Consejo Nacional de la Cultura y las Artes

JFT / VPS

ACTUALIZA POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN DEL CONSEJO NACIONAL DE LA CULTURA Y LAS ARTES.

EXENTA Nº 2195 *27.11.2015

VALPARAÍSO,

VISTO:

Lo dispuesto en la Ley Nº 19.891 que crea el Consejo Nacional de la Cultura y las Artes; en el Decreto N° 83, de 2004, del Ministerio Secretaría General de la Presidencia, que Aprueba Norma Técnica para los Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los Documentos Electrónicos; en las Resoluciones N° 268, de 2013, y Exentas N° 5621, de 2012, N° 940 y N° 2015, ambas de 2015, todas 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.

CONSIDERANDO:

Que la Ley Nº 19.891, creó el Consejo Nacional de la Cultura y las Artes, en adelante también "el Consejo" o "el Servicio" indistintamente, como un servicio público autónomo, descentralizado y territorialmente desconcentrado, con personalidad jurídica y patrimonio propio, cuyo objeto es apoyar el desarrollo de las artes y la difusión de la cultura, contribuir a conservar, incrementar y poner al alcance de las personas el patrimonio cultural de la Nación y promover la participación de éstas en la vida cultural del país.

Que el Decreto N° 83, de 2004, del Ministerio Secretaría General de la Presidencia, que Aprueba Norma Técnica para los Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los Documentos Electrónicos, dispone en su artículo 11 que dentro de cada institución, deberá establecerse una política que fije las directrices generales orientadoras en materia de seguridad, que reflejen claramente el compromiso, apoyo e interés en el fomento y desarrollo de una cultura de seguridad institucional.

Que en cumplimiento del mandato precedente, el Consejo actualizó su Política General de Seguridad de la Información mediante Resolución Exenta N° 5621, de 2012, estableciendo esta última que la misma será objeto de revisión una vez al año para la evaluación de estatus y cumplimiento y, en todo caso, a lo menos cada tres años.

Que, en este contexto, se hace necesario revisar y actualizar la Política General de Seguridad de la Información del Consejo, de acuerdo a lo solicitado mediante Memorando N° 02/886 de Subdirección Nacional.

Que a su vez, el numeral 41) de la letra a) del artículo primero de la Resolución Exenta Nº 268, de 2013, de este Servicio, delega en el/la Subdirector/a Nacional la facultad de impartir instrucciones y dictar los demás actos y resoluciones destinadas a implementar en el Servicio el Sistema de Gestión de Seguridad de la Información establecido en el precitado Decreto N° 83, de 2004, del Ministerio General de la Presidencia, y las demás normas que lo complementan.

Que en mérito de las consideraciones y antecedentes legales y reglamentarios expuestos precedentemente, es necesario dictar el correspondiente acto administrativo. Por tanto,

RESUELVO:

ARTÍCULO PRIMERO: Apruébase la Política General de Seguridad de la Información Institucional del Consejo Nacional de la Cultura y las Artes, cuyo tenor es el siguiente:

1. DECLARACIÓN INSTITUCIONAL

El Consejo Nacional de la Cultura y las Artes, en adelante "CNCA", "Servicio" o "Consejo" indistintamente, según lo dispuesto en la Ley N° 19.891 es un servicio público autónomo, descentralizado y territorialmente desconcentrado, con personalidad jurídica y patrimonio propio, en el que se integra la participación de la sociedad civil, dando origen a una manera distinta de enfrentar el diseño, implementación y evaluación de las políticas públicas. Tiene por objetivo apoyar el desarrollo de las artes y la difusión de la cultura, contribuir a conservar, incrementar y poner al alcance de las personas el patrimonio cultural de la Nación y promover la participación de éstas en la vida cultural del país; debiendo, además, observar como principio básico la búsqueda de un desarrollo cultural armónico y equitativo entre las regiones, provincias y comunas del país.

Para apoyar el cumplimiento de sus funciones, el CNCA ha desarrollado una plataforma tecnológica a través de la cual se registra, procesa, transmite y almacena información mediante diferentes Activos de Información, que permiten interactuar con la comunidad cultural, ciudadanía en general y los integrantes del CNCA en todo el país, con la información requerida para dar cumplimiento a las funciones que el mandato legal exige, considerando que la información resguardada puede ser propia de los sistemas del Consejo, tanto de los servicios o sus procesos, como de los usuarios internos o externos.

El CNCA reconoce que la información que posee es un bien estratégico para sus funciones, por lo que requiere protección en su obtención, procesamiento, transmisión y almacenamiento. Por tanto, todo el personal que integra la organización será responsable de la confidencialidad, integridad y disponibilidad de la información que, por cargo y función, les corresponde administrar y gestionar.

La información y los procesos de apoyo, representados por la Infraestructura Tecnológica de Información y Comunicaciones (TIC), son bienes de máxima importancia, que deben asegurar la confidencialidad, integridad y disponibilidad de la información, conforme a las exigencias que el marco legal impone al CNCA.

Debe considerarse además, que el CNCA en sus sistemas de información y redes se enfrenta en forma creciente a las amenazas de seguridad desde una amplia gama de fuentes, que van desde hechos naturales, pasando por fallas de equipos o aplicaciones, hasta ataques intencionales, por lo que sus sistemas informáticos requieren estar protegidos.

Para el CNCA, es de alta importancia el almacenamiento y tratamiento que se le da a los Activos de Información, entendiendo por tales, todo elemento en que se registre, se almacene y/o procesen datos e información, sea a través de medios tecnológicos o no, tales como bases de datos y archivos, contratos y acuerdos, documentación del sistema, manuales de usuario, material de entrenamiento, procedimientos operacionales o de soporte, plan de continuidad de negocio, información de auditorías, información archivada, activos de software, activos físicos y servicios, entre otros.

1.1 Objetivos

Establecer normas que regulen el correcto uso de los servicios y la información, a través de las distintas actividades que el personal del CNCA realiza en el desempeño de sus funciones, con el fin de asegurar la confidencialidad, integridad y disponibilidad de los mismos.

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

1.2 Alcance

La presente Política General de Seguridad de la Información del CNCA expresa, en forma clara y sucinta, los lineamientos generales con respecto al buen uso de los Activos de información, tanto compartidos, como de cada uno de los usuarios, internos o externos.

Estas directrices de alto nivel, están destinadas a servir de guía para la definición de normas específicas que se contendrán en las disposiciones complementarias, de carácter administrativo y técnico, que se dicten para el cumplimiento de lo dispuesto en la presente Política.

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

2. POLÍTICA DE SEGURIDAD

2.1 Organización de la Seguridad de la Información

La seguridad de la información, abordada como responsabilidad institucional, hace necesaria la participación de todo el personal del CNCA y de aquellos organismos externos que tienen roles y responsabilidades -establecidas en los respectivos contratos y/o acuerdos-, de contribución al logro de los objetivos de confidencialidad, disponibilidad e integridad de la información.

Con el propósito de optimizar la gestión de seguridad informática y darle la transversalidad organizacional que ésta requiere, mediante Resolución Exenta N° 2493, de 2011, se creó el Comité de Seguridad de la Información Institucional, cuya regulación fue actualizada por Resolución Exenta N° 2015, de 2015, ambas de este Consejo. El Comité es presidido por el Encargado de Seguridad de la Información Institucional, cuyo objetivo es crear, implantar y gestionar las distintas Políticas de Seguridad de la Información del CNCA, mantenerlas y adecuarlas en el tiempo, de acuerdo a la normativa vigente.

El Comité de Seguridad de la Información Institucional tiene por misión "**velar por la confidencialidad, integridad y disponibilidad de la información y los medios tecnológicos que la soportan**", para lo cual debe elaborar políticas específicas, procedimientos, medidas administrativas, determinar los medios tecnológicos a utilizar y dictar las demás disposiciones que se deriven de la presente política.

La integración, sesiones, quórum, actas y Comisiones de Trabajo del Comité de Seguridad de la Información Institucional, se encuentran establecidas en la Resolución Exenta N° 2015, de 2015, de este Servicio.

A su vez, las funciones del Encargado de Seguridad de la Información Institucional se encuentran establecidas en la Resolución Exenta N° 940, de 2015, que le asigna las siguientes:

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

b) Coordinar la respuesta a incidentes de seguridad que afecten los activos de información Institucionales.

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

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

a) Propondrá disposiciones generales para el uso de Activos de Información;
b) Propondrá capacitaciones pertinentes para el personal del CNCA;
c) Propondrá capacitaciones a dicho personal referidas a la política de seguridad informática y de procedimientos del área TIC, en las competencias requeridas conforme al perfil de cada cargo;
d) Gestionará el procedimiento que se inicie en virtud de la denuncia de un incidente de seguridad;
e) Propondrá la realización de procesos internos de auditoría de acuerdo a las necesidades establecidas por el Subdirector Nacional;
f) Adoptará las medidas necesarias para resguardar los Activos de Información en conformidad a las instrucciones impartidas por el Comité de Seguridad de la Información Institucional, y
g) Adoptará las medidas para garantizar la seguridad en el uso de dispositivos móviles, y la protección de la información que se accede, procesa o almacena en los lugares de trabajo remoto

Finalmente, cada usuario, ya sea interno o externo, será responsable de los equipos de procesamiento de datos entregados para su trabajo y de respetar las normas de seguridad respecto a la información que por su cargo deba acceder, procesar y/o generar.

2.2 Seguridad Ligada al Recurso Humano

El Departamento de Gestión y Desarrollo de las Personas, previo a la contratación, deberá verificar los antecedentes de todos los candidatos al empleo, de acuerdo con la normativa vigente, y en proporción a los requisitos del negocio, la clasificación de la información a ser accedida, y los riesgos percibidos. Además, los acuerdos contractuales deberán señalar responsabilidades en cuanto al rol del empleado en materia de seguridad de la información.

Con el objeto de reducir los riesgos de error humano o mal uso de los recursos informáticos, el Departamento de Gestión y Desarrollo de las Personas en conjunto con la Sección de Tecnologías de Información de la Subdirección Nacional, propondrán anualmente al Comité de Seguridad de la Información Institucional, los requerimientos de actualización de competencias para el personal involucrado en la Gestión de la Seguridad de la Información en el Consejo, que les permita cumplir adecuadamente las misiones de su responsabilidad.

El Departamento de Gestión y Desarrollo de las Personas dispondrá de un proceso de inducción para el personal que ingresa al Consejo, en materias correspondientes a la confidencialidad de la información y sistemas informáticos que sean puestos a disposición de los integrantes del Servicio para el desempeño de sus funciones.

De igual forma, se considerarán capacitaciones al personal del Consejo por parte de la Sección de Tecnologías de Información, de acuerdo al plan de inducción establecido por la Sección de Gestión y Desarrollo de las Personas, referida a la política de seguridad informática y de procedimientos del área TIC, en las competencias requeridas conforme al perfil de cada cargo.

En caso que funcionarios/as del Consejo infrinjan las normas de seguridad de la información, deberá instruirse un proceso disciplinario en conformidad a lo dispuesto en el Estatuto Administrativo, a fin de determinar la eventual responsabilidad administrativa que corresponda y aplicar las medidas disciplinarias que correspondan, sin perjuicio de la responsabilidad civil o penal que pudiera existir.

Para el evento que las mencionadas infracciones sean cometidas por toda otra persona, natural o jurídica, vinculada contractualmente al Servicio, se procederá de acuerdo a lo establecido en los respectivos contratos y/o acuerdos vigentes, a fin de determinar las sanciones pertinentes, sin perjuicio de la responsabilidad civil o penal que pueda corresponder.

Finalmente, en caso de desvinculación o cambio de relación laboral, se deberán definir y comunicar las responsabilidades y funciones de la seguridad de la información que siguen en vigor, después de la desvinculación o cambio de funciones. Además, toda información generada por personal del Servicio en el desempeño de sus funciones, sea que éstos hayan sido realizados individualmente o de manera colectiva, son propiedad del Consejo.

2.3 Gestión de Activos

El Comité de Seguridad de la Información, mantendrá un registro de los Activos de Información del CNCA, un catastro de equipos y la identificación del personal responsable de cada uno de ellos. Además, deberá asegurar que la información reciba el nivel de protección adecuado, teniendo en cuenta su clasificación, etiquetado y manipulación.

De igual forma, propondrá las medidas necesarias para la correcta administración y uso de los equipos de procesamiento de datos por parte de los usuarios internos y/o externos, para el soporte por parte de la Sección de Logística y Mantención del Departamento de Administración y Finanzas, y para los cambios de configuraciones que se realicen a estos equipos.

A su vez, es responsable de la adecuada gestión de los medios de almacenamiento, tanto estáticos como removibles, implementando de manera correcta los procedimientos establecidos para su administración y eliminación.

Respecto al derecho de acceso a la información de los órganos de la Administración del Estado, deberán respetarse los principios establecidos en el artículo 11 de la Ley Nº 20.285.

2.4 Control de Accesos

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

El acceso a la información será conforme a un Plan de Gestión de acceso de usuarios, propuesto por la Sección de Tecnologías de Información, en conjunto con el/la Subdirector/a Nacional y las Jefaturas de Departamento, el que será aprobado por el Comité de Seguridad de la Información Institucional, el cual deberá garantizar el acceso de personal autorizado y evitar el acceso sin autorización a los sistemas del Servicio. Los privilegios de acceso que se asignen a los respectivos mandos, se otorgarán de acuerdo a su ámbito de acción y responsabilidades.

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

Por otro lado, la Sección de Tecnologías de Información será la encargada de gestionar el control de acceso a los sistemas y aplicaciones, con el fin de evitar el acceso sin autorización a los sistemas y aplicaciones.

2.5 Criptografía

El acceso a la información debe asegurar el uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad o integridad de la información.

Para ello, la Sección de Tecnologías de Información desarrollará e implementará una política, previa aprobación del Comité de Seguridad de la Información, sobre el uso de controles criptográficos para la protección de la información y una política sobre el uso, protección de las claves criptográficas durante toda su vida útil.

2.6 Seguridad Física y Ambiental

Se considerará dentro de las áreas críticas, las instalaciones en las que se encuentren activos de información que se consideren indispensables para las operaciones del Consejo. Dentro de estas áreas se encuentran: sala de servidores, dependencias donde se encuentran equipos de comunicaciones pertenecientes al cableado estructurado de la red LAN, oficina de administradores y monitoreo, oficinas de desarrolladores, taller de soporte, estaciones de trabajo de los usuarios y todas las instalaciones que el Comité de Seguridad de la Información Institucional determine como críticas.

Se deberá evitar accesos físicos no autorizados, daños e interferencias contra las instalaciones de procesamiento de la información y la información del CNCA consideradas críticas. Para ello se deberán establecer procedimientos que restrinjan el acceso a estas áreas, estableciendo perímetros de seguridad, controles de acceso y protección contra las amenazas externas y ambientales, con el fin de evitar, entre otros, pérdidas, robos y hurtos de información.

2.7 Seguridad en las Operaciones

La Sección de Tecnologías de Información gestionará los procedimientos de apoyo, los servicios informáticos y de seguridad de la información, e instalaciones de información, de acuerdo a las normas establecidas por el Comité de Seguridad de la Información Institucional, con este fin deberá:

- Implementar los mecanismos de protección preventiva y activa contra software maliciosos, que puedan llegar en forma física o lógica, a la red o estaciones de trabajo.
- La información de los sistemas y configuraciones de los servidores de servicios importantes para las funciones del CNCA, deberán ser respaldados periódicamente.
- registrar eventos, generar evidencia y establecer procedimientos para proteger dichos procesos.
- Separar los roles de las áreas de desarrollo, prueba y administración.
- Asegurar la integridad de los sistemas operacionales.
- Restringir la instalación de software por parte de los usuarios.

Por su parte, la Unidad de Auditoría Interna del Gabinete del Ministro Presidente realizará procesos internos de auditoría de seguridad informática de acuerdo a las necesidades establecidas por el Comité de Seguridad de la Información.

2.8 Seguridad en las Comunicaciones

A fin de asegurar la protección de la información en las redes y sus instalaciones de procesamiento de información de apoyo, la Sección de Tecnologías de Información gestionará y controlará la información en los sistemas y aplicaciones de la institución.

Para ello, se establecerán mecanismos de seguridad, los niveles de servicios y los requisitos de la gestión de todos los servicios de red que se deben identificar e incluir en los acuerdos de

servicios de red, ya sea que estos servicios sean prestados dentro de la organización o por terceros.

Para cumplir con lo señalado, la Sección de Tecnologías de Información propondrá las políticas, procedimientos y controles de transferencia formal que deben estar en consonancia con la protección de la transferencia de información por parte de los usuarios internos o externos del CNCA, las que deberán ser aprobadas por el Comité de Seguridad de la Información Institucional.

2.9 Adquisición, Desarrollo y Mantenimiento de los Sistemas de la Información

Todo Activo de Información que se requiera mejorar o incorporar al CNCA, deberá ser evaluado por la Subdirección Nacional, través de la Sección de Tecnologías de Información, analizando los riesgos, e incorporando los requisitos de seguridad de información pertinentes antes de su compra o actualización, a fin de considerarlos en el proceso de adquisición o desarrollo.

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

Por otro lado, se deberá garantizar que la seguridad de la información esté diseñada e implementada dentro del ciclo de desarrollo de los sistemas de información, debiendo ser considerada en cada etapa del mismo, independiente del modelo que se aplique. Con este fin se deberán establecer políticas y procedimientos para el desarrollo seguro de software.

Los software computacionales, compilaciones de datos, adaptaciones y cualquier documento relacionado con ello, son de propiedad del CNCA, por cuanto han sido realizados por personal del CNCA en el desempeño de sus funciones, sea que éstos hayan sido realizados individualmente o de manera colectiva.

2.10 Relación con Proveedores

El Comité de Seguridad de la Información desarrollará políticas y procedimientos de seguridad para proveedores, con el objetivo de mitigar los riesgos asociados al acceso por parte de éstos a los activos del Consejo, buscando asegurar la protección de la información.

Los requisitos de seguridad deberán ser definidos e incorporados con cada proveedor que pueda acceder, procesar, almacenar, comunicar o proporcionar componentes de infraestructura TI para la información del Consejo. Estos requisitos deberán abordar los riesgos de seguridad de la información asociados a los servicios de la tecnología de la información y las comunicaciones, y la cadena de suministro del producto, los que serán incluidos en cada acuerdo que se celebre con los proveedores.

Por otro lado, se establecerán mecanismos de supervisión y revisión de los servicios prestados por los proveedores. Además, de gestionar los cambios al suministro de los servicios por parte de estos, incluido el mantenimiento y la mejora de las políticas de seguridad de la información existentes, procedimientos y controles, al considerar la criticidad de la información del negocio, los sistemas y procesos involucrados y la reevaluación de los riesgos, dentro de su ámbito de operación.

2.11 Gestión de Incidentes en la Seguridad de la Información

El Comité de Seguridad de la Información Institucional definirá los procedimientos a seguir en la gestión de incidentes de seguridad, los que deberán ser implementados por la Sección de Tecnologías de Información, bajo la coordinación del/la Encargado/a de Seguridad de la Información Institucional.

La Sección de Tecnologías de Información deberá garantizar que los eventos y debilidades en la seguridad asociados con los sistemas de información, se comuniquen de modo que se puedan realizar acciones correctivas oportunas, aplicando un enfoque consistente y eficaz.

Por otro lado, todo el personal que tenga conocimiento de incidentes de seguridad, entendiendo por tales todo evento que impida el normal funcionamiento de los Activos de Información y que afecte a la seguridad de la información, deberá ser informado en la forma más rápida y expedita posible a la Mesa de Ayuda de la Sección de Tecnologías de Información, la que deberá disponer de un procedimiento de gestión de incidentes, que deberá ser coordinado por el Encargado de Seguridad de la Información Institucional.

Por último, los incidentes deberán ser evaluados, con el fin de decidir si serán considerados como incidentes de seguridad de la información.

2.12 Gestión de la Continuidad del Negocio

La Sección de Tecnologías de Información, deberá aplicar una estrategia, aprobada por el Comité de Seguridad de la Información, que asegure la continuidad operacional de los procesos críticos del Consejo frente a situaciones adversas. A su vez, deberá gestionar los planes de contingencia y recuperación, conforme a la estrategia definida.

Los Activos de Información identificados como importantes para la continuidad del accionar del CNCA, deberán contar con contrato de mantenimiento y/o soporte con los proveedores, a fin de asegurar su funcionamiento o reemplazo conforme a los niveles de servicio requeridos y su actualización.

2.13 Cumplimiento

Con el objetivo de controlar el fiel cumplimiento de la Política de Seguridad de la Información del Consejo Nacional de la Cultura y las Artes, así como las restricciones requeridas en las diferentes leyes, normativas, políticas, procedimientos asociadas al gobierno electrónico, el Comité de Seguridad de la Información deberá aplicar una estrategia que contemple la realización de revisiones periódicas de todas las áreas del Organismo.

3. REVISIONES

El Comité de Seguridad de la Información Institucional efectuará una revisión de esta Política al menos una vez cada dos años para la evaluación de estatus y cumplimiento, sin embargo, ante eventuales cambios drásticos en las tecnologías de la información, dicha revisión se realizará cada vez que la situación lo amerite, sin perjuicio de que pueda ser evaluada en cualquier momento, dependiendo de la necesidad de la organización.

4. DIFUSIÓN

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

5. GLOSARIO DE TÉRMINOS

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

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

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

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

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

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

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

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

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

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

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

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

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

Integridad: Mantenimiento de la exactitud y totalidad de la información.

Red de Área Local (LAN): Estructura de comunicación entre los dispositivos que se encuentran en las dependencias del CNCA.

Mesa de Ayuda: Oficina de Servicios Tecnológicos, que atiende y da solución a los requerimientos técnicos de los usuarios del CNCA.

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

Riesgo: Amenaza de impacto y vulnerabilidad de la seguridad.

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

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

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

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

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

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

ARTICULO SEGUNDO: Adóptense por el Comité de Seguridad de la Información Institucional, a través de su Presidente, todas las medidas necesarias para la oportuna y debida difusión de la Política General de Seguridad de la Información, a todo el personal de este Servicio.

ARTÍCULO TERCERO: Derógase, a contar de la fecha de total tramitación de este acto administrativo, la Resolución Exenta N° 5621, de 28 de diciembre de 2012, del Consejo Nacional de la Cultura y las Artes.

ARTÍCULO CUARTO: Una vez tramitada, publíquese la presente resolución en el sitio electrónico de Gobierno Transparente del Consejo Nacional de la Cultura y las Artes, por la Sección Secretaría Documental, en las categorías "Marco normativo aplicable" y "Potestades, competencias, responsabilidades, funciones, atribuciones y/o tareas", ambas de la sección "Marco Normativo", a objeto de dar cumplimiento con lo previsto en el artículo 7º de la Ley Nº 20.285 sobre Acceso a la Información Pública y en el artículo 51 de su Reglamento.

ANÓTESE

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

RAFAEL ARAYA BUGUEÑO
SUBDIRECTOR NACIONAL (S)
CONSEJO NACIONAL DE LA CULTURA Y LAS ARTES

OCL/ASV
Resol. Nº 04/964
Distribución:
- Gabinete Ministro Presidente, CNCA
- Subdirección Nacional, CNCA
- Departamento de Fomento de la Cultura y las Artes, CNCA
- Departamento de Ciudadanía Cultural, CNCA
- Departamento de Educación y Formación en Artes y Cultura, CNCA
- Departamento de Pueblos Originarios, CNCA
- Departamento de Patrimonio Cultural, CNCA
- Departamento de Planificación y Presupuesto, CNCA
- Departamento de Estudios, CNCA
- Departamento de Administración y Finanzas, CNCA
- Departamento Jurídico, CNCA
- Departamento de Gestión y Desarrollo de las Personas, CNCA
- Departamento de Comunicaciones, CNCA
- Direcciones Regionales CNCA, Regiones I, II, III, IV, V, VI, VII, VIII, IX, X, XI, XII, XIV, XV y R.M.
- Unidad de Auditoría Interna, CNCA