Municipalidad Provincial de Canchis

RESOLUCIÓN DE GERENCIA MUNICIPAL N° 0346-2022-GM-MPC

Sicuani, 07 de diciembre de 2022.

VISTO:

La Resolución de Alcaldía N° 232-2022-MPC de fecha 15/06/2022; Informe N° 0103-2021-SGTIS/GAF-MPC de fecha 18/05/2022; Informe N° 22-GPP-SGPRyCT-MPC-2022 de fecha 05/07/2022; Informe Técnico N° 001-2022-SGTIS/GAF-MPC de fecha 06/08/2022; Informe N° 0200-2021-SGTIS/GAF-MPC de fecha 19/08/2022; Informe Técnico N° 34-GPP-SGPRyCT-MPC-2022 de fecha 13/09/2022; Informe N° 374-2022-GPP-MPC de fecha 13/09/2022; Informe N° 374-2022-OAJ-MPC de fecha 20/09/2022; Memorándum N° 2795-2022-GAF/GM-MPC de fecha 23/09/2022; Opinión Legal N° 1021-2022-OAJ-MPC de fecha 23/09/2022 y demás actuados;

CONSIDERANDO:

Que, conforme a lo establecido en el artículo 194° de la Constitución Política del Perú y el Art. II del Título Preliminar de la Ley Orgánica de Municipalidades N° 27972, prevé que los gobiernos locales gozan de autonomía política, económica y administrativa en los asuntos de su competencia. La autonomía que la Constitución del Perú establece para las Municipalidades radica en la facultad de ejercer actos de gobierno, administrativos y de administración con sujeción al ordenamiento jurídico;

Que, el Articulo VIII del Título Preliminar de la Ley N° 27972, Ley Orgánica de Municipalidades, establece que: "Los gobiernos locales están sujetos a las leyes y disposiciones que, de manera general y de conformidad con la Constitución Política del Perú, regulan las actividades y funcionamiento del Sector Público, así como las normas técnicas referidas a los servicios y bienes públicos, y a los sistemas administrativos del Estado que por su naturaleza son de observancia y cumplimiento obligatorio (...)";

Que, asimismo el artículo 26° de la citada Ley, señala que la administración municipal adopta una estructura gerencial sustentándose en principios de programación, dirección, ejecución, supervisión, control concurrente y posterior. Se rige por los principios de legalidad, economía, transparencia, simplicidad eficacia, eficiencia, participación y seguridad ciudadana, y por los contenidos en la Ley N° 27444, así como las facultades y funciones se establecen en los instrumentos de gestión y la Ley N° 27972;

Que, el artículo 39° tercer párrafo del mismo cuerpo normativo, establece que **"las gerencias resuelven los aspectos administrativos a su cargo a través de resoluciones y directivas"**; consecuentemente en ese marco normativo la Gerencia Municipal se encuentra facultado para dictar directivas internas, con ello además contribuir el control interno de la Municipalidad, tal y conforme lo establece la Ley N° 28716 – Ley de Control Interno de las Entidades del Estado que en su artículo 6° indica que son obligaciones del titular y funcionarios de la entidad, relativas a la implementación y funcionamiento de control interno lo establecido en el inciso d) Documentar y divulgar internamente las políticas, normas y procedimientos de gestión y control (...);

Que, de acuerdo al artículo 43° del Reglamento de Organización de Funciones – ROF de la Municipalidad Provincial de Canchis, la Gerencia Municipal es el órgano de dirección, responsable de dirigir la administración municipal y de conducir y direccionar el planeamiento, organización, ejecución, supervisión y evaluación de las acciones y actividades relacionadas con la prestación de los servicios públicos a la comunidad, encargado de cumplir y hacer cumplir las políticas y objetivos de desarrollo socio económico y de gestión municipal aprobados por el concejo municipal. Asimismo, en merito a las funciones y atribuciones de la Gerencia Municipal, el artículo 45° en su numeral 1° señala que la Gerencia Municipal tiene la función y atribución de "Proponer, garantizar, dirigir, supervisar, coordinar y controlar las actividades de los órganos internos a su cargo, en concordancia con las políticas de gestión establecidas y las disposiciones impartidas por el Órgano de Gobierno" y el numeral 10° indica que la Gerencia Municipal tiene la función y atribución de "Proponer todos los instrumentos de Gestión requeridos por Ley para su aprobación según corresponda, mediante Resoluciones de Alcaldía o en Sesión de Concejo Municipal, así como velar por su respectivo desarrollo, implementación y ejecución";

Que, mediante Informe N° 0103-2021-SGTIS/GAF-MPC de fecha 18/05/2022, el Sub Gerente de Tecnologías de Información y Sistemas, presenta ante la Gerencia de Planeamiento y Presupuesto, la

propuesta de Directiva denominada "LINEAMIENTOS PARA EL USO ADECUADO DE EQUIPOS DE CÓMPUTO, SERVICIOS INFORMÁTICOS Y SEGURIDAD DE LA INFORMACIÓN EN LA MUNICIPALIDAD PROVINCIAL DE CANCHIS", la cual será de aplicación para la Sub Gerencia de Tecnologías de Información y Sistemas. Expediente que es proveído ante la Sub Gerencia de Planeamiento, Racionalización y Cooperación Técnica, para su informe técnico;

Que, mediante Informe N° 22-GPP-SGPRyCT-MPC-2022 de fecha 05/07/2022, la encargada de la Sub Gerencia de Planeamiento, Racionalización y Cooperación Técnica, informa ante la Gerencia de Planeamiento y Presupuesto y Sub Gerencia de Tecnologías de Información y Sistemas, que de la revisión y evaluación a la propuesta de la directiva "LINEAMIENTOS PARA EL USO ADECUADO DE EQUIPOS DE CÓMPUTO, SERVICIOS INFORMÁTICOS Y SEGURIDAD DE LA INFORMACIÓN EN LA MUNICIPALIDAD PROVINCIAL DE CANCHIS", presentada por la Sub Gerencia de Tecnologías de Información y Sistemas, se tiene observaciones y recomendaciones, que deben ser implementadas oportunamente por la Unidad Orgánica proponente, ello aplicando la Directiva N° 002-MPC-2015 "DIRECTIVA MARCO PARA LA ELABORACIÓN Y ACTUALIZACIÓN Y APROBACIÓN DE DIRECTIVAS INTERNAS DE LA MUNICIPALIDAD PROVINCIAL DE CANCHIS";

Que, mediante Informe Técnico N° 001-2022-SGTIS/GAF-MPC de fecha 06/08/2022, el Sub Gerente de Tecnologías de Información y Sistemas, alcanza ante la Gerencia de Planeamiento y Presupuesto el informe técnico reformulado respecto a la propuesta de la directiva N° 006-MPC-2022 - "LINEAMIENTOS PARA EL USO ADECUADO DE EQUIPOS DE CÓMPUTO, SERVICIOS INFORMÁTICOS Y SEGURIDAD DE LA INFORMACIÓN EN LA MUNICIPALIDAD PROVINCIAL DE CANCHIS", teniendo en cuenta que la Municipalidad Provincial de Canchis debe contar con un documento administrativo interno de gestión, que regule el uso de la Tecnología, manejo y seguridad de la información, en el ámbito administrativo de la Municipalidad Provincial de Canchis;

Que, mediante Informe N° 0200-2021-SGTIS/GAF-MPC de fecha 19/08/2022, el Sub Gerente de Tecnologías de Información y Sistemas, remite ante la Gerencia de Planeamiento y Presupuesto, el informe técnico de la propuesta de la directiva denominada "LINEAMIENTOS PARA EL USO ADECUADO DE EQUIPOS DE CÓMPUTO, SERVICIOS INFORMÁTICOS Y SEGURIDAD DE LA INFORMACIÓN EN LA MUNICIPALIDAD PROVINCIAL DE CANCHIS", con las observaciones y recomendaciones, levantadas y aplicadas. Expediente que es proveído ante la Gerencia de Planeamiento, Racionalización y Cooperación Técnica, para su informe técnico;

Que, mediante Informe Técnico N° 034-GPP-SGPRyCT-MPC-2022 de fecha 13/09/2022, la encargada de la Sub Gerencia de Planeamiento, Racionalización y Cooperación Técnica, presenta ante la Gerencia de Planeamiento y Presupuesto, el informe técnico favorable respecto a la propuesta de Directiva N° 006-MPC-2022 "LINEAMIENTOS PARA EL USO ADECUADO DE EQUIPOS DE CÓMPUTO, SERVICIOS INFORMÁTICOS Y SEGURIDAD DE LA INFORMACIÓN EN LA MUNICIPALIDAD PROVINCIAL DE CANCHIS" formulada por la Sub Gerencia de Tecnologías de Información y Sistemas. Indicando que esta cumple con las características mínimas establecidas en la Directiva N° 002-MPC-2015 "DIRECTIVA MARCO PARA LA ELABORACIÓN Y ACTUALIZACIÓN Y APROBACIÓN DE DIRECTIVAS INTERNAS DE LA MUNICIPALIDAD PROVINCIAL DE CANCHIS";

Que, mediante Informe N° 374-2022-GPP-MPC de fecha 13/09/2022, el Gerente de Planeamiento y Presupuesto, remite ante la Gerencia Municipal, el informe técnico con opinión favorable a la Directiva N° 006-MPC-2022 "LINEAMIENTOS PARA EL USO ADECUADO DE EQUIPOS DE CÓMPUTO, SERVICIOS INFORMÁTICOS Y SEGURIDAD DE LA INFORMACIÓN EN LA MUNICIPALIDAD PROVINCIAL DE CANCHIS", para su aprobación correspondiente. Expediente que es proveído ante la Oficina de Asesoría Jurídica, para su opinión legal;

Que, mediante Informe N° 374-2022-OAJ-MPC de fecha 20/09/2022, el jefe de la Oficina de Asesoría Jurídica, solicita a la Gerencia de Administración y Finanzas, emita informe de conformidad a la propuesta de Directiva N° 006-MPC-2022 "LINEAMIENTOS PARA EL USO ADECUADO DE EQUIPOS DE CÓMPUTO, SERVICIOS INFORMÁTICOS Y SEGURIDAD DE LA INFORMACIÓN EN LA MUNICIPALIDAD PROVINCIAL DE CANCHIS";

Que, mediante Memorándum N° 2795-2022-GAF/GM-MPC de fecha 23/09/2022, el Gerente de Administración y Finanzas, devuelve el expediente ante la Oficina de Asesoría Jurídica, indicando que la gerencia que dirige, no emite informes de conformidad a las propuestas de directivas, más aun cuando se

evidencia que este ya cuenta con el informe técnico de la Sub Gerencia de Tecnologías de Información y Sistemas como área proponente y la opinión favorable de la Sub Gerencia de Planeamiento, Racionalización y Cooperación Técnica;

Que, mediante Opinión Legal N° 1021-2022-OAJ-MPC de fecha 23/09/2022, el jefe de la Oficina de Asesoría Jurídica, opina por declarar procedente la aprobación de la Directiva N° 006-MPC-2022 "LINEAMIENTOS PARA EL USO ADECUADO DE EQUIPOS DE CÓMPUTO, SERVICIOS INFORMÁTICOS Y SEGURIDAD DE LA INFORMACIÓN EN LA MUNICIPALIDAD PROVINCIAL DE CANCHIS", cuyo objetivo es contar con las directrices y los controles necesarios que permitan orientar a los usuarios de la Municipalidad Provincial de Canchis, para el buen uso de los equipos de cómputo, directrices de seguridad donde se debe mantener la integridad, disponibilidad, privacidad, control y autenticidad de la información manejada en la computadora;

Que, las directivas son documentos normativos elaborados y expedidos por los diversos órganos de la Entidad, precisando políticas institucionales y determinando los procedimientos que deban realizarse en la ejecución de una determinada acción, concordante con las disposiciones legales vigentes. Las disposiciones emitidas por los diferentes órganos de la Entidad enmarcados en asuntos de su competencia que necesariamente deberán ser aprobados mediante el documento técnico normativo denominado "Directiva";

Que, en merito a ello la Municipalidad Provincial de Canchis, cuenta con la Directiva N° 002-MPC-2015 "DIRECTIVA MARCO PARA LA ELABORACIÓN Y ACTUALIZACIÓN Y APROBACIÓN DE DIRECTIVAS INTERNAS DE LA MUNICIPALIDAD PROVINCIAL DE CANCHIS", el que tiene como objetivo establecer lineamientos para la formulación actualización y aprobación de las Directivas internas que se elaboran en las diferentes Unidades Orgánicas de la Municipalidad Provincial de Canchis, directiva que en su numeral 6.4, establece el procedimiento a seguir para la revisión y aprobación de las directivas propuestas, señalando lo siguiente:

a) Las propuestas de las Directivas que cumplan con lo establecido en los numerales precedentes, deberán ser remitidos en medio físico y magnético (CD, correo electrónico corporativo) a la Sub Gerencia de Planeamiento, racionalización y cooperación técnica.
b) La Sub Gerencia de Planeamiento, Racionalización y Cooperación Técnica, de considerarlo necesario podrá solicitar a la Unidad Orgánica que propone la Directiva mejoras en la misma, información adicional y/o reuniones de trabajo con otras unidades orgánicas involucradas.
c) Culminado el proceso de revisión, conjunta y una vez consolidados todos los aportes, la Sub Gerencia de Planeamiento, Racionalización y Cooperación Técnica, remitirá el proyecto de la directiva a la unidad orgánica proponente, otorgando un plazo de 03 días hábiles para la ratificación y V° B° del responsable.
d) Recibida la ratificación correspondiente, la Sub Gerencia de Planeamiento, Racionalización y Cooperación Técnica emitirá un informe técnico con opinión favorable a la Gerencia de Planeamiento y Presupuesto.
e) La Gerencia de Planeamiento y Presupuesto emitirá un informe a la Gerencia Municipal para su revisión y posterior remisión del proyecto de la Directiva a la Oficina de Asesoría Jurídica, adjuntando el informe técnico y la opinión favorable de la Sub Gerencia de Planeamiento, Racionalización y Cooperación Técnica.
f) La Oficina de Asesoría Jurídica, teniendo en consideración el informe técnico sustentatorio de la Unidad Orgánica que propone la Directiva, la opinión técnica favorable de la Sub Gerencia de Planeamiento, Racionalización y Cooperación Técnica y de la Gerencia de Planeamiento y Presupuesto emitirá el dictamen legal correspondiente, dirigido a la Gerencia Municipal.
g) La aprobación de las Directivas, se efectuará mediante Resolución de Alcaldía y/o Resolución de Gerencia Municipal, según sea el caso, previa vización de la Gerencia de Planeamiento y Presupuesto y de la Oficina de Asesoría Jurídica, las mismas que llevarán los sellos y las firmas correspondientes en todos los folios de la directiva aprobado, las mismas que deberán imprimirse en papel membretado de la Municipalidad;

Que, asimismo la Directiva antes mencionada en su numeral 6.5 señala que: a) Las directivas aprobadas tienen vigencia a partir del día siguiente de su aprobación, *salvo que se indique en fecha posterior, de ser el caso debe precisarse*. Ello concordado con el Artículo 44° de la Ley 27972, que respecto a la Publicidad de las normas municipales, señala: (...) Las normas municipales rigen a partir del día siguiente de su publicación, *salvo que la propia norma postergue su vigencia* (...);

Municipalidad Provincial de Canchis

Que, la propuesta de Directiva N° 006-MPC-2022 "LINEAMIENTOS PARA EL USO ADECUADO DE EQUIPOS DE CÓMPUTO, SERVICIOS INFORMÁTICOS Y SEGURIDAD DE LA INFORMACIÓN EN LA MUNICIPALIDAD PROVINCIAL DE CANCHIS", fue formulada por la Sub Gerencia de Tecnologías de Información y Sistemas, la cual cuenta con las opiniones técnicas emitidas por las áreas correspondientes, asimismo se puede observar que la directiva propuesta tiene por objetivo contar con las directrices y los controles necesarios que permitan orientar a los usuarios de la Municipalidad Provincial de Canchis, para el buen uso de los equipos de cómputo, directrices de seguridad donde se debe mantener la integridad, disponibilidad, privacidad, control y autenticidad de la información manejada en la computadora. Así como también tiene la finalidad de definir normas, procedimientos y responsabilidades en el uso y cuidado de equipos de cómputo y periféricos, servicios informáticos en red y seguridad de la información, en todas las dependencias de la Municipalidad Provincial de Canchis;

Por estas consideraciones y en uso de las atribuciones conferidas por la Constitución Política del Estado, la Ley Orgánica de Municipalidades, en cumplimiento del Reglamento de Organización y Funciones, la delegación de facultades encomendadas mediante Resolución de Alcaldía N° 232-2022-MPC, de fecha 15/06/2022, demás informes y normas legales pertinentes;

SE RESUELVE:

ARTÍCULO PRIMERO.- APROBAR la **Directiva N° 006-MPC-2022 "LINEAMIENTOS PARA EL USO ADECUADO DE EQUIPOS DE CÓMPUTO, SERVICIOS INFORMÁTICOS Y SEGURIDAD DE LA INFORMACIÓN EN LA MUNICIPALIDAD PROVINCIAL DE CANCHIS",** cuyo texto forma parte integrante de la presente resolución, la cual entrara en vigencia a partir del día siguiente de su aprobación.

ARTÍCULO SEGUNDO.- DEJAR SIN EFECTO cualquier acto administrativo y/o acto de administración que contravenga la presente.

ARTÍCULO TERCERO.- DISPONER que la Sub Gerencia de Tecnologías de Información y Sistemas, Gerencia de Administración y Finanzas, Gerencia de Planeamiento y Presupuesto, Sub Gerencia de Planeamiento, Racionalización y Cooperación Técnica, den estricto cumplimiento a la presente Directiva.

ARTÍCULO CUARTO.- DISPONER que la Gerencia de Planeamiento y Presupuesto y Sub Gerencia de Planeamiento, Racionalización y Cooperación Técnica, realicen la custodia, reproducción, difusión y distribución de la presente directiva, a todas las Unidades Orgánicas de la Municipalidad que tengan incidencia con la emisión de este acto resolutivo.

ARTÍCULO QUINTO.- NOTIFICAR la presente resolución a las áreas correspondientes de la Municipalidad Provincial de Canchis, para la implementación de las acciones que correspondan según sus atribuciones.

ARTÍCULO SEXTO.- DISPONER que la Sub Gerencia de Tecnologías de Información y Sistemas, publique la presente directiva en el Portal Institucional de la Municipalidad Provincial de Canchis.

REGÍSTRESE, COMUNÍQUESE, CÚMPLASE Y ARCHIVESE.

MUNICIPALIDAD PROVINCIAL DE CANCHIS

Ing. Wilber R. Hurtado Terraza
GERENTE MUNICIPAL

C.c.
Alcaldía.
Gerencia de Administración y Finanzas
Sub Gerencia de Tecnologías de Información y Sistemas
Gerencia de Planeamiento y Presupuesto
Sub Gerencia de Planeamiento, Racionalización y Cooperación Técnica
OCI
Archivo.
WRHT/GM/2022.

DIRECTIVA Nº 006-MPC-2022

"LINEAMIENTOS PARA EL USO ADECUADO DE EQUIPOS DE CÓMPUTO, SERVICIOS INFORMATICOS Y SEGURIDAD DE LA INFORMACIÓN EN LA MUNICIPALIDAD PROVINCIAL DE CANCHIS".

I. OBJETIVO

Contar con las directrices y los controles necesarios que permitan orientar a los usuarios de la Municipalidad Provincial de Canchis, para el buen uso de los equipos de cómputo, directrices de seguridad donde se debe mantener la integridad, disponibilidad, privacidad, control y autenticidad de la información manejada en la computadora.

II. FINALIDAD

Definir normas, procedimientos y responsabilidades en el uso y cuidado de equipos de cómputo y periféricos, servicios informáticos en red y seguridad de la información, en todas las dependencias de la Municipalidad Provincial de Canchis.

III. VIGENCIA

La presente directiva entrará en vigencia al día siguiente de su aprobación mediante Resolución de Gerencia Municipal.

IV. BASE LEGAL

- Ley N° 27972, Ley Orgánica de Municipalidades.
- Decreto Supremo N° 004-2019- JUS, que aprueba el Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General.
- Ley N° 27815, Ley de Código de Ética de la Función Pública.
- Decreto Supremo N° 033-2018-PCM, que crea la Plataforma Digital Única del Estado Peruano y establecen disposiciones adicionales para el desarrollo del Gobierno Digital y sus modificatorias.
- Resolución Ministerial N°041-2017-PCM, que aprobó el uso obligatorio de la Norma Técnica Peruana "NTP-ISP/IEC12207:2016 Ingeniería de Software y Sistemas, Procesos de Ciclo de Vida de Software, 3ra Edición" en todas las entidades integrantes les del Sistema Nacional de Informática.

- Decreto Supremo N° 013-2003-PCM, Dictan medidas para garantizar la legalidad de la adquisición de programas de software en entidades y dependencias del Sector Público.
- Resolución Ministerial N° 246-2007-PCM: que aprueba el uso obligatorio de la Norma Técnica Peruana NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información 2da Edición en todas las entidades integrantes del Sistema Nacional de Informática.
- Resolución Ministerial Nº 073-2004-PCM, Guía para la Administración Eficiente del Software legal en la Administración Pública.
- Resolución Jefatura N° 090-95-INEI, que aprueba la Directiva N° 008-95-INEI referida a "Recomendaciones Técnicas para la Protección Física de los Equipos y Medios de Procesamiento de la Información en la Administración Pública".
- Resolución de Contraloría N° 320-2006-CG – Aprueban Normas de Control Interno para las Entidades del Estado.
- Resolución Jefatural N° 088-2003 INEI: Aprueban Directiva sobre "Normas para el uso del servicio de correo electrónico en las entidades de la Administración Pública".
- Reglamento de Organización y Funciones de la Municipalidad Provincial de Canchis (ROF- Modificado), aprobado mediante Ordenanza Municipal N° 012-2018-MPC.
- Directiva Nº 002-MPC-2015 aprobado mediante Resolución de Gerencia Municipal N° 109-2015-GM-MPC - Directiva marco para la elaboración, actualización y aprobación de directivas internas de la Municipalidad Provincial de Canchis.

V. ÁMBITO DE APLICACIÓN

La presente Directiva es de cumplimiento obligatorio, bajo responsabilidad, para todo el personal que hace uso de una computadora, periférico o servicios informáticos en red, independientemente del régimen laboral, de todas las Gerencias y Unidades Orgánicas de la Municipalidad Provincial de Canchis.

VI. RESPONSABILIDAD

Son responsabilidades de la Sub gerencia de Tecnologías de Información y Sistemas, de aquí en adelante se denominará SGTIS:

- La SGTIS es la responsable de desarrollar, actualizar la presente Directiva según nuevas necesidades.
- La SGTIS, será la encargada de informar velar y exhortar del cumplimiento de la presente Directiva a todo el personal de la Municipalidad.
- La SGTIS, será responsable de administrar el soporte para la base de datos o similares; de administrar los procesos de la seguridad de la información incluso de los que se dieron de baja y las comunicaciones; de la operatividad oportuna y continua de todos los equipos y componentes informáticos de la Institución.
- La SGTIS, deberá supervisar el cumplimiento de la presente directiva y comunicará a la Sub Gerencia de Recursos Humanos, sobre el incumplimiento de la Directiva y su aplicación de la sanción descrita en el numeral 9.13.
- La SGTIS, detallará las características técnicas de los equipos de cómputo de las áreas usuarias.
- La SGTIS, será responsable de la custodia de todas las licencias de software original, discos CD/DVD ROM, documentación técnica, así como del inventario de estas licencias, así como de su actualización y valorización, de corresponder.
- La SGTIS, será la responsable de la administración, gestión y cuidado de los centros de datos a nivel de la Municipalidad Provincial de Canchis, tanto en infraestructura física como en los recursos humanos disponibles. Dada la envergadura de la información técnica y administrativa y el alto grado de sensibilidad que tienen los Centros de Datos en sus actividades cotidianas deben cumplir con los estándares de mantenimiento y operación.
- La SGTIS, coordinara con las Unidades Orgánicas que tienen equipos, el soporte remoto y presencial de las acciones que se tomen, para mantener la continuidad y seguridad de la información, para lo cual, en su oportunidad, definirá las acciones que permiten un adecuado control de inspección en dichos bienes.

- La SGTIS, será responsable de definir los periodos de retención y la frecuencia de los backups, a fin de garantizar la continuidad de las operaciones y la consulta histórica de su información, dichos backup no incluyen archivos personales de tipo música o fotografías.
- La SGTIS será responsable de garantizar a la Municipalidad Provincial de Canchis que, se comience almacenando en forma adecuada los backups de información en un repositorio de otra sede que garanticen la continuidad de los servicios de la plataforma tecnológica.
- La SGTIS, establecerá el plan anual de mantenimiento preventivo de los equipos de cómputo, el procedimiento de las atenciones de incidencias en los equipos de cómputo y el procedimiento de atención de los equipos de cómputo bajo garantía.
- La SGTIS, instruirá al personal sobre el uso del recurso de información, los compromisos, normas y procedimientos que han adquirido al acceder a los sistemas instalados en la Municipalidad Provincial de Canchis.
- La SGTIS, debe implementar y mantener las conexiones de las redes de datos de la Municipalidad Provincial de Canchis.
- La SGTIS, deberá establecer los controles de seguridad, con el objeto de asegurar la integridad y el adecuado uso de la información que se produce en la Municipalidad Provincial de Canchis.
- La SGTIS, autorizará el uso de los equipos diseñados por el procesamiento, almacenamiento y transporte de la información como, grabadoras de CD, DVD, USB, discos duros externos, entre otros.
- La SGTIS, debe instalar o desinstalar programas informáticos en los equipos de cómputo de Municipalidad Provincial de Canchis, según las licencias existentes.
- La SGTIS, se encargará de establecer los controles de datos fuente, los controles de operación y los controles de seguridad, con el objeto de asegurar la integridad y adecuado uso de la información que se produce en la Municipalidad Provincial de Canchis.

ES RESPONSABILIDAD DE LAS ÁREAS USUARIAS:

- La Presente Directiva es de aplicación obligatoria bajo responsabilidad por el personal o usuarios de las estaciones de trabajo de todas las Unidades Orgánicas de la Municipalidad Provincial de Canchis.
- Cada usuario es responsable sobre el cumplimiento en todos sus extremos de la presente Directiva.
- Será responsabilidad de los usuarios hacer una copia de la información necesaria en los directorios públicos que residen en los servidores.
- El personal será responsable de mantener depurada la información de sus archivos públicos, como buenas prácticas de optimización de uso adecuado de los recursos entregados por la Municipalidad Provincial de Canchis.

VII. DISPOSICIONES GENERALES

7.1. La Sub Gerencia de Tecnologías de Información y Sistemas se encargará de administrar el soporte para la base de datos o similares; de administrar los procesos de la seguridad de la información incluso de los que se dieron de baja y las comunicaciones; de la operatividad oportuna y continua de todos los equipos y componentes informáticos de la Municipalidad Provincial de Canchis.

7.2. Para efectos de la presente directiva, se entenderá por usuario a toda aquella persona que labora o presta servicios en la Municipalidad Provincial de Canchis, sin distinción de su relación, contractual o laboral, sea servidor, funcionario, directivo o prestador de servicio.

7.3. La Sub Gerencia de Tecnologías de Información, asignará un nombre de usuario y una clave al personal que tenga asignado un equipo de cómputo para el acceso a los recursos de la red informática según el perfil establecido de acuerdo al área al que pertenece, el cual será personal e intransferible.

7.4. El usuario que recibe el equipo de cómputo y servicios informáticos solicitados para el desempeño de sus labores, será responsable del uso adecuado de los mismos, así como el software instalado, la información, el buen uso de los servicios informáticos.

7.5. El usuario no deberá prestar o intercambiar los equipos de cómputo que le han sido asignados por la institución bajo responsabilidad, siendo la Sub Gerencia de Tecnologías de Información y Sistemas el

encargado de esta actividad previa coordinación con la Sub Gerencia de Control Patrimonial.

7.6. El usuario será responsable del cuidado físico y lógico de los equipos de cómputo asignados, no deberán ingerir alimentos sobre los equipos de cómputo o realizar cualquier otra actividad que pueda dañar o alterar su correcto funcionamiento.

7.7. El usuario será responsable de las actividades que se realicen con su nombre de usuario y contraseña de red asignada, en caso la ceda su acceso a otra persona seguirá siendo responsable de las actividades que este tercero realice.

7.8. Los equipos de cómputo entregados a los usuarios tendrán instalado el software base necesario para realizar sus funciones de acuerdo al perfil otorgado, cualquier necesidad adicional debe ser solicitado a la Sub Gerencia de Tecnologías de Información y Sistemas.

7.9. En temas de Seguridad, en el Perú, por R.M. Nº 004-2016-PCM, publicada el 14 de enero del 2016, se aprobó el uso obligatorio de la NTP ISO/IEC 27001:2014. Tecnologías de la Información, Técnicas de Seguridad, Sistemas de Gestión de Seguridad de la Información. Que contiene lo siguiente:

a. Objeto y Campo de Aplicación: La Norma Técnica Peruana 27001:2014 especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información, dentro del contexto de la organización. Incluye requisitos para la evaluación y tratamiento de los riesgos de seguridad de la información.

b. Implementación: Las entidades integrantes del Sistema Nacional de Informática, tendrán un plazo máximo de dos años para la implementación y/o adecuación la norma. Sin embargo, dichas entidades públicas tendrán un plazo de 60 días contados a partir de la fecha de publicación, para la presentación del cronograma de implementación y/o adecuación del sistema de gestión de la seguridad de la información, que deberá ser presentado a la Oficina Nacional de Gobierno Electrónico (ONGEI) de la Presidencia del Consejo de Ministros.

c. Certificación: Las entidades que requieran certificarse de acuerdo a lo establecido en la Norma Técnica Peruana NTP ISO/IEC 27001:2014, lo podrán realizar de forma opcional y con recursos propios de cada entidad.

d. Comité de Gestión de Seguridad de la Información: Cada entidad designará un Comité de Gestión de Seguridad de la Información, el cual estará conformado por:

- El Titular de la entidad.
- El responsable de administración o quien haga sus veces.
- El responsable de planeamiento o quien haga sus veces.
- El responsable del área de informática o quien haga sus veces.
- El responsable del área legal o quien haga sus veces y
- El oficial de seguridad de la información.

Las funciones del Comité de Gestión de Seguridad de la Información, serán establecidas por cada entidad.

e. Responsabilidad de la implementación: La responsabilidad de la implementación de la norma será del titular de cada entidad

VIII. DISPOSICIONES ESPECIFICAS

8.1. DEL USO Y CUIDADO DE LOS EQUIPOS DE CÓMPUTO

8.1.1. Los equipos de cómputo son exclusivamente para uso oficial, bajo responsabilidad directa del usuario.

8.1.2. Los usuarios son responsables del adecuado uso y control de los componentes de los equipos de cómputo que le han asignado.

8.1.3. Los usuarios que instalen de forma arbitraria software en sus equipos de cómputo son responsables de los problemas que podrían ocasionar en el equipo instalado y en los demás equipos conectados a la red, y de las licencias de software instalado.

8.1.4. El usuario, bajo ninguna circunstancia debe abrir los equipos de cómputo o periféricos, retirar o cambiar componentes de los mismos, alterar o eliminar el software que se encuentra a su disposición, cambiar la configuración determinada a su entrega por el personal de la Sub Gerencia de Tecnologías de

Información y Sistemas. En caso de que el usuario incurra en cualquiera de las situaciones señaladas será reportado por la Sub Gerencia de Tecnologías de Información y Sistemas a la Gerencia de Administración y Finanzas, solicitando la sanción correspondiente.

8.1.5. El usuario no deberá ingerir o dejar alimentos y/o bebidas encima de los equipos informáticos.

8.1.6. El usuario a quien se le haya asignado un equipo de cómputo, deberá seguir las pautas que se describen, según componente:

A. CPU (Unidad Central de Procesamiento)

a. La Sub Gerencia de Tecnologías de Información y Sistemas realizará periódicamente el mantenimiento preventivo y correctivo, cuando se requiera, y si cuenta con los recursos necesarios.

b. El usuario deberá revisar los USB que inserte en el equipo a través del programa antivirus instalado en el sistema, para evitar el contagio de virus.

c. El usuario deberá evitar mantener materiales magnéticos cerca del CPU.

d. La parte posterior del CPU debe estar libre (por lo menos 10 cm.) para asegurar una ventilación mínima adecuada.

e. El usuario deberá guardar su información dentro de la unidad D a fin de salvaguardar su trabajo.

B. EL MONITOR

a. Evitar colocar o pasar materiales magnéticos sobre la pantalla.

b. Evitar manipular agresivamente los botones de graduación - ajuste.

c. Utilizar una franela seca para la limpieza de la pantalla.

C. EL TECLADO

a. Evitar manchar el teclado o el cable de éste con cualquier clase de tinte. Los teclados manchados no serán cambiados por el proveedor, perderán su garantía

y su reposición será por cuenta del usuario responsable y determinando su correspondiente responsabilidad económica.

b. Evitar comer o beber sobre el teclado. Todo desperfecto que se origine por esta causa será de responsabilidad del usuario y su reposición seguirá la misma pauta que se da en el párrafo anterior.

c. Abstenerse de realizar maniobras sobre las partes internas del teclado. Las revisiones de los teclados son efectuadas por personal autorizado de la Sub Gerencia de Tecnologías de Información y Sistemas.

D. EL MOUSE

No deberá maniobrar ninguna de las partes internas del mouse, ni manipular incorrectamente el cable que sirve de conexión al CPU.

E. LA IMPRESORA

a. Se deberá efectuar únicamente la limpieza externa del equipo por parte del usuario.

b. Evitar manipular las partes del equipo mientras esté imprimiendo.

c. La colocación de las cintas, cartuchos de tinta y tóner se realizará de acuerdo a las instrucciones del manual de usuario del equipo y a las pautas que emita la Sub Gerencia de Tecnologías de Información y Sistemas.

d. La configuración de la impresora es responsabilidad del personal de la Sub Gerencia de Tecnologías de Información y Sistemas.

e. Si se atascara el papel cuando la impresora está imprimiendo, se deberá cancelar todo trabajo de impresión, no jalar ni arrancar el papel; se deberá comunicar de inmediato a la Sub Gerencia de Tecnologías de Información y Sistemas.

F. EL UPS (Sistema de Alimentación Ininterrumpida)

Este componente permite proteger al equipo de cómputo en situación de corte de fluido eléctrico, por lo que, en esos casos, el usuario deberá inmediatamente salvar su información y luego proceder a apagar el equipo de cómputo y el UPS (en ese orden), el mismo que no deberá continuar funcionando por más de cinco minutos.

8.2. POLÍTICA PARA LA IMPLEMENTACIÓN DE APLICACIONES

8.2.1. Descripción

Esta política debe utilizarse para evaluar la seguridad del impacto de nuevas aplicaciones. Cuando nuevas aplicaciones son desarrolladas o adquiridas para ofrecer diversas funcionalidades a los usuarios, el impacto de la nueva funcionalidad debe ser evaluada a fin de mantener la estabilidad de la red. Iniciar con un proceso de evaluación de datos ayudará a dar fluidez al proceso.

8.2.2. Finalidad

Esta política está diseñada para proteger los recursos informáticos de la Municipalidad compartidos en la red, mediante la definición de requisitos para nuevas aplicaciones en la Institución. Esta política exige una evaluación de la seguridad, incluyendo una evaluación de los niveles de seguridad de los datos, el medio por el cual se transmitirá la información, una evaluación de riesgos, y la determinación de los requisitos del sistema.

8.2.3. Proceso

Los usuarios deberán trabajar junto con la Sub Gerencia de Tecnologías de Información y Sistemas (desarrolladores de aplicaciones y los expertos en seguridad informática) para evaluar las necesidades de datos para cualquier aplicación nueva. Los usuarios deberán especificar sus necesidades para las aplicaciones y los desarrolladores de aplicaciones trabajarán con el usuario para identificar y clasificar los datos de acuerdo al proceso de evaluación de la seguridad del desarrollo de aplicaciones.

Bajo ninguna circunstancia la seguridad general de la red debe verse seriamente comprometida para el beneficio de cualquier proyecto.

8.3. DE LOS SERVICIOS INFORMÁTICOS

8.3.1. Los Gerentes, Sub Gerentes, Responsables de los Proyectos y Comisiones, solicitarán a la Sub Gerencia de Tecnologías de Información y Sistemas, mediante un documento, la asignación de un usuario en la Red (Login) y acceso a los servicios informáticos.

Los tipos de acceso que solicitarán podrán ser todos o algunos de lo que se detallan a continuación.

a) Acceso a los programas de trabajo.

b) Acceso a correo electrónico.

c) Acceso a Internet.

8.3.2. La Sub Gerencia de Tecnologías de Información y Sistemas deberá brindar, a solicitud, el acceso del usuario a la red conforme a lo solicitado.

8.3.3. Los Gerentes, Sub Gerentes, Responsables de los Proyectos y Comisiones solicitarán a la Sub Gerencia de Tecnologías de Información y Sistemas, mediante documento, la ampliación y/o eliminación de los accesos a los servicios informáticos, otorgados a los usuarios en su oportunidad.

8.3.4. Los usuarios son responsables de las actividades que realicen con sus accesos, como su identificación de usuario y contraseña a los servicios informáticos. En caso de que el usuario ceda su acceso a cualquier servicio informático a otra persona, seguirá siendo responsable de las actividades que este tercero realice.

8.3.5. La Sub Gerencia de Tecnologías de Información y Sistemas entregará información almacenada en la red, servicios y medios informáticos a las Áreas Usuarias que lo soliciten, del personal que labora.

8.3.6. La Sub Gerencia de Tecnologías de Información y Sistemas brindará el mantenimiento técnico preventivo y correctivo a los

recursos informáticos de la Municipalidad Provincial de Canchis.

8.3.7. Los Usuarios que soliciten a la Sub Gerencia de Tecnologías de Información y Sistemas la atención de un servicio técnico, deberán firmar conjuntamente con el Gerente, Sub Gerente o Responsable del Proyecto / Comisión, la "Orden de Atención de Soporte Técnico" anexa a la presente, en calidad de conformidad de la atención prestada.

8.3.8. Del Correo Electrónico:

a. La Municipalidad Provincial de Canchis cuenta con correo corporativo, los mismos que fueron creados uno por cada Gerencia, así como también para algunas unidades como la Sub Gerencia de Logística, Responsable del Libro de Reclamaciones y demás que requieran hacer uso del mismo. Estos correos son administrados por la Sub Gerencia de Tecnologías de Información y Sistemas, en cuanto a su creación, capacidad asignada, reseteo de contraseñas, etc., más no en cuanto al uso que se le otorgue al mismo.

b. El servicio de correo electrónico, es para uso exclusivo de envío y recepción de información concerniente a las funciones que el usuario cumple para la Municipalidad Provincial de Canchis. Por lo tanto esta información forma parte del activo de la Municipalidad Provincial de Canchis.

c. El uso frecuente y continuo, exige tener sujetos estos programas a controles y revisiones técnicas y mantenimiento de forma periódica por la Sub Gerencia de Tecnologías de Información y Sistemas.

d. La cuenta de correo electrónico es de uso exclusivo del usuario asignado; por tanto, bajo ninguna circunstancia éste podrá usar la cuenta de otro usuario.

e. Los mensajes tendrán una permanencia no mayor de 60 días, desde la fecha de entrega o recepción de los mismos. Superada la fecha de permanencia, los mensajes serán

eliminados del servidor de correo, salvo que por razones de función amerite su almacenamiento en el servidor por más tiempo del establecido, lo que deberá ser coordinado previamente con la Sub Gerencia de Tecnologías de Información y Sistemas.

f. Las consecuencias posibles, por el contenido de un correo, son de responsabilidad exclusiva del usuario de la cuenta de correo, por lo que se debe realizar el cambio de clave (password) de la cuenta con una frecuencia mínima de 30 días.

g. El tamaño máximo permitido para el envío de un correo lo determinará la Sub Gerencia de Tecnologías de Información y Sistemas. No se aplicarán restricciones a la recepción de correo. En caso de que la función de algunos usuarios requiera de una mayor capacidad del máximo permitido, esto deberá ser coordinado previamente con la Sub Gerencia de Tecnologías de Información y Sistemas.

h. En caso el usuario reciba correos no deseados o de procedencia dudosa, deberá notificar el hecho a la Sub Gerencia de Tecnologías de Información y Sistemas.

i. Los mensajes de correo deberán tener un asunto (subject) que refleje o resuma su contenido.

j. Las notificaciones institucionales también podrán efectuarse mediante correo electrónico, conforme lo establece el numeral 20.1.2 del artículo 20 de la Ley Nº 27444 Ley de Procedimiento Administrativo General.

8.4. POLÍTICA DE CONEXIÓN A INTERNET

8.4.1. Descripción

La política de conexión a Internet consta de componentes orientadas a que un usuario haga cumplimiento de una política interna propuesta por la Sub Gerencia de Tecnologías de Información y Sistemas, con la aprobación de Gerencia Municipal.

Los usuarios deben hacer fiel cumplimiento de las políticas especificadas para la aprobación de todas las conexiones a Internet u otras redes privadas. Esto requiere que todas las conexiones, ya sea por cable o por medios de conexión inalámbrica, a una red privada o de Internet sean aprobados por Gerencia Municipal. Las conexiones de orden técnico por mantenimiento, reparación o de orden técnico serán gestionadas por la Sub Gerencia de Tecnologías de Información y Sistemas.

Esta política de conexión a Internet solicita a los usuarios utilizar el Internet solo para fines laborales y así evitar el acceso a sitios web maliciosos que podrían comprometer la seguridad. Los usuarios de Internet deben tener conocimiento que sus actividades pueden ser accesadas y monitoreadas por la Sub Gerencia de Tecnologías de Información y Sistemas. Este sistema se utilizará para impedir el acceso a determinados sitios web que comprometan la seguridad, de igual manera a aquellos que saturen el ancho de banda, páginas con contenido sexual, etc.

8.4.2. Finalidad

La presente política está diseñada para proteger los recursos de la Municipalidad Provincial de Canchis contra la intrusión de malware (software que tiene como objetivo infiltrarse en el sistema y dañar la computadora sin el conocimiento del usuario, con finalidades diversas), que pueden introducirse en la red por los usuarios que utilizan Internet. También está diseñada para evitar las conexiones a Internet no autorizadas y sin protección que puede permitir la entrada de una serie de contenidos peligrosos en la red de la Municipalidad y con compromiso de velar por la integridad de los datos y la seguridad del sistema en toda la red.

8.4.3. Conexión Física de Internet

a. Las conexiones físicas de Internet o conexiones a otras redes privadas serán autorizadas y aprobadas por

Gerencia Municipal. Los usuarios tendrán acceso a Internet a través de la conexión brindada por la Sub Gerencia de Tecnologías de Información y Sistemas. Las conexiones adicionales pueden ser:

- Conexión de módem, de un ordenador o dispositivo de comunicación que permita una conexión a la red.
- Puntos de acceso inalámbricos o dispositivos con capacidad inalámbrica no se permiten a menos que sea aprobado para su uso por la Sub Gerencia de Tecnologías de Información y Sistemas. Si alguno de los ordenadores u otros dispositivos (Laptops, teléfonos móviles, Palms, etc.) tienen capacidad inalámbrica, ésta debe ser apagada antes de conectar a la red, a menos que sea aprobado para el funcionamiento inalámbrico por la Sub Gerencia de Tecnologías de Información y Sistemas.
- Cualquier otra conexión a Internet no suministrada por la Sub Gerencia de Tecnologías de Información y Sistemas debe ser revisada y aprobada exclusivamente por Gerencia Municipal.

8.4.4. Utilización de Internet

a. Todos los empleados autorizados deben hacer uso de Internet para fines netamente laborales.

b. El uso de Internet de todos los trabajadores autorizados puede ser controlado y accesado incluyendo todos los sitios visitados, la duración de las visitas, cantidad de datos descargados, y los tipos de datos descargados. El tiempo de actividad registrada también puede ser accesado.

c. La Sub Gerencia de Tecnologías de Información y Sistemas está autorizada para la implementación de un sistema de auditoría de páginas web visitadas y servicios utilizados por cada usuario, la misma que podrá ser entregada a los Gerentes, Sub Gerentes o Responsables de los Proyectos que lo soliciten.

d. Los trabajadores deben tener precaución al visitar sitios de Internet desconocidos, manteniendo su navegador configurado a través de las normas aprobadas con el fin de protegerse de las infecciones de malware.

e. Debido a la proliferación de virus informáticos, se restringe el uso del servicio de Internet para el acceso a servidores de correos externos, servicios de archivos compartidos y servicios de mensajería instantánea (chats).

f. En caso que la Sub Gerencia de Tecnologías de Información y Sistemas verifique el mal uso de Internet, podrá bloquear el acceso a dicho usuario y procederá a informar a Gerencia Municipal sobre la utilización inadecuada del servicio.

8.4.5. Aplicación

Dado que el uso indebido de las computadoras puede ocasionar que programas hostiles puedan destruir la integridad de los recursos de la red y los sistemas, la prevención de estos eventos es fundamental para la seguridad de la organización y de todos los individuos, por lo que los empleados que no se adhieren a esta política pueden ser objeto a una acción disciplinaria.

8.5. SEGURIDAD DEL PERSONAL

8.5.1. Control y Política del Personal.

El responsable de la Sub Gerencia de Recursos Humanos llevará a cabo controles de verificación del personal en el momento en que se solicita el puesto. Estos controles incluirán todos los aspectos que indiquen las normas para tal efecto.

8.5.2. Compromiso de Confidencialidad.

Los empleados firmarán un Compromiso de Confidencialidad o no divulgación, como parte de sus términos y condiciones iniciales de empleo, en lo que respecta al tratamiento de la información de la Municipalidad Provincial de Canchis.

Asimismo, mediante el Compromiso de Confidencialidad, el empleado declarará conocer y aceptar la existencia de

determinadas actividades que pueden ser objeto de control y monitoreo. Estas actividades deben ser detalladas a fin de no violar el derecho a la privacidad del empleado.

La copia firmada del compromiso deberá ser guardada en forma segura por el responsable de la Sub Gerencia de Recursos Humanos.

El responsable de la Sub Gerencia de Recursos Humanos desarrollará un procedimiento para la suscripción del Compromiso de Confidencialidad donde se incluirán aspectos sobre:

- Suscripción inicial del compromiso por parte de la totalidad del personal.
- Método de resuscripción, en caso de modificación del texto del compromiso.

8.5.3. Términos y Condiciones del Empleo.

Los términos y condiciones del empleo establecerán la responsabilidad del empleado en materia de seguridad de la información. Cuando corresponda, los términos y condiciones de empleo establecerán que estas responsabilidades se extienden más allá de los límites de la Municipalidad Provincial de Canchis y del horario normal de trabajo.

Los derechos y obligaciones del empleado relativos a la seguridad de la información, por ejemplo, en relación con las leyes de propiedad intelectual o la legislación de protección de datos, se encontrarán aclarados e incluidos en los términos y condiciones de empleo.

8.6. SEGURIDAD FÍSICA Y AMBIENTAL.

8.6.1. Perímetro de Seguridad Física.

La protección física se llevará a cabo mediante la creación de diversas barreras o medidas de control físicas alrededor de las sedes de la Municipalidad Provincial de Canchis y de las instalaciones de procesamiento de información. La Municipalidad Provincial de Canchis utilizará perímetros de seguridad para proteger las áreas que contienen instalaciones

de procesamiento de información, de suministro de energía eléctrica, y cualquier otra área considerada crítica para el correcto funcionamiento de los sistemas de información. Un perímetro de seguridad está delimitado por una barrera, por ejemplo, una pared, una puerta de acceso controlado por dispositivo de autenticación o un escritorio u oficina de recepción atendidos por personas.

Se considerarán e implementarán los siguientes lineamientos y controles, según corresponda:

- ✓ Definir claramente el perímetro de seguridad.
- ✓ Ubicar las instalaciones de procesamiento de información dentro del perímetro de un edificio o área de construcción físicamente sólida (por ejemplo, no deben existir aberturas en el perímetro o áreas donde pueda producirse fácilmente una irrupción).
- ✓ Las paredes externas del área deben ser sólidas y todas las puertas que comunican con el exterior deben estar adecuadamente protegidas contra accesos no autorizados, por ejemplo, mediante mecanismos de control, vallas, alarmas, cerraduras, etc.
- ✓ Verificar la existencia de un área de recepción atendida por personal. Si esto no fuera posible se implementarán medios alternativos de control de acceso físico al área o edificio. El acceso a dichas áreas y edificios estará restringido exclusivamente al personal autorizado.
- ✓ Extender las barreras físicas necesarias desde el piso (real) hasta el techo (real), a fin de impedir el ingreso no autorizado y la contaminación ambiental, por ejemplo, por incendio, humedad e inundación.

8.6.2. Controles de Acceso Físico.

Las áreas protegidas se resguardarán mediante el empleo de controles de acceso físico, los que serán determinados por el Responsable de la Unidad Orgánica con el asesoramiento del Responsable de Seguridad Informática y el Responsable de

Seguridad Física, a fin de permitir el acceso sólo al personal autorizado.

Los controles de acceso físico tendrán las siguientes características:

- ✓ Supervisar o inspeccionar a los visitantes a áreas protegidas y registrar la fecha y hora de ingreso y egreso.
- ✓ Controlar y limitar el acceso a la información clasificada y a las instalaciones de procesamiento de información, exclusivamente a las personas autorizadas.
- ✓ Revisar y actualizar semestralmente los derechos de acceso a las áreas protegidas, los que serán documentados y firmados por el Responsable de la Unidad Orgánica de la que dependa.

8.6.3. Protección de Oficinas e Instalaciones.

Para la selección y el diseño de un área protegida se tendrá en cuenta la posibilidad de daño producido por incendio, inundación, explosión, agitación civil, y otras formas de desastres naturales o provocados por el hombre. También se tomarán en cuenta las disposiciones y normas (estándares) en materia de sanidad y seguridad. Asimismo, se considerarán las amenazas a la seguridad que representan los edificios y zonas aledañas, por ejemplo: filtración de agua desde otras instalaciones.

Se establecen las siguientes medidas de protección para áreas protegidas:

- ✓ Ubicar las instalaciones críticas en lugares a los cuales no pueda acceder personal no autorizado.
- ✓ Establecer que las áreas donde se realicen actividades de procesamiento de información sean discretas y tengan un señalamiento mínimo de su propósito, sin signos obvios, exteriores o interiores.
- ✓ Establecer que las puertas y ventanas permanecerán cerradas cuando no haya vigilancia.

- ✓ Se agregará protección externa a las ventanas, en particular las que se encuentran en planta baja o presenten riesgos potenciales.
- ✓ Implementar mecanismos de control para la detección de intrusos, los mismos que serán instalados según estándares y probados periódicamente. Estos mecanismos de control comprenderán todas las puertas exteriores y ventanas accesibles.
- ✓ Almacenar los materiales peligrosos o combustibles en lugares seguros a una distancia prudencial de las áreas protegidas de la Municipalidad Provincial de Canchis.

8.6.4. Ubicación y Protección de Activos Físicos.

Los activos físicos, que incluyen el equipamiento, los medios de almacenamiento (informáticos o no), y las copias de respaldo serán ubicados y protegidos de tal manera que se reduzcan los riesgos ocasionados por amenazas y peligros ambientales, y las oportunidades de acceso no autorizado, teniendo en cuenta los siguientes puntos:

- ✓ Ubicar dichos activos en un sitio donde se minimice el acceso innecesario y provea un control de acceso adecuado.
- ✓ Ubicar las instalaciones de procesamiento y almacenamiento de información que manejan datos clasificados, en un sitio que permita la supervisión durante su uso.
- ✓ Aislar los elementos que requieren protección especial para reducir el nivel general de protección requerida.

8.6.5. Suministros de Energía.

Los equipos estarán protegidos frente a probables fallas en el suministro de energía u otras anomalías eléctricas. El suministro de energía estará de acuerdo con las especificaciones del fabricante o proveedor de cada equipo. Para asegurar la continuidad del suministro de energía, se contemplarán las siguientes medidas de control:

- ✓ Disponer de múltiples enchufes o líneas de suministro para evitar un único punto de falla en el suministro de energía.
- ✓ Contar con un suministro de energía ininterrumpido (UPS) para asegurar el apagado regulado y sistemático o la ejecución continua del equipamiento que sustenta las operaciones críticas de la Municipalidad Provincial de Canchis.
- ✓ Montar un generador de respaldo (motor o grupo electrógeno) para los casos en que el procesamiento deba continuar ante una falla prolongada en el suministro de energía.

8.6.6. Mantenimiento de Equipos.

Se debe considerar los siguientes aspectos:

- ✓ Realizar mantenimiento preventivo de los equipos de cómputo y comunicaciones, de acuerdo con los intervalos de servicio y especificaciones recomendados por el proveedor.
- ✓ Establecer que sólo el personal de mantenimiento autorizado puede brindar mantenimiento y llevar a cabo reparaciones en el equipamiento.
- ✓ Registrar todas las fallas y el mantenimiento preventivo y correctivo realizado.
- ✓ Registrar el retiro de equipamiento de la sede de la Municipalidad Provincial de Canchis para su mantenimiento.
- ✓ Proteger la información contenida en los equipos, realizándose previamente las respectivas copias de resguardo.

8.7. POLÍTICA DE SEGURIDAD DE LA INFORMACION

Para establecer una política de seguridad de la información hay varios temas a tener en cuenta, como protección por contraseñas, restricciones de accesos, uso de firewall, etc.

8.7.1. Descripción general

Todos los empleados, funcionarios, autoridades y personal contratado que tienen acceso a los sistemas de la Institución deben adherirse a las políticas definidas en cuanto a seguridad, con el fin de proteger la integridad de los datos y los sistemas informáticos.

8.7.2. Propósito

Esta política está diseñada para proteger los recursos de la Municipalidad Provincial de Canchis administrados a través de la red de datos.

8.7.3. Ámbito

Esta política se aplica a todo el personal que tiene alguna cuenta en el computador o sistemas informáticos, que requiere una contraseña para ingresar a la red de datos de la Municipalidad Provincial de Canchis.

8.7.4. De la Información

a. Con el objeto de garantizar la confidencialidad de la información del usuario en la red de datos, los sistemas informáticos deben estar configurados de tal manera que obliguen a los usuarios a realizar el cambio de su password, cuando acceda por primera vez a la red, y de forma periódica.

b. La información almacenada en los equipos de cómputo y servidores de la red de datos, son de propiedad de la Municipalidad Provincial de Canchis, los Jefes de las Unidades Orgánicas son los encargados de autorizar a su personal, los accesos a los recursos informáticos necesarios para el cumplimiento de sus funciones.

c. El usuario que encuentre alguna irregularidad en los equipos de cómputo y/o con el servicio informático, deberá comunicarlo inmediatamente a la Sub Gerencia de Tecnologías de Información y Sistemas, a fin de que se adopten las medidas correctivas.

d. El usuario cuenta con una contraseña para el acceso a la red LAN y correo electrónico. Estos servicios son

considerados confidenciales y de uso exclusivo del usuario asignado, esta contraseña es de carácter personal.

e. Cada usuario que haga uso de los sistemas informáticos a los que se le ha dado acceso, se hará responsable de la información que manipule durante su uso.

f. Los Gerentes, Sub Gerentes, Jefes de Oficinas, Responsables de Proyectos / Comisiones, deberán informar a la Sub Gerencia de Tecnologías de Información y Sistemas, la relación de personas que ingresan y dejan de laborar en su área. Así mismo, en un plazo no mayor de 48 horas, la Sub Gerencia de Tecnologías de Información y Sistemas deberá restringir los accesos y servicios informáticos asignados al personal retirado.

g. El uso de los equipos de cómputo será de lunes a viernes. Los días sábados, domingos y feriados, se deberá contar con la autorización de los Gerentes, Sub Gerentes, Jefes de Oficinas, Responsables de Proyectos / Comisiones.

h. La Sub Gerencia de Tecnologías de Información y Sistemas podrá desinstalar cualquier producto de uso no oficial, personal o software que no cuente con la licencia correspondiente, comunicando a la Gerencia de Administración y Finanzas.

i. Está terminantemente prohibido a que los usuarios traten de generar copias a las Datas de los aplicativos o sistemas utilizados en la Municipalidad Provincial de Canchis, ya que pueden generar daños a la DATA, la Sub Gerencia de Tecnologías de Información y Sistemas realizara en un primer momento la evaluación o seguimiento para posterior ser realizada por un externo.

8.7.5. Protección de Contraseña

Entre las consideraciones a tener en cuenta al respecto de contraseñas, se pueden mencionar las siguientes:

a) Nunca escriba sus contraseñas.

b) Nunca envíe una contraseña a través del correo electrónico.

c) Nunca incluya una contraseña en algún documento almacenado de forma no encriptada.

d) Nunca le diga a nadie su contraseña.

e) Nunca revele o de pista de su contraseña en un formulario en Internet.

f) Nunca use el "Recordar Contraseña", característica de la aplicación de programas como Internet Explorer, su programa de correo electrónico, o cualquier otro programa.

g) Nunca use su contraseña en una cuenta a través de Internet que no tiene un ingreso seguro, solo debe usarse cuando la dirección del navegador empieza por https:// en lugar de http://

h) Informe cualquier sospecha de ruptura de su contraseña al encargado de la seguridad de tecnologías de la información.

i) No utilice siglas comunes como parte de su contraseña.

j) No utilice nombres de personas o lugares, como parte de su contraseña.

k) No utilice parte de su nombre de usuario en su contraseña.

l) No utilice partes de números que pueda recordar fácilmente.

m) Tenga cuidado con dejar ver a alguien cuando escriba su contraseña.

8.7.6. Requisitos para la Contraseña

Al establecer los requisitos de contraseña se debe recordar que las reglas de contraseña demasiado difícil pueden llegar a disminuir la seguridad si los usuarios ven normas imposibles o muy difíciles de cumplir. Si las contraseñas se cambian con demasiada frecuencia, los usuarios tienden a escribir o hacer que su contraseña sea una variante de una contraseña anterior, con la que un atacante puede adivinar la contraseña antigua.

Se deben considerar los siguientes requisitos de contraseña:

a) Longitud mínima - 6 caracteres.

b) Longitud máxima - 14 caracteres.

c) Complejidad mínima - Las contraseñas deben utilizar tres de los siguientes cuatro tipos de caracteres: Minúsculas, Mayúsculas, Números, Caracteres especiales como: !@#$%^&*(){}[]

d) Las contraseñas deben ser sensibles a mayúsculas y minúsculas, y los nombres de usuario o ID de inicio de sesión no deben ser sensibles a mayúsculas y minúsculas.

e) Edad máxima de la contraseña - 90 días

f) Edad mínima de la contraseña - 30 días

g) Cuenta bloqueada temporalmente - 3 intentos de acceso fallido.

h) Restablecer la cuenta después del bloqueo temporal - El tiempo es tomado entre el acceso fallido y antes de que se cuente el acceso fallido, es de 30 minutos. Esto significa que, si hay tres intentos fallidos en 30 minutos, la cuenta será bloqueada.

i) Los usuarios deben tener la costumbre de no salir de sus equipos al estar desbloqueados. En caso contrario, se debe pulsar las teclas CTRL-ALT-DEL y seleccione "Bloquear equipo".

8.7.7. Elección de las Contraseñas

Utilice una contraseña como a continuación se aconseja:

a. Insertar una palabra o parte de una palabra dentro de otra.

b. Utilice una frase que es personal y utilizar el carácter de primer, segundo o tercer lugar en cada palabra de cada frase. La frase puede ser una pregunta y frase de respuesta.

c. Use una representación numérica de las letras del alfabeto por parte de la frase o una palabra en su frase. Por ejemplo, A es 1, B es 2, C es 3, etc.

d. Use puntuación o caracteres especiales en parte de su frase.

e. Utilizar letras mayúsculas y minúsculas.

f. Entremezclar números y caracteres de una manera que pueda recordar.

8.8. POLÍTICA DE COPIAS DE RESPALDO

8.8.1. Descripción General

Este documento permite definir la política de copias de seguridad de los datos almacenados en los discos duros de los servidores y/o computadoras personales de propiedad de la Municipalidad Provincial de Canchis.

8.8.2. Propósito

La presente política está orientada principalmente a proteger la información en la Municipalidad Provincial de Canchis, para asegurar de que no se pierda y que pueda ser recuperada en caso de una avería del equipo, la destrucción intencional de datos u otro tipo de desastre.

8.8.3. Ámbito

Esta política deberá ser aplicada por los propietarios de los archivos que están almacenados magnéticamente en las computadoras y servidores asignados para sus labores dentro de la Municipalidad Provincial de Canchis.

8.8.4. Periodicidad del Procedimiento de Respaldo

Las copias de seguridad se realizarán según su origen:

a. Bases de Datos de los Servidores: se realizarán durante los días de la semana según criterio del Administrador de los Servidores, pero obligatoriamente semanal, mensual y anualmente.

b. Archivos de ofimática (word, excel, power point, acrobat, etc.), autocad y base de datos locales, durante los días del mes se realizarán según criterio del usuario, recomendable cada vez que realicen modificaciones significativas y/o creaciones de archivos.

c. En forma obligatoria se realizarán mensual y anualmente, y una copia de éstas deberán ser entregadas a la Sub Gerencia de Tecnologías de Información y Sistemas.

8.8.5. Almacenamiento

a. Respecto a la información contenida en los servidores, las copias de seguridad a utilizar serán mediante disco duro externo, dedicado exclusivamente para tal fin.
b. Las unidades de almacenamiento de respaldo serán verificadas mensualmente para comprobar su correcto estado.
c. Al momento de realizarse el almacenamiento se debe registrar en la hoja de control: la fecha, nombre del archivo, nombre del responsable, y en caso de existir se registrará alguna observación.

8.8.6. Responsabilidades

a. El jefe de la Sub Gerencia de Tecnologías de Información y Sistemas, es responsable de las copias de seguridad de los Servidores.
b. Las copias de seguridad de la información contenida en las computadoras personales de cada Oficina son de responsabilidad de cada usuario, de requerir apoyo lo solicitará a la Sub Gerencia de Tecnologías de Información y Sistemas.

8.8.7. Propiedad de los Archivos

Los archivos que se crean, modifican o almacenan dentro de los servidores o computadoras personales son de propiedad exclusiva de la Municipalidad Provincial de Canchis, los usuarios en caso de dejar la Institución deberán entregar una copia de su información al jefe inmediato donde laboró.

8.8.8. Restauración

Los usuarios que necesitan restaurar algún archivo contenido en los servidores deberán presentar una solicitud dirigida a la Sub Gerencia de Tecnologías de Información y Sistemas. Deberán incluir información que contenga el nombre del archivo, y la fecha y hora aproximada en que fue eliminado.

8.9. ADMINISTRACIÓN DE LA RED

8.9.1. De la Red LAN (red de área local):

a. La Red LAN es el conjunto de componentes que permiten la interconexión de los equipos de cómputo a fin de que los usuarios puedan compartir y utilizar los recursos informáticos implementados. Está compuesto por los servidores (donde se almacena toda la información de los sistemas y servicios informáticos), medios de conexión (cable o medio, tarjetas de red y distribuidores de conexiones), y las estaciones de trabajo (equipo de cómputo del usuario).

b. La Sub Gerencia de Tecnologías de Información y Sistemas es la encargada de la administración de las Redes LAN de la Municipalidad Provincial de Canchis.

c. El usuario podrá acceder a la red LAN desde un equipo de cómputo autorizado e instalado por la Sub Gerencia de Tecnologías de Información y Sistemas.

d. Además de los recursos ofrecidos por el equipo de cómputo asignado a cada usuario, éstos contarán con los recursos que les ofrece la red, tales como: compartir impresoras, compartir archivos, almacenar archivos en los servidores principales, correo electrónico y acceder a Internet. Estos recursos deben ser usados racionalmente y sin perjudicar a otros usuarios.

e. Para el uso de los recursos de la Red en cada área, se cuenta con diferentes equipos que llevan la señal hasta cada estación de trabajo (switches, concentradores, cables de fibra óptica, cables UTP, entre otros). Los Gerentes, Sub Gerentes, Jefes de Divisiones y Responsables de los Proyectos, Comisiones y Unidades Orgánicas brindarán las facilidades del caso al personal de la Sub Gerencia de Tecnologías de Información y Sistemas para las instalaciones físicas necesarias.

f. La Sub Gerencia de Tecnologías de Información y Sistemas es la responsable del mantenimiento de las cuentas del usuario de red (Login) y el establecimiento de

las normas de seguridad para la protección de la información almacenada en los servidores.

g. El usuario que haga uso de los recursos de la red, será registrado con los datos del cargo y oficina (Unidad Orgánica, Proyecto o Comisión) a la cual pertenece, heredando los privilegios y restricciones establecidas.

8.9.2. Control de Red.

Se debe garantizar la seguridad de los datos y los servicios conectados en la red de la Municipalidad Provincial de Canchis, contra el acceso no autorizado, considerando la ejecución de las siguientes acciones:

a. Establecer procedimientos para la administración del equipamiento remoto, incluyendo los equipos en las áreas usuarias.

b. Establecer controles especiales para salvaguardar la confidencialidad e integridad del procesamiento de los datos que pasan a través de redes públicas, y para proteger los sistemas conectados.

c. Implementar controles para mantener la disponibilidad de los servicios de red y computadoras conectadas.

d. Garantizar mediante actividades de supervisión, que los controles se aplican uniformemente en toda la infraestructura de procesamiento de información.

8.9.3. Administración y Seguridad de los Medios de Almacenamiento.

El Responsable de Seguridad Informática definirá procedimientos para la administración de medios informáticos extraíbles, como USB, discos externos, etc.

Se deberán considerar las siguientes acciones para la implementación de los procedimientos:

a. Eliminar de forma segura los contenidos, si ya no son requeridos, de cualquier medio reutilizable que ha de ser retirado o reutilizado por la Municipalidad Provincial de Canchis.

b. Almacenar todos los medios en un ambiente seguro y protegido, de acuerdo con las especificaciones de los fabricantes o proveedores.

8.10. BAJA DE EQUIPOS DE TIC

8.10.1. El usuario reporta a la Sub Gerencia de Tecnologías de Información y Sistemas, cuando el equipo de TIC asignado a un usuario presenta problemas en su funcionamiento

8.10.2. El equipo de TIC reportado es evaluado por el personal técnico de Sub Gerencia de Tecnologías de Información y Sistemas, con el fin de determinar si puede o no ser reparado.

8.10.3. En caso el equipo de TIC no pueda ser reparado por el personal técnico de la Sub Gerencia de Tecnologías de Información y Sistemas, se emite el informe técnico, para solicitar la baja correspondiente, o la revisión técnica por parte de una empresa especialista o por el proveedor en caso se encuentre con garantía vigente.

8.10.4. Se realiza copia de seguridad (Backup) de la información contenida en el equipo de TIC a dar de baja, en caso el órgano o unidad orgánica, y el usuario, así lo requieran. Y posteriormente se blanquea totalmente para que no pueda ser recuperada posteriormente por personas ajenas a la Institución.

8.10.5. La baja del equipo de TIC es realizada por el órgano y/o unidad orgánica responsable del equipo con la Sub Gerencia de Control Patrimonial y, de la Sub Gerencia de Logística y Servicios Generales, adjuntando el informe técnico, emitido por la Sub Gerencia de Tecnologías de Informática y Sistemas.

8.10.6. El equipo de TIC es recogido por la Sub Gerencia de Control Patrimonial y, de la Sub Gerencia de Logística y Servicios Generales, de acuerdo a lo indicado por el órgano o unidad orgánica.

8.11. DE LAS PROHIBICIONES Y RESTRICCIONES

Queda prohibido:

Queda prohibido:

8.11.1. Utilizar los recursos de los equipos de cómputo para beneficios personales.

8.11.2. Instalar software no licenciado o no autorizado por la Sub Gerencia de Tecnologías de Información y Sistemas en los equipos de cómputo.

8.11.3. Almacenar en los equipos de cómputo instaladores de software ilegal.

8.11.4. Almacenar en los equipos de cómputo información de otro usuario, sin el consentimiento expreso del propietario.

8.11.5. El uso de equipos de cómputo por personal ajeno a la Municipalidad Provincial de Canchis.

8.11.6. Ejecutar programas ya sean propios u obtenidos a través de Internet o correo u otro medio.

8.11.7. Instalar servidores y clientes de correo electrónico sin el conocimiento, consentimiento y aprobación de la Sub Gerencia de Tecnologías de Información y Sistemas.

8.11.8. La manipulación de los equipos de comunicación (concentradores, switches, ruteadores, antenas, cableados, etc.) por los usuarios.

8.11.9. El acceso a lugares electrónicos obscenos y de almacenar en los equipos de cómputo en cualquier formato digital (videos, imágenes, literatura) información que atente contra la moral en perjuicio de terceros.

8.11.10. Ingresar y utilizar páginas web que permitan obtener contraseñas de software o sistemas informáticos.

8.11.11. Ingresar y utilizar páginas web dedicadas a la mensajería instantánea y salas de chat recreativas.

8.11.12. Ingresar y utilizar páginas web que permitan la transmisión interactiva de videos, programas musicales y utilización de juegos.

8.11.13. Ingresar y utilizar páginas web a fin de descargar software ilegal o no licenciado.

8.11.14. El uso de Internet en cualquier actividad que sea lucrativa o comercial de carácter individual, así como el uso del servicio de correo para propósitos fraudulentos, publicitarios o para la propagación de mensajes no relacionados con la actividad laboral.

8.11.15. Acceder mediante el servicio de Internet asignado a contenidos que puedan estar relacionados con servidores generadores de spam o virus, o que puedan contener programas que permitan romper las claves de acceso, u otros que puedan utilizarse con fines no lícitos o no autorizados y dañinos tanto para la institución como para terceros.

8.11.16. Utilizar medios informáticos (hardware y software) a fin de obtener las claves de acceso de otro usuario o recurso que no se le ha dado acceso. Esto ameritará una sanción de acuerdo al grado de responsabilidad, la misma que se elevará a la Gerencia de Administración y Finanzas, para la evaluación respectiva.

8.11.17. Utilizar los servicios de comunicación, incluyendo el correo electrónico o cualquier otro recurso, para intimidar, insultar o acosar a otras personas, interferir con el trabajo de los demás, provocando un ambiente de trabajo no deseable dentro de la Municipalidad Provincial de Canchis.

8.11.18. Utilizar los recursos de la institución para acceso no autorizado a redes y sistemas remotos.

8.11.19. Provocar deliberadamente el mal funcionamiento de computadoras, estaciones o componentes periféricas de redes y sistemas.

8.11.20. La suplantación o uso no autorizado de la cuenta de otra persona serán considerados como falta grave.

8.11.21. Decodificar el tráfico en la red o cualquier intento de obtención de información de correo confidencial que se transmita a través de la misma.

8.11.22. El iniciar o continuar cadenas de mensajes tales como los que pretenden "traer buena suerte", "chistes" o cualesquiera que

8.11.23. Suscribirse a las listas de interés que no guardan relación con la actividad laboral asignada.

8.12. DE LAS INFRACCIONES

8.12.1. Manipular la configuración de red; agregar o eliminar protocolos de comunicaciones de red o modificar el nombre de la computadora y/o grupo de trabajo establecido.

8.12.2. Instalar software no autorizado por la Sub Gerencia de Tecnologías de Información y Sistemas.

8.12.3. Consentir a personal ajeno a la entidad a utilizar los equipos informáticos.

8.13. SANCIONES

8.13.1. Se considera una falta a toda acción u omisión, voluntaria o involuntaria, que contravenga las recomendaciones y prohibiciones establecidas en la presente Directiva.

8.13.2. Las faltas cometidas por los usuarios serán comunicadas a la Sub Gerencia de Recursos Humanos de la entidad, a fin de que determine la gravedad de la misma, las cuales pueden ser: leves o graves.

Se consideran faltas leves aquellas acciones realizadas por el usuario que no sigan las recomendaciones establecidas por la presente Directiva.

Se consideran faltas graves aquellas violaciones primarias o reiterativas a las prohibiciones establecidas en la presente Directiva.

8.13.3. Las sanciones aplicables a los usuarios por el incumplimiento a las recomendaciones y prohibiciones establecidas en la presente Directiva, se asentarán en Acta administrativa o Sanción administrativa.

8.14. RECOMENDACIONES PARA EL USUARIO

8.14.1. Al inicio de las labores

El usuario verificará que los equipos, cables y el sistema estén completos y conectados en forma correcta, caso contrario informará a la Sub Gerencia de Tecnologías de Información y Sistemas.

8.14.1. Al inicio de las labores

El usuario verificará que los equipos, cables y el sistema estén completos y conectados en forma correcta, caso contrario informará a la Sub Gerencia de Tecnologías de Información y Sistemas.

La ubicación de las computadoras debe considerar los siguientes aspectos:

a. La zona debe ser de baja temperatura
b. No debe existir agua o goteras que lo puedan dañar.
c. La superficie debe ser de madera, lejos de campos magnéticos para evitar que el equipo se recargue de iones.
d. Evitar colocar los equipos sobre lunas.
e. Lejos del calor o del fuego.
f. El usuario es responsable de su información, por tanto, deberá tener una copia de seguridad de su información, tanto en la unidad D de su equipo como en su USB, disco externo o CD según sea el caso.

8.14.2. Encendido del equipo de cómputo

Se debe considerar el siguiente orden:

a. Estabilizador o supresor de pico.
b. UPS, si posee.
c. Monitor.
d. CPU.

Inmediatamente después que se encienden los equipos, el sistema del CPU empieza a revisar la operatividad de todos los dispositivos, se encienden las luces del tablero y el led del disco duro. Finalizada la revisión, el sistema normalmente busca en la lectora de CD al sistema operativo; al no hallarlo, se dirigirá a la unidad "C" del disco duro. Al encontrar el sistema operativo, la computadora se encuentra lista para recibir órdenes.

8.14.3. Uso del Computador

a. Evitar desconectar bruscamente el equipo o moverlo más allá de la distancia permitida por los cordones o apagar el estabilizador sin antes haber apagado la máquina.

b. En caso de interrupción de fluido eléctrico:
   - Apagar todos los equipos de cómputo (monitor, CPU, impresora).
   - Si posee UPS, grabar la información, salir del ambiente en que se encuentra trabajando y apagar los equipos. Restablecido el fluido, esperar aproximadamente 5 minutos para encender sus equipos.

c. No dejar las pantallas encendidas por más de 12 horas.

d. No abrir las cubiertas de una impresora láser.

e. No golpear el teclado de la computadora.

IX. DISPOSICIONES COMPLEMENTARIAS Y FINALES

Los aspectos no considerados ni establecidos en la presente Directiva serán resueltos por la SGTIS, guardando concordancia con las disposiciones internas de la Municipalidad Provincial de Canchis y otras emitidas por la Autoridad competente o la Secretaria de Gobierno Digital.

X. DISPOSICIONES TRANSITORIAS.

En la Municipalidad Provincial de Canchis no se cuenta con un documento similar; por lo que, a partir de su aprobación entrará en vigencia en todos sus extremos la presente directiva. Transitoriamente se seguirá trabajando con las normativas vigentes y bajo la supervisión de la Secretaria de Gobierno Digital.

XI. GLOSARIO DE TERMINOS

ACCESO: Acción de poder ingresar a cualquier equipo de la entidad por parte del personal autorizado de la Sub Gerencia de Tecnologías de Información y Sistemas, de manera local o remota.

CHAT: Comunicación escrita en tiempo real a través de internet entre dos o más personas.

CPU: Término genérico utilizado para referirse a las computadoras de escritorio.

EQUIPO DE COMPUTO: Conjunto (Kit) compuesto por una pantalla, teclado, mouse, impresora, UPS, estabilizador, cables, supresor de pico y/o estabilizador de corriente, CPU y protector de pantalla.

HARDWARE: Parte física de una computadora: placa, microprocesador, tarjetas, monitor, etc.

IMPRESORA: Dispositivo periférico que reproduce texto e imágenes en papel. Los principales tipos son: de matriz de puntos, de chorro de tinta y láser.

INFRAESTRUCTURA TECNOLOGICA: Conjunto de bienes que se consideran necesarios para garantizar el funcionamiento de los servicios informáticos soportados en tecnología, entre los que podemos mencionar: equipos de cómputo personal o portátil, impresoras, scanner, servidores, estaciones de trabajo, entre otros.

INTERNET: Red de ordenadores a nivel mundial. Ofrece distintos servicios, como el envío y recepción de correo electrónico, la posibilidad de ver información en las páginas web, de participar en foros de discusión, de enviar y recibir ficheros, de charlar en tiempo real, etc.

LAN (Local Área Network): Nombrado así a la interconexión de 2 o más computadoras que comparten servicios y recursos en común.

LOGIN: Cuenta de usuario para el acceso a los recursos en la red Institucional.

MONITOR: Unidad de visualización, pantalla.

PASSWORD: Contraseña de seguridad de uso personal.

PROGRAMAS DE TRABAJO: Programas diseñados por la Institución o adquiridos a través de terceros para el desempeño de actividades (SIAF, SIGA, SIADEG, etc.)

PERIFÉRICO: Se refiere a cámaras web (webcam), scanner, mouse, teclado, monitor, impresoras, parlantes.

SISTEMAS BASE: Conjunto de programas mínimos necesarios para el uso del equipo de cómputo dentro de la Institución (Windows, Word, Excel, Internet Explorer).

SISTEMA DE INFORMACION: Todo aquel programa o software informático que se ha confeccionado para brindar un servicio de manejo de información,

el mismo que puede haber sido creado por personal de la entidad, o se haya adquirido.

SOFTWARE: Cada uno de los programas que, una vez ejecutados, permiten trabajar con la computadora. Por ejemplo, los procesadores de texto (Microsoft Word), hojas de cálculo (Microsoft Excel), bases de datos (SQL Server), programas de dibujo (Corel Draw), paquetes estadísticos (S-Plus), etc.

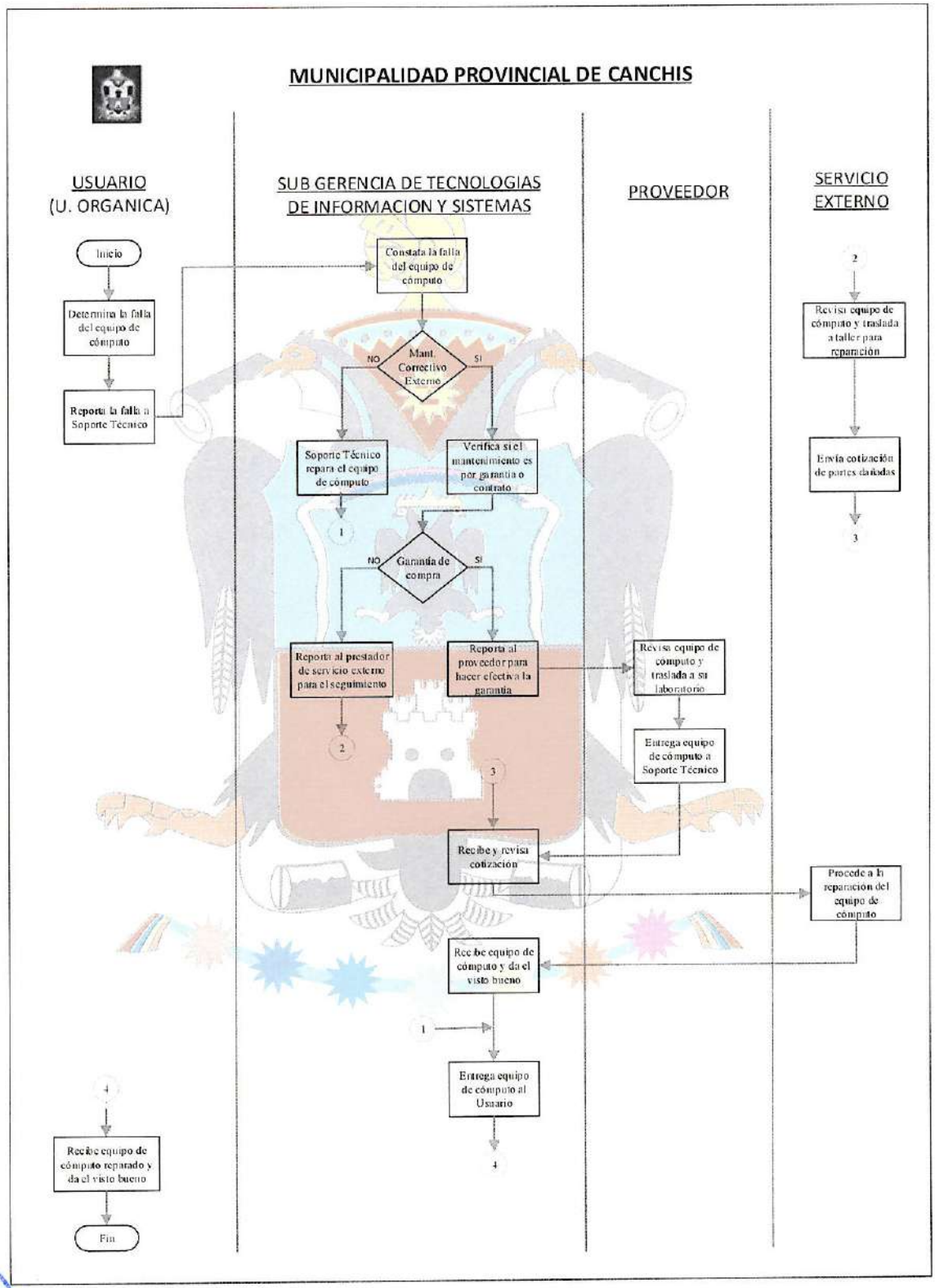
UPS: Sistema de alimentación ininterrumpida, diseñado para proporcionar energía eléctrica de manera automática, sin retardo, durante un período cuando el suministro normal de energía eléctrica no puede funcionar de manera aceptable.

USB: Sigla del inglés "universal serial bus", permite conectar diferentes periféricos a una computadora.

USUARIO: Persona que presta servicios en la institución, bajo cualquier régimen laboral y que interactúa con la computadora.

XII. FLUJOGRAMA

12.1. PROCEDIMIENTO PARA EL MANTENIMIENTO DE EQUIPOS DE CÓMPUTO



XIII. ANEXOS.

13.1. ORDEN DE SOPORTE TECNICO

MUNICIPALIDAD PROVINCIAL DE CANCHIS					
FICHA DE MANTENIMIENTO DE EQUIPOS DE COMPUTO					
UNIDAD ORGANICA					
RESPONSABLE					
USUARIO		CARGO			
CARACTERISTICAS FISICAS DEL EQUIPO					
PC / LAPTOP/IMPRESORA		MARCA		COD. PAT.	
MONITOR / TECLADO / MOUSE		SERIE			
PROCESADOR				DIRECCION IP	
DISCO DURO				GATEWAY	
MEMORIA RAM					
TARJETA DE VIDEO					
TARJETA DE SONIDO					
OBSERVACIONES					
MOTIVO DE INGRESO	FECHA / /	TRABAJO EFECTUADO		FECHA / /	
SGTIS		Firma del Usuario			

13.2. FORMATO DE CREACION DE CORREO INSTITUCIONAL

	MUNICIPALIDAD PROVINCIAL DE CANCHIS
	FICHA DE CREACION DE CORREO INSTITUCIONAL
	FECHA:
GERENCIA	
OFICINA O DEPENDENCIA	
NOMBRES Y APELLIDOS	
CARGO	
DNI	

SGTIS

Firma del Usuario

13.3. FORMATO DE CARTA DE CONFIDENCIALIDAD.

CARTA DE CONFIDENCIALIDAD PARA TRABAJADORES DE LA MUNICIPALIDAD PROVINCIAL DE CANCHIS.

Estimado señor:

Por medio de la siguiente carta, YO _____identificado con DNI N° _____ mayor de edad y en plenas facultades mentales, me obligo a mí mismo a no divulgar ni utilizar en mi conveniencia personal la distinta información obtenida mediante mi colaboración en el cargo de _____, ni proporcionaré a otras personas o empresas y/o entidades públicas, ni de manera verbal, ni de manera escrita, o digital ya sea directa o indirectamente, información alguna que pueda perjudicar los intereses de la Municipalidad Provincial de Canchis.

- ✓ No revelaré ninguna información sobre la disposición de las oficinas.
- ✓ No revelaré ninguna información sobre las herramientas de trabajo ni el equipo informático que se utiliza dentro ni fuera de las instalaciones.
- ✓ No revelaré ninguna información sobre el sistema de comunicación.

Este acuerdo de confidencialidad será mantenido de manera indefinida, ahora y en el futuro, hasta que la Municipalidad Provincial de Canchis lo de por finalizado.

Atentamente:

_____

NOMBRE:

N° DNI:

13.4. FICHA DE AUTORIZACION NUEVO USUARIO SIADEG

FICHA DE AUTORIZACION NUEVO USUARIO SIADEG

SIADEG

GERENCIA	
OFICIA O DEPENDENCIA	
NOMBRES Y APELLIDOS	
CARGO	
DNI N°	
META N°	
AUTORIZACION DE META (GERENCIA DE PLANEAMIENTO Y PRESUPUESTO)	
JEFE INMEDIATO SUPERIOR	

FECHA:

13.5. FICHA DE AUTORIZACION NUEVO USUARIO SIAF

FICHA DE AUTORIZACION NUEVO USUARIO SIAF

GERENCIA	
OFICIA O DEPENDENCIA	
NOMBRES Y APELLIDOS	
CARGO	
DNI N°	
MODULOS A UTILIZAR	
AUTORIZACION DEL JEFE (FIRMA Y SELLO)	
FECHA	

13.6. FICHA DE AUTORIZACION NUEVO USUARIO SISTEMAS RENTAS

FICHA DE AUTORIZACION NUEVO USUARIO RENTAS

GERENCIA	
OFICIA O DEPENDENCIA	
NOMBRES Y APELLIDOS	
CARGO	
DNI N°	
MODULO O SISTEMA A UTILIZAR	
AUTORIZACION DEL JEFE (FIRMA Y SELLO)	
FECHA	