y aplicaciones. Es esencial que su uso sea limitado y minuciosamente controlado.

- Se considerará la provisión de alarmas silenciosas para los usuarios(as) que podrían ser objetos de coerción. La decisión de suministrar una alarma de esta índole se basará en una evaluación de riesgos que realizará el(a) Encargado(a) de Seguridad de la Información junto con la Jefatura de Sección de Servicios Tecnológicos. En este caso, se definirán y asignarán funciones y procedimientos para responder a la utilización de una alarma silenciosa.

5.5. **Cierre de una Sesión por Inactividad (Tiempo Muerto).**

- El(a) Encargado(a) de Seguridad de la Información, junto con Los(as) Propietarios(as) de la Información de que se trate, definirán cuáles se consideran terminales de alto riesgo, por ejemplo, áreas públicas o externas fuera del alcance de la gestión de seguridad del CNCA, o que sirven a sistemas de alto riesgo.
- Las mismas se apagarán después de un periodo definido de inactividad o tiempo muerto, para evitar el acceso de personas no autorizadas. Esta herramienta de desconexión por tiempo muerto deberá limpiar la pantalla de la terminal y deberá cerrar tanto la sesión de la aplicación como la de red.
- El lapso por tiempo muerto responderá a los riesgos de seguridad del área y de la información que maneje la terminal.

5.6. **Limitación del Tiempo de Conexión.**

- Las restricciones al horario de conexión deben suministrar seguridad adicional a las aplicaciones de alto riesgo.
- La limitación del periodo durante el cual se permiten las conexiones de terminales a los servicios informáticos reduce el espectro de oportunidades para el acceso no autorizado.
- Se implementará un control de esta índole para aplicaciones informáticas sensibles, especialmente aquellas terminales instaladas en ubicaciones de alto riesgo, por ejemplo, áreas públicas o externas que estén fuera del alcance de la gestión de seguridad del Servicio.

6. Control de Acceso a las Aplicaciones.

6.1. **Restricción del Acceso a la Información.**

Los usuarios(as) de sistemas de aplicación, con inclusión del personal de soporte, tendrán acceso a la información y a las funciones de los sistemas de aplicación de conformidad con la Política de Control de Acceso definida, sobre la base de los requerimientos de cada aplicación, y conforme a la política del CNCA para el acceso a la información. Se aplicarán los siguientes controles, para brindar apoyo a los requerimientos de limitación de accesos:

- Proveer una interfaz para controlar el acceso a las funciones de los sistemas de aplicación.
- Restringir el conocimiento de los usuarios(as) acerca de la información o de las funciones de los sistemas de aplicación a las cuales no sean autorizados a acceder, con la adecuada edición de la documentación de usuario(a).
- Controlar los derechos de acceso de los usuarios(as), por ejemplo, lectura, escritura, supresión y ejecución.
- Garantizar que las salidas de los sistemas de aplicación que administran información sensible, contengan sólo la información que resulte pertinente para el uso de la salida, y que la misma se envíe solamente a las terminales y ubicaciones autorizadas.
- Revisar periódicamente dichas salidas a fin de garantizar la remoción de la información redundante.
- Restringir el acceso a la información por fuera del sistema encargado de su procesamiento, es decir, la modificación directa del dato almacenado.

6.2. **Aislar el Sistema Confidencial.**

- Los sistemas sensibles podrían requerir de un ambiente informático dedicado (aislado).

- Algunos sistemas de aplicación son suficientemente sensibles a pérdidas potenciales y requieren un tratamiento especial. La sensibilidad puede señalar que el sistema de aplicación debe ejecutarse en una computadora dedicada, que sólo debe compartir recursos con los sistemas de aplicación confiables, o no tener limitaciones.

7. Monitoreo del Acceso y Uso de los Sistemas.

7.1. Registro de Eventos.

- Se generarán registros de auditoría que contengan excepciones y otros eventos relativos a la seguridad, estos registros deberán contener el máximo de información de los eventos, incidentes o excepciones ocurridas.
- En todos los casos, los registros de auditoría serán archivados preferentemente en un equipo diferente al que los genere y conforme los requerimientos de la Política de Retención de Registros.
- Los(as) Propietarios(as) de la Información junto con la Unidad de Auditoría Interna o en su defecto quien sea propuesto por el Comité de Seguridad de la Información, definirán un cronograma de depuración de registros en línea en función a normas vigentes y a sus propias necesidades.

7.2. Monitoreo del Uso de los Sistemas.

7.2.1. Procedimientos y Áreas de Riesgo.

- Se desarrollarán procedimientos para monitorear el uso de las instalaciones de procesamiento de la información, a fin de garantizar que los usuarios(as) sólo estén desempeñando actividades que hayan sido autorizadas explícitamente.
- Todos los funcionarios(as) deben conocer el alcance preciso del uso adecuado de los recursos informáticos, y se les advertirá que determinadas actividades pueden ser objeto de control y monitoreo.
- El alcance de estos procedimientos deberá corresponderse a la evaluación de riesgos que realice el(a) Encargado(a) de Seguridad de la Información junto con la Jefatura de Sección de Servicios Tecnológicos.

7.2.2. Factores de Riesgo.

- Entre los factores de riesgo que se deben considerar se encuentran:
  - La criticidad de los procesos de aplicaciones.
  - El valor, la sensibilidad o criticidad de la información involucrada.
  - La experiencia acumulada en materia de infiltración y uso inadecuado del sistema.
  - El alcance de la interconexión del sistema (en particular las redes públicas). Los(as) Propietarios(as) de la Información manifestarán la necesidad de registrar aquellos eventos que consideren críticos para la operatoria que se encuentra bajo su responsabilidad

7.2.3. Registro y Revisión de Eventos.

- Se implementará un procedimiento de registro y revisión de los registros de auditoría, orientado a producir un informe de las amenazas detectadas contra los sistemas y los métodos utilizados.
- La periodicidad de dichas revisiones será definida por los(as) Propietarios(as) de la Información y el(a) Encargado(a) de Seguridad de la Información, de acuerdo a la evaluación de riesgos efectuada.
- Si el volumen de la información contenida en alguno de los registros fuera muy grande, el procedimiento indicará cuales de los registros más significativos se copiarán automáticamente en registros auxiliares.
- Por otra parte, la Jefatura de Sección de Servicios Tecnológicos, podrá disponer la utilización de herramientas de auditoría o utilitarios adecuados para llevar a cabo el control de los registros.
- En la asignación de funciones en materia de seguridad de la información, se deberá separar las funciones entre quienes realizan la revisión y aquellos cuyas actividades están siendo monitoreadas.

- La Unidad de Auditoría Interna o en su defecto quien sea propuesto por el Comité de Seguridad de la Información, tendrá acceso a los registros de eventos a fin de colaborar en el control y efectuar recomendaciones sobre modificaciones a los aspectos de seguridad.
- Adicionalmente podrían evaluar las herramientas de registro, pero no tendrán libre acceso a ellas.

8. Computación Móvil y Trabajo Remoto.

8.1. Computación y Comunicaciones Móviles.

- Cuando se utilizan dispositivos informáticos móviles se debe tener especial cuidado en garantizar que no se comprometa la información del CNCA.
- Se deberá tener en cuenta, en este sentido, cualquier dispositivo móvil y/o removible, incluyendo: notebooks, laptop o PDA (Asistente Personal Digital), teléfonos celulares y sus tarjetas de memoria, dispositivos de almacenamiento removibles, tales como CDs, DVDs, disquetes, tapes, y cualquier dispositivo de almacenamiento de conexión USB, tarjetas de identificación personal (control de acceso), dispositivos criptográficos, cámaras digitales, etc.
- Esta lista no es taxativa, ya que deberán incluirse todos los dispositivos que pudieran contener información confidencial del CNCA y, por lo tanto, ser posibles de sufrir un incidente en el que se comprometa la seguridad del mismo.
- Se deberá desarrollar procedimientos que definan adecuados controles para la administración de éstos.

8.2. Trabajo Remoto.

- El trabajo remoto utiliza tecnología de comunicaciones para permitir que el personal trabaje en forma remota desde un lugar externo al Servicio.
- El trabajo remoto sólo será autorizado por el Jefe de Departamento respectivo, o superior jerárquico correspondiente, a la cual pertenezca el usuario(a) solicitante, conjuntamente con el(a) Encargado(a) de Seguridad de la Información, cuando se verifique que son adoptadas todas las medidas que correspondan en materia de seguridad de la información, de modo de cumplir con la política, normas y procedimientos existentes.
- Estos casos serán de excepción y serán contemplados en situaciones que justifiquen la imposibilidad de otra forma de acceso y la urgencia, tales como horarios del CNCA, solicitud de las autoridades, etc.
- Se deberá se establecerán normas y procedimientos para el trabajo remoto.

POLÍTICA DE SEGURIDAD
ADQUISICIÓN, DESARROLLO Y MANTENCIÓN DE LOS SISTEMAS DE INFORMACIÓN

CONSEJO NACIONAL DE LA CULTURA Y LAS ARTES

AÑO 2011

CONTROL E HISTORIAL DE VERSIONES

N° Versión	Fecha	Descripción de las Modificaciones	Páginas Modificadas	Autor
1.0	15-07-2011	Elaboración de versión inicial	Todas	JGMV
1.1	15-11-2011	Correcciones de contenido, estilo, lenguaje, ordenamiento y presentación de temas	Todas	RAM

DECLARACIÓN CORPORATIVA

Durante el análisis y diseño de los procesos que soportan estas aplicaciones se deben identificar, documentar y aprobar los requerimientos de seguridad a incorporar durante las etapas de desarrollo e implementación. Adicionalmente, se deberán diseñar controles de validación de datos de entrada, procesamiento interno y salida de datos. Dado que los(as) analistas y programadores(as) tienen el conocimiento total de la lógica de los procesos en los sistemas, se deben implementar controles que eviten maniobras dolosas por parte de estas personas u otras que puedan operar sobre los sistemas, bases de datos y plataformas de software de base y en el caso de que se lleven a cabo, identificar rápidamente al responsable. Asimismo, es necesaria una adecuada administración de la infraestructura de base, sistemas operativos y software de base, en las distintas plataformas, para asegurar una correcta implementación de la seguridad, ya que en general los aplicativos se asientan sobre este tipo de software.

ÁMBITO

- Esta Política se aplica a todos los sistemas informáticos, tanto desarrollos propios o de terceros, y a todos los sistemas operativos y/o software de base que integren cualquiera de los ambientes administrados por el CNCA en donde residan los desarrollos mencionados.

ROLES Y RESPONSABILIDADES

- **Encargado(a) de Seguridad de la Información**
  - Definir los controles a ser implementados en los sistemas desarrollados internamente o por terceros, en función de una evaluación previa de riesgos.
  - Definir en función a la criticidad de la información, los requerimientos de protección mediante métodos criptográficos.

- **Jefatura Sección de Servicios Tecnológicos**
  - Proponer para su aprobación por parte del superior jerárquico que corresponda, la asignación de funciones de "implementador" y "administrador de programas fuentes" al personal de su área que considere adecuado, cuyas responsabilidades se detallan en el presente capítulo.
  - Verificar el cumplimiento de las definiciones establecidas sobre los controles y las medidas de seguridad a ser incorporadas a los sistemas.
  - Proponer quiénes realizarán la administración de las técnicas criptográficas y claves.

- **Jefatura Departamento Jurídico**
  - En conjunto con el(a) Encargado(a) de Seguridad de la Información y la Jefatura de Sección de Servicios Tecnológicos, la Jefatura del Departamento de Jurídico incorporará aspectos relacionados con el licenciamiento, la calidad del software y la seguridad de la información en los contratos con terceros por el desarrollo de software.

REGLAS DE LA POLÍTICA

1. Requerimiento de Seguridad de los Sistemas.

Los sistemas de información del CNCA, que incluyen la infraestructura, aplicaciones de negocio y aplicaciones desarrolladas por los usuarios deben tener incorporados los controles de seguridad correspondientes.

Se deben identificar y acordar los requerimientos de seguridad que deben contener los sistemas de información de la organización antes de su desarrollo e implementación.

Los requerimientos de seguridad para el desarrollo de los sistemas de información deben quedar documentados como parte del proceso de negocio del proyecto de implementación de sistemas de información.

1.1. **Análisis y Especificaciones de los Requerimientos de Seguridad**.

- Los requerimientos y los controles de seguridad deben reflejar el valor comercial de los activos de información involucrados y el daño comercial potencial que podría resultar de una falla o ausencia de seguridad.
- Los requerimientos de seguridad para la seguridad de la información y los procesos para implementar la seguridad deben ser integrados en las primeras etapas de los proyectos de sistemas de información.
- Los controles introducidos en la etapa de diseño deben ser significativamente más baratos de implementar y mantener que aquellos incluidos durante o después de la implementación.
- Si los productos son comprados, se debe realizar un proceso de prueba y adquisición formal.
- Los contratos con el proveedor deben tratar los requerimientos de seguridad identificados.
- Cuando la funcionalidad de seguridad de un producto propuesto no satisface el requerimiento especificado entonces se debe reconsiderar el riesgo introducido y los controles asociados antes de comprar el producto.
- Donde se suministra funcionalidad adicional y causa un riesgo de seguridad, este debe ser desactivado o se debe revisar la estructura de control propuesta para determinar si se puede obtener alguna ventaja de la funcionalidad mejorada disponible.

2. Procesamiento Correcto en las Aplicaciones.

Para las aplicaciones y sistemas de información se deben diseñar e implementar medidas de control de seguridad y registros de auditoría o de actividades correspondientes a cada aplicación. En el diseño de los controles se deben incluir las validaciones de los datos de entrada, procesamiento interno y datos de salida que maneja la aplicación.

Se pueden requerir controles adicionales para los sistemas que procesan o tienen impacto sobre la información reservada, valiosa o crítica. Estos controles se deben determinar sobre la base de los requerimientos de seguridad y la evaluación del riesgo.

2.1. **Validación de la Data de Entrada**.

- Se definirá un procedimiento que durante la etapa de diseño, especifique controles que aseguren la validez de los datos ingresados, tan cerca del punto de origen como sea posible, controlando también datos permanentes y tablas de parámetros.

2.2. **Control de Procesamiento Interno**.

- Se definirá un procedimiento para que durante la etapa de diseño, se incorporen controles de validación a fin de eliminar o minimizar los riesgos de fallas de procesamiento y/o vicios por procesos de errores.

2.3. **Integridad del Mensaje**.

- Cuando se envíe un mensaje de una persona a otra, o bien, de una máquina a otra, este mensaje no deberá ser modificado, sin que el destinatario pueda comprobarlo. La modificación se refiere tanto a una modificación explícita por alguien como a una modificación debido a un error.

2.4. **Validación de la Data de Salida**.

- Para el procesamiento de datos se debe validar la salida de los datos de una aplicación para asegurar que la integridad y el procesamiento de la información almacenada sea el correcto y apropiado para las circunstancias.

3. Controles Criptográficos.

Toda la información reservada, sensible o en riego de la Organización debe estar protegida por sistemas y técnicas criptográficas en caso de que otras medidas y controles no le puedan proporcionar la protección apropiada y necesaria para su seguridad.

3.1. **Política Sobre el Uso de Controles Criptográficos**.

- Se debe desarrollar una política sobre el uso de controles criptográficos, estableciendo una gestión clave para sostener el uso de estas técnicas. Se tomaran en consideración los siguientes aspectos al desarrollar una política criptográfica:

3.2. **Gestión de Claves**.

- Todas las claves de encriptación deben tener protección contra modificación, pérdida y destrucción. Además, las claves privadas y secretas necesitan protección contra divulgación no autorizada.
- El equipo usado para generar, almacenar y archivar las claves debe estar protegido por medios físicos (con llave).
- Un sistema de gestión de claves se debe basar en un conjunto acordado de normas, procedimientos y método seguros.

4. Seguridad de los Archivos del Sistema.

Todos los accesos otorgados a los archivos de los sistemas de la Organización deben estar controlados, para asegurar que las actividades de soporte y proyectos de Tecnologías de la Información son llevados a cabo de forma segura.

4.1. **Control del Software Operacional**.

- Se deberá Garantizar que los desarrollos y actividades de soporte a los sistemas se lleven a cabo de manera segura, controlando el acceso a los archivos del mismo.
- Con el fin de minimizar el riesgo de alteración de los sistemas, se definen los siguientes controles a realizar durante la implementación del software en producción:

4.2. **Protección de la Data del Sistema**.

- Se debe evitar el uso de bases de datos operacionales que contengan información reservada para propósitos de pruebas.
- Si se utiliza información personal o de otra forma sensible para propósitos de prueba, todos los detalles y el contenido sensible se deben retirar o modificar antes del uso para evitar el reconocimiento.
- Todos los detalles confidenciales deben ser removidos o modificados más allá de todo reconocimiento antes de utilizarlos.
- Cuando se utiliza la data operacional para propósitos de prueba se deben aplicar los siguientes lineamientos:

4.3. **Control de Cambio de Datos Operativos**.

- La modificación, actualización o eliminación de los datos operativos serán realizados a través de los sistemas que procesan dichos datos y de acuerdo al esquema de control de accesos implementado en los mismos.
- Una modificación por fuera de los sistemas a un dato almacenado, ya sea en un archivo o base de datos, podría poner en riesgo la integridad de la información.
- Los casos en los que no fuera posible la aplicación de la precedente política, se considerarán como excepciones.
- La Jefatura de la Sección de Servicios Tecnológicos definirá procedimientos para la gestión de dichas excepciones.

4.4. **Control del Acceso al Código de Fuente del Programa**.

- Para reducir la probabilidad de alteración de programas fuentes, la Sección de Servicios Tecnológicos debe implementar controles de versión, controles de acceso, manejo de respaldos de código y bases de datos, y registro de modificación al código fuente.

5. Seguridad de los Procesos de Desarrollo y Soporte.

Se deben establecer normas para el control de los entornos del proyecto y procesos de desarrollo y soporte en el mantenimiento de la seguridad del software y de la información manejada por las aplicaciones de los sistemas de la Organización. Cada cambio propuesto para los diferentes sistemas de información debe ser revisado para asegurar que no afecta la seguridad del mismo o la del sistema operativo.

5.1. **Procedimiento del Control de Cambio**.

- Los procedimientos formales de control de cambios se deben documentar y hacer cumplir para minimizar la corrupción de los sistemas de información.
- La introducción de sistemas nuevos y de cambios importantes en los sistemas existentes deben seguir un proceso formal de documentación, especificación, prueba, control de calidad e implementación con gestión.
- Este proceso debe incluir una evaluación de riesgos, análisis de los impactos de los cambios y especificación de los controles de seguridad necesarios.
- Este proceso también debe garantizar que la seguridad y los procesos de control existentes no se exponen a riesgos o peligros, cuando se da acceso a los programadores de soporte sólo a aquellas partes del sistema necesarias para su trabajo y que existe acuerdo y aprobación formal para cualquier cambio.

5.2. **Revisión Técnica de la Aplicación después de Cambios en el Sistema**.

- Cuando se cambian los sistemas operativos, las aplicaciones críticas para el negocio se deberían revisar y someter a prueba para asegurar que no hay impacto adverso en las operaciones ni en la seguridad de la organización.

5.3. **Restricciones sobre los Cambios en los Paquetes de Software**.

- En caso de considerarlo necesario, la modificación de paquetes de software suministrados por proveedores se realizará previa autorización de la Jefatura de la Sección de Servicios Tecnológicos.

5.4. **Filtración de Información**.

- Se deben evitar las oportunidades para que se produzca fuga de información.
- Se deben considerar los siguientes aspectos para limitar el riesgo de fuga de información:

5.5. **Desarrollo de Software Abastecido Externamente**.

- La organización debe supervisar, monitorear el desarrollo de software realizado por instituciones externas.

6. Gestión de Vulnerabilidad Técnica.

Se deben establecer normas y controles para reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas publicadas.

La gestión de la vulnerabilidad técnica se debe implementar de forma eficaz, sistemática y repetible con toma de mediciones para confirmar su eficacia. Estas consideraciones deben incluir a los sistemas operativos y otras aplicaciones en uso.

6.1. **Control de Vulnerabilidades Técnicas**.

- Se debe obtener información oportuna sobre las vulnerabilidades técnicas de los sistemas de información que están en uso, evaluar la exposición de la organización a dichas vulnerabilidades y tomar las acciones apropiadas para tratar los riesgos asociados.
- Debe obtenerse información oportuna relacionada con las vulnerabilidades técnicas de los sistemas de información y equipos de red utilizados por MCR, evaluar la exposición a dichas vulnerabilidades y adoptar los controles adecuados para manejar los riesgos.
- El(a) Encargado(a) de Seguridad de la Información, junto a la Jefatura de la Sección de Servicios Tecnológicos y al(a) Encargado(a) del Área de Redes,

deben establecer los procedimientos de gestión de vulnerabilidades técnicas de los activos de información.

POLÍTICA DE SEGURIDAD

GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

CONSEJO NACIONAL DE LA CULTURA Y LAS ARTES

AÑO 2011

CONTROL E HISTORIAL DE VERSIONES

N° Versión	Fecha	Descripción de las Modificaciones	Páginas Modificadas	Autor
1.0	15-07-2011	Elaboración de versión inicial	Todas	JGMV
1.1	15-11-2011	Correcciones de contenido, estilo, lenguaje, ordenamiento y presentación de temas	Todas	RAM

DECLARACIÓN CORPORATIVA

La administración de la continuidad de las actividades es un proceso crítico que debe involucrar a todos los niveles del Consejo Nacional de la Cultura y las Artes (CNCA). El desarrollo e implementación de planes de contingencia es una herramienta básica para garantizar que las actividades de la Organización puedan restablecerse dentro de los plazos requeridos. Dichos planes deben mantenerse actualizados y transformarse en una parte integral del resto de los procesos de administración y gestión, debiendo incluir, necesariamente, controles destinados a identificar y reducir riesgos, atenuar las consecuencias de eventuales interrupciones de las actividades del Servicio y asegurar la reanudación oportuna de las operaciones indispensables.

ÁMBITO

- Esta Política se aplica a todos los procesos críticos identificados del Consejo Nacional de la Cultura y las Artes (CNCA).

ROLES Y RESPONSABILIDADES

- **Encargado(a) de Seguridad de la Información**
  - Participar activamente en la definición, documentación, prueba y actualización de los planes de contingencia.
  - Identificar las amenazas que puedan ocasionar interrupciones de los procesos y/o las actividades del Organismo.
  - Evaluar los riesgos para determinar el impacto de dichas interrupciones.
  - Identificar los controles preventivos.
  - Desarrollar un plan estratégico para determinar el enfoque global con el que se abordará la continuidad de las actividades.
  - Elaborar los planes de contingencia necesarios para garantizar la continuidad de las actividades.

- **Dueños(as) de Procesos**
  - Revisar periódicamente los planes bajo su incumbencia, como así, también, identificar cambios en las disposiciones relativas a las actividades del Organismo aún no reflejadas en los planes de continuidad.
  - Verificar el cumplimiento de los procedimientos implementados para llevar a cabo las acciones contempladas en cada plan de continuidad.

REGLAS DE LA POLÍTICA

1.Aspectos de Seguridad de la Información en la Gestión de la Continuidad.

1.1 **Proceso de la Administración de la Continuidad del Negocio**.

- El Comité de Seguridad de la Información, será el responsable de la coordinación del desarrollo de los procesos que garanticen la continuidad de las actividades del CNCA.
- Este Comité de Seguridad de la Información tendrá a cargo la coordinación del proceso de administración de la continuidad de la operatoria de los sistemas de tratamiento de información del CNCA frente a interrupciones imprevistas.

1.2 **Continuidad del Negocio y Evaluación del Riesgo**.

- Identificar los eventos (amenazas) que puedan ocasionar interrupciones en los procesos de las actividades; por ejemplo, fallas en el equipamiento, delitos civiles, interrupción del suministro de energía eléctrica, inundación, incendio, desastres naturales, atentados, etc.
- Evaluar los riesgos para determinar el impacto de dichas interrupciones, tanto en términos de magnitud de daño como del periodo de recuperación. Dicha evaluación debe identificar los recursos críticos, los impactos producidos por una interrupción, los tiempos de interrupción aceptables o permitidos, y debe especificar las prioridades de recuperación.
- Identificar los controles preventivos; por ejemplo, sistemas de supresión de fuego, detectores de humo y fuego, contenedores resistentes al calor y a prueba de agua para los medios de respaldo, los registros no electrónicos vitales, etc.
- Según los resultados de la evaluación del punto anterior, se desarrollará un plan estratégico para determinar el enfoque global con el que se abordará la continuidad de las actividades.
- Una vez que se ha creado este plan, el mismo debe ser propuesto por el Comité de Seguridad de la Información al Jefe de Servicio del CNCA para su aprobación.

1.3 **Desarrollo e Implementación de Planes de Continuidad del Negocio que Incluyan la Seguridad de la Información**.

- Se deben desarrollar e implementar planes para mantener o recuperar las operaciones y asegurar la disponibilidad de la información en el grado y la escala de tiempo requerido, después de la interrupción o la falla de procesos críticos.
- El proceso de planificación se debe centrar en los objetivos requeridos del negocio; por ejemplo, la restauración de servicios de comunicación específicos para los clientes en un lapso de tiempo aceptable.
- Los servicios y recursos que lo facilitan deben identificarse, incluyendo el personal, los recursos no relacionados con el procesamiento de información, al igual que las disposiciones de respaldo para los servicios de procesamiento de información. Estas disposiciones de respaldo pueden incluir arreglos con terceras partes en forma de acuerdos recíprocos o servicios de suscripción comercial.
- Los planes de continuidad del negocio deben afrontar las vulnerabilidades de la organización y, por tanto, pueden contener información sensible que es necesario proteger adecuadamente.
- Las copias de los planes de la continuidad del negocio se deben almacenar en un lugar lejano, a suficiente distancia como para escapar de cualquier daño por algún desastre en la sede principal.
- La dirección debe garantizar que las copias de los planes de continuidad del negocio están actualizadas y protegidas con el mismo nivel de seguridad que se aplica en la sede principal.
- De igual modo, el otro material necesario para ejecutar los planes de continuidad se debe almacenar en un sitio lejano.

- Si se utilizan lugares alternos temporales, el nivel de los controles de seguridad implementados en estos lugares debe ser equivalente al de la sede principal.

1.4. **Marco Referencial de la Planeación de la Continuidad del Negocio**.

- Se debe mantener una sola estructura de los planes de continuidad del negocio, para asegurar que todos los planes y los requisitos de la seguridad de la información sean de forma consistente, así como identificar las prioridades para pruebas y mantenimiento.
- Cada plan de continuidad del negocio debe describir el enfoque para la continuidad; por ejemplo, el enfoque para garantizar la disponibilidad y seguridad de la información o del sistema de información.
- Cada plan debe especificar el plan de escalada y las condiciones para su activación, así como las personas responsables de ejecutar cada componente del plan.
- Cuando se identifican nuevos requisitos, todos los procedimientos de emergencia existentes, por ejemplo, planes de evacuación o disposiciones de respaldo, se deben modificar apropiadamente.
- Los procedimientos se deben incluir en el programa de gestión de cambios de la Organización para garantizar el tratamiento adecuado de los aspectos de la continuidad el negocio.
- Cada plan debe tener un dueño específico.
- Los procedimientos de emergencia, los planes de recursos de emergencia manuales y de reanudación deben ser responsabilidad de los dueños de los recursos o procesos apropiados del negocio involucrados.
- Las disposiciones de respaldo para los servicios técnicos alternos, como servicios de procesamiento de información y comunicaciones, usualmente deben ser responsabilidad de los proveedores del servicio.

1.5. **Prueba, Mantenimiento y Reevaluación de los Planes de Continuidad del Negocio**.

- Debido a que los planes de continuidad de las actividades del CNCA pueden fallar, por suposiciones incorrectas, errores o cambios en el equipamiento, etc., se establecen las siguientes pautas de acción.
  - El Comité de Seguridad de la Información establecerá un cronograma de pruebas periódicas de cada uno de los planes de contingencia.
  - El cronograma indicará quienes son los responsables de llevar a cabo cada una de las pruebas y de elevar el resultado obtenido al citado Comité.
- Los planes de continuidad de las actividades del CNCA serán revisados y actualizados periódicamente, para garantizar su eficacia permanente.
- Se incluirán procedimientos en el programa de administración de cambios del CNCA para garantizar que se aborden adecuadamente los tópicos de continuidad de las actividades.
- Cada uno de los Dueños(as) de Procesos es el responsable de las revisiones periódicas de cada uno de los planes de continuidad de su incumbencia, como así, también, de la identificación de cambios en las disposiciones relativas a las actividades del CNCA aún no reflejadas en dichos planes.
- Todas las modificaciones efectuadas serán propuestas por el Comité de Seguridad de la Información al Jefe de Servicio del CNCA para su aprobación.

CONTROL E HISTORIAL DE VERSIONES

N° Versión	Fecha	Descripción de las Modificaciones	Páginas Modificadas	Autor
1.0	15-07-2011	Elaboración de versión inicial	Todas	JGMV
1.1	15-11-2011	Correcciones de contenido, estilo, lenguaje, ordenamiento y presentación de temas	Todas	RAM

DECLARACIÓN CORPORATIVA

La comunicación es fundamental en todo proceso, por tanto, se debe trabajar con reportes de los eventos y debilidades de la seguridad de la información, asegurando una comunicación tal que permita que se realice una acción correctiva oportuna, llevando la información a través de los canales gerenciales apropiados lo más rápidamente posible. De la misma manera se debe contar con reportes de las debilidades en la seguridad, requiriendo que todos los funcionarios, proveedores y terceros de los sistemas y servicios de información tomen nota de los incidentes y reporten cualquier debilidad de seguridad observada o sospechada en el sistema o los servicios. Aprender de los errores es sabio, por ello, se deben establecer mecanismos para permitir cuantificar y monitorear los tipos, volúmenes y costos de los incidentes en la seguridad de la información, siempre con la idea de no volver a cometer los errores que ya se cometieron, y mejor aún, aprender de los errores que ya otros cometieron.

ÁMBITO

- La política se aplica para todo proceso de gestión de seguridad de la información del Consejo Nacional de la Cultura y las Artes (CNCA).

ROLES Y RESPONSABILIDADES

- **Encargado(a) de Seguridad de la Información**
  - Definir el procedimiento para el reporte de eventos de seguridad, como así también el procedimiento de respuesta y escalamiento de los incidentes, y activar las acciones que deben adoptarse ante la recepción de eventos de seguridad de la información.
  - Formular procedimientos y métodos de evaluación y análisis que permitan utilizar la información de los incidentes de seguridad experimentados en pos de la identificación y prevención de situaciones recurrentes o de alto impacto, y la necesidad de adoptar más o mejores controles.
  - En conjunto con la Jefatura de Departamento de Recursos Humanos, deben desarrollar normas y procedimientos internos para la recolección, manipulación y presentación de evidencia con el propósito de aplicar sanciones disciplinarias dentro del ámbito del CNCA.

- **Jefatura Departamento de Recursos Humanos**
  - En conjunto con el(a) Encargado(a) de Seguridad de la Información deben desarrollar normas y procedimientos internos para la recolección, manipulación y presentación de evidencia con el propósito de aplicar sanciones disciplinarias dentro del ámbito del CNCA.

- **Jefatura Departamento Jurídico**
  - Sancionar legalmente normas y procedimientos internos para la recolección, manipulación y presentación de evidencia con el propósito de aplicar sanciones disciplinarias dentro del ámbito del CNCA.

REGLAS DE LA POLÍTICA

1. Reporte de Eventos y Puntos Débiles.

1.1. Reporte de Eventos en la Seguridad de la Información.

- Se debe establecer un procedimiento formal para el reporte de eventos en la seguridad de la información, junto con un procedimiento de respuesta y de intensificación de incidentes, estableciendo la acción a tomarse al recibir un reporte de un evento en la seguridad de la información.
- Se debe establecer un punto de contacto para el reporte de eventos en la seguridad de la información, asegurando que este punto de contacto sea conocido a través de toda la organización, que siempre esté disponible y sea capaz de proporcionar una respuesta adecuada y oportuna.

1.2. Reporte de la Debilidades en la Seguridad de la Información.

- Se debe asegurar que los eventos y las debilidades de la seguridad de la información asociados con los sistemas de información se comunican de forma tal que permiten tomar las acciones correctivas oportunamente.
- Todos los(as) funcionarios(as) deben tener conciencia sobre los procedimientos para el reporte de los diferentes tipos de eventos y debilidades que puedan tener impacto en la seguridad de los activos de la organización.
- Se debe exigir que se reporten formalmente todos los eventos de seguridad de la información y las debilidades tan pronto sea posible al punto de contacto designado.

2. Gestión de Incidentes y Mejoras.

Con el fin de asegurar que se aplique un enfoque consistente y eficaz para la gestión de los incidentes de seguridad de la información, es conveniente establecer las responsabilidades y los procedimientos para manejar los eventos y debilidades de la seguridad de la información de manera eficaz una vez se han reportado. Se debería aplicar un proceso de mejora continua a la respuesta para monitorear, evaluar y gestionar en su totalidad los incidentes de seguridad de la información.

2.1. Responsabilidades y Procedimientos.

- Se debe establecer las responsabilidades y los procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.
- Se deben instaurar procedimientos para manejar los diferentes tipos de incidentes de seguridad de la información en al menos los siguientes puntos:
  - Fallas en el sistema de información y pérdida del servicio.
  - Códigos maliciosos.
  - Negación del servicio.
  - Errores resultantes de datos incompletos o no actualizados.
  - Violaciones de la confidencialidad y la integridad.
  - Uso inadecuado de los sistemas de información.

2.2. Aprender de los Incidentes en la Seguridad de la Información.

- Deben existir procesos que permitan documentar, cuantificar y monitorear los tipos, volúmenes y costos de los incidentes y anomalías.
- La información que se obtiene de la evaluación de los incidentes de seguridad de la información se debe utilizar para identificar los incidentes recurrentes o de alto impacto.
- La evaluación de los incidentes de seguridad de la información puede indicar la necesidad de mejorar o agregar controles para limitar la frecuencia, el daño y el costo de futuras recurrencias, o de considerarlos en el proceso de revisión de la política de seguridad

2.3. Recolección de Evidencia.

- Se deberá recolectar, retener y presentar adecuadamente la evidencia relacionada con las violaciones a la seguridad que deriven en acciones legales contra personas u organizaciones. Para ello se deben desarrollar y

cumplir procedimientos internos cuando se recolecta y se presenta evidencia con propósitos de acción disciplinaria dentro de la organización.

POLÍTICA DE SEGURIDAD

CUMPLIMIENTO

CONSEJO NACIONAL DE LA CULTURA Y LAS ARTES

AÑO 2011

CONTROL E HISTORIAL DE VERSIONES

N° Versión	Fecha	Descripción de las Modificaciones	Páginas Modificadas	Autor
1.0	15-07-2011	Elaboración de versión inicial	Todas	JGMV
1.1	15-11-2011	Correcciones de contenido, estilo, lenguaje, ordenamiento y presentación de temas	Todas	RAM

DECLARACIÓN CORPORATIVA

La Política de Seguridad de la Información es un documento fundamental para la gestión adecuada y efectiva del proceso de seguridad de la información del Consejo Nacional de la Cultura y las Artes (CNCA). No obstante, las directivas establecidas en este documento no pueden aplicarse en un marco aislado, sino que deben estar alineadas con los requisitos legales, normativos, estatutarios y contractuales que son relevantes para las actividades de la Institución, tanto en el orden local, regional, nacional e internacional. En consecuencia, es imprescindible garantizar el perfecto encuadramiento legal de la Política de Seguridad de la Información. Adicionalmente, debe comprobarse que los controles indicados en la Política de Seguridad de la Información sean aplicados consistente y correctamente en todas las áreas del CNCA.

ÁMBITO

- Esta Política se aplica a todos los sistemas informáticos, normas, procedimientos, documentación y personal del CNCA.

ROLES Y RESPONSABILIDADES

- **Encargado(a) de Seguridad de la Información**
  - En conjunto con la Jefatura de la Sección de Servicios Tecnológicos, deberán definir normas y procedimientos para garantizar el cumplimiento de las restricciones legales, normativas, estatutarias y contractuales al uso del material protegido por normas de propiedad intelectual y a la conservación de registros.
  - Realizar revisiones periódicas de todas las áreas del CNCA a efectos de garantizar el cumplimiento de la política, normas y procedimientos de seguridad.
  - Verificar periódicamente que los sistemas de información cumplan la política, normas y procedimientos de seguridad establecidos.

- **Jefatura Departamento Jurídico**
  - Sancionar legalmente normas y procedimientos para garantizar el cumplimiento de las restricciones legales, normativas, estatutarias y contractuales al uso del material protegido por normas de propiedad intelectual y a la conservación de registros.

- **Jefatura Sección de Servicios Tecnológicos**
  - En conjunto con el(a) Encargado(a) de Seguridad de la Información deberán definir normas y procedimientos para garantizar el cumplimiento de las restricciones legales, normativas, estatutarias y contractuales al uso del material protegido por normas de propiedad intelectual y a la conservación de registros.

REGLAS DE LA POLÍTICA

1. Cumplimiento de los Requisitos Legales.

La formulación e implementación de la política de seguridad y todos sus documentos subordinados aprobados por el CNCA deben ser encuadrados jurídicamente, con el objetivo de evitar infracciones a las leyes, estatutos, regulaciones, obligaciones contractuales o requerimientos de seguridad. Para ello, se deberá buscar la asesoría sobre los requerimientos legales específicos de los asesores legales de la organización o profesionales legales calificados. Los requisitos legales varían de un país a otro y pueden variar para la información creada en un país y que se transmite a otro.

1.1. **Identificación de la Legislación Aplicable**.

- Se deben definir y documentar claramente todos los requisitos normativos y contractuales pertinentes para cada sistema de información.
- Del mismo modo, se definirán y documentaran los controles específicos y las responsabilidades y funciones individuales para cumplir dichos requisitos.

1.2 **Derechos de Propiedad Intelectual**.

- Se deben implementar los procedimientos apropiados para asegurar el cumplimiento de las leyes, regulaciones y requerimientos contractuales relacionados con el uso de material protegido por derechos de propiedad intelectual y el uso de productos de software licenciado o patentado.
- Se deben considerar los siguientes lineamientos para proteger cualquier material que se considere de propiedad intelectual:
  - No copiar completamente o en parte libros, artículos, reportes u otros documentos aparte de aquellos permitidos por la ley de derechos de autor.
  - Los derechos de propiedad intelectual incluyen derechos de copia de software o de documentos, derechos de diseño, marcas registradas, patentes y licencias de códigos fuente.
  - Los productos de software patentados usualmente se suministran bajo un acuerdo de licencia que especifica los términos y condiciones de la licencia, por ejemplo, limitar el uso de los productos a máquinas específicas o limitar el copiado a la creación de copias de respaldo únicamente.
  - Los requisitos legales, reglamentarios y contractuales pueden imponer restricciones a la copia de material patentado. En particular pueden exigir que únicamente se utilice el material desarrollado por la organización o que tenga licencia y es suministrado a la organización por quien lo desarrolla.
  - La violación de los derechos de copia puede conducir a acciones legales que pueden implicar procedimientos judiciales.

1.3 **Protección de Registros Institucionales**.

- Los registros importantes se deben proteger contra pérdida, destrucción y falsificación, de acuerdo con los requisitos estatutarios, reglamentarios, contractuales y del negocio.
- Los registros se deben clasificar en tipos de registro, por ejemplo registros de contabilidad, registros de bases de datos, registros de transacciones, registros de auditoría, procedimientos operativos, etc., cada uno con detalles de los periodos de retención y los tipos de medio de almacenamiento.
- Todo material relacionado con claves criptográficas y programas asociados con archivos encriptados o firmas digitales, también se debe almacenar para

permitir el descifrado de los registros durante el periodo de tiempo durante el cual se retienen los registros.

- Al seleccionar los medios de almacenamiento electrónico, se debe incluir los procedimientos para garantizar la capacidad de acceso a los datos (facilidad tanto del medio como del formato) durante todo el periodo de retención para salvaguardar contra pérdida debido a cambio en la tecnología futura.
- Los sistemas de almacenamiento de datos se deben seleccionar de forma tal que los datos requeridos se puedan recuperar en el periodo de tiempo y el formato aceptable, dependiendo de los requisitos que se deben cumplir.
- El sistema de almacenamiento y manipulación debe garantizar la identificación de los registros y de su periodo de retención tal como se define en los reglamentos o la legislación nacional o regional, si se aplica.
- Este sistema debe permitir la destrucción adecuada de los registros después de este periodo, si la organización no los necesita.

1.4 **Protección de la Data y Privacidad de la Información Personal**.

- Se debe garantizar la protección de los datos y la privacidad, de acuerdo con los requerimientos legales, los reglamentos pertinentes y cláusulas del contrato.
- El(a) Encargado(a) de Seguridad de la Información, la Jefatura de la Sección de Servicios Tecnológicos y la Jefatura de Departamento Jurídico, deben definir la política de protección de datos y privacidad de la Institución.
- La política debe ser comunicada a todo el personal, especialmente a las personas involucradas en el procesamiento de información personal.

1.5 **Prevención del Mal Uso de los Medios de Procesamiento de la Información**.

- Se debe disuadir a los usuarios de utilizar las instalaciones de procesamiento para fines no autorizados.
- Todos los usuarios deben tomar conocimiento, y aceptar el alcance preciso de sus accesos permitidos, y de las actividades de monitoreo ejecutadas por el CNCA.
- En oportunidad de solicitar una sesión con un sistema, los usuarios deben recibir una advertencia respecto a la necesidad de contar con la debida autorización para proceder.
- El usuario debe reconocer el mensaje y reaccionar apropiadamente para continuar con el proceso de ingreso.

1.6 **Regulación de Controles Criptográficos**.

- Los controles basados en sistemas criptográficos deben ser usados en cumplimiento de los acuerdos, leyes y regulaciones relevantes.
- El(a) Encargado(a) de Seguridad de la Información, la Jefatura de la Sección de Servicios Tecnológicos y la Jefatura de Departamento Jurídico, deben definir el estándar de cumplimiento legal de los controles basados en sistemas criptográficos utilizados por el CNCA, tomando en consideración que existen restricciones de importación/exportación del hardware y software que incluyen sistemas criptográficos, y que existen restricciones en el uso de funciones de cifrado.

2. Cumplimiento de las Políticas y Normas de Seguridad y Cumplimiento Técnico.

Debe revisarse regularmente los sistemas para verificar el cumplimiento de los controles de seguridad y asegurar que los cumplen con las directivas y controles de la política de seguridad y sus documentos relacionados.

2.1 **Cumplimiento con las Políticas y Estándares de Seguridad**.

- Se debe asegurar que todos los controles y procedimientos de seguridad se aplican correctamente en todo el ámbito del CNCA.
- Las Jefaturas de Departamento, Sección, Unidad y/o Programas deben revisar con regularidad, en su área de responsabilidad, el cumplimiento del procesamiento de información con las políticas de seguridad adecuadas, las normas y cualquier otro requisito de seguridad.

- Se deben chequear regularmente los sistemas de información y las redes para verificar el cumplimiento de la implementación con los estándares de seguridad.
- La comprobación del cumplimiento técnico comprende el examen de los sistemas en producción para asegurar que los controles de hardware y software están correctamente implementados.
- El(a) Encargado(a) de Seguridad de la Información y la Jefatura de la Sección de Servicios Tecnológicos, deben definir y elaborar los procedimientos para verificar el cumplimiento tecnológico de los sistemas y redes con los controles adoptados.

3. Consideraciones de la Auditoría de los Sistemas de Información.

Deben existir controles para proteger, simultáneamente, los sistemas operativos y las herramientas de revisión durante las actividades de auditoría, y así maximizar la efectividad de revisión de los sistemas, minimizando la interferencia mutua con las herramientas de auditoría.

3.1. Controles de Auditoría de los Sistemas de Información.

- Los requisitos y las actividades de auditoría que implican verificaciones de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar el riesgo de interrupciones de los procesos de negocio.
- Las personas que ejecutan la auditoría deben ser independientes de las actividades auditadas.

3.2. Protección de las Herramientas de Auditoría de los Sistemas de Información.

- Se protegerá el acceso a los elementos utilizados en las auditorías de sistemas, o sea, archivos de datos o software, a fin de evitar el mal uso o el compromiso de los mismos.
- Dichas herramientas estarán separadas de los sistemas en producción y desarrollo, y se les otorgará el nivel de protección requerido.

ARTÍCULO SEGUNDO: Una vez que se encuentre totalmente tramitada, publíquese la presente resolución en el sitio electrónico de Gobierno Transparente del Consejo Nacional de la Cultura y las Artes, por la Secretaria Administrativa y Documental del Servicio, en la categoría "Marco Normativo Aplicable", a objeto de dar cumplimiento a lo previsto en el artículo 7º de la Ley N° 20.285 sobre Acceso a la Información Pública y en el artículo 51 de su Reglamento.

ANÓTESE

CONSEJO NACIONAL DE CULTURA Y LAS ARTES
SUBDIRECTOR NACIONAL (S)

JAVIER CHAMAS CACERES
SUBDIRECTOR NACIONAL SUPLENTE
CONSEJO NACIONAL DE LA CULTURA Y LAS ARTES

Resol. Nº 04/932
Distribución:

- Gabinete Ministro Presidente, CNCA
- Subdirección Nacional, CNCA
- Sección de Planificación Estratégica y Control de Gestión, Departamento de Planificación y Presupuesto, CNCA
- Departamento Jurídico, CNCA
- Unidad de Auditoría, CNCA
- Secretaría Administrativa y Documental, CNCA