"Decenio de las Personas con Discapacidad en el Perú"
"Año de la Consolidación del Mar de Grau"

CONADIS Consejo Nacional para la Integración de la persona con discapacidad
OFICINA DE ASESORÍA JURÍDICA
04 OCT 2016
RECIBIDO
Reg. N° ..... Folios ..... 408

# Resolución de Presidencia

## N° 077 -2016-CONADIS/PRE

Lima, 03 OCT. 2016

**VISTOS:**

El Memorando N° 1730-2015-CONADIS/OAD de la Oficina de Administración, el Informe N° 127-2016-CONADIS/OPP de la Oficina de Planeamiento y Presupuesto, el Informe N° 0064-2016-CONADIS/OAD-UTI de la Unidad de Tecnología e Informática, y el Informe N° 199-2016-CONADIS/OAJ de la Oficina de Asesoría Jurídica; y,

**CONSIDERANDO:**

Que, el "Plan de Desarrollo de la Sociedad de la Información en el Perú - La Agenda Digital Peruana 2.0", aprobado mediante Decreto Supremo N° 066-2011-PCM, entre sus diversos objetivos, establece la necesidad de promover una Administración Pública de calidad orientada a la población, determinando entre sus estrategias, la implementación de mecanismos para mejorar la seguridad de la información y la necesidad de contar con una Estrategia Nacional de Ciberseguridad con el objetivo de minimizar los riesgos en caso de sufrir algún tipo de incidente en los recursos informáticos del Estado, así como, la disuasión del crimen cibernético, que se producen mediante el uso de redes teleinformáticas, entre otros;

Que, la Política Nacional de Gobierno Electrónico 2013-2017, aprobada por el Decreto Supremo N° 081-2013-PCM, prevé determinados Lineamientos Estratégicos para el Gobierno Electrónico en el Perú, siendo entre otros, la Seguridad de la Información, la cual busca velar por la integridad, seguridad y disponibilidad de los datos, debiendo establecerse lineamientos de seguridad de la información con la finalidad de aminorar el riesgo de exposición de información sensible del ciudadano;

Que, mediante Resolución N° 129-2014-CNB–INDECOPI, la Comisión de Normalización y de Fiscalización de Barreras Comerciales No Arancelarias del Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual - Indecopi, aprobó entre otras, la Norma Técnica Peruana, NTP-ISO/IEC 27001:2014, Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad dela Información. Requisitos. 2ª. Edición, con el objeto especificar los requisitos para establecer, implementar, mantener y mejorar permanentemente un sistema de gestión de la seguridad de la información, dentro del contexto de la organización;

Que, a través de la Resolución Ministerial N° 004-2016-PCM, se aprobó el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014, Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª Edición", en todas las entidades integrantes del Sistema Nacional de Informática, dentro de las cuales están comprendidas las Oficinas Sectoriales de Estadística e Informática y demás Oficinas de Estadística e Informática de los Ministerios, de los Organismos Centrales, Instituciones Públicas Descentralizadas y Empresas del Estado, conforme al artículo 6 del Decreto Legislativo N° 604, Ley de Organización y Funciones del Instituto Nacional de Estadística e Informática; asimismo, determina que

# Resolución de Presidencia

## N° 077 -2016-CONADIS/PRE

cada entidad designará un Comité de Gestión de Seguridad de la Información, cuyas funciones serán establecidas de acuerdo a la Norma Técnica Peruana "NTP ISO/IEC 27001:2014;

Que, el artículo 63 de la Ley N° 29973, Ley General de la Persona con Discapacidad, establece que el Consejo Nacional para la Integración de la Persona con Discapacidad – Conadis es el órgano especializado en cuestiones relativas a la discapacidad; estando constituido como un organismo público ejecutor adscrito al Ministerio de la Mujer y Poblaciones Vulnerables, con autonomía técnica, administrativa, de administración, económica y financiera; constituyendo un pliego presupuestario;

Que, mediante la Resolución de Presidencia N° 048-2016-CONADIS/PRE de fecha 17 de junio de 2016, se conformó el Comité de Gestión de Seguridad de la Información del Consejo Nacional para la Integración de la Persona con Discapacidad – Conadis, el mismo que tiene entre sus funciones formular y proponer la aprobación de la política de seguridad de la información; para lo cual, en la Sesión de fecha 30 de junio de 2016, propuso el proyecto de Directiva que regula el procedimiento para el buen uso y seguridad de la información del personal del Consejo Nacional para la Integración de la Persona con Discapacidad – Conadis; lo cual cuenta con la opinión favorable de la Oficina de Planeamiento y Presupuesto;

Con la visación de la Secretaría General, de la Oficina de Administración, de la Oficina de Planeamiento y Presupuesto y de la Oficina de Asesoría Jurídica; y

De conformidad con lo dispuesto por la Ley N° 29973, Ley General de la Persona con Discapacidad, su Reglamento aprobado por el Decreto Supremo N° 002-2014-MIMP, el Decreto Legislativo N° 604, Ley de Organización y Funciones del Instituto Nacional de Estadística e Informática, el Decreto Supremo N° 066-2011-PCM, que aprueba el Plan de Desarrollo de la Sociedad de la Información en el Perú - La Agenda Digital Peruana 2.0, el Decreto Supremo N° 081-2013-PCM, que aprueba la Política Nacional de Gobierno Electrónico 2013-2017, la Resolución Ministerial N° 004-2016-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP ISO/ICE 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad dela Información. Requisitos. 2ª. Edición", la Resolución N° 129-2014/CNB-INDECOPI, que aprueba Normas Técnica Peruanas sobre tecnología de la información, alimentos obtenidos por medios biotecnológicos modernos y otros, el Reglamento de Organización y Funciones del Consejo Nacional para la Integración de la Persona con Discapacidad – Conadis, aprobado por Decreto Supremo N° 002-2016-MIMP y la Resolución Suprema N° 003-2016-MIMP;

**SE RESUELVE:**

**Artículo 1.- APROBAR** la Directiva N° 11-2016-CONADIS/PRE, "Procedimientos para el buen uso y seguridad de la información del personal del Consejo Nacional para la Integración de la Persona con Discapacidad", la misma que, en

# Resolución de Presidencia

## Nº 077 -2016-CONADIS/PRE

documento adjunto y debidamente visada, forma parte integrante de la presente Resolución.

**Artículo 2.- DISPONER** que la Oficina de Administración, a través de la Unidad de Tecnología e Informática, publique la presente Directiva en el Portal Institucional del Consejo Nacional para la Integración de la Persona con Discapacidad – Conadis (www.conadisperu.gob.pe).

**Artículo 3.- DISPONER** que la Oficina de Administración, a través de la Unidad de Tecnología e Informática se encargue de la difusión, seguimiento y cumplimiento de las disposiciones contenidas en la Directiva aprobada en la presente Resolución.

**Artículo 4.- NOTIFICAR** la presente Resolución de Presidencia a los Órganos, Unidades Orgánicas, Órganos Desconcentrados y Centro de Educación Técnico Productivo – CETPRO "Alcides Salomón Zorrilla" del Consejo Nacional para la Integración de la Persona con Discapacidad – Conadis, para su conocimiento y cumplimiento.

Regístrese, comuníquese y cúmplase

CECILIA BARBIERI QUINO
PRESIDENTA (e)
CONSEJO NACIONAL PARA LA INTEGRACIÓN
DE LA PERSONA CON DISCAPACIDAD

# Resolución de Presidencia

## Nº 077 -2016-CONADIS/PRE

Directiva N° 11 -2016-CONADIS/PRE

**"PROCEDIMIENTOS PARA EL BUEN USO Y SEGURIDAD DE LA INFORMACION DEL PERSONAL DEL CONSEJO NACIONAL PARA LA INTEGRACIÓN DE LA PERSONA CON DISCAPACIDAD"**

**Formulada por:** Unidad de Tecnología e Informática (UTI)

## I. OBJETIVO

Establecer normas que permitan regular los procedimientos para el buen uso y seguridad de la información del personal del Consejo Nacional para la Integración de la Persona con Discapacidad - Conadis.

## II. FINALIDAD

Crear una cultura de seguridad institucional, a fin de que el personal del Consejo Nacional para la Integración de la Persona con Discapacidad – Conadis, que maneja información de carácter secreta, reservada o confidencial, o que careciendo de dicho carácter conforme a la Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública, resulte privilegiada por su contenido relevante, asuma una responsabilidad activa en su buen uso y seguridad.

## III. BASE LEGAL

**3.1** Constitución Política del Perú.
**3.2** Ley N° 29973, Ley General de la Persona con Discapacidad.
**3.3** Ley N° 27815, Ley del Código de Ética de la Función Pública.
**3.4** Ley N° 28493, Ley que regula el uso del correo electrónico comercial no solicitado (SPAM).
**3.5** Ley N° 27269, Ley de Firmas y Certificados Digitales.
**3.6** Ley N° 30096, Ley de Delitos Informáticos.
**3.7** Ley N° 28716, Ley de Control Interno de las Entidades del Estado.
**3.8** Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública.
**3.9** Ley N° 29733, Ley de Protección de Datos Personales.
**3.10** Decreto Supremo N° 002-2014-MIMP, que aprueba el Reglamento de la Ley General de la Persona con Discapacidad.
**3.11** Decreto Supremo N°002-2016-MIMP, aprueba el Reglamento de Organización y Funciones (ROF) del Consejo Nacional para la Integración de la Persona con Discapacidad – Conadis.
**3.12** Decreto Supremo N° 033-2005-PCM, que aprueba el Reglamento de la Ley del Código de Ética de la Función Pública.
**3.13** Decreto Supremo N° 031-2005-MTC, que aprueba el Reglamento de la Ley que regula el uso del correo electrónico comercial no solicitado (SPAM).
**3.14** Decreto Supremo N° 052-2008-PCM, que aprueba el Reglamento de la Ley de Firmas y Certificados Digitales.

# Resolución de Presidencia

## Nº 077 -2016-CONADIS/PRE

**3.15** Decreto Supremo N° 043-2003-PCM, que aprueba el Texto Único Ordenado de la Ley de Transparencia y Acceso a la Información Pública.

**3.16** Decreto Supremo N° 072-2003-PCM, que aprueba el Reglamento de la Ley de Transparencia y Acceso a la Información Pública.

**3.17** Decreto Supremo N° 003-2013-JUS, que aprueba la Ley de Protección de Datos Personales.

**3.18** Resolución Ministerial N° 004-2016-PCM, aprueba el uso obligatorio de la Norma Técnica Peruana "NTP ISO/ICE 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad dela Información. Requisitos. 2ª. Edición", en todas las entidades integrantes del Sistema Nacional de Informática.

**3.19** Resolución N° 129-2014/CNB-INDECOPI, que aprueba Normas Técnica Peruanas sobre tecnología de la información, alimentos obtenidos por medios biotecnológicos modernos y otros.

**3.20** Resolución Jefatural N° 088-2003-INEI, que aprueba la Directiva N° 005-2003-INEI/DTNP, Normas para el uso de Servicio de Correo Electrónico en las Entidades de la Administración Pública.

**3.21** Resolución de Contraloría Nº 0320-2006-CG, que aprueba las Normas de Control Interno.

## IV. ALCANCE

La presente Directiva es de aplicación para todos los Órganos, Unidades Orgánicas, Órganos Desconcentrados y Centro de Educación Técnico Productivo – CETPRO "Alcides Salomón Zorrilla" del Consejo Nacional para la Integración de la Persona con Discapacidad – Conadis.

## V. DISPOSICIONES GENERALES

Los procedimientos establecidos en la presente directiva tienen por objeto establecer lineamientos, medidas, técnicas y metodologías de organización de las tecnologías de la información y de las personas (usuarios) que hacen uso de la información que es proporcionada por el Conadis, con la finalidad de minimizar los riesgos en el uso y manejo de la información de la entidad.

### 5.1 Definiciones operativas

**5.1.1** Contraseña (password): Es una cadena de caracteres que es utilizada para iniciar una sesión en un equipo y obtener acceso a archivos, programas y otros recursos.

**5.1.2** Copia de respaldo (backup): Copia de los datos de un archivo automatizado en un soporte que posibilite su recuperación.

**5.1.3** Correo electrónico (e-mail): Es un servicio de red que permite a los usuarios enviar y recibir mensajes y archivos rápidamente, denominados mensajes

# Resolución de Presidencia

## Nº 077 -2016-CONADIS/PRE

electrónicos o cartas electrónicas, a través de sistemas de comunicación electrónicos.

**5.1.4** Correo web: Es un programa de ordenador usado para leer y enviar mensajes de correo electrónico, que provee una interfaz web por la que se accede al mencionado correo.

**5.1.5** Dato: Es una representación simbólica (numérica, alfabética, algorítmica) de un atributo o variable cuantitativa; asimismo, los datos describen hechos empíricos, sucesos y entidades, siendo un valor o referente que recibe el computador por diferentes medios.

**5.1.6** Dominio: Conjunto de computadoras conectadas en una red informática que confían a uno de los equipos de dicha red, la administración de los usuarios y los privilegios que cada uno de los usuarios tiene en dicha red, asociada a un grupo de dispositivos o equipos conectados a la red Internet.

**5.1.7** Información Privilegiada: Información a la que los servidores y funcionarios acceden en el ejercicio de sus funciones y que por tener carácter secreta, reservada o confidencial conforme a ley, o careciendo de dicho carácter, resulte privilegiada por su contenido relevante, y que por tanto sea susceptible de emplearse en beneficio propio o de terceros, directa o indirectamente.

**5.1.8** Hardware: Se refiere a las partes físicas tangibles de un sistema informático, entre las que están comprendidas sus componentes eléctricos, electrónicos, electromecánicos y mecánicos.

**5.1.9** Malware (código malicioso o software mal intencionado): software que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario.

**5.1.10** Navegador web (browser): Programa que permite el acceso a internet, interpretando la información de archivos y sitios web para que estos puedan ser leídos; entre los más utilizados se encuentran: Microsoft Explorer, Google Chrome, Mozilla, Firefox, Opera, entre otros.

**5.1.11** Nube (cloud): Servicio que funciona a través de internet que permite a los usuarios guardar información de cualquier de tipo.

**5.1.12** Recursos informáticos: Son todos aquellos elementos de hardware y software que constituyen el medio de uso del usuario para poder realizar sus actividades, procesos administrativos dentro de una organización.

**5.1.13** Red informática: Denominada a la red de computadoras, también llamada red de ordenadores o red de comunicaciones de datos, definido como el conjunto de equipos informáticos y software conectados entre sí por medio de

# Resolución de Presidencia

## Nº 077-2016-CONADIS/PRE

dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios.

**5.1.14** Servidor de red: Es un equipo que ofrece varios recursos compartidos de computadoras y otros servidores en una red informática.

**5.1.15** Sistema informático: Sistema integrado por hardware, software y recursos humanos (administrador de la red informática y el personal de soporte técnico).

**5.1.16** Software: Equipamiento lógico o soporte lógico de un sistema informático, que comprende el conjunto de los componentes lógicos que hacen posible la realización de tareas específicas, en contraposición a los componentes físicos que son llamados hardware.

**5.1.17** Spam (correo basura o mensaje basura): Mensajes no solicitados, no deseados o de remitente no conocido (correo anónimo), habitualmente de tipo publicitario, generalmente enviados en grandes cantidades (masivas) que perjudican de alguna o varias maneras al receptor del mismo.

**5.1.18** UserID (Usuario): Identidad de un usuario específico, el cual es generado por la primera letra de su nombre y el primer apellido completo del mismo; en caso de haber similitud entre los usuarios se opta por utilizar el segundo nombre o segundo apellido.

**5.1.19** Usuario: Denominación para los servidores y funcionarios del Consejo Nacional para la Integración de la Persona con Discapacidad – Conadis, que se encuentran debidamente registrados en el sistema informático de la entidad, a través de una cuenta de usuario y con una contraseña de acceso al mismo.

**5.1.20** Usuario externo: Persona natural que, sin tener una vinculación con la institución, presta servicios al Conadis sin relación de subordinación, el mismo que se encuentra registrado en el sistema informático a través de una cuenta de usuario y una contraseña de acceso a determinados recursos de la red previamente autorizados por la autoridad de la institución.

**5.1.21** Virus informático: Es un código malicioso o software mal intencionado, que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario.

### 5.2 De la Unidad de Tecnología e Informática (UTI)

**5.2.1** La Unidad de Tecnología e Informática es la responsable de planificar, administrar e implementar las tecnologías de la información y comunicación

# Resolución de Presidencia

## Nº 077 -2016-CONADIS/PRE

para contribuir al logro de los objetivos institucionales. Asimismo, desarrolla sistemas de información y brinda opinión y asistencia técnica al Conadis en cuanto a tecnologías de la información y comunicación - TIC´s aplicadas a la temática de discapacidad.

**5.2.2** Conforme al marco establecido en la presente Directiva, la Unidad de Tecnología e Informática (UTI), como responsable de la Infraestructura de TIC´s, desempeñara las siguientes funciones:

a) Asignación de las cuentas y accesos a los recursos informáticos del Conadis.

b) Administrar y asegurar los recursos de la red informática, garantizando su integridad, disponibilidad y operatividad.

c) Capacitar a los servidores y funcionaros del Conadis en materia de seguridad de la Red Informática, uso del correo electrónico institucional y accesos lógicos.

### 5.3 Procedimientos sobre seguridad y control

Los procedimientos considerados en la presente directiva son seis (6) y corresponden a:

- De los Procedimientos de Seguridad para el Personal.
- De los Procedimientos de Seguridad de Resguardo y Protección de la Información.
- De la Seguridad de la red informática.
- De los Procedimientos de Controles de Acceso Lógico.
- De los Procedimientos del Cumplimiento de la Seguridad Informática.
- Otras Consideraciones.

## VI. DISPOSICIONES ESPECÍFICAS

### 6.1 De los Procedimientos de Seguridad para el Personal

Todo el personal del Conadis que utilice y/o maneje Información Privilegiada de propiedad de la entidad previamente aceptará las condiciones del uso adecuado de los recursos informáticos, observando el estricto cumplimiento de la presente directiva.

#### 6.1.1 Sobre los Usuarios

6.1.1.1 La Unidad de Recursos Humanos deberá remitir a la Unidad de Tecnología e Informática (UTI) la relación de servidores y/o funcionarios que se incorporen al Conadis dentro del plazo de 72 horas de iniciadas sus labores

# Resolución de Presidencia

## Nº 077-2016-CONADIS/PRE

en el Conadis, a fin de brindar los derechos correspondientes y activación (alta) de acceso a la red (DOMINIO Conadis), cuenta de correo y acceso a la información correspondiente.

6.1.1.2 Asimismo, la Unidad de Recursos Humanos deberá remitir a la Unidad de Tecnología e Informática (UTI), la relación de servidores y/o funcionarios que han dejado de laborar en la entidad, dentro del plazo de 72 horas de finalizadas sus labores en el Conadis, para la desactivación (baja) de sus cuentas de correo y accesos a la red institucional, bajo responsabilidad; también, en el mismo plazo la Unidad de Recursos Humanos deberá informar del personal que se encuentra con licencia y/o vacaciones.

6.1.1.3 Todo el personal que ingresa a la institución será capacitado (inducción) por la Unidad de Tecnología e Informática (UTI) sobre los procedimientos y estándares de seguridad de la información para Usuarios del Consejo Nacional de Integración para la Persona con Discapacidad - Conadis, así como de las obligaciones y sanciones que en caso de incumplimiento.

6.1.1.4 En aquellos casos en que el personal del Conadis sea reasignado o rotado a otra dirección, gerencia o área de la entidad, una vez que la Unidad de Tecnología e Informática (UTI) haya tomado conocimiento del hecho, esta dará de "baja" a los accesos, aplicaciones, sistemas y/o archivos compartidos que utilizo la persona.

Asimismo, la Unidad de Tecnología e Informática (UTI) dará al personal reasignado o rotado el "alta" correspondiente a los accesos a las aplicaciones, sistemas y/o archivos compartidos que sean requeridos por el jefe inmediato.

En los casos antes descritos, la Unidad de Tecnología e Informática (UTI) mantendrá activos la cuenta de correo y el acceso a la red.

6.1.1.5 Para efectuar los procedimientos de activación (alta) y desactivación (baja) de los servidores y/o funcionarios del Conadis, se utilizará el formato: "FORM-CONADIS-UTI-001-V1: Alta y baja de Servicios a Usuarios" (Anexo N° 1)

### 6.2 De los Procedimientos de Seguridad de Resguardo y Protección de la Información

**6.2.1** El usuario deberá proteger la información que se encuentre en las diferentes unidades de almacenamiento y que estén bajo su administración o permiso de uso, aun cuando no se utilicen y contengan Información Privilegiada.

**6.2.2** Es responsabilidad del usuario evitar en todo momento la fuga de información propiedad del Conadis que se encuentran almacenadas en los equipos de

# Resolución de Presidencia

## Nº 077 -2016-CONADIS/PRE

cómputo asignados a su nombre; por lo cual, deberán proteger toda Información Privilegiada que por necesidades institucionales deba ser almacenada o trasmitida, ya sea dentro de la red Conadis, redes externas o internet.

**6.2.3** Los usuarios deberán asegurar que toda la Información Privilegiada se encuentre guardada en los servidores de red de propiedad del Conadis, designados para tal fin; asimismo, la Unidad de Tecnología e Informática (UTI) no será responsable por la pérdida de información que no se halle dentro de los servidores antes mencionados.

**6.2.4** En caso de una ocurrencia de pérdida de información dentro de los servidores de red del Conadis, el usuario podrá solicitar la recuperación de a mismas, indicando el nombre del archivo y la ruta donde se encontraba el mismo para su recuperación en los sistemas de respaldo de la entidad.

**6.2.5** Todo medio de ingreso y salida de datos (puertos USB, lectoras de discos digitales, disqueteras, lectoras de mini SDs, entre otros) de las equipos informáticos (PC's, laptops, tabletas, entre otros) del Conadis, serán restringidos salvo previa autorización del Jefe inmediato del área solicitado a la Unidad de Tecnología e Informática (UTI).

**6.2.6** El usuario no brindará directamente información institucional a externos bajo criterio de "Transparencia", ya que la misma solo podrá ser entregada conforme a los canales establecidos por Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública.

**6.2.7** El usuario que tenga conocimiento de un incidente de seguridad informática deberá reportarlo de forma inmediata a la Unidad de Tecnología e Informática (UTI), brindando el detalle de lo ocurrido.

**6.2.8** El usuario que tenga conocimiento que Información Privilegiada de la entidad ha sido expuesta, modificada, alterada o borrada sin la autorización de las áreas responsables de la misma, deberá reportarlo de forma inmediata a la Unidad de Tecnología e Informática (UTI).

### 6.3 De la Seguridad de la red informática

**6.3.1** Se considerará como ataque a la seguridad informática y por consecuencia una falta grave, cualquier actividad no autorizada por la Unidad de Tecnología e Informática (UTI), en la cual el usuario realice la exploración de los recursos informáticos de la red del Conadis, así como todo lo que se encuentre sobre dicha red operando, con fines de detectar y explotar una posible vulnerabilidad.

# Resolución de Presidencia

## Nº 077 -2016-CONADIS/PRE

**6.3.2** También se considerará como una vulneración a la seguridad informática y por consecuencia una falta grave, si el usuario ingresa sin el permiso correspondiente con algún equipo informático (PC's, laptops, tabletas, entre otros) que no sea de propiedad del Conadis y que este sea conectado a la red informática de la entidad sin autorización.

**6.3.3 Del Uso del Correo Electrónico**

6.3.3.1 El correo electrónico institucional es una herramienta de comunicación e intercambio de información oficial entre personas, no es una herramienta de difusión indiscriminada de información, con la excepción de las listas de interés establecidas por el Conadis para fines institucionales.

6.3.3.2 Las cuentas de correo electrónico institucional deben usarse para actividades que estén relacionadas con el cumplimiento de las funciones asignadas a los servidores y funcionarios en el Consejo Nacional para la Integración de la Persona con Discapacidad – Conadis.

6.3.3.3 Los mensajes que contienen los correos electrónicos deben ser manejados como una comunicación privada y directa entre emisor y receptor.

6.3.3.4 El usuario no utilizará las cuentas de correo electrónico institucional asignados a otros usuarios, ni tampoco tendrá permitido que éste reciba mensajes en cuentas de otros correos de la institución.

6.3.3.5 Los usuarios podrán enviar vía correo electrónico Información Privilegiada de clasificación secreta, reservada o confidencial conforme a la Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública, siempre y cuando la misma sea remitida en forma encriptada, destinada exclusivamente a personas autorizadas de acuerdo a sus funciones y atribuciones.

6.3.3.6 Sera considerada como una falta grave la acción de falsear, esconder, suprimir o sustituir la identidad de un usuario de una cuenta de correo electrónico del Conadis.

6.3.3.7 Sera considerada como una falta grave el interceptar, revelar o ayudar a terceros a interceptar o revelar las comunicaciones efectuadas a través de los correos electrónicos institucionales.

6.3.3.8 Sera considerado una falta el utilizar la cuenta de correo institucional para suscribirse a grupos o listas de interés personal, catálogos, para recibir ofertas de productos, para recibir publicidad o para cualquier actividad que no esté relacionada a las labores institucionales.

# Resolución de Presidencia

## Nº 077 -2016-CONADIS/PRE

6.3.3.9 El Consejo Nacional para la Integración de la Persona con Discapacidad – Conadis, a través de la Unidad de Tecnología e Informática (UTI), podrá implementar filtros de correos Spam o bloquear correos electrónicos que puedan poner en riesgo la seguridad de la Red informática del Conadis.

6.3.3.10 El usuario deberá manejar los mensajes de correo electrónico y los archivos adjuntos a estos, como propiedad del Consejo Nacional para la Integración de la Persona con Discapacidad – Conadis;

6.3.3.11 El usuario que reciba un correo electrónico con archivos adjuntos de dudoso contenido o un correo electrónico Spam, deberá abstenerse de abrirlo y reportar a la brevedad el hecho a la Unidad de Tecnología e Informática (UTI); asimismo, el usuario será responsable por lo sucedido en la red institucional, de comprobarse que debido a estos correos se causó algún perjuicio en su operatividad y funcionamiento.

### 6.3.4 Del Uso de la Internet

6.3.4.1 El acceso a Internet que se brinda a los usuarios del Conadis, es de uso exclusivo para las actividades relacionadas con las funciones que desempeñan.

6.3.4.2 Todos los accesos a Internet serán provistos a través de los canales de acceso brindados por la Unidad de Tecnología e Informática (UTI).

6.3.4.3 Los usuarios que accedan a Internet de la institución deberán reportar o comunicar todo los incidentes de seguridad informática a la Unidad de Tecnología e Informática (UTI), describiendo el incidente.

6.3.4.4 Los usuarios que utilicen el servicio de Internet institucional aceptan lo siguiente:

a) Estarán sujetos al monitoreo de las actividades que se realicen en Internet.
b) Tienen pleno conocimiento que están prohibidos al acceso de páginas no autorizadas.
c) Tienen pleno conocimiento que está prohibido la transmisión de Información Privilegiada de la entidad no autorizada, o subirlos a la Nube (cloud).
d) Tienen pleno conocimiento que está prohibido la descarga de software sin la autorización de la Unidad de Tecnología e Informática (UTI).
e) El uso del Internet institucional no es para uso con propósitos personales.

# Resolución de Presidencia

## Nº 077-2016-CONADIS/PRE

### 6.4 De los Procedimientos de Controles de Acceso Lógico

Los usuarios son responsables de los mecanismos de control de acceso que el Conadis proporciona; esto es, su identidad como usuario (UserID) y la contraseña (password) para acceder a la información y a la infraestructura tecnológica de la institución; por lo cual, el uso de dichos mecanismos de acceso deberá efectuarse con la reserva pertinente.

Los permisos de acceso a la información que se encuentran en la infraestructura tecnológica del Conadis, serán proporcionados por la Unidad de Tecnología e Informática (UTI) conforme a las solicitudes que efectúen los jefes inmediatos de cada área responsable de la información, los mismos que definirán los permisos mínimos y necesarios para que los usuarios desempeñen sus funciones.

### 6.4.1 De los Controles de Acceso Lógico

6.4.1.1 Los usuarios se identificarán por los mecanismos de control de acceso provistos por la Unidad de Tecnología e Informática (UTI) para el uso de la infraestructura tecnológica de la institución, para lo cual, estos contaran con una credencial de usuario (UserID) única y personalizado, la cual es creada y otorgada por la Unidad de Tecnología e Informática (UTI) para acceder a la infraestructura tecnológica de la institución, la misma que podrá ser utilizada por otros usuarios.

6.4.1.2 Los usuarios son totalmente responsables de todas las actividades realizadas con su credencial de usuario (UserID), debiendo inhibirse de divulgar sus credenciales de usuario y prohibir que otras personas utilicen estas; asimismo, están impedidos de utilizar la credencial de usuario (UserID) de otros servidores o funcionarios de la entidad.

6.4.1.3 Los usuarios no tienen permitido brindar información a terceros ajenos al Conadis, de los medios de control de acceso a la infraestructura tecnológica de la institución, salvo por autorización del jefe inmediato previa coordinación con la Unidad de Tecnología e Informática (UTI).

### 6.4.2 Niveles de acceso

Para efectuar los cambios de acceso (roles y responsabilidades) a la infraestructura tecnológica de la institución de los usuarios, las solicitudes deberán ser formuladas por el jefe inmediato o superior a la Unidad de Tecnología e Informática (UTI).

# Resolución de Presidencia

## Nº 077 -2016-CONADIS/PRE

### 6.4.3 De la Administración y Uso de Contraseñas

6.4.3.1 La asignación de contraseñas (password) será efectuada por la Unidad de Tecnología e Informática (UTI), la misma que se realizará de manera individual a cada usuario, en sobre cerrado, las mismas que deberán ser cambiadas en el momento por el usuario, estando prohibido el uso compartido de estas contraseñas.

6.4.3.2 En los casos que el usuario olvide su contraseña (password) o bloquee su ingreso al sistema, debido al límite de intentos de acceso, deberá solicitar a la Unidad de Tecnología e Informática (UTI) que se le proporcione una nueva contraseña (password) de acceso.

6.4.3.3 El usuario deberá asegurarse que su contraseña (password) sea segura, para lo cual es recomendable que esta tenga las siguientes características:

a) Fáciles de recordar.
b) Contar con un mínimo de ocho (8) caracteres de extensión.
c) Combinar letras, números, mayúsculas y minúsculas.
d) Deben ser distintas en cada acceso diferente.
e) Deberán ser cambiadas por lo menos cada sesenta (60) días.

6.4.3.4 Está prohibido, bajo responsabilidad del usuario, que las contraseñas que se encuentran en cualquier medio escrito se expongan en lugares de alto tránsito de personas no autorizadas.

6.4.3.5 Las contraseñas (password) no deberán ser compartidas y/o reveladas, ya que se responsabilizará al usuario que brindó la misma de todas las acciones y usos que se realicen.

6.4.3.6 Cuando el usuario tenga la presunción de que su contraseña es conocida por otra persona, deberá informar sobre el hecho a la Unidad de Tecnología e Informática (UTI) con el fin de efectuar el cambio de la misma.

6.4.3.7 Por seguridad, y bajo responsabilidad los usuarios no deberán almacenar sus contraseñas en ningún aplicativo, programas o sistema.

### 6.4.4 De los Controles de Accesos Remotos

6.4.4.1 La administración o acceso remoto de equipos del Consejo Nacional para la Integración de la Persona con Discapacidad – Conadis conectados a internet no está permitida.

6.4.4.2 En aquellos casos, que este acceso remoto se otorgue, este deberá contar con la autorización del jefe inmediato en coordinación con la Unidad de Tecnología e Informática (UTI), quien deberá indicar si se cuentan con los

# Resolución de Presidencia

## Nº 077 -2016-CONADIS/PRE

mecanismos apropiados de control de acceso seguro de acuerdo a las normas de seguridad.

Asimismo, el jefe de área que brinde la autorización del acceso remoto, será el responsable de las actividades que se realicen con el mismo, mientras dure.

### 6.5 De los Procedimientos del Cumplimiento de la Seguridad Informática

La Unidad de Tecnología e Informática (UTI), tiene la función de revisar y proponer el cumplimiento de los procedimientos, normas y políticas de seguridad, que garanticen acciones preventivas y correctivas para la salvaguarda de equipos e instalaciones de computo, así como la información y el banco de datos que se encuentren en los mismos.

### 6.5.1 De la Propiedad Intelectual

El Consejo Nacional para la Integración de la Persona con Discapacidad – Conadis tiene los derechos de propiedad intelectual sobre todos los sistemas, aplicativos, manuales, y documentos físicos digitalizados desarrollados por los usuarios y usuarios externos que se encuentren en las plataformas informáticas de la institución, el uso o disposición de los mismos, deberá ser autorizado por la entidad.

### 6.5.2 De las Revisiones del Cumplimiento

6.5.2.1 El Comité de Gestión de Seguridad de la Información del Consejo Nacional para la Integración de la Persona con Discapacidad – Conadis, tendrá la función de revisar el cumplimiento de los procedimientos, políticas, normas y estándares de seguridad informática convenientes y cualquier otro requerimiento de seguridad.

6.5.2.2 La Unidad de Tecnología e Informática (UTI) es responsable de supervisar el cumplimiento de los manuales de procedimientos, políticas y estándares de Seguridad Informática y de la Información, que se implementen o estén implementados.

6.5.2.3 La Unidad de Tecnología e Informática (UTI) podrá implementar herramientas de control que identifiquen tendencias y determinen estadísticas respecto al uso de los recursos informáticos de parte de los usuarios, con el fin de verificar las actividades de los mismos en los procesos que ejecutan y la estructura de los archivos que estos procesan.

De la misma forma, el mal uso de los recursos informáticos que se detecten será reportado conforme a lo determinado en la presente directiva.

# Resolución de Presidencia

**Nº 077 -2016-CONADIS/PRE**

### 6.5.3 Infracciones de seguridad informática

6.5.3.1 Está prohibido el uso de herramientas informáticas (hardware y software) para vulnerar los controles de seguridad informática.

6.5.3.2 Está prohibido que los usuarios realicen pruebas de fallas de vulnerabilidad o fallas de seguridad informática.

6.5.3.3 Está prohibido que los usuarios escriban, generen, copien, coleccionen, propaguen, ejecuten o introduzcan cualquier tipo de código (programa) conocidos como virus, (gusanos o caballos de Troya, entre otros), desarrollados para auto replicar, dañar o afectar el funcionamiento o acceso a los equipos de cómputo, redes o información de la entidad.

## 6.6 Otras Consideraciones

### 6.6.1 Para el Acceso al Correo Electrónico Institucional

El usuario que acceda a su correo electrónico institucional vía correo web (internet) desde lugares públicos, deberá tener los cuidados correspondientes al ingresar su credencial de usuario (UserID) y contraseña (password), verificando que personas ajenas no estén observando las mismas; asimismo, al término de la sesión el usuario deberá comprobar que haya cerrado adecuadamente la misma, siendo el usuario responsable de las consecuencias que se puedan presentar el uso de su acceso.

### 6.6.2 Accesos Temporales, Controles y Forzado de Claves

6.6.2.1 El usuario al ausentarse de su lugar de labores, deberá mantener su equipo de cómputo con controles de acceso al mismo, como contraseñas o protectores de pantalla, previamente instalados y autorizados por la Unidad de Tecnología e Informática (UTI).

6.6.2.2 El usuario que utilice de manera temporal un equipo de cómputo que no le fue asignado y pertenezca a otro usuario que se encuentre ausente por diferentes motivos, deberá tener en cuenta lo siguiente:

a) Contar con la autorización del jefe del área, quien deberá solicitar a la Unidad de Tecnología e Informática (UTI) el cambio temporal de la contraseña (password) del equipo de cómputo, indicando los motivos y tiempo que dure el uso del equipo.

b) El jefe del área que autorice el uso del equipo asignado a otro usuario, es responsable de todas las actividades que realice el usuario asignado temporalmente a este equipo.

# Resolución de Presidencia

## Nº 077 -2016-CONADIS/PRE

6.6.2.3 Las contraseñas de acceso (passwords) solo podrán ser cambiadas por la Unidad de Tecnología e Informática (UTI) en las siguientes circunstancias.

a) Cuando el servidor o funcionario ya no labore en la institución y la cuenta haya sido dada de baja.

b) Cuando concurran una o más infracciones descritas en el punto 6.5.3 de la presente directiva.

c) Cuando sea requerido por auditorías, investigaciones o peritajes.

## VII. DISPOSICIONES COMPLEMENTARIAS

**7.1** El personal de Soporte Técnico y Administrador de Red de informática de la Unidad de Tecnología e Informática (UTI), es responsable de brindar el apoyo correspondiente, en la solución técnica de incidencias, en la seguridad de la red informática, correo electrónico y los accesos lógicos.

**7.2** En el caso de detectarse el uso indebido de la información, de los accesos a internet/intranet/extranet y del correo electrónico, la Unidad de Tecnología e Informática (UTI) bloqueará estos servicios y comunicará a los jefes inmediatos y superiores del usuario infractor, a fin de que se efectúen las acciones administrativas, civiles y/o penales.

**7.3** En caso falta grave del usuario, la Unidad de Tecnología e Informática (UTI) procederá a anular todos los accesos definitivamente, sin perjuicio de las responsabilidades administrativas, civiles y/o penales a que hubiera lugar.

## VIII. RESPONSABILIDADES

**8.1** El Jefe de la Unidad de Tecnología e Informática (UTI) y el Oficial de Seguridad de la Información, serán responsables de velar por el cumplimiento y actualización de la presente directiva, estando encargados de garantizar la seguridad de la información de la red informática en el ámbito institucional.

**8.2** Los Directores, Gerentes y Jefes de Unidades de los diferentes Órganos y Unidades Orgánicas del Consejo Nacional para la Integración de la Persona con Discapacidad – Conadis, son responsables de cumplir y supervisar el cumplimiento de las disposiciones de la presente directiva.

**8.3** El usuario y el usuario externo del sistema informático del Consejo Nacional para la Integración de la Persona con Discapacidad – Conadis, son responsables de cumplir las disposiciones de la presente Directiva.

# Resolución de Presidencia

**Nº 077 -2016-CONADIS/PRE**

## IX. ANEXOS

Anexo N° 1: FORM-CONADIS-UTI-001-V1: Alta y baja de Servicios a Usuarios.

# FORMATO DE ALTAS Y BAJAS DE USUARIO

**UTI - 2016**

N° AT: | FECHA : / /

**1.USUARIO**

**UNIDAD ORGANICA**

**2 ESTADO DE USUARIO**

NUEVO ☐ ROTACION ☐ BAJA ☐

**3.ESTADO DE CUENTAS**

| HABILITACION ☐ | DESABILITACION ☐ |
|---|---|

| | PERFIL | | PERFIL |
|---|---|---|---|
| ☐ CUENTA DE RED | | ☐ CUENTA SIAF | |
| ☐ CORREO INSTITU. | | ☐ S.T.D | |
| ☐ KIMETIC | | ☐ DICOM | |
| ☐ SPIJ | | ☐ OTROS | |

| HABILITACION | PERFIL | DESABILITACION | PERFIL |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |

ENTREGA DE SOBRE CON CLAVE (S) ☐ CAMBIO DE CLAVE (S) POR EL USUARIO ☐

**3.PROGRAMAS INSTALADOS**

| | | | |
|---|---|---|---|
| OFFICE | ☐ | MELISA | ☐ |
| S.T.D | ☐ | DICOM | ☐ |
| SIAF | ☐ | JAWS | ☐ |
| KIMETIC | ☐ | OTROS | ☐ |

| OTROS |
|---|
| |

**4.DESARROLLO DE LABORES**

Inicio: / / Hora: Fin: / / Hora:

OBSERVACIONES :

**5. SITUACIÓN:**

At. Abierta ☐ At. Cerrada ☐

Firma Usuario

Firma Técnico

CONADIS PRESIDENCIA

OFICINA ASESORIA JURIDICA V°B° CONADIS

CONADIS V°B° PLANEAMIENTO Y PRESUPUESTO OFICINA DE

SECRETARIA GENERAL V°B° CONADIS