Lima, 11 de Noviembre del 2022

RESOLUCIÓN DE SECRETARIA GENERAL N° D000074-2022-CONADIS-SG

VISTOS:

El Informe N° D000001-2022-CONADIS-UTI-HBM y los Memorandos N° D000226 y D000248-2022-CONADIS-UTI, emitidos por la Unidad de Tecnología e Informática; el Informe N° D000006-2022-CONADIS-OPP-LCM y el Memorando N° D000438-2022-CONADIS-OPP, emitidos por la Oficina de Planeamiento y Presupuesto; y el Informe Nº D000352-2022-CONADIS-OAJ, emitido por la Oficina de Asesoría Jurídica; y,

CONSIDERANDO:

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 – (en adelante CONADIS), es el órgano especializado en cuestiones relativas a la discapacidad. Está constituido como un organismo público ejecutor adscrito al Ministerio de la Mujer y Poblaciones Vulnerables, con autonomía técnica, administrativa, de administración, económica y financiera;

Que, mediante el artículo 1 del Decreto Legislativo N° 1412, que aprueba la Ley de Gobierno Digital, establece que, la presente Ley tiene por objeto establecer el marco de gobernanza del gobierno digital para la adecuada gestión de la identidad digital, servicios digitales, arquitectura digital, interoperabilidad, seguridad digital y datos, así como el régimen jurídico aplicable al uso transversal de tecnologías digitales en la digitalización de procesos y prestación de servicios digitales por parte de las entidades de la Administración Pública en los tres niveles de gobierno;

Que, los numerales 6.1 y 6.2 del artículo 6 de la citada norma establecen que, el gobierno digital es el uso estratégico de las tecnologías digitales y datos en la Administración Pública para la creación de valor público. Se sustenta en un ecosistema compuesto por actores del sector público, ciudadanos y otros interesados, quienes apoyan en la implementación de iniciativas y acciones de diseño, creación de servicios digitales y contenidos, asegurando el pleno respeto de los derechos de los ciudadanos y personas en general en el entorno digital; y, comprende el conjunto de principios, políticas, normas, procedimientos, técnicas e instrumentos utilizados por las entidades de la Administración Pública en la gobernanza, gestión e implementación de tecnologías digitales para la digitalización de procesos, datos, contenidos y servicios digitales de valor para los ciudadanos;

Que, mediante, la Resolución Ministerial N° 004-2016-PCM, se aprueba el uso obligatorio de la Norma Técnica Peruana NTPISO/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;

V° B°
Firmado digitalmente por RUIZ ATAU Jessica Melina FAU 20433270461 soft
Motivo: Doy V° B°
Fecha: 11.11.2022 13:59:06 -05:00

V° B°
Firmado digitalmente por DIAZ FUENTES Kim Vladimir FAU 20433270461 soft
Motivo: Doy V° B°
Fecha: 11.11.2022 13:24:43 -05:00

V° B°
Firmado digitalmente por PIRO MARCOS Sandra Pilar FAU 20433270461 soft
Motivo: Doy V° B°
Fecha: 11.11.2022 12:23:21 -05:00

Que, en cumplimiento de las normas citadas en los considerandos precedentes mediante la Resolución de Presidencia N° 077-2016-CONADIS/PRE del 03 de octubre de 2016, se aprueba 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 (en adelante la Directiva" (en adelante la Directiva N° 11-2016-CONADIS/PRE); la citada Directiva tiene como objeto establecer normas que permitan regular los procedimientos para el buen uso y seguridad de la información de los usuarios del CONADIS;

Que, a través de la Resolución de Presidencia N° 027-2020-CONADIS/PRE del 05 de junio de 2020, se aprueba el Plan de Gobierno Digital del Consejo Nacional para la Integración de la Persona con Discapacidad – PDG CONADIS 2020 – 2023, en el cual se precisa que uno de los desafíos o retos del CONADIS para el desarrollo del gobierno digital, es garantizar la seguridad de la Información;

Que, con la Resolución de Presidencia N° D000048-2022-CONADIS-PRE del 12 de abril de 2022, se aprueba el Plan de Implementación del Reglamento de Organización y Funciones del CONADIS (en adelante ROF del CONADIS), en el cual se incluye el cronograma que contempla entre otras actividades la evaluación para la actualización de documentos normativos (Directivas lineamientos u otros);

Que, dentro de este marco normativo la Unidad de Tecnología e Informática, a través, del Informe N° D000001-2022-CONADIS-UTI-HBM y de los Memorandos N° D000226 y D000248-2022-CONADIS-UTI, realizo la revisión y actualización de la Directiva N° 11-2016-CONADIS/PRE:

Que, conforme a lo dispuesto en el numeral 7.2.3, de la Directiva N° 003-2021-CONADIS-SG: "Normas y Procedimientos para la Formulación, Modificación y Aprobación de los Documentos Normativos en el CONADIS", aprobada por la Resolución de Secretaría General N° 025-2021-CONADIS-SG (en adelante, la Directiva N° 003-2021-CONADIS-SG), la citada Unidad remite adjunto al referido informe: **a)** Proyecto de documento "Procedimientos para el Buen Uso y Seguridad de la Información del Personal del CONADIS" modificado y/o actualizado (en formato PDF visado y el documento con versión editable). **b)** Informe técnico que sustenta la propuesta de modificación y/o actualización el cual contiene el Cuadro Nº 001 – Análisis Comparativo "Procedimientos para el Buen Uso y Seguridad de la Información del Personal del CONADIS" con la justificación técnico y legal. **c)** Informe técnico de la Unidad de Recursos Humanos emitiendo opinión técnica respecto al Proyecto de Directiva, como unidad involucrada;

Que, mediante el Memorando N° D000438-2022-CONADIS-OPP la Oficina de Planeamiento y Presupuesto remite el Informe N° D000006-2022-CONADIS-OPP-LCM, emite opinión favorable referente al proyecto de modificación y/o actualización de la Directiva N° 011-2016-CONADIS/PRE, precisando que se ha elaborado dentro de los parámetros funcionales que le competen a la Unidad de Tecnología e Informática de acuerdo con las disposiciones de la Directiva N° 003-2021-CONADIS-PRE;

Que, en cumplimiento de lo dispuesto en el numeral 7.3.4 de la Directiva N° 003-2021-CONADIS-SG, la Oficina de Asesoría Jurídica, a través, del Memorando N° D000242-2022-CONADIS-OAJ, remitió las observaciones realizadas a la propuesta

de directiva a la Unidad de Tecnología e Informática, quien las subsanó mediante el Memorando N° D000248-2022-CONADIS-UTI;

Que, dentro de los cambios propuestos por la Unidad de Tecnología e Informática se encuentra el de la denominación de la directiva, la misma que originalmente se aprobó como 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"; sin embargo, la unidad proponente opina que se debe modificar su denominación por "Procedimientos para el Buen Uso y Seguridad de la Información en el Consejo Nacional Para la Integración de la Persona con Discapacidad - CONADIS";

Que, posteriormente a la emisión de la Directiva N° 11-2016-CONADIS/PRE, se aprueba la Directiva N° 003-2021-CONADIS-SG, que en su subnumeral 6.5 del numeral 6 dispone que la Secretaría General es responsable de aprobar las propuestas de documentos normativos de gestión interna, cuando el órgano proponente es uno de Administración Interna;

Que, mediante el Informe N° D000352-2022-CONADIS-OAJ, la Oficina de Asesoría Jurídica, concluye que resulta jurídicamente viable aprobar la Directiva denominada "Procedimientos para el Buen Uso y Seguridad de la Información del Consejo Nacional para la Integración de la Persona con Discapacidad - CONADIS". Asimismo, precisa que, corresponde que la aprobación de la Directiva propuesta por la Unidad de Tecnología e Informática, la cual es un órgano de Administración Interna, sea aprobada por la Secretaría General en cumplimiento del subnumeral 6.5 del numeral 6 de la Directiva N° 003-2021-CONADIS-SG;

Que, mediante la Resolución de Presidencia Nº D000148-2022-CONADIS-PRE del 08 de noviembre de 2022 se deroga la Resolución de Presidencia N° 077-2016-CONADIS/PRE que aprobó 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";

Con el visto bueno de la Unidad de Tecnología e Informática, de la Oficina de Planeamiento y Presupuesto y la Oficina de Asesoría Jurídica; y,

De conformidad con lo dispuesto en la Ley N° 29973, Ley General de la Persona con Discapacidad y modificatorias; la Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado; el Decreto Legislativo N° 1412, que aprueba la Ley de Gobierno Digital y modificatoria y su Reglamento, aprobado mediante Decreto Supremo N° 029-2021-PCM; la Resolución Ministerial N° 004-2016-PCM, que aprueba la Norma Técnica Peruana NTPISO/IEC-27001:2014. Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª. Edición; el Texto Integrado del Reglamento de Organización y Funciones del Consejo Nacional para la Integración de la Persona con Discapacidad - CONADIS, aprobado por la Resolución de Presidencia N° D000052-2022-CONADIS-PRE; la Directiva N° 003-2021-CONADIS-SG: "Normas y Procedimientos para la Formulación, Modificación y Aprobación de los Documentos Normativos en el CONADIS";

SE RESUELVE:

Artículo 1.- APROBAR la Directiva Nº D000004-2022-CONADIS/SG, Directiva denominada "Procedimientos para el Buen Uso y Seguridad de la Información del Consejo Nacional para la Integración de la Persona con Discapacidad - CONADIS", conforme al Anexo adjunto que forma parte integrante de la presente Resolución.

Artículo 2.- DISPONER la publicación de la presente Resolución y su Anexo, en el Portal Institucional del Consejo Nacional para la Integración de la Persona con Discapacidad (https://www.gob.pe/mimp/conadis), hecha la publicación, la directiva entrara en vigencia.

Regístrese, comuníquese y cúmplase.

RICARDO JAVIER FLORES HERRERA
Secretario General (e)
Consejo Nacional para la Integración de la Persona con Discapacidad
(DOCUMENTO CON FIRMA DIGITAL)

Lima, 11 de Noviembre del 2022

DIRECTIVA N° D000004-2022-CONADIS-SG

DIRECTIVA DENOMINADA:

""Procedimientos para el Buen Uso y Seguridad de la Información del Consejo Nacional para la Integración de la Persona con Discapacidad - CONADIS"

Formulada por: Oficina de Tecnologías de la Información (OTI)

V° B°
Firmado digitalmente por RUIZ ATAU Jessica Melina FAU 20433270461 soft
Motivo: Doy V° B°
Fecha: 11.11.2022 13:58:42 -05:00

V° B°
Firmado digitalmente por DIAZ FUENTES Kim Vladimir FAU 20433270461 soft
Motivo: Doy V° B°
Fecha: 11.11.2022 13:25:00 -05:00

V° B°
Firmado digitalmente por PIRO MARCOS Sandra Pilar FAU 20433270461 soft
Motivo: Doy V° B°
Fecha: 11.11.2022 12:29:38 -05:00

I. OBJETIVO

Establecer normas que permitan regular los procedimientos para el buen uso y seguridad de la información por parte de los usuarios del Consejo Nacional para la integración de la Persona con Discapacidad - CONADIS.

II. FINALIDAD

Crear una cultura de seguridad institucional, a fin de que los usuarios del 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° 27269, Ley de Firmas y Certificados Digitales y sus modificatorias.
3.3 Ley N° 27815, Ley del Código de Ética de la Función Pública y sus modificatorias.
3.4 Ley N° 28493, Ley que regula el uso del correo electrónico comercial no solicitado (SPAM) y sus modificatorias.
3.5 Ley N° 28716, Ley de Control Interno de las Entidades del Estado y sus modificatorias.
3.6 Ley N° 29733, Ley de Protección de Datos Personales y sus modificatorias.
3.7 Ley N° 29973, Ley General de la Persona con Discapacidad y sus modificatorias.
3.8 Ley N° 30096, Ley de Delitos Informáticos.
3.9 Decreto Supremo N° 072-2003-PCM, que aprueba el Reglamento de la Ley de Transparencia y Acceso a la Información Pública y sus modificatorias.
3.10 Decreto Supremo N° 031-2005-MTC, que aprueba el Reglamento de la Ley que regula el uso del correo electrónico comercial no solicitado (SPAM).
3.11 Decreto Supremo N° 033-2005-PCM, que aprueba el Reglamento de la Ley del Código de Ética de la Función Pública y sus modificatorias.
3.12 Decreto Supremo N° 052-2008-PCM, que aprueba el Reglamento de la Ley de Firmas y Certificados Digitales y sus modificatorias.
3.13 Decreto Supremo N° 003-2013-JUS, que aprueba el Reglamento de la Ley de Protección de Datos Personales.
3.14 Decreto Supremo N° 002-2014-MIMP, que aprueba el Reglamento de la Ley General de la Persona con Discapacidad y sus modificatorias.
3.15 Decreto Supremo N° 021-2019-JUS, que aprueba el Texto Único Ordenado de la Ley de Transparencia y Acceso a la información Pública.
3.16 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 de la información. Requisitos. 2º. Edición", en todas las entidades integrantes del Sistema Nacional de informática y sus modificatorias.
3.17 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.
3.18 Resolución de Contraloría N° 0320-2006-CG, que aprueba las Normas de Control Interno.
3.19 Resolución de Presidencia N° D000052-2022-CONADIS-PRE, aprueba el Texto Integrado del Reglamento de Organización y Funciones (ROF) del Consejo Nacional para la integración de la Persona con Discapacidad — Conadis.
3.20 Resolución N° 129-2014/CNB-INDECOPI, que aprueba Normas Técnica Peruanas sobre tecnología de la información, alimentos obtenidos por medios biotecnológicos modernos y otros.

IV. ALCANCE

La presente Directiva es de aplicación a todas las unidades de organización del CONADIS.

V. GLOSARIO DE TERMINOS

5.1 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.

5.2 Correo electrónico (e-mail): Es un servicio de red que permite a los usuarios enviar y recibir mensajes y archivos rápidamente, denominados mensajes electrónicos o cartas electrónicas, a través de sistemas de comunicación electrónicos.

5.3 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.

5.4 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.

5.5 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.

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

5.7 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.

5.8 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.

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

5.10 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.

5.11 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 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.

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

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

5.14 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.

5.15 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.

5.16 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.

5.17 Usuario: Denominación para los servidores y funcionarios del 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.

5.18 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.

5.19 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.

5.20 TIC's: Tecnologías de Información y Comunicaciones, se refieren a las técnicas y herramientas utilizadas para la transmisión de información. Entiéndase a Internet o las telecomunicaciones como TIC.

5.21 Equipo informático: Está formado por distintos dispositivos electrónicos que permiten la ejecución de programas informáticos.

VI. DISPOSICIONES GENERALES

6.1 De la Oficina de Tecnologías de la Información (OTI)

6.1.1 La Oficina de Tecnologías de la Información es la responsable de conducir, desarrollar, implementar y supervisar los sistemas de información, base de datos, infraestructura tecnológica y telecomunicaciones.

6.1.2 Conforme al marco establecido en la presente Directiva, la Oficina de Tecnologías de la Información (OTI), 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) Supervisar, administrar y mantener la capacidad, disponibilidad, continuidad y seguridad de la infraestructura tecnológica de redes de comunicaciones, plataforma tecnológica de los portales de la entidad, servicios informáticos, entre otros.

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

6.2 Procedimientos sobre seguridad y control

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

- De los Procedimientos de Seguridad para los usuarios
- 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.

VII. DISPOSICIONES ESPECÍFICAS

7.1 De los Procedimientos de Seguridad para los usuarios

Todos los usuarios del CONADIS que utilicen y/o manejen 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.

7.1.1 Sobre los Usuarios

7.1.1.1 La Unidad de Recursos Humanos deberá remitir a la Oficina de Tecnologías de la Información (OTI) la relación de servidores civiles, secigristas y practicantes que se incorporen a la entidad, dentro del plazo de 72 horas de iniciadas sus labores y/o prácticas correspondientes, a fin de aperturar y activar (alta) los accesos a la red (DOMINIO CONADIS), cuenta de correo y carpetas compartidas correspondientes.

7.1.1.2 Asimismo, la Unidad de Recursos Humanos deberá remitir a la Oficina de Tecnologías de la Información (OTI), la relación de servidores civiles, secigristas y practicantes desvinculados de la entidad, dentro del plazo de 72 horas de finalizadas sus labores y/o prácticas correspondientes, para desactivar (baja) sus cuentas de correo y accesos a la red institucional, bajo responsabilidad; también, dentro del mismo plazo la Unidad de Recursos Humanos deberá informar la relación y el periodo de los usuarios que se encuentran con licencia y/o vacaciones.

7.1.1.3 Todo el personal que ingresa a la institución será capacitado (inducción) por la Oficina de Tecnologías de la Información (OTI) sobre los procedimientos y estándares de seguridad de la información para usuarios del CONADIS, así como de las obligaciones y sanciones en caso de incumplimiento.

7.1.1.4 En aquellos casos en que los usuarios del CONADIS sea reasignado o rotado a otra unidad de organización, una vez que la Oficina de Tecnologías de la Información (OTI) haya tomado conocimiento del hecho, esta dará de “baja” a los accesos, aplicaciones, sistemas y/o archivos compartidos que utilizo la persona.

Asimismo, la Oficina de Tecnologías de la Información (OTI) dará al usuario 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 Oficina de Tecnologías de la Información (OTI) mantendrá activos la cuenta de correo y el acceso a la red.

7.1.1.5 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: Formato de Altas y bajas de servicios a usuarios" (Anexo N° 1)

7.2 De los Procedimientos de Seguridad de Resguardo y Protección de la información

7.2.1 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.

7.2.2 Es responsabilidad del usuario evitar en todo momento la fuga de información propiedad del CONADIS que se encuentran almacenadas en los equipos de 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.

7.2.3 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 Oficina de Tecnologías de la Información (OTI) no será responsable por la pérdida de información que no se halle dentro de los servidores antes mencionados.

7.2.4 En caso de una ocurrencia de pérdida de información dentro de los servidores de red del CONADIS, el usuario podrá solicitar la recuperación de las 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.

7.2.5 Todo medio de ingreso y salida de datos (puertos USB, lectoras de discos digitales, disqueteras, lectoras, entre otros) de los equipos informáticos (PC’s, laptops, tabletas, entre otros) del CONADIS, serán restringidos salvo previa autorización del jefe inmediato del área solicitado a la Oficina de Tecnologías de la Información (OTI).

7.2.6 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 la Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública.

7.2.7 El usuario que tenga conocimiento de un incidente de seguridad informática deberá reportarlo de forma inmediata a la Oficina de Tecnologías de la Información (OTI), brindando el detalle de lo ocurrido.

7.2.8 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 Oficina de Tecnologías de la Información (OTI).

7.3 De la Seguridad de la red informática

7.3.1 Se considerará como ataque a la seguridad informática y por/en consecuencia una falta grave, a cualquier actividad no autorizada por la Oficina de Tecnologías de la Información (OTI), 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.

7.3.2 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.

7.3.3 **Del Uso del Correo Electrónico**

7.3.3.1 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.

7.3.3.2 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 CONADIS.

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

7.3.3.4 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.

7.3.3.5 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.

7.3.3.6 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.

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

7.3.3.8 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.

7.3.3.9 El CONADIS, a través de la Oficina de Tecnologías de la Información (OTI), podrá implementar filtros de correos Spam o bloquear correos electrónicos que puedan poner en riesgo la seguridad de la Red informática del CONADIS.

7.3.3.10 El usuario deberá manejar los mensajes de correo electrónico y los archivos adjuntos a estos, como propiedad del CONADIS.

7.3.3.11 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 Oficina de Tecnologías de la Información (OTI); 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.

7.3.4 Del Uso de la Internet

7.3.4.1 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.

7.3.4.2 Todos los accesos a Internet serán provistos a través de los canales de acceso brindados por la Oficina de Tecnologías de la Información (OTI).

7.3.4.3 Los usuarios que accedan a Internet de la institución deberán reportar o comunicar todos los incidentes de seguridad informática a la Oficina de Tecnologías de la Información (OTI), describiendo el incidente.

7.3.4.4 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 está/n prohibido/s el/al acceso a/de páginas no autorizadas.
c) Tienen pleno conocimiento que está prohibido la transmisión de Información Privilegiada de la entidad que no ha sido debidamente autorizada, o subir dicha información a la Nube (cloud).
d) Tienen pleno conocimiento que está prohibido la descarga e instalación de software sin la autorización de la Oficina de Tecnologías de la Información (OTI).
e) El uso del Internet institucional no es para uso con propósitos personales.

7.4 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 Oficina de Tecnologías de la Información (OTI) 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.

7.4.1 De los Controles de Acceso Lógico

7.4.1.1 Los usuarios se identificarán por los mecanismos de control de acceso provistos por la Oficina de Tecnologías de la Información (OTI) para el uso de la infraestructura tecnológica de la institución, para lo cual, estos contaran con una credencial de usuario (UserID) única y personalizado/a, la cual es creada y otorgada por la Oficina de Tecnologías de la Información (OTI) para acceder a la infraestructura tecnológica de la institución, la misma que no podrá ser utilizada por otros usuarios.

7.4.1.2 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.

7.4.1.3 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 Oficina de Tecnologías de la Información (OTI).

7.4.2 **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 Oficina de Tecnologías de la Información (OTI).

7.4.3 **De la Administración y Uso de Contraseñas**

7.4.3.1 La asignación de contraseñas (password) será efectuada por la Oficina de Tecnologías de la Información (OTI), 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.

7.4.3.2 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 Oficina de Tecnologías de la Información (OTI) que se le proporcione una nueva contraseña (password) de acceso.

7.4.3.3 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.

7.4.3.4 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.

7.4.3.5 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.

7.4.3.6 Cuando el usuario tenga la presunción de que su contraseña es conocida por otra persona, deberá informar sobre el hecho a la Oficina de Tecnologías de la Información (OTI) con el fin de efectuar el cambio de la misma.

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

7.4.4 **De los Controles de Accesos Remotos**

7.4.4.1 La administración o acceso remoto de los equipos informáticos del CONADIS conectados a internet no está permitida.

7.4.4.2 En aquellos casos, que este acceso remoto se otorgue, este deberá contar con la autorización del jefe inmediato en coordinación con la Oficina de Tecnologías de la Información (OTI), quien deberá indicar si se cuentan con los 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.

7.5 De los Procedimientos del Cumplimiento de la Seguridad informática

La Oficina de Tecnologías de la Información (OTI), 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 los equipos e instalaciones de cómputo, así como la información y el banco de datos que se encuentren en los mismos.

7.5.1 **De la Propiedad Intelectual**

El 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.

7.5.2 **De las Revisiones del Cumplimiento**

7.5.2.1 El Comité de Gobierno Digital del 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.

7.5.2.2 La Oficina de Tecnologías de la Información (OTI) 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.

7.5.2.3 La Oficina de Tecnologías de la Información (OTI) 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.

7.5.3 **Infracciones de seguridad informática**

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

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

7.5.3.3 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.

7.6 Otras Consideraciones

7.6.1 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 (UserlD) 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 por el uso de sus credenciales y contraseña durante su acceso.

7.6.2 Accesos Temporales, Controles y Forzado de Claves

7.6.2.1 El usuario al ausentarse de su lugar de labores, deberá mantener su equipo de cómputo con controles de acceso, como contraseñas o protectores de pantalla, previamente instalados y autorizados por la Oficina de Tecnologías de la Información (OTI).

7.6.2.2 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 Oficina de Tecnologías de la Información (OTI) 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.

7.6.2.3 Las contraseñas de acceso (passwords) solo podrán ser cambiadas por la Oficina de Tecnologías de la Información (OTI) 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 7.5.3 de la presente directiva.

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

VIII. DISPOSICIONES COMPLEMENTARIAS

8.1 El personal de Soporte Técnico y Administrador de Red de informática de la Oficina de Tecnologías de la Información (OTI), 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.

8.2 En el caso de detectarse el uso indebido de la información, de los accesos a internet/intranet/extranet y del correo electrónico, la Oficina de Tecnologías de la Información (OTI) 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.

8.3 En caso de falta grave por parte del usuario, la Oficina de Tecnologías de la Información (OTI) procederá a anular todos los accesos definitivamente, sin perjuicio de las responsabilidades administrativas, civiles y/o penales a que hubiera lugar.

8.4 Los aspectos no contemplados en la presente Directiva serán resueltos por la Oficina de Tecnologías de la Información (OTI).

IX. RESPONSABILIDADES

9.1 El jefe de la Oficina de Tecnologías de la Información (OTI) y el Oficial de Seguridad Digital, 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.

9.2 Los Directores, Gerentes y Jefes de Unidades de los diferentes Órganos y Unidades Orgánicas del CONADIS, son responsables de cumplir y supervisar el cumplimiento de las disposiciones de la presente directiva.

9.3 El usuario y el usuario externo del sistema informático del CONADIS, son responsables de cumplir las disposiciones de la presente Directiva.

X. ANEXOS

Anexo N° 1. FORM-CONADIS-UTI-001-V1: Formato de Altas y bajas de servicios a usuarios.

CONADIS

OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN (OTI)

La columna "***No***" se utiliza para la baja o eliminación de los accesos.
De no marcar con una "X" en el casillero "***Si***", se asumirá que no se autorizan dichos accesos.

N° DE SOLICITUD

ANEXO N° 1
FORM-CONADIS-UTI-001-V1
Formato de altas y bajas de servicios a usuarios

Resolución Ministerial N°246-2007-PCM que aprueba la NTP-ISO/IEC 17799:2007 "*Código de buenas prácticas para la gestión de la Seguridad de la Información. 2a Edición* "

Versión 1.0

Fecha:

DATOS DEL ÁREA SOLICITANTE:

Oficina / Dirección:

Apellidos y Nombres del Director / Jefe:

Unidad / Sub Dirección:

Apellidos y Nombres del Jefe / Coordinador:

DATOS DEL USUARIO A ASIGNAR/RETIRAR SERVICIOS:

Apellido Paterno:

Apellido Materno:

Nombres:

DNI / Pasaporte:

Cargo:

Anexo :

Condición Laboral: ☐ CAS ☐ Practicante ☐ **Servicio Terceros** u otro tipo de Contrato

Atención: En el caso de ***Servicio Terceros*** o que el beneficiario del servicio mantenga un tipo de contrato que no sea CAS, Practicante, se debe remitir un Memorándum y/o correo institucional al Director(a) de la Oficina de Tecnologias de la Información, solicitando los accesos.

ESTADO DE RECURSOS INFORMÁTICOS:

Requerimiento: CREACIÓN ☐ ROTACIÓN ☐ BAJA ☐

Indique Usuario:

Servicios a solicitar:	Si	No		Si	No		Si	No
Acceso a Red	☐	☐						
Correo electrónico			Acceso Correo CONADIS	☐	☐	Acceso Correo mediante el Celular	☐	☐
Acceso Telefónico			Salida Externa	☐	☐	Llamada a Celular	☐	☐
Internet Alámbrico	☐		Internet Inalámbrico	☐				

Número de anexo telefónico

Marque con una "X" los accesos a incluir o retirar. Puede marcar más de una opción:

4:Audio y Video.	**3**:Redes Sociales.	**2**:Páginas en general (Públicas y Privadas).	**1**:Páginas solo gobierno.

La solicitud de acceso a internet se asigna a base de las necesidades del área solicitante y cargo que lo requiere. Los accesos marcados como 4 y 3 serán aprobados por el/la Director(a) de la Oficina de Tecnologias de la Información.

Acceso a Servidor de Archivos — Si ☐ No ☐

En caso marcar "SI" para el acceso al Servidor de Archivos, debe especificar la relación de Archivos, según tabla adjunta.

TABLA DE RECURSOS COMPARTIDOS DE INFORMACIÓN - CONSEJO NACIONAL PARA LA INTEGRACION DE LA PERSONA CON DISCAPACIDAD - CONADIS

NOMBRE DEL RECURSO COMPARTIDO	PRIVILEGIO DE ACCESO		NOMBRE DEL RECURSO COMPARTIDO	PRIVILEGIO DE ACCESO	
	LECTURA (L)	ESCRITURA (E)		LECTURA (L)	ESCRITURA (E)

De requerir alguna carpeta adicional que no se indique en la tabla adjunta, sírvase indicarlo a continuación:

ASIGNACIÓN/RETIRO DE ACCESOS A SISTEMAS DE INFORMACIÓN:

Requerimiento: CREACIÓN ☐ ROTACIÓN ☐ BAJA ☐

Sistemas a solicitar → Indique Usuario: _____

Sistema de Gestión Administrativa (SIGA) del MEF	Si / No	**Accesos al SIGA**: Debe ser visado por la Unidad de Abastecimiento de la Oficina de Administración, autorizándose el uso del SIGA, en el área de visado al final de este documento.
Sistema de Integrado de Administración Financiera (SIAF)	Si / No	**Accesos al SIAF**: Debe ser visado por la Oficina de Planeamiento, Presupuesto y Modernización, autorizándose el uso del SIAF, en el área de visado al final de este documento.
Sistema de Gestión Documental (SGD)	Si / No	**Accesos al SGD**: Debe ser visado por la Unidad Funcional de Atencion al Ciudadano y Gestion Documental de la Oficina de Administración, autorizándose el uso del SGD, en el área de visado al final de este documento.
Sistema Peruano de Información Juridica (SPIJ)	Si / No	**Accesos al SPIJ**: Debe ser visado por la Oficina de Asesoría Jurídica, autorizándose el uso del SPIJ, en el área de visado al final de este documento.

Otros Sistemas/Módulos/Perfil

.....
.....
.....

Observaciones

.....
.....
.....

Para uso de los responsables de brindar accesos a recursos informáticos de otras áreas

_____ **V° B° Director(a) de la Unidad de Abastecimiento para los casos que se requiere el SIGA**	_____ **V° B° Director(a) de la Oficina de Planeamiento y Presupuesto para los casos que se requiere el SIAF**	_____ **V° B° Coordinador(a) de la UF de Atención al Cuidadano y Gestión Documental para los casos que se requiere el SGD**	_____ **V° B° Director(a) de la Oficina de Asesoría Jurídica para los casos que se requiere el SPIJ**

OBSERVACIONES: _____

_____

Para uso del área técnica de la OTI - Para ser llenado durante la atención del requerimiento de accesos

_____ **V° B° Recepción OTI** Fecha : _____	_____ **V° B° Especialista OTI** Fecha : _____	_____ **V° B° Director(a) de la OTI** **Fecha :** _____

OBSERVACIONES: _____

_____

Autorizaciones del área solicitante

_____ **V° B° Director(a) o Jefe(a) de la Oficina / Dirección del solicitante**	_____ **V° B° Jefe(a) o Coordinador(a) de la Unidad / Sub Dirección del solicitante**

De requerir apoyo en el llenado de este formulario, puede comunicarse al correo instirucional apoyouti03@conadisperu.gob.pe