Municipalidad Provincial de Canchis

RESOLUCION DE ALCALDIA N° 178-2016-A-MPC.

Sicuani, 12 de setiembre de 2016.

VISTOS: El Informe N° 0270-2016-GM-MPC, de fecha 07 de setiembre de 2016, emitido por el Gerente Municipal, el Informe Nº 131-SGPRyCT-GPP-MPC-2016, de fecha 11 de agosto de 2016, emitido por la Sub Gerente de Planeamiento, Racionalización y Cooperación Técnica, el Informe N° 031A-2016-SGTIS/GAF-MPC, de fecha 18 de julio de 2016, emitido por el Sub Gerente de Tecnologías de Información y Sistemas y la Opinión Legal N° 628-2016-MPC-OAJ/OVG, de fecha 16 de agosto de 2016, emitido por el Asesor Jurídico de la Municipalidad.

I CONSIDERANDO:

1. Que, el Art. 194º de la Constitución Política del Perú, concordante con el Art. II del Título Preliminar de la Ley Orgánica de Municipalidades, Ley Nº 27972. ***"Los Gobiernos Locales gozan de autonomía política, económica y administrativa en los asuntos de su competencia (...)."***

2. Que, conforme a lo dispuesto por el Art. 6º de la Ley Orgánica de Municipalidades ***"La alcaldía es el órgano ejecutivo del gobierno local. El alcalde es el representante legal de la municipalidad y su máxima autoridad administrativa".***

3. Que, el Art. 20° numeral 6 del cuerpo normativo en referencia, establece que entre otras son atribuciones del alcalde: ***"Dictar decretos y resoluciones de alcaldía, con sujeción a las leyes y ordenanzas"***.

4. Que, asimismo el Art. 39º del mismo cuerpo normativo establece ***"Las resoluciones de alcaldía aprueban y resuelven los asuntos de carácter administrativo".***

5. Que, la Ley de Organización y Funciones del Instituto Nacional de Estadística e Informática – Decreto Legislativo N° 604, en su artículo 7° establece que los Sistemas Nacionales de Estadística e Informática están integrados por: f. ***Los órganos de estadística y/o informática de las Municipalidades... (...);*** En esa línea normativa con Resolución Ministerial N° 004-2016-PCM, se ha aprobado el uso obligatorio de la Norma Técnica Peruana NTP ISO/IEC 27001:2014 Tecnología de la información. Técnica de seguridad. Sistemas de Gestión de Seguridad de la Información, en todas las Entidades integrantes del Sistema Nacional de Informática.

6. Que, La Oficina Nacional de Gobierno Electrónico e Informática – ONGEI, de la Presidencia del Concejo de Ministros, ha publicado en su Portal Web, la Guía para la Elaboración del Plan de Contingencias y Seguridad de la Información de las distintas instituciones estatales, proponiendo como actividad permanente la formulación y evaluación del Plan Operativo Informático de las Entidades de la Administración Pública y su respectiva Guía de Elaboración.

7. Que, Conforme a la Resolución Ministerial N° 019-2011-PCM se aprobó la Formulación y Evaluación del Plan Operativo Informático de las Entidades de la Administración Pública, y su Guia de Elaboración, en la que señala que las entidades a la que se refiere el artículo 3° de la Ley Orgánica del Sistema Nacional de Control y de la Contraloría General de la República se encuentran sujetas al Sistema Nacional de Informática, siendo de aplicación la referida Resolución Ministerial.

8. Que, dentro de dicho contexto, debemos señalar que el Plan de Contingencia y Seguridad de la Información de nuestra Entidad, tiene como objetivo general de asegurar la información mediante políticas que conlleven a un nivel de protección

aceptable, garantizar la continuidad de las actividades de la Municipalidad Provincial de Canchis, ante eventos que podrían alterar el normal funcionamiento de las Tecnologías de la Información y Comunicaciones, a fin de minimizar el riesgo no previsible, emergencias y responder de forma inmediata en la recuperación de las actividades.

9. Que, mediante Informes N° 0270-2016-GM-MPC, de fecha 07 de setiembre de 2016, el Gerente Municipal, solicita la aprobación del Plan de Contingencia y Seguridad de la Información de la Municipalidad Provincial de Canchis, conforme a la propuesta presentada por el Sub Gerente de Tecnologías de Información mediante Informe N° 031A-2016-SGTIS/GAF-MPC, de fecha 18 de julio de 2016, el mismo que cuenta con opinión favorable de la Sub Gerencia de Planeamiento, Racionalización y Cooperación Técnica, conforme se tiene del Informe N° 131-SGPRyCT-GPP-MPC-2016, de fecha 11 de agosto de 2016; Asimismo se tiene que al respecto, se ha emitido la Opinión Legal N° 628-2016-MPC-OAJ/OVG, de fecha 16 de agosto de 2016, mediante el cual el Asesor Jurídico de la Municipalidad, declara procedente la aprobación del referido Plan de Contingencia y Seguridad.

Por estas consideraciones y en uso de las atribuciones conferidas por la Constitución Política del Estado, la Ley Orgánica de Municipalidades y demás normas pertinentes;

SE RESUELVE:

ARTICULO PRIMERO: APROBAR EL **PLAN DE CONTINGENCIA Y SEGURIDAD DE LA INFORMACION DE LA MUNICIPALIDAD PROVINCIAL DE CANCHIS,** desarrollado en diez (10) Capítulos, nueve (09) Consideraciones Finales y cinco (05) Anexos, contenidos en un anillado de ochenta y un (81) folios, que como anexo forma parte de la presente Resolución.

ARTICULO SEGUNDO: ENCARGAR a la Gerencia Municipal para que en coordinación con la Gerencia de Administración y Finanzas y la Sub Gerencia de Tecnologías de Información y Sistemas, den cumplimiento a lo dispuesto en la presente Resolución.

ARTICULO TERCERO: DISPONER que la Sub Gerencia de Tecnologías de Información y Sistemas, cumpla con publicar la presente Resolución y anexos en el Portal Web de la Entidad.

ARTICULO CUARTO: DISPONER la notificación de la presente Resolución a Gerencia Municipal y demás instancias que correspondan, para su implementación y fines correspondientes.

REGISTRESE, COMUNIQUESE Y CUMPLASE.

MUNICIPALIDAD PROVINCIAL DE CANCHIS
Lic. Manuel J. Zvietcovich Alvarez
ALCALDE
DNI: 23813727

C.C.
Alcaldía.
Ger. Municipal.
Ger. Administración.
Ger. Planeamiento.
Sub Ger. Plan y Racionalización.
Sub Ger. Téc. Información.
Archivo.
MJZA/sca.

Municipalidad Provincial de Canchis
ABOG. SALOMÓN CRUZ ARAGÓN
SECRETARIO GENERAL

MUNICIPALIDAD PROVINCIAL DE CANCHIS

"PLAN DE CONTINGENCIA Y SEGURIDAD DE LA INFORMACIÓN DE LA MUNICIPALIDAD PROVINCIAL DE CANCHIS"

Versión 1.01

Este es un documento electrónicamente controlado y publicado. Cualquier impresión o copia dura debe ser verificada

HOJA DE INFORMACION

PLAN:	Plan de Contingencia y Seguridad de la Información.
ENTIDAD:	Municipalidad Provincial de Canchis
ELABORADO POR:	Sub Gerencia de Tecnologías de Información y Sistemas
VERSIÓN:	1.01
FECHA DE EDICION:	03/07/2016
NOMBRE DE ARCHIVO:	PLAN-001-SGTIS-MPC-2016.PDF
RESUMEN:	PLAN DE CONTINGENCIA Y SEGURIDAD DE LA INFORMACIÓN DE LA MUNICIPALIDAD PROVINCIAL DE CANCHIS.

Control de Versión

REVISIÓN	Numeral del Plan	MODIFICACIÓN REALIZADA	Nombre y Firma de quien autoriza	FECHA DEL CAMBIO

ÍNDICE

INTRODUCCIÓN

La Municipalidad Provincial de Canchis cuenta con un amplio parque informático conformado por una gran cantidad de equipos de cómputo e impresión, equipos de comunicaciones, etc. que facilitan el almacenamiento, procesamiento, transporte y presentación de la información, la que representa un activo valioso de la organización.

La información es un activo que tiene un elevado valor para la Entidad, lo que requiere que se genere una protección adecuada, debido a que pudiera estar expuesta a un alto número de amenazas y vulnerabilidades.

Es importante resaltar para que la organización logre sus objetivos necesita garantizar tiempos de disponibilidad eficientes, tanto en sus recursos informáticos como en las comunicaciones; es decir se debe minimizar las interrupciones de la disponibilidad de la información en todo momento, por causa de algún incidente interno o externo a la organización por lo que se debe adoptar medidas de seguridad para la información y así mismo estar preparados para poder afrontar contingencias y desastres de tipo diverso, para lo cual se debe establecer un Plan de Contingencia y Seguridad de la Información que sea eficiente en todas las áreas operativas.

Es necesario, por tanto adoptar políticas de seguridad basadas en estándares y normas actuales emanadas del ente rector del Sistema Nacional de Informática cuya dirección recae en la Oficina Nacional de Gobierno Electrónico e Informática ONGEI que a su vez depende de la Presidencia del Consejo de Ministros.

La Subgerencia de Tecnologías de la Información y Sistemas, en adelante SGTIS, está comprometido en la seguridad de la información, así como asegurar su disponibilidad para la continuidad de los procesos y servicios institucionales. En base a ello elabora el Plan de Contingencia y Seguridad de la Información de la Municipalidad Provincial de Canchis.

Este Plan debe conllevar en el futuro a establecer, implementar, mantener y mejorar continuamente un efectivo Sistema de Gestión de Seguridad de la Información en la Municipalidad Provincial de Canchis.

La adopción de un SGSI debe ser una decisión estratégica de la Alta Dirección de la Municipalidad, teniendo en cuenta las necesidades y objetivos institucionales, los requisitos de seguridad, procesos, tamaño y estructura de la organización.

El presente Plan en lo que se refiere a la Seguridad de la Información tiene como fundamento legal la Resolución Ministerial N° 04-2016-PCM que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2da Edición", en todas las entidades integrantes del Sistema Nacional de Informática y al mismo tiempo deroga la Resolución Ministerial N° 129-2012-PCM, que aprobó la Norma Técnica Peruana NTP-ISO/IEC 27001 2008 EDI.

El estándar ISO 27001 es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan.

La Gestión de la Seguridad de la Información se complementa con las buenas prácticas o controles establecidos en la norma ISO 27002 (anteriormente denominada ISO 17799)

La Subgerencia de Tecnologías de Información y Sistemas

CAPITULO I

1. GENERALIDADES

1.1. OBJETIVOS

Generales:

- Asegurar la información mediante políticas que conlleven a un nivel de protección aceptable y garantizar la continuidad de las actividades de la Municipalidad Provincial de Canchis, ante eventos que podrían alterar el normal funcionamiento de las Tecnologías de la Información y Comunicaciones - TICs, a fin de minimizar el riesgo no previsible, críticos o de emergencia, y responder de forma inmediata hacia la recuperación de las actividades normales.

Específicos:

- Preservar la confidencialidad, integridad y disponibilidad de la información aplicando un proceso de gestión de riesgos.
- Contar con documentación actualizada de procedimientos que garanticen a la Municipalidad Provincial de Canchis la continuidad de las operaciones de los sistemas informáticos sin sufrir paralizaciones o pérdidas relevantes.
- Identificar y analizar riesgos posibles que pueden afectar las operaciones y procesos informáticos de la entidad.
- Establecer las estrategias adecuadas para asegurar la continuidad de los servicios informáticos en caso de interrupción y que ésta no exceda las 24 horas.
- Contar con personal debidamente capacitado y organizado para afrontar adecuadamente las contingencias que puedan presentarse.

1.2. ALCANCE

El Plan de Contingencia y Seguridad de la Información comprende a todas las áreas de la Municipalidad Provincial de Canchis que utilicen sistemas de información, equipos servidores y respectivos equipos cliente, infraestructura informática, servicios informáticos y otros relacionados, con la finalidad de garantizar la seguridad de la información y minimizar eventuales riesgos ante situaciones adversas que pudieran presentarse.

1.3. BASE LEGAL

- Ley 27972 - Ley Orgánica de Municipalidades.
- Resolución Ministerial N° 04-2016-PCM que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2da Edición", en todas las entidades integrantes del Sistema Nacional de Informática. Quedando derogada la Resolución Ministerial N° 129-2012-PCM.
- Decreto Supremo N° 066-2011-PCM que aprueba el "Plan de Desarrollo de la Sociedad de la información en el Perú - La Agenda Digital Peruana 2.0", y

que en su Objetivo N° 7, establece la necesidad de promover una Administración Pública de calidad orientada a la población, y la necesidad de contar con una Estrategia Nacional de Ciberseguridad, con el objetivo de minimizar los riesgos en caso de sufrir algún tipo de incidente en los recursos informáticos del Estado, así como, la disuasión del crimen cibernético, que se producen mediante el uso de redes teleinformáticas, entre otros.

- Resolución Ministerial N° 246-2007-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana NTP-ISO/IEC 17799:2007 EDI Tecnologías de la Información, Código de Buenas Prácticas para la Gestión de Seguridad de la Información 2da edición en todas las entidades integrantes del Sistema Nacional de Informática.
- Decreto Supremo N° 031-2006-PCM, que aprueba el "Plan de Desarrollo de la Sociedad de la información en el Perú - La Agenda Digital Peruana".
- Resolución Ministerial No 274-2006-PCM, que aprueba la "Estrategia Nacional de Gobierno Electrónico".
- Resolución de Contraloría General N° 320-2006-CG, que aprueba las "Normas de Control Interno", que son de aplicación a las entidades del Sector Público.

CAPITULO II

2. SITUACIÓN ACTUAL

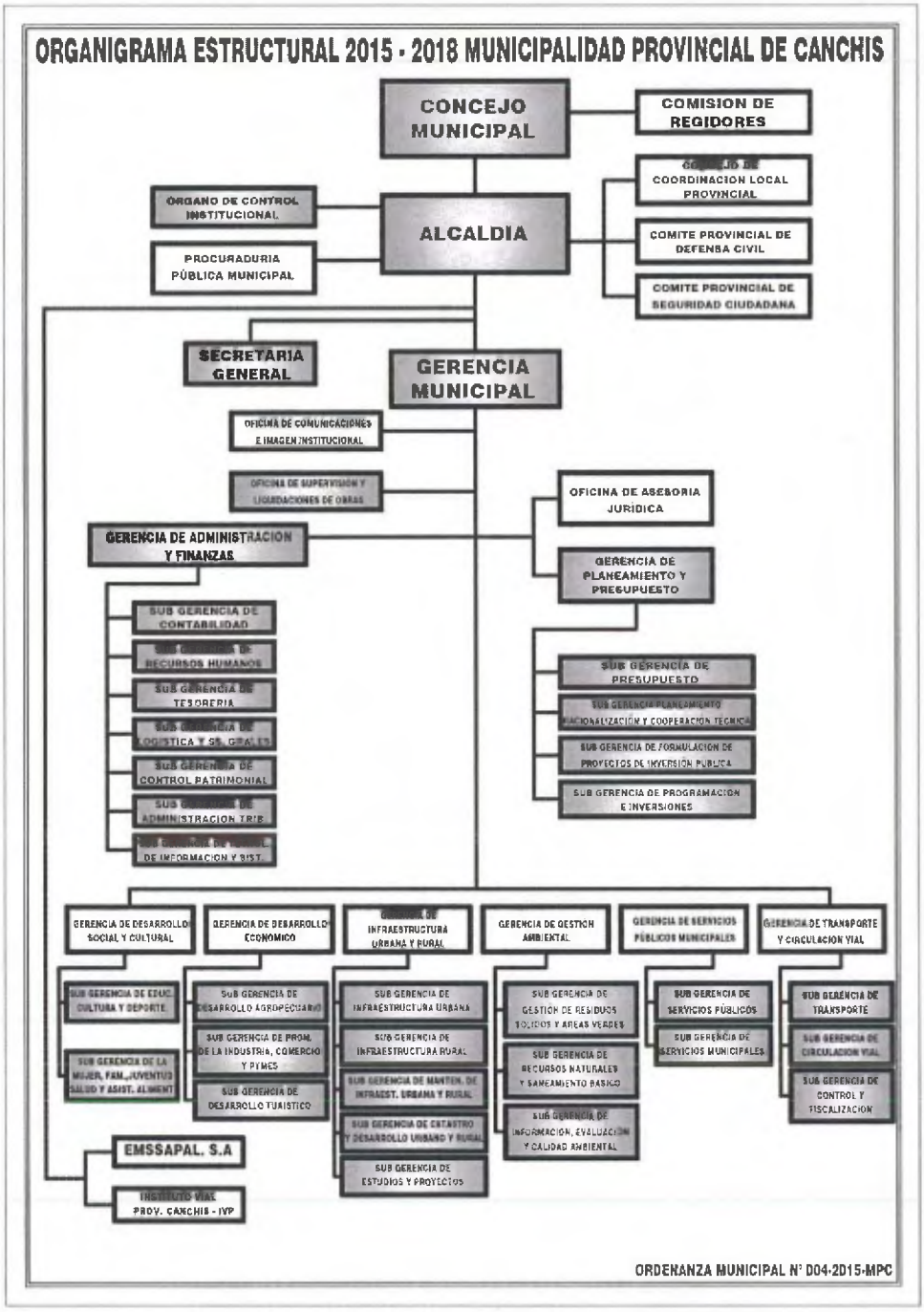
2.1. DIAGNOSTICO

Efectuada una revisión del aspecto situacional de riesgos de Tecnologías de Información de la Municipalidad Provincial de Canchis consideramos que debe elaborarse un Plan de Contingencia y Seguridad de la Información que sirva como metodología, guía o marco de trabajo que ayude a la identificación de riesgos y determinar controles para mitigarlos.

Dentro de los distintos aspectos a considerar en la seguridad de la información, es necesario elaborar Políticas de Seguridad de la Información y una clasificación de seguridad de los Activos de Información de la Municipalidad. Cabe mencionar que se ha verificado la existencia de un Plan de Contingencia y Seguridad de la Información y directivas internas que considera la seguridad lógica y el control de los accesos a los sistemas de información así como los procedimientos técnicos establecidos para el otorgamiento de dichos accesos.

2.2. ORGANIZACIÓN

2.2.1. ORGANIGRAMA



2.2.2. ESTRUCTURA Y FUNCIONES

a. El Concejo Municipal

El Concejo Municipal, es el órgano de Gobierno de la Municipalidad Provincial de Canchis, presidido por el alcalde e integrado por Regidores, quienes conjuntamente con el Alcalde son elegidos en las elecciones Municipales.

El Concejo Municipal ejerce funciones normativas y fiscalizadoras.

b. Alcaldía

La Alcaldía es el órgano ejecutivo del Gobierno Local. El alcalde es el representante legal y la mayor autoridad administrativa de la Municipalidad y representante máximo de la voluntad ciudadana y el que personifica a su comunidad, sus funciones están señaladas en la Ley Nº 27972 "Ley Orgánica de Municipalidades".

c. Oficina de Control Interno

La Oficina de Control Interno es el órgano de Control Institucional, responsable de ejecutar el control gubernamental interno preventivo y posterior en la Municipalidad Provincial de Canchis, para la correcta y transparente gestión de los recursos y bienes de la Municipalidad, cautelando la legalidad y eficiencia de sus actos y operaciones, así como el cumplimiento de las metas y logro de sus resultados previstos.

d. Procuraduría Pública Municipal

La Procuraduría Pública Municipal es el órgano de defensa, encargado de la representación y defensa de los intereses y derechos de la Municipalidad Provincial de Canchis.

Está a cargo del Procurador Público Municipal, quien es designado por el Alcalde, y depende administrativamente de la Municipalidad y funcional y normativamente del Consejo de Defensa Judicial del Estado.

e. Gerencia Municipal

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.

La Gerencia Municipal está a cargo de un Gerente Municipal quien depende del Alcalde.

f. Oficina de Asesoría Jurídica

La Oficina de Asesoría Jurídica es el órgano de asesoramiento a la alta dirección, desarrollando funciones consultivas en materia jurídica, así como brinda asesoramiento sobre la adecuada interpretación y difusión de las normas legales de competencia municipal.

La oficina de Asesoría Legal depende funcionalmente y jerárquicamente de la Gerencia Municipal.

g. Gerencia de Planeamiento y Presupuesto

La Gerencia de Planeamiento y Presupuesto es el órgano de asesoramiento, responsable de dirigir, ejecutar y evaluar las actividades referidas a los Sistemas de Planificación, Presupuesto y Racionalización, la gestión de proyectos, la promoción de Inversiones y la Gestión de Cooperación Técnica. Coordina sus acciones con los diferentes órganos de la Municipalidad, así como con otros sectores Públicos o Privados cuyas funciones tienen relaciones con el desarrollo de la Provincia.
Está a cargo de un Gerente, quien depende del Gerente Municipal.

h. Gerencia de Administración y Finanzas
La Gerencia de Administración y Finanzas es el órgano de apoyo responsable de asegurar la unidad, racionalidad y eficiencia de los sistemas administración tributaria, Contabilidad, Tesorería, Personal, Logística y servicios generales y Tecnologías de Información y Sistemas.
Está a cargo de un Gerente quien depende del Gerente Municipal.

FORMULACIÓN

i. Sub Gerencia de Proyectos de Inversión Publica
La Sub Gerencia de Proyectos de Inversión Publica, es el órgano de asesoramiento responsable de conducir la formulación de proyectos en la fase de pre inversión, en el marco del Sistema Nacional de Inversión Publica (SNIP).
Está a cargo de un Sub Gerente quien depende del Gerente de Planeamiento y Presupuesto.

j. Gerencia de Desarrollo Social y Cultural
La Gerencia de Desarrollo Social y Cultural, es el órgano de Línea, responsable de la organización de los servicios de salud, educación, cultura y deporte, promueve las actividades relacionadas con el desarrollo social en procura de una mejor calidad de vida en el ámbito provincial.
La Gerencia de Desarrollo Social y Cultural depende jerárquicamente del Gerente Municipal.

k. Gerencia de Desarrollo Económico
La Gerencia de Desarrollo Económico es el Órgano de Línea, responsable de planificar, organizar, dirigir y supervisar las actividades, proyectos y/o programas relacionados con la promoción del desarrollo económico local y el fomento a la competitividad, promoción y fortaleçimiento de capacidades de los diferentes sectores productivos del territorio, actividades empresariales, industriales y micro empresariales.
Está a cargo de un Gerente, quien depende del Gerente Municipal.

l. Gerencia de Infraestructura Urbana y Rural
La Gerencia de Infraestructura Urbana y Rural es el Órgano de Línea, responsable de planificar, organizar, ejecutar y supervisar las acciones referidas al acondicionamiento territorial, vivienda, elaboración y

Actualización del Catastro y del Plan Director, la ejecución de obras por administración "directa, y la conservación y restauración del patrimonio cultural, local y monumentos arqueológicos en el ámbito Urbano y Rural. Está a cargo de un Gerente, quien depende del Gerente Municipal.

m. Gerencia de Servicios Públicos Municipales

La Gerencia de Servicios Públicos Municipales es el Órgano de Línea responsable de formular, proponer, planificar, programar, dirigir, ejecutar, supervisar y administrar las políticas de servicios a la comunidad, tales como Registro Civil, Seguridad Ciudadana, Policía Municipal, el Comercio Ambulatorio y mercados, el Camal Municipal, Limpieza Pública y la Administración del Terminal Terrestre.

n. Oficina de Comunicaciones e imagen institucional

La Oficina de Comunicaciones e imagen institucional, es el órgano de apoyo a la Alta Dirección encargada de planificar, programar, dirigir, ejecutar, coordinar y controlar las actividades de comunicación y difusión así como los actos protocolares internos y externos de la Municipalidad, del mismo modo desarrolla actividades relacionadas a la buena imagen de la Gestión Municipal al interior y exterior a través de los medios y canales de difusión.
Está a cargo de un Jefe de Oficina, quien depende del Gerente Municipal.

o. Subgerencia de Tecnologías de Información y Sistemas

La Subgerencia de Tecnologías de Información y Sistemas es el órgano de apoyo encargado de la Planificación, evaluación, adopción, aplicación, administración y control de las tecnologías de la Información que permitan el soporte a las funciones Municipales, con procesos y procedimientos modernos de manera que las actividades y tareas de la Institución se realice con eficacia y eficiencia, para reducir los costos.
Está a cargo de un Sub Gerente quien depende del Gerente de Administración y Finanzas.

2.2.3. RECURSOS INSTITUCIONALES

El Plan de Contingencia y Seguridad Informática, se organiza para que la Entidad pueda asegurar la información mediante políticas que conlleven a un nivel de protección aceptable y en caso de contingencia recuperar la operatividad de los procesos ante eventos internos o externos que incidan negativamente en las operaciones de los procesos informáticos, y que les permitan seguir activas asegurando la continuidad de los mismos.

El presente Plan de Contingencia y Seguridad de la Información requiere de algunos requisitos para la eficacia de los resultados de la puesta en marcha del plan:

a. Humanos

Están dadas por el personal que conforman los equipos de trabajo contemplados en el presente Plan, las cuales deberán estar plenamente capacitados, quienes aplicaran los procedimientos para ejecutar el Plan

de Contingencia y Seguridad de la Información en sus diversas fases o etapas.
Se debe establecer claramente los líderes de los equipos de trabajo que funcionalmente serán los Gerentes de cada área operativa, que deben comprender la importancia de la aplicación del plan.

b. Materiales

El despliegue del Plan de Contingencia y Seguridad de la Información Informático requiere de herramientas de soporte, computadores y o servidores de relevo, equipos de impresión, soporte de almacenamiento externo, necesario para llevar a cabo el plan. Además deberá contarse con zonas o locaciones alternativas para que se dé continuidad a los procesos informáticos en casos de desastres mayores.

c. Financieros

Los recursos financieros con que se requiere contar para la aplicación del presente Plan de Contingencia, deberá contemplarse en la formulación del Presupuesto Anual Institucional y como parte del Plan Operativo Informático de la SGTIS.

d. Entrenamiento

El personal participante deberá ser entrenado para la aplicación correcta del Plan de tal manera que se cumplan con los objetivos trazados, que se debe traducir en la minimización del impacto negativo de la contingencia.

e. Responsabilidad

La Alta Dirección habrá de ejercer la función de control y asegurará que las tareas desarrolladas, sean cumplidas de acuerdo a los planteamientos y objetivos del plan.

CAPITULO III

3. PLAN DE CONTINGENCIA Y SEGURIDAD DE LA INFORMACIÓN

El Plan de Contingencia y Seguridad de la Información implica un análisis de los posibles riesgos a los cuales pueden estar expuestos nuestros equipos de cómputo y la información contenida en los diversos medios de almacenamiento, por lo que en necesario realizar un análisis de los Riesgos, cómo reducir su posibilidad de ocurrencia y los procedimientos a seguir en caso que se presentara el problema.

Pese a todas nuestras medidas de seguridad puede ocurrir un desastre, por tanto es necesario que el Plan de Contingencia y Seguridad de la Información incluya un Plan de Recuperación de Desastres, el cual tendrá como objetivo, restaurar los servicios informáticos en forma rápida, eficiente y con el menor costo y pérdidas posibles.

Si bien es cierto que se pueden presentar diferentes niveles de daños, también se hace necesario presuponer que el daño ha sido total, con la finalidad de tener un Plan de Contingencia y Seguridad de la Información y lo más completo posible.

Haciendo un esquema, el Plan de Contingencia y Seguridad de la Información abarcara los siguientes aspectos:

3.1. PLAN DE REDUCCIÓN DE RIESGOS (PLAN DE SEGURIDAD)

Para asegurar que se consideran todas las posibles eventualidades, se ha de elaborar la lista de todos los riesgos conocidos, para lo cual se deberá realizar un análisis de riesgos.

3.1.1. ANÁLISIS DE RIESGOS

Es análisis de riesgos supone más que el hecho de calcular la posibilidad de que ocurran cosas negativas. Se ha de poder obtener una evaluación económica del impacto de estos sucesos negativos. Este valor se podrá utilizar para contrastar el costo de la protección dela información en análisis, versus el costo de volver a producir (reproducir). Se ha de tener en cuenta la probabilidad de que sucedan cada uno de los problemas posibles. De esta forma se pueden priorizar los problemas y su coste potencial desarrollando un plan de acción adecuado.

¿A qué riesgos en la seguridad informática se enfrenta la Institución?

- Al fuego, que puede destruir los equipos y archivos.
- Al robo común, perdida de los equipos y archivos.
- Al vandalismo, que dañen los equipos y archivos.
- A fallas en los equipos, que dañen los archivos.
- A equivocaciones que produzcan daños a los archivos.
- A la acción de virus, que dañen los equipos y archivos.
- A terremotos, que destruyen el equipo y los archivos.
- A accesos no autorizados, filtrándose datos no autorizados.
- Al robo de datos, difundiéndose los datos sin autorización

- Al fraude informático, desviando fondos merced a la computadora.

¿Qué probabilidad hay de que tenga efecto alguno de los riesgos mencionados?

Al fuego, que puede destruir los equipos y los archivos
La Institución no cuenta con protección contra incendios en cada una de las áreas que cuenta con activos informáticos, especialmente el Data Center donde se encuentran instaladas los equipos servidores, solo cuenta con alguna protección contra incendios el área de Gerencia de Obras.
Falta capacitación al personal referente a cómo actuar en caso de incendio.

A un robo común, pérdida de los equipos y archivos
La institución se encuentra en el centro de la ciudad y se han registrado pérdidas de celulares, cámara fotográfica, laptops, existiendo una sola puerta de ingreso, la que es custodiada por el personal de guardianía tanto en horario de oficina como fuera del horario de oficina.

Al vandalismo, que dañen los equipos y archivos
No existen antecedentes al respecto, pero hubo incidentes debido a factores sociales o políticos que produjeron hechos violentos contra el palacio municipal debido a protestas por parte de ciertos sectores de la población quienes atacaron con piedras y produjeron destrozos en las ventanas de la entidad.

A fallas en los equipos, que dañen los archivos
Las fallas que vienen reportando los equipos en la mayoría de los casos han sido originadas por el tiempo de vida de los equipos, los cuales tenían más de cinco años de antigüedad.

A equivocaciones que produzcan daños en los archivos
El personal o área usuaria reporta cualquier problema del funcionamiento de su equipo a la Subgerencia de Tecnologías de Información y Sistemas, para que solucione el problema.
Pero es de conocimiento que de manera accidental o incidental algunos usuarios eliminaban o formateaban las unidades del disco duro, trayendo como consecuencia la perdida de la información.

A la acción de virus, que dañen los archivos
Lamentablemente, algunos usuarios no cumplen con la normativa de prohibición de instalar programas por su cuenta, que los únicos autorizado a instalar es la Subgerencia de Tecnologías de Información y Sistemas.
El personal no autorizado puede instalar programas que en algunos casos contiene virus informático, debido a que fue descargado de internet o procedía de una fuente no confiable.
Se supervisa que los antivirus estén operativos y actualizados.

A terremotos, que destruyen los equipos y archivos
La institución se encuentra en una zona de poca actividad sísmica, el edificio es de construcción con material noble.

A accesos no autorizados, filtrándose datos importantes
Se cuenta con modem de acceso a internet los cuales tienen los puertos cerrados para evitar que algún intruso pueda ingresar a la red interna de la entidad.
Pero en algunas ocasiones se abren ciertos puertos para que se realice el mantenimiento de los sistemas informáticos por parte de los proveedores que solicitan el acceso remoto para realizar tareas de mantenimiento correctivo a los sistemas de información. Cabe mencionar que todos los Sistemas de Información instalados en los diferentes equipos servidores y equipos clientes son adquiridos a terceros ya que la Subgerencia de Tecnologías de Información y Sistemas no cuenta con un departamento de desarrollo de sistemas.

Actualmente se utiliza una red con Grupos de Trabajo, para el acceso a usuarios autorizados a los sistemas de información como el SIAF, SIGA, Sistema de Rentas y arbitrios Municipales, Sistema Integrado de Logística y Requerimientos, Sistema de Registro Civil.

Al robo de datos; difundiéndose los datos sin autorización.
La única forma de acceso a los servidores de las Bases de Datos es a través de la red interna por parte del personal autorizado los cuales poseen una cuenta de acceso y son responsables de su uso y seguridad de los mismos. No hay incidentes o reportes de robo de información conocidos. Se cuenta con Bases de datos en los servidores de la entidad en las que se encuentran instalados los Sistemas de Información de Rentas y Arbitrios Municipales, SIAF (Contabilidad, Tesorería, Planificación y Presupuestos), SIGA, Registro Civil, Sistema Integrado de Logística y Requerimientos Lord Pro.

Al fraude, desviando fondos merced a la computadora.
La institución realiza transferencias electrónicas a los bancos, se trabaja de manera normal, no existiendo ningún antecedente.

Resumen de los riesgos ordenados por el factor de riesgo de cada uno

Tipos de Riesgo	Factor de Riesgo
Robo	Medio
Fuego	Medio
Fallas en los equipos	Medio
Acción de virus	Medio
Equivocaciones	Bajo
Terremotos	Bajo
Accesos no autorizados	Bajo
Robo de datos	Bajo
Fraude	Muy bajo
Vandalismo	Muy bajo

PROTECCIONES ACTUALES

- Robo común, se cierran las puertas de entrada y ventanas fuera de hora trabajo.
- Vandalismo, se cierra la puerta principal cuando hay problemas con manifestaciones.

- Falla de los equipos, se tratan con cuidado, se realiza el mantenimiento de forma regular a solicitud del usuario
- Daño por virus, el software a instalar se analiza utilizando software antivirus. Los programas de dominio público y de uso compartido (Shareware), sólo se usan si proceden de una fuente fiable.
- Equivocaciones, los empleados tienen cierta formación que pueden ser entregadas por equivocación a un receptor no autorizado.
- Terremoto, baja incidencia o nada.
- Acceso no autorizado, se cierra la puerta principal y de oficinas. Solo personal autorizado de cada oficina puede usar equipos de su oficina y en horario de trabajo.
- Robo de datos, se cierra la puerta principal y de oficinas fuera del horario de trabajo.
- Fuego, en la actualidad se tiene sistema de detección contra incendios solo en la Gerencia de Obras Urbanas.

3.2. PLAN DE RECUPERACIÓN DE DESASTRES

Es importante definir los procedimientos y planes de acción para el caso de una posible falla, siniestro o desastre principalmente en el Data Center de la Entidad donde se encuentra instalados los equipos servidores.
Cuando ocurra una contingencia, es esencial que se conozca al detalle el motivo que la origino y el daño producido, lo que permitirá recuperar en el menor tiempo posible el proceso perdido.
Los procedimientos deberán ser de ejecución obligatoria y bajo la responsabilidad de los encargados de la realización de los mismos, debiendo haber procesos de verificación de su cumplimiento.
Los procedimientos de planes de recuperación de desastres deben de emanar de la máxima autoridad institucional, para garantizar su difusión y estricto cumplimiento.

Las actividades a realizar en un Plan de Recuperación de Desastres se pueden clasificaren tres etapas:
3.2.1. Actividades Previas al Desastre.
3.2.2. Actividades Durante el Desastre.
3.2.3. Actividades Después del Desastre.

3.2.1. Actividades Previas al Desastre

Son todas las actividades de planeamiento, preparación, entrenamiento y ejecución de las actividades de resguardo de la información, que nos aseguren un proceso de Recuperación con el menor costo posible a nuestra Institución.

Podemos detallar las siguientes Actividades Generales:

3.2.2.1. Establecimiento de Plan de Acción

En esta fase de Planeamiento se debe de establecer los procedimientos relativos a:

a) **Sistemas de Información.** La Institución deberá tener una relación de los Sistemas de información con los que cuenta, tanto las instalaciones realizadas en el centro de cómputo como las realizadas en las áreas usuarias. Debiendo identificar toda información sistematizada o no, que sea necesaria para la buena marcha Institucional. La relación de Sistemas de información se señala en el **Anexo N° 03**.

b) **Equipos de Cómputo.** Se deberá considerar las siguientes acciones:

1. Inventario actualizado de los equipos de manejo de información, especificando sus características (según formato - **Anexo N° 04**), en la que debe identificarse el contenido (Software que usa, principales archivos que contiene), su ubicación y nivel de uso Institucional.
2. Señalización o etiquetado de los Computadores de acuerdo a la importancia de su contenido, para ser priorizados en caso de evacuación. Por ejemplo etiquetar (colocar un sticker) de color rojo a los servidores, color amarillo a las computadoras con información importante o estratégica y color verde a las computadoras de contenidos normales.
3. Tener siempre actualizada una relación de computadoras requeridas como mínimo para cada Sistema Informático permanente de la Institución (que por sus funciones constituyen el eje central de los Servicios Informáticos de la Institución), las funciones que realizaría y su posible uso en dos o tres turnos de trabajo, para cubrir las funciones básicas y prioritarias de cada uno de estos Sistemas.

c) **Obtención y almacenamiento de los Respaldos de información (BACKUPS).** Se deberá establecer los procedimientos para la obtención de copias de Seguridad de todos los elementos de software necesarios para asegurar la correcta ejecución de los Sistemas o aplicativos de la Institución. Para lo cual se debe contar con:

1. Backups del Sistema Operativo (en caso de tener varios Sistemas Operativos o versiones, se contará con una copia de cada uno de ellos).
2. Backups del Software Base (Paquetes y/o Lenguajes de Programación con los cuales han sido desarrollados o interactúan nuestros Aplicativos Institucionales).
3. Backups del Software Aplicativo (Considerando tanto los programas fuentes, como los programas objetos correspondientes, y cualquier otro software o procedimiento que también trabaje con la data, para producir los resultados con los cuales trabaja el usuario final). Se debe considerar también las copias de los listados fuentes de los programas definitivos, para casos de problemas.
4. Backups de los Datos (Bases de Datos, índices, tablas de validación, passwords, y todo archivo necesario para la correcta ejecución del Software Aplicativo de la Institución).

d) Políticas (Normas y Procedimientos de Backups). Se debe establecer los procedimientos, normas, y determinación de responsabilidades en la obtención de los Backups mencionados anteriormente en el punto (c), debiéndose incluir:

1. Los Backup se deberán realizar de manera periódica en discos externos.
2. Respaldo de Información de movimiento entre los períodos que no se sacan Backups (backups incrementales) en la unidades D o E de manera automatizada por medio de scripts o procesamiento por lotes (batch) programados.
3. Uso obligatorio de un formulario estándar para el registro y control de los Backups en el cual se detallara las fechas en que se realizan los backups.
4. Almacenamiento de los Backups en condiciones ambientales óptimas, en el área de la Subgerencia de Tecnologías de Información y Sistemas.
5. Almacenamiento de los Backups en locales diferentes donde reside la información primaria (evitando la pérdida si el desastre alcanzo todo el edificio o local estudiado).
6. Pruebas periódicas de los Backups (Restore), verificando su funcionalidad, a través de los sistemas, comparando contra resultados anteriores confiables.
7. Correspondencia entre la relación de Sistemas de Información necesarias para la buena marcha de la organización (mencionado en el punto (a), y los backups efectuados.

3.2.2.2. Formación de Equipos Operativos

En cada unidad operativa de la Institución, que almacene información y sirva para la operatividad institucional, se deberá designar un responsable de la seguridad de la información de su unidad. Pudiendo ser el jefe de dicha Área Operativa.

Entre las acciones a tomar en coordinación con la SGTIS serán:

1. Ponerse en contacto con los propietarios de las aplicaciones y trabajar con ellos.
2. Proporcionar soporte técnico para las copias de respaldo de las aplicaciones.
3. Supervisar procedimientos de respaldo y restauración.
4. Supervisar la carga de archivos de datos de las aplicaciones, y la creación de los respaldos incrementales.
5. Organizar la prueba de hardware y software.
6. Ejecutar trabajos de recuperación.
7. Participar en las pruebas y simulacros de desastres

3.2.2.3. Formación de Equipos de Evaluación (Auditoría de cumplimiento de los procedimientos sobre Seguridad)

Esta función debe ser realizada por el personal de la Subgerencia de Tecnologías de Información y Sistemas.

1. Revisar que las Normas y procedimientos con respecto a Backups y seguridad de equipos y data se cumpla.
2. Supervisar la realización periódica de los backups, por parte de los equipos operativos, comprobando físicamente su realización, adecuado registro y almacenamiento.
3. Revisar la correlación entre la relación de Sistemas e Informaciones necesarios para la buena marcha de la Institución (detallados en (a)), y los backups realizados.
4. Informar de los cumplimientos e incumplimientos de las Normas, para las acciones de corrección respectivas.

3.2.2. Actividades Durante el Desastre

Una vez presentada la Contingencia o Siniestro, se deberá ejecutar las siguientes actividades, planificadas previamente:

3.2.2.1 Plan de Emergencias.
3.2.2.2 Formación de Equipos.
3.2.2.3 Entrenamiento

3.2.2.1. Plan de Emergencias

En este plan se establecen las acciones que se deben realizar cuando se presente un Siniestro, así como la difusión de las mismas.

Se preverá los posibles escenarios de ocurrencia del Siniestro:
- Durante el día.
- Durante la noche.

El Plan de Evacuación del Personal deberá seguir lo descrito en el Plan de Contingencia Institucional presentado por la Oficina de Defensa Civil. En la que se debe considerar:

1. El Plan de puesta a buen recaudo de los activos (incluyendo los activos de Información) de la Institución (si las circunstancias del siniestro lo posibilitan) y la ubicación.
2. La señalización de los elementos contra el siniestro (extinguidores, cobertores contra agua, etc.)
3. La secuencia de llamadas en caso de siniestro, tener a la mano: elementos de iluminación (linternas), lista de teléfonos de Bomberos / Ambulancia, Jefatura de Seguridad y de su personal (equipos de seguridad) nombrados para estos casos.

3.2.2.2. Formación de Equipos Emergencias

Establecer claramente cada equipo (nombres, puestos, ubicación, etc.) con funciones claramente definidas a ejecutar durante el siniestro. Si bien la premisa básica es la protección de la Integridad del personal, en caso de que el siniestro lo permita (por estar en un inicio o estar en una área cercana, etc.), deberá de existir dos

equipos de personas que actúen directamente durante el siniestro, un equipo para combatir el siniestro (Plan de Contingencia Institucional – Defensa Civil) y otro para el salvamento de los recursos Informáticos, de acuerdo a los lineamientos o clasificación de prioridades, para salvaguardar los equipos y este equipo estará conformado por los responsables de cada Área (**Anexo N° 05**).

3.2.2.3. Entrenamiento

Las practicas o simulacros serán coordinados y fijados por la Oficina de Defensa Civil. Un aspecto importante es que el personal tome conciencia de que los siniestros (incendios, inundaciones, terremotos, apagones, etc.) pueden realmente ocurrir, y tomen con seriedad y responsabilidad estos entrenamientos, para tal efecto es conveniente que participen los elementos directivos, dando el ejemplo de la importancia que la Alta Dirección otorga a la Seguridad Institucional.

3.2.3. Actividades Después del Desastre

Después de ocurrido el Siniestro o Desastre es necesario realizar las actividades que se detallan a continuación:

3.2.3.1 Evaluación de Daños.
3.2.3.2 Priorización de Actividades del Plan de Acción.
3.2.3.3 Ejecución de Actividades.
3.2.3.4 Evaluación de Resultados.
3.2.3.5 Retroalimentación del Plan de Acción.

3.2.3.1. Evaluación de Daños.

Inmediatamente después que el siniestro ha concluido, se deberá evaluar la magnitud del daño que se ha producido, que sistemas se están afectando, que equipos han quedado no operativos, cuales se pueden recuperar, y en cuanto tiempo, etc.

3.2.3.2. Priorización de actividades del Plan de Acción

Toda vez que el Plan de acción es general y contempla una pérdida total, la evaluación de daños reales y su comparación contra el Plan, nos dará la lista de las actividades que debemos realizar, siempre priorizándola en vista a las actividades estratégicas y urgentes de nuestra Institución.

Es importante evaluar la dedicación del personal a actividades que puedan no haberse afectado, para ver su asignación temporal a las actividades afectadas, en apoyo al personal de los sistemas afectados y soporte técnico.

3.2.3.3. Ejecución de Actividades.

La ejecución de actividades implica la creación de equipos de trabajo para realizar las actividades previamente planificadas en el Plan de acción (3.2.1.1). Cada uno de estos equipos deberá contar con un coordinador que deberá reportar diariamente el avance de los

trabajos de recuperación y, en caso de producirse algún problema, reportarlo de inmediato a la jefatura a cargo del Plan de Contingencia y Seguridad de la Información.

Los trabajos de recuperación tendrán dos etapas, la primera la restauración del servicio usando los recursos de la institución o local de respaldo, y la segunda etapa es volver a contar con los recursos en las cantidades y lugares propios del Sistema de Información, debiendo ser esta última etapa lo suficientemente rápida y eficiente para no perjudicar la operatividad de los servicios de la institución o local de respaldo.

3.2.3.4. Evaluación de Resultados.

Una vez concluidas las labores de Recuperación del (los) Sistema(s) que fueron afectados por el siniestro, debemos de evaluar objetivamente, todas las actividades realizadas, que tan bien se hicieron, que tiempo tomaron, que circunstancias modificaron (aceleraron o entorpecieron) las actividades del plan de acción, como se comportaron los equipos de trabajo, etc.

De la Evaluación de resultados y del siniestro en sí, deberían de salir dos tipos de recomendaciones, una la retroalimentación del Plan de Contingencia y Seguridad de la Información y otra una lista de recomendaciones para minimizar los riesgos y pérdida que ocasionaron el siniestro.

3.2.3.5. Retroalimentación del Plan de Acción.

Con la evaluación de resultados, debemos de optimizar el plan de acción original, mejorando las actividades que tuvieron algún tipo de dificultad y reforzando los elementos que funcionaron adecuadamente.

El otro elemento a evaluar es cuál hubiera sido el costo de no haber tenido nuestra institución el Plan de Contingencia y Seguridad de la Información llevado a cabo.

CAPITULO IV

4. ASPECTOS GENERALES DE LA SEGURIDAD DE LA INFORMACIÓN

4.1. CONCEPTOS GENERALES

a) Acceso
Es la recuperación o grabación de datos que han sido almacenados en un sistema de computación. Cuando se consulta a una base de datos, los datos son primeramente recuperados hacia la computadora y luego transmitidos a la pantalla del terminal.

b) Ataque
Termino general usado para cualquier acción o evento que intente interferir con el funcionamiento adecuado de un sistema informático, o intento de obtener de modo no autorizado la información confiada a una computadora.

c) Ataque activo
Acción iniciada por una persona que amenaza con interferir el funcionamiento adecuado de una computadora, o hace que se difunda de modo no autorizado información confiada a una computadora personal. Ejemplo: El borrado intencional de archivos, la copia no autorizada de datos o la introducción de un virus diseñado para interferir el funcionamiento de la computadora.

d) Ataque pasivo
Intento de obtener información o recursos de una computadora personal sin interferir con su funcionamiento, como espionaje electrónico, telefónico o la interceptación de una red. Todo esto puede dar información importante sobre el sistema, así como permitir la aproximación de los datos que contiene.

e) Amenaza
Cualquier cosa que pueda interferir con el funcionamiento adecuado de una computadora personal, o causar la difusión no autorizada de información confiada a una computadora.
Ejemplo: Fallas de suministro eléctrico, virus, saboteadores o usuarios descuidados.

f) Activo
Es algo que tenga un gran valor para la organización.

g) Análisis del riesgo
Utilización sistemática de la información para identificar todas las fuentes que puedan generar algún riesgo.
Evaluación del riesgo
Es el proceso general de análisis y evaluación de riesgo.

h) Base de Datos

Una base de datos es un conjunto de datos organizados, entre los cuales existe una correlación y que además, están almacenados con criterios independientes de los programas que los utilizan.

También puede definirse, como un conjunto de archivos interrelacionados que es creado y manejado por un Sistema de Gestión o de Administración de Base de Datos (Data Base Management System - DBMS).

Las características que presenta un DBMS son las siguientes:

- Brinda seguridad e integridad a los datos.
- Provee lenguajes de consulta (interactivo).
- Provee una manera de introducir y editar datos en forma interactiva.
- Existe independencia de los datos, es decir, que los detalles de la organización delos datos no necesitan incorporarse a cada programa de aplicación.

i) Control

Es la herramienta de gestión del riesgo, en el que se incluyen las políticas, las pautas, las estructuras organizacionales, que sean de naturaleza administrativa, técnica o legal.

j) Datos

Los datos son hechos y cifras que al ser procesados constituyen una información, sin embargo, muchas veces datos e información se utilizan como sinónimos.

En su forma más amplia los datos pueden ser cualquier forma de información: campos de datos, registros, archivos y bases de datos, texto (colección de palabras), hojas de cálculo (datos en forma matricial), imágenes (lista de vectores o cuadros de bits), vídeo (secuencia de tramas), etc.

k) Disponibilidad

Acceso a la información y los sistemas de tratamiento de la misma por parte de los usuarios autorizados cuando lo requieran.

l) Evento de Seguridad de la Información

Es una ocurrencia que se encuentra identificada por un sistema, servicio o red en el que se indica una posible fisura en la política de seguridad de información o algún posible fallo en las situaciones relevantes para la seguridad.

m) Golpe (Breach)

Es una violación con éxito de las medidas de seguridad, como el robo de información, el borrado de archivos de datos valiosos, el robo de equipos, PC, etc.

n) Gestión del riesgo

Son actividades coordinadas para dirigir y controlar una organización considerando el riesgo que puede producir.

o) Inventario de activos

Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, reputación de la organización, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

p) Integridad

Se refiere a que los valores de los datos se mantengan tal como fueron puestos intencionalmente en un sistema. Las técnicas de integridad sirven para prevenir que existan valores errados en los datos provocados por el software de la base de datos, por fallas de programas, del sistema, hardware o errores humanos.

El concepto de integridad abarca la precisión y la fiabilidad de los datos, así como la discreción que se debe tener con ellos.

q) Incidente

Cuando se produce un ataque o se materializa una amenaza, tenemos un incidente, como por ejemplo las fallas de suministro eléctrico o un intento de borrado de un archivo protegido.

r) Incidente de Seguridad de la Información

Se encuentra indicado por diferentes eventos que no son esperados o no deseados, y que tienen una gran probabilidad de poner en un compromiso las operaciones de negocios y las amenazas de Seguridad de la Información.

s) Política de Seguridad

Es un documento en el que se expresa los objetivos que tiene una organización a la hora de implementa un Sistema de Seguridad de la Información. Se encuentra firmada por la gerencia de la empresa y tiene que estar disponible para todo el mundo que desee verla.

t) Privacidad

Se define como el derecho que tienen los individuos y organizaciones para determinar, ellos mismos, a quién, cuándo y qué información referente a ellos serán difundidos o transmitidos a otros.

u) Seguridad de la información.

Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio y fiabilidad pueden ser también consideradas.

Se refiere a las medidas tomadas con la finalidad de preservar los datos o información que en forma no autorizada, sea accidental o intencionalmente, puedan ser modificados, destruidos o simplemente divulgados.

En el caso de los datos de una organización, la privacidad y la seguridad guardan estrecha relación, aunque la diferencia entre ambas radica en que la primera se refiere a la distribución autorizada de información, mientras que la segunda, al acceso no autorizado de los datos.

El acceso a los datos queda restringido mediante el uso de palabras claves, de forma que los usuarios no autorizados no puedan ver o actualizar la información de una base de datos o a subconjuntos de ellos.

v) Riesgo
Es la combinación de probabilidad de que ocurra un incidente y las consecuencias de éste.

w) Tratamiento del riesgo
Es el proceso por el que se selecciona e implementa las medidas para modificar el riesgo.

x) Valoración del riesgo
Es el proceso mediante el cual se compara el riego estimado con el riesgo dado.

y) Vulnerabilidad
Es la debilidad presentada por un activo o grupo de activos que pueden ser explotados por una o más amenazas.

4.2. ACCESO NO AUTORIZADO

La función del procesamiento de datos es un servicio de toda la institución, que apoya no solo a los sistemas de información administrativa sino también a las operaciones funcionales. La Seguridad es un aspecto de mucha importancia en la correcta administración informática, lo es también de toda la Institución.
Las medidas de seguridad están basadas en la definición de controles físicos, funciones, procedimientos y programas que conlleven no sólo a la protección de la integridad de los datos, sino también a la seguridad física de los equipos y de los ambientes en que éstos se encuentren.
En relación a la seguridad misma de la información, estas medidas han de tenerse en cuenta para evitar la pérdida o modificación de los datos, información o software inclusive, por personas no autorizadas, para lo cual se deben tomar en cuenta una serie de medidas.

La seguridad de la información y por consiguiente de los equipos informáticos, es una cuestión que llega a afectar, incluso, a la vida privada de la persona humana, de ahí que resulte obvio el interés creciente que día a día se evidencia sobre este aspecto de la nueva sociedad informática.
Ladrones, manipuladores, saboteadores, espías, etc. reconocen que el centro de cómputo de una institución es su nervio central, que normalmente tiene información confidencial y que, a menudo, es vulnerable a cualquier ataque.

La seguridad de la información tiene dos aspectos:

- El primero consiste en negar el acceso a los datos a aquellas personas que no tengan derecho a ellos, al cual también se le puede llamar protección de la privacidad, si se trata de datos personales, y mantenimiento de la seguridad en el caso de datos institucionales.
- Un segundo aspecto de la protección es garantizar el acceso a todos los datos importantes a las personas que ejercen adecuadamente su privilegio

de acceso, las cuales tienen la responsabilidad de proteger los datos que se les ha confiado.

En general, la protección de los datos requiere ejercer un control sobre la lectura, escritura y empleo de esa información. Para obtener mayor eficiencia en la protección se debe tener siempre presente la protección de los datos, el mantenimiento de la privacidad y la seguridad del secreto.
El secreto se logra cuando no existe acceso a todos los datos sin autorización. La privacidad adecuada puede lograrse cuando los datos que puedan obtenerse no pueden enlazarse a individuos específicos o no pueden utilizarse para imputar hechos acerca de ellos.
Por otro lado, es importante incorporar dispositivos de seguridad durante el diseño del sistema en vez de añadirlas después. Los diseñadores de sistemas deben entender que las medidas de seguridad han llegado a ser criterios de diseño tan importantes como otras posibilidades funcionales, así como el incremento de costos que significa agregar funciones, después de desarrollado un Sistema de Información.
Sin adecuadas medidas de seguridad se puede producir accesos no autorizados a:

- Área de Sistemas (Centro de Datos).
- Computadoras personales y/o Terminales de la red.
- Información Confidencial.

4.2.1. Control de Acceso al Data Center

La libertad de acceso al área del Data Center puede crear un significativo problema de seguridad.
El acceso normal debe ser dado solamente para el personal que regularmente trabaja en esta área. Cualquier otra persona, de otro modo puede tener acceso únicamente bajo control supervisado.
Mantener la seguridad física de su área de sistema es su primera línea de defensa.
Para ello deberá tomar en consideración el valor de sus datos, el costo de protección, el impacto que su pérdida podría tener en su organización y la motivación, competencia y oportunidades de la gente que podría querer dañar los datos o el sistema.

4.2.2. Acceso Limitado a los Terminales

Los terminales que son dejados sin protección pueden ser mal usados. Cualquier terminal que puede ser utilizado como acceso a los datos de un Sistema controlado, debe ser encerrado en un área segura o guardado, de tal manera que no sean usados, excepto por aquellos que tengan autorización para ello.
Igualmente, se deberá considerar la mejor manera de identificar a los operadores de terminales del Sistema, y el uso de contraseñas, cuando un terminal no sea usado pasado un tiempo predeterminado (5 -10 Min.).

Restricciones que pueden ser aplicadas:

- Determinación de los períodos de tiempo para los usuarios o las terminales.
- Designación del usuario por terminal o del terminal por usuario.
- Limitación del uso de programas para usuario o terminales.
- Límite de tentativas para la verificación del usuario.
- Tiempo de validez de las contraseñas.

4.2.3. Control de acceso a la información

Algunos usuarios o extraños (personal no autorizado) pueden encontrar alguna forma mediante la cual, logren el acceso al sistema o la base de datos y descubrir información clasificada o datos no autorizados.
Se deberá considerar la existencia de:
Palabra de Acceso (Password). Es una palabra especial o código que debe teclearse al sistema de computadora antes que se realice un proceso. Constituye un procedimiento de seguridad que protege los programas y datos contra los usuarios no autorizados, la identificación de un individuo debe ser muy difícil de imitar y copiar. Aunque su nombre pueda ser único, es fácil que cualquiera que observe a quienes tienen acceso al sistema copie, por lo que no es una clave adecuada.
Una vez que se obtiene una clave de acceso al sistema, ésta se utiliza para entrar al Sistema de la base de datos desde el sistema operativo. La responsabilidad del manejo de la clave corresponde tanto al que accesa como al sistema operativo.
A fin de proteger el proceso de obtención de una llave del sistema, cuando el usuario realiza la entrada (en inglés LOGIN), solicita una clave de acceso con el nombre del usuario, la cual consiste de unas cuantas letras elegidas por el usuario.
Un intruso puede intentar descubrirla de dos maneras: una, observando el ingreso de la clave y otra, utilizando un método de ensayo y error para introducir posibles claves de acceso y lograr entrar.
El sistema de computación debe cerrarse después que un individuo no autorizado falle dos veces al intentar ingresar una clave de acceso.
No se puede depender de que la ausencia de un operador o responsable de un computador trabe la operatividad normal de una institución, por lo que puede ser necesario el establecimiento de un procedimiento de tener un duplicado de los passwords asignados, bajo un esquema de niveles jerárquicos, en sobre lacrado.
Esto es, el Jefe Inmediato superior tendrá en un sobre lacrado, los passwords de su personal, debiendo utilizar un cuaderno de control, cuando exista la necesidad de romper el sobre lacrado (anotando fecha, hora, motivo, etc.), así como un procedimiento de cambio de passwords periódicos y por dichas eventualidades.

4.2.3.1. Niveles de Acceso.

Los programas de control de acceso deberán identificar a los usuarios autorizados a usar determinados sistemas, con su correspondiente nivel de acceso. Las distinciones que existen en los niveles de acceso están referidas a la lectura o modificación en sus diferentes formas.

De acuerdo a ello se tienen los siguientes niveles de acceso a la información:

- Nivel de consulta de la información no restringida o reservada.
- Nivel de mantenimiento de la información no restringida o reservada.
- Nivel de consulta de la información incluyendo la restringida o reservada.
- Nivel de mantenimiento de la información incluyendo la restringida.

a) Nivel de consulta de la información

El privilegio de lectura está disponible para cualquier usuario y sólo se requiere un conocimiento de la estructura de los datos, o del Sistema de otro usuario para lograr el acceso. La autorización de lectura permite leer pero no modificar la base de datos.

b) Nivel de mantenimiento de la información

Él concepto de mantenimiento de la información consiste en:

Ingreso. Permite insertar datos nuevos pero no se modifica los ya existentes.

Actualización. Permite modificar la información pero no la eliminación de datos.

Borrado. Permite la eliminación de datos.

La forma fundamental de autoridad es la que se le da al administrador de la base de datos, que entre otras cosas puede autorizar nuevos usuarios, reestructurar la base de datos, etc. Esta forma de autorización es análoga a la que se provee a un "super usuario" o al operador para un sistema operativo.

4.3. DESTRUCCIÓN

Sin adecuadas medidas de seguridad la Municipalidad Provincial de Canchis pueden estar a merced no sólo de la destrucción de la información sino también de la destrucción de su equipo informático.

La destrucción del equipo puede darse por una serie de desastres como son: incendios, inundaciones, sismos, o posibles fallas eléctricas, etc.

Cuando se pierden los datos y no hay disponibles copias de seguridad, se han de volver a crear los datos o trabajar sin ellos. De hecho, se puede comprobar cómo una gran parte del espacio en disco está ocupado por archivos, que es útil tener a mano pero que no son importantes para el funcionamiento normal. Un ejemplo típico son las copias de la correspondencia en forma de archivos del procesador de textos. Estos archivos se guardan muchas veces como referencia o, por si hubiera que enviar cartas parecidas en un futuro. Sin embargo, probablemente también existe copia en papel de estas cartas. Si se borran los archivos, puede ser molesto, pero las consecuencias en la organización pueden ser mínimas.

Sin los datos al día, el funcionamiento se vería seriamente dañado. Para evitar daños mayores al ser destruida la información, debe hacerse backups de la información vital para la entidad y almacenarse en lugares

adecuadamente preparados para ese fin y de preferencia aparte del local donde se encuentran los equipos que usualmente lo manejan.
Hay que protegerse también ante una posible destrucción del hardware o software por parte de personal no honrado. Por ejemplo: hay casos en los que, empleados que han sido recientemente despedidos o están enterados que ellos van a ser despedidos, han destruido o modificado archivos para su beneficio inmediato o futuro.

4.4. REVELACIÓN O INFIDENCIA

La revelación o infidencia es otra forma que utilizan los malos empleados para su propio beneficio. La información, que es de carácter Confidencial, es vendida a personas ajenas con la institución. Para tratar de evitar este tipo de problemas se debe tener en cuenta lo siguiente:

Control del uso de información en paquetes abiertos CDs y otros datos residuales. La información puede ser conocida por personas no autorizadas, cuando se deja en paquetes abiertos o CDs que otras personas pueden usar.
Se deben tomar medidas para deshacerse del almacenaje secundario de información importante o negar el uso de ésta a aquellas personas que pueden usar mal los datos residuales de éstas.

Mantener datos sensitivos fuera del personal de limpieza
El material de papel en la plataforma de la descarga de la basura puede ser una fuente altamente sensitiva de recompensa para aquellos que esperan el recojo de la basura. Los datos sensitivos deben ser apartados de este procedimiento para tener una mayor seguridad de protección de la información, cuando éstos son descartados o eliminados, debiendo recurrirse a destructores o picadoras de papel.

Preparar procedimientos de control para la distribución de información. Una manera de controlar la distribución y posible diversificación de información, es mantener un rastro de copias múltiples indicando confidencialidad o usando numeración, como "Pág. 1 de 9".
Desafortunadamente, es muy común ver grandes volúmenes de información sensitiva tirada alrededor de las oficinas y relativamente disponible a gran número de personas.

4.5. MODIFICACIONES

La importancia de los datos que se modifican de forma ilícita, está condicionada al grado en que la organización depende de los datos para su funcionamiento y toma de decisiones.
Determinar procedimientos para controlar los programas de aplicación adicionalmente a proteger sus programas de Aplicación como activos, es a menudo necesario establecer controles rígidos sobre las modificaciones a los programas, para estar seguros de que los cambios no causan daños accidentales o intencionados a los datos o a su uso no autorizado.

Particular atención debe ser dada al daño potencial que pueda efectuar un programador a través de una modificación no autorizada.

Nuestra mejor protección contra la pérdida de datos consiste en hacer copias de seguridad, almacenando copias actualizadas de todos los archivos valiosos en un lugar seguro.

La entidad debe tener muy en cuenta los siguientes puntos para la protección de sus datos de una posible contingencia.

1. Hacer de la copia de seguridad una política, no una opción.
2. Hacer que la copia de seguridad resulte deseable.
3. Facilitar la ejecución de la copia de seguridad; (equipos adecuados, disponibilidad, suministros).
4. Hacer la copia de seguridad obligatoria.
5. Asegurarse de que los usuarios cumplen la política de copias de seguridad (Política de Auditoría a las Copias de Seguridad)

CAPITULO V

5. SEGURIDAD E INTEGRIDAD DE LA INFORMACIÓN

5.1. POLÍTICAS DE SEGURIDAD

Es necesario que la institución defina políticas de seguridad, en las cuales se deben tener en cuenta que:

La Seguridad debe ser considerada desde la fase de diseño de un Sistema, como parte integral del mismo. Debe darse mayor importancia a la toma de medidas de seguridad, teniendo siempre presente que es indispensable, no sólo para el buen funcionamiento sino también para el mantenimiento del sistema.

Los encargados de soporte, aquellos que son responsables de gestionar la Seguridad informática en la organización, han de considerar las siguientes medidas:

Distribuir las reglas de seguridad. Escribir en una lista las reglas básicas de seguridad que los usuarios han de seguir, para mantener la seguridad y ponerlas en un lugar público destacado. Se puede incluir un dibujo en un póster para dar mayor referencia. Se debe considerar la posibilidad de distribuir las reglas por todas las computadoras personales.

Hacer circular regularmente avisos sobre la seguridad. Utilice ejemplos de daños y problemas procedentes de periódicos, revistas, para ilustrar la necesidad de la vigilancia por mantener la seguridad. Intente que estos avisos sean interesantes, sin entrar en muchos detalles, ya que en caso contrario podría inspirar imitaciones.

Establezca una línea de comunicación sobre seguridad. El personal debe conocer dónde puede obtener consejos sobre los temas de seguridad. También deben de poder informar sobre violaciones de la seguridad o

actividades sospechosas de forma anónima. Por otro lado, ofrezca recompensas por informar de las violaciones de seguridad.
Las normas de seguridad también describen el modo de funcionamiento de los dispositivos de seguridad y su administración.

5.1.1. Responsables de la Seguridad

En este documento se ha de fijar la responsabilidad de cada nivel dentro de la organización respecto a las medidas de seguridad. Definición de responsabilidades para la Seguridad de Datos, Sistemas y Programas. En general, la persona con el control físico en un activo (datos, sistemas y programas), debe ser el responsable inmediato de su protección.

Las normas se han de trasladar en la jerarquía para que las personas clave, implementen las medidas de seguridad dadas y ejecuten las acciones adicionales necesarias. Por ejemplo:
Cualquiera que utilice una computadora personal deberá grabar su trabajo y desconectar la computadora, siempre que la deje de usar.

El responsable del servicio de informática realizará comprobaciones puntuales para asegurar que las copias de seguridad se realizan según el plan aprobado.

Cuando se elabora la política de seguridad, también se debe tener muy en cuenta:

Adoctrinar al personal de procesamiento de datos en la importancia de la seguridad y la responsabilidad de cada uno en su mantenimiento.
Es necesario que el personal de Procesamiento de Datos esté enterado de cómo afecta su rol clave, en cada una de las áreas que soporta. Esto puede ayudarlos a entender la magnitud de los problemas que pueden crear, si no están continuamente alertas a la necesidad de proteger los datos encargados a ellos.

Cuando la gente de Procesamiento de Datos este consciente de la importancia de sus actividades, la organización entera puede beneficiarse.

5.2. INTEGRIDAD DE LA INFORMACIÓN

Aunque la seguridad e integridad de la información guardan una estrecha relación, los conceptos de ambas son diferentes. La seguridad se refiere a la protección de los datos contra una revelación, alteración o destrucción no autorizada, mientras que la integridad se refiere a la exactitud o validez de la información, contenida en una base de datos.
En este sentido, algunos manejadores de Archivos son más bien, deficientes. Casi toda la verificación de integridad se realiza mediante códigos de procedimientos escrito por los usuarios.

La integridad de un sistema se provee de la integridad de sus componentes. En teoría, ésta facilidad de integridad puede ser demostrada lógicamente, por inspección o por examen. Cuanto más complejo sea el sistema, sin embargo, hay mayor dificultad para lograr componentes de integridad.
Por esta razón, los sistemas complejos deben ser diseñados para tener una integridad funcional, es decir, diseñados de modo que la falla de un solo componente, no cause la falla de todo el sistema.
Para determinar la integridad de sistemas debe hacerse una prueba de predictibilidad, mediante la cual se puede predecir la respuesta de si el sistema se ejecuta apropiadamente o tiene fallas.
Por ejemplo, un programa tiene integridad si la respuesta a todos sus ingresos anticipados es la salida esperada. Para ingresos no anticipados, el ingreso deberá
Permanecer predicho (mensajes de error o código de retorno). Si el programa no da siempre la misma salida para una entrada dada, o si la salida para entradas no previstas no es predicha, entonces éste carece de integridad.

5.2.1. Concurrencia

En un sistema de gestión de base de datos, existen, problemas conocidos como concurrencia, que se generan cuando existen procesos en los que dos o más usuarios deben accesar y/o actualizar la misma información de una base de datos.

El control de concurrencia es el mecanismo para mantener los datos correctamente en un ambiente, donde existen muchas fuentes de actualización en forma simultánea.

En un sistema de gestión de base de datos centralizado, el mecanismo consiste en bloquear la porción de los datos durante la actualización, para prevenir resultados inconsistentes que puedan generarse. Cuando una transacción accede a un registro bloqueado, espera hasta que el bloqueo sea eliminado y el registro esté nuevamente en un estado consistente.

En un sistema de gestión de base de datos distribuido, en el que las actualizaciones pueden provenir de cualquier modo o de copias en diferente orden y pueden producir resultados inconsistentes, a pesar de existir un control de consistencia local, la consistencia se da mediante la sincronización.

Una base de datos es coherente si después de ejecutar varias transacciones concurrentes, su estado es idéntico al que hubiese tenido, si es que éstas se hubiesen ejecutado consecutivamente en cualquier orden.

CAPITULO VI

6. AMENAZAS MÁS COMUNES CONTRA LA SEGURIDAD

6.1. EL FUEGO

El fuego es un elemento comprendido dentro de las principales amenazas contra la seguridad. El fuego es un problema crítico en un centro de cómputo por varias razones: El hardware y el cableado pueden ser también fuente de serios incendios. Desgraciadamente los sistemas anti fuego dejan mucho que desear, causando casi igual daño que el propio fuego, sobre todo a los elementos electrónicos. El dióxido de carbono, actual alternativa del agua, resulta peligroso para los propios empleados si quedan atrapados en la sala de cómputo.

El fuego es considerado el principal enemigo del computador ya que puede destruir fácilmente los ficheros de información y programas.

Es necesario e imprescindible implementar en la institución, un sistema que nos permita en primer lugar detectar la posible ocurrencia de un siniestro de este tipo en cualquiera de los ambientes de la Municipalidad y así mismo sofocar el fuego en el caso de producirse.

6.1.1. Extinguidores manuales.

Muchas veces el contar con sistemas automáticos anti fuego (sprinklers de agua o sistemas de rociado de gas) no es debido a su alto costo. Se debe actuar con rapidez para poder sofocar el incendio, para ello se debe tener en cuenta el material que está siendo consumido por el fuego. Para cada tipo de situación hay un agente anti fuego ideal, así tenemos:

	Gas Carbónico (CO_2)	**Espuma**	**Agua**
Papel, Madera Este tipo de material que deja brasa o ceniza requiere un agente que moje o enfrié	Apaga solamente en la superficie.	Sofoca	Excelente enfría y empapa apaga totalmente
Equipamiento Eléctrico	Excelente, no deja residuos, no daña el equipamiento y no es conductor de electricidad	Conduce la electricidad y además daña el equipo	Conductora de electricidad
Líquidos Inflamables (Aceites, gasolina, grasa, etc.) Requiere acción rápida de sofocar y enfriar	Bueno; no deja residuos y es inofensivo	Excelente, produce una sábana de espuma que sofoca y enfría	

6.1.2. Procedimiento para el correcto uso de extintores.

Se debe tener en cuenta para el correcto uso de extintores, las siguientes indicaciones:

Material	Modo de Operarlos
CO2	1.- Retirar la traba de seguridad 2.- Asegure firmemente el mango difusor. 3.- Apretar el gatillo. 4.- Oriente el chorro hacia la base del fuego haciendo un barrido. Alcance: 1 a 2 metros Sustancia: Bióxido de carbono. Momento del Recargo: Pérdida del más del 10% o más del peso.
Polvo Químico	1.- Abra la ampolla de gas. 2.- Asegure firmemente el mango difusor 3.- Apretar el gatillo 4.- Oriente el chorro de manera de crear una cortina de polvo sobre el fuego. Alcance: de 2 a 4 metros. Sustancia: Polvo Químico seco y CO2 producido por el contacto del polvo con fuego. Momento de Recargo: Pérdida de peso de la ampolla superior al 10%
Espuma	1.- Inversión del aparato para abajo 2.- Oriente el chorro para la base del fuego. Alcance: de 9 a 18 metros Sustancia: Espuma formada por burbujas consistentes llenas de CO2 Momento del Recargo: Anualmente.
Agua - Gas	Simple maniobra de apertura a la ampolla de CO2 que sirve de propagador Alcance: de 9 a 20 metros Sustancia: Agua. Momento de recargo: Anualmente.

6.1.3. Recomendaciones

El personal designado para usar extinguidores de fuego debe ser entrenado en su uso. Ellos deben recibir algunas lecciones de instrucciones en el mecanismo de lucha contra el fuego y luego estar entrenados de cómo opera el extinguidor de mano.

Es muy importante que todos los colaboradores reciban la instrucción de no interferir con este proceso y evitar su actuación en el sistema de extinción.

Muchas veces la sensibilidad de comienzo de fuego en los ambientes laborales es muy alta. Esto genera falsas alarmas y los colaboradores se acostumbrar a fomentar el pánico, sin observar realmente si hay fuego.

Ello implica tener en cuenta algunos detalles más como son:

- Cuidado al seleccionar e implementar los sistemas de extinción y su conexión si es efectuada con fuerza eléctrica.
- Tener a mano el número telefónico de la Compañía de Bomberos y demás números de emergencia.
- Mantener procedimientos planificados para recibir y almacenar abastecimientos de papel.

6.2. EL AGUA

Otro de los peligros relevantes es el agua. El agua puede entrar en una sala de computadores por varios conductos.

Realmente el agua es una amenaza para los componentes del computador y cables.

Los daños por agua pueden ocurrir como resultado de goteo del techo, inundación de baños interiores, inundaciones por lluvias, goteos de tuberías del techo, filtraciones de agua y de operaciones de sistemas de regadío en pisos sobre las oficinas. Es necesario entonces que el equipo así como los muebles y cabinas cuenten con protección contra agua y trazar un plan para la rápida eliminación de algo de agua que podría entrar en el área.

Poner atención en la instalación de desagües bajo el piso construido donde están instalados los sistemas de cables. La conveniencia de cubiertas plásticas es necesaria en la protección del equipo contra el agua, procedente de filtraciones a través del techo.

6.3. INSTALACIONES ELÉCTRICAS

Para que funcionen adecuadamente, las computadoras personales necesitan de una fuente de alimentación eléctrica fiable, es decir, una que se mantenga dentro de parámetros específicos. Si se interrumpe inesperadamente la alimentación eléctrica o varía en forma significativa, fuera de los valores normales, las consecuencias pueden ser serias. Pueden perderse o dañarse los datos que hay en memoria, se puede dañar el hardware, interrumpirse las operaciones activas y la información podría quedar temporal o definitivamente inaccesible.

Las computadoras personales toman la electricidad de los circuitos eléctricos domésticos normales, a los que se llama tomas de corriente. Esta corriente es bastante fuerte. La mayor parte de las computadoras personales incluyen un elemento denominado **fuente de alimentación**, la cual recibe corriente alterna de las tomas de corriente y la convierte o transforma en la corriente continua de baja potencia que utilizan los componentes de la computadora.

La fuente de alimentación es un componente vital de cualquier computadora personal, y es la que ha de soportar la mayor parte de las anomalías del suministro eléctrico. Actualmente existe el concepto de fuente de alimentación redundante, la cual entrará en operación si se detecta una falla en la fuente de alimentación principal.

En nuestro medio se han podido identificar los siguientes problemas de energía más frecuente:

1. Fallas de energía.
2. Ruido electromagnético.
3. Bajo voltaje.
4. Alto voltaje.

Existen dispositivos que protegen de estas consecuencias negativas, los cuales tienen nombres como:

1. Supresores de picos.
2. Estabilizadores, y
3. Sistemas de alimentación ininterrumpida (SAI o UPS).

6.4. FALLAS QUE GENERAN ALTAS TEMPERATURAS

La electricidad llega desde la central eléctrica hasta los enchufes de la oficina, sale por el hilo activo y a continuación vuelve a la central a través de la línea de retorno (neutro), tras haber realizado su trabajo. Los materiales a través de los cuales la electricidad fluye libremente, como es el cobre de los cables de la oficina, se denominan conductores. La electricidad es esencialmente perezosa, intentando volver a la central eléctrica lo más rápidamente posible a través de cualquier conductor disponible.

Lo que impide que la electricidad vuelva demasiado pronto es el aislamiento, el cual impide el paso de la electricidad. La goma, el plástico y una gran cantidad de materiales no metálicos son buenos aislantes. Por ejemplo la carcasa de algunas computadoras está hecha de metal conductor, pero si se toca ésta no da una descarga eléctrica, porque los aislantes mantienen la corriente dentro de los componentes internos del sistema.

Las fallas en los circuitos eléctricos se producen a menudo por un aislante o un conductor que no trabaja adecuadamente, generando inconvenientes, por lo general, altas temperaturas. Existen formas de prever estas fallas y tecnologías para minimizar el impacto de éstas; como por ejemplo:

6.4.1. TOMAS DE TIERRA

Es la comunicación entre un circuito eléctrico y el suelo natural para dar seguridad a las personas protegiéndolas de los peligros procedentes de una rotura del aislamiento eléctrico. También se le llama puesta a tierra. La comunicación con tierra se logra mediante la conexión de un circuito dado (tomacorriente) a un conductor en contacto con el suelo. Estas conexiones a tierra se hacen frecuentemente por medio de placas, varillas o tubos de cobre enterrados profundamente en la tierra húmeda, con o sin agregados de ciertos componentes como carbón vegetal, sal o elementos químicos, según especificaciones técnicas indicadas para las instalaciones eléctricas.

Las tomas de tierra, en la práctica sirve para proteger de contactos accidentales las partes de una instalación no destinada a estar bajo tensión

y, para disipar sobretensiones de origen atmosférico o de origen industrial, ya sea por maniobra o por pérdida de aislamiento.

La toma a tierra limita la tensión que, con respecto a tierra, puede aparecer en cualquier elemento conductor de una instalación y asegura con ello la correcta actuación de los dispositivos de protección de la instalación eléctrica.

Funciones. Cumplirá las siguientes:

- Proteger a las personas, limitando la tensión que respecto a tierra puedan alcanzar las masas metálicas.
- Proteger los equipos y materiales, asegurando la actuación de los dispositivos de protección como: pararrayos, descargadores eléctricos de líneas de energía o señal, así como interruptores diferenciales.
- Facilitar el paso a tierra de las corrientes de defecto y de las descargas de origen atmosférico u otro.

Partes. Consta de las siguientes:

- Toma de Tierra o Puesta a Tierra.
- Línea principal de tierra.
- Derivaciones de las líneas principales de tierra.
- Conductores de protección.

Mantenimiento. Las inspecciones deben realizarse anualmente, con el fin de comprobar la resistencia y las conexiones. Está labor se efectuará en los meses de verano o en tiempo de sequía, con el fin de evaluarlas en el momento más crítico del año por falta de humedad.

El mantenimiento preventivo se recomienda realizar de 3 a 4 años dependiendo de las propiedades electroquímicas estables.

6.4.2. FUSIBLES

Al cablear la computadora, la carcasa normalmente se conecta a la tercera patilla del cable de alimentación. En algunos casos, puede que la tierra se conecte también al neutro. Si la electricidad pasara a través del aislante y llegase a la carcasa, entonces pasaría directa desde el conductor de tierra hasta ésta. Simultáneamente, esta derivación de electricidad aumentaría la intensidad de corriente que va por el circuito. Este incremento puede ser detectado por un fusible o un diferencial. Estos dos dispositivos están diseñados para interrumpir un circuito si se sobrecargan (Un fusible debe ser sustituido tras fundirse, mientras que un diferencial se debe restaurar tras saltar).

Si una parte de una computadora funde un fusible o hace saltar un diferencial, primero se debe desconectar el equipo. A continuación debe desconectarse el cable de alimentación que lleva al equipo y buscar la falla que ha hecho saltar el fusible. Arreglado el problema, se puede volver a conectar el equipo. Vuelva a encender el equipo, pero esté preparado para tener que apagarlo de nuevo, y rápidamente, si el problema no se hubiera arreglado adecuadamente.

Entre las causas menos problemáticas para que se fundan los fusibles o salten los diferenciales se encuentra la sobrecarga de un circuito eléctrico. Para corregir esto se necesita reorganizar la distribución de enchufes sobre las placas, distribuyendo la carga de forma más uniforme.

Entre las fallas más serias, se incluyen los cables dañados de forma que el aislante entre los conductores se ha roto. En los aparatos, los aislantes pueden decaer o fundirse, dando lugar a cortocircuitos. Al sustituir los fusibles de una computadora, se ha de tener cuidado que todos los equipos deben estar apagados y desconectados antes de cambiar el fusible. No se debe olvidar que algunos elementos del equipo, como es el caso de los monitores, pueden mantener una carga de alto voltaje incluso, después de haberse apagado.

Debe asegurarse que el fusible de recambio es de la misma capacidad que el fundido. Por ejemplo, si el fusible fundido viene marcado como de 2 amperios, no se debe sustituir por uno de 3 amperios. Un fusible de 3 amperios dejará pasar 1 amperio más de intensidad de lo que fijó el diseñador del equipo. Si se siguen fundiendo fusibles en el equipo, entonces hay algo que funciona mal.

No se aprueba las reparaciones de los fusibles, usando hilos de cobre o similares.

6.4.3. EXTENSIONES ELÉCTRICAS Y CAPACIDADES

Las computadoras personales a veces ocupan rápidamente todas las tomas de corriente. Pocas oficinas se encuentran equipadas con las suficientes placas de pared. Dado que es necesario conectar además algún equipo que no es informático, es fácil ver que son muy necesarias las extensiones eléctricas múltiples. El uso de estas extensiones eléctricas debe ser controlado con cuidado por los responsables de las oficinas. No sólo para que no queden a la vista, sino también porque suponen un peligro considerable para aquellos que tengan que pasar por encima. Aparte del daño físico que puede provocar engancharse repentinamente con el cable, se trata de una forma rápida y poco agradable de desconectar un sistema completo.

Por razones de seguridad física y de trabajo se sugiere tener en cuenta las siguientes reglas:

- Las extensiones eléctricas deben estar fuera de las zonas de paso, siempre que sea posible.
- Se debe utilizar canaletas de goma adecuadas para cubrir los cables, si van a cruzar una zona de paso.
- No se debe encadenar sucesivos múltiples, ya que esto puede hacer que pase más corriente de la que los cables están diseñados para soportar. Utilice los enchufes de pared siempre que sea posible.
- Si es posible, utilizar extensiones eléctricas que incluyan fusibles o diferenciales. Esto puede ayudar a limitar el daño ante fallas eléctricas.
- Se debe comprobar siempre la carga frente a las extensiones eléctricas. La mayor parte de ellas llevan los amperios que admite cada extensión, no debiendo superar esta cifra el amperaje total de todos los aparatos conectados a ellas.

- Adquiera toma corrientes de pared y/o extensiones eléctricas mixtas, capaces de trabajar tanto con enchufes de patas planas, como cilíndricas.
- Tanto los toma corrientes de pared como las extensiones eléctricas deben tener toma a tierra.

6.5. CAÍDAS Y SUBIDAS DE TENSIÓN

Las caídas y subidas de tensión y los picos tienen un impacto negativo en todo tipo de aparato electrónico, entre los que se incluyen las computadoras personales, los monitores, las impresoras y los demás periféricos.

Lo que causa problemas en las computadoras personales son las grandes oscilaciones en el voltaje. Por ejemplo, una caída por debajo de los 200V y una subida por encima de los 240V. Si una caída dura más de una fracción de segundo, puede generar una falta de alimentación a la memoria de acceso aleatorio, con lo que los datos que allí se encuentren, pueden perderse o, como mínimo, resultar desordenados. Es más, el efecto de la vuelta de la corriente a su valor normal puede tener también efectos perniciosos.

Los efectos de una subida son difíciles de predecir, dependiendo hasta cierto punto de la fuente de alimentación de la computadora. Esta tiene un efecto moderador sobre subidas de la corriente, pero puede que no sea suficiente para evitar cortes temporales en los circuitos que lleven a que se desordenen los datos o incluso se dañen los circuitos impresos. Un comportamiento errático es el primer síntoma de una subida de tensión.

Si se es cuidadoso, es bastante aconsejable medir el voltaje. Un típico multímetro digital, dará una medición del voltaje si introduce sus terminales en el enchufe.

Si la lectura del voltaje continúa fluctuando, anote la medida más alta y la más baja. Si se encuentran dentro de un margen del 5 por 100, alrededor del voltaje esperado, probablemente no causará ningún problema. Si las oscilaciones se encuentran fuera de este margen, puede ser recomendable pedir que un electricista revise el cableado e invertir en algún equipo de acondicionamiento de corriente (Estabilizadores de Voltaje).

6.5.1. Supresores de subidas de tensión

Una protección relativamente barata ante las subidas de tensión es un supresor de subidas. Este es un dispositivo eléctrico situado entre la computadora personal y la fuente de corriente. Incluye una circuitería electrónica que recorta el voltaje cuando éste comienza a subir por encima de un nivel aceptable. El supresor de subidas evita que las subidas de la corriente de alimentación peligrosas lleguen al equipo.

La circuitería del supresor de subidas es bastante compacta, por lo que estas unidades pueden encontrarse con distintas formas y tamaños. Cualquier buen supresor de subidas de tensión debe contar con las siguientes características:

a. Ruptor de circuito

Cualquier supresor de sobretensiones debe incluir un ruptor del circuito, un conmutador rearmable que corta la alimentación si se sobrecargan los circuitos (normalmente un switch). Este es el mínimo nivel de protección para cualquier dispositivo, debiendo incluso la extensión eléctrica múltiple más sencilla, de incluir uno. También cabe señalar el hecho de que una extensión eléctrica múltiple tenga un ruptor, no lo convierte en un supresor de sobretensiones. Se ha de señalar que si un ruptor ha saltado, no se debe rearmar (apretar el switch) hasta que no se haya determinado primero la causa que lo hizo saltar.

b. Protección separada

Muchos supresores de subidas de tensión ofrecen varios puntos de conexión para conectar el sistema. El diseño de la unidad debe proteger cada punto de conexión de forma separada. Con este diseño es fácil que pueda hacer frente a subidas más grandes que con otro en que simplemente se protege la línea que va al múltiple. La protección separada también puede contribuir a reducir la interferencia de ruido entre los distintos elementos conectados al mismo circuito de alimentación.

c. Medidas

Se puede encontrar distintas medidas relativas a los supresores de subidas de tensión en la documentación que traen. Una medida básica es la capacidad, en términos de la corriente total que el dispositivo está diseñado para proteger. Esta medida tiene aquí el mismo significado que para una extensión eléctrica múltiple. Si éste o el supresor presentan un valor de 10 amperios, en ese caso el total de intensidad de todos los equipos conectados al elemento no debe superar esa cantidad. El voltaje de cierre inicial es la tensión a la que se produce el efecto de cierre de la circuitería del elemento.

6.5.2. Picos

Una variación en la corriente más peligrosa y difícil de medir son los picos. Estos consisten en una súbita subida de tensión a niveles muy altos. Muchos de estos picos son causados por la conexión y desconexión de grandes aparatos eléctricos. Los picos son de dos tipos distintos:

- Modo Normal y
- Modo Común.

Los sucesos de modo normal se pueden medir entre los hilos activo y neutro del circuito eléctrico del edificio. Los de modo común se miden entre el neutro y la tierra.

Un pico en modo normal de gran magnitud puede dañar la fuente de alimentación de la microcomputadora. Sin embargo, un pico en modo común de sólo unas pocas docenas de voltios puede dañar los circuitos lógicos o producir errores entre las computadoras.

Protección frente a Picos. Los circuitos supresores de sobretensiones ofrecen buena protección frente a picos en modo normal, pero podría causar algunos de modo común. Por ello, muchos supresores de sobretensión también poseen una circuitería para bloqueo de picos separada, y se comercializan como protectores para sobretensiones y picos.

Los criterios de adquisición de un protector ante picos son en gran parte los mismos que los de los protectores ante sobretensiones, **siendo normal y deseable que una misma unidad ofrezca protección ante ambos**, aunque se debe comprobar sus especificaciones para asegurarse. La capacidad de impedir que los picos alcancen el equipo a veces se miden en *julios*.

Un *julio* es una medida de energía, la energía consumida durante cierto período de tiempo, así por ejemplo, un producto puede venir con la especificación de que suprime picos de 140 julios. También puede venir con una especificación en amperios, como sería "picos de 140 julios a 6.500 amperios". Por lo general, cuando mayor sea el voltaje - julios - amperios que el protector puede tratar, se considera mejor.

6.6. RUIDO ELECTRÓNICO

Las subidas y caídas de tensión y los picos no son el único problema eléctrico al que se han de enfrentar los usuarios de computadoras. También está el tema del Ruido, no se trata del que se puede oír, sino del ruido eléctrico que interfiere en el funcionamiento de los componentes electrónicos.

Para describir el ruido se utilizan dos términos:

- Interferencia de radiofrecuencia (RFI)
- Interferencia electromagnética (EMI)

Este ruido se puede ver literalmente cuando se utiliza un taladro eléctrico cerca de un televisor. El motor eléctrico del taladro hará que aparezcan líneas, nieve u otras alteraciones en la pantalla. Una interferencia similar puede ser causada por las bujías de un automóvil. También puede generarse interferencia de radio con teléfonos inalámbricos que utilizan ondas de radio para comunicar entre la unidad móvil y la base. No sólo la recepción de la TV, sino también la integridad de los datos dentro de una computadora están en peligro ante éstas u otras fuentes de interferencia.

Las computadoras personales corren el riesgo de sufrir tanto interferencias externas como emisiones electromagnéticas y de radio creadas por las propias computadoras. Muchos de los circuitos de una computadora generan EMI y RFI.

El ruido eléctrico también afecta a las transmisiones telefónicas. Se pueden conseguir filtros para las líneas telefónicas que realizan transmisión de datos y fax. En algunos casos, éstos vienen combinados con supresores de subidas de

tensión y picos. La línea de teléfono de la pared se acopla a la unidad supresora, y a continuación se conecta el teléfono - modem - fax a la unidad, quedando la línea telefónica filtrada y protegida.

El otro aspecto de los problemas de ruido con el teléfono es la interferencia de los teléfonos con las computadoras personales.

Esto ocurría a menudo con los primeros teléfonos inalámbricos, pudiendo ser necesario tener la unidad de base del teléfono inalámbrico lejos de la computadora.

6.6.1. Protección ante el Ruido

Para proteger las computadoras de las interferencias electromagnéticas y de radio frecuencia es necesario considerar lo siguiente:

Ruido en la línea de alimentación. Algunos supresores de subidas de tensión y picos están diseñados con una circuitería que filtra el ruido de la fuente de alimentación. La supresión del ruido se mide en decibeles.

Situación de los Aparatos. Como regla general se puede decir que las computadoras personales y los aparatos eléctricos de gran consumo no congenian. Cuando se instalan puestos de trabajo con computadoras se debe intentar tenerlos lejos de estos equipos. Es difícil suprimir la interferencia generada por las potentes corrientes que circulan por estas máquinas, como son las grúas, ascensores, prensas de imprenta y los soldadores eléctricos. En la mayor parte de las oficinas esto no es un problema, otros aparatos de oficina, como son las fotocopiadoras, están normalmente apantalladas. Sin embargo, los ascensores pueden ser un problema en los edificios de oficinas, y el uso industrial de las computadoras crece rápidamente. Por ello, en algunos casos será necesario encerrar la computadora personal en una caja metálica, para protegerla de las interferencias del ruido eléctrico.

Otros equipos informáticos. Un buen supresor de subidas de tensión y ruido, filtrará la interferencia por ruido en la red entre los distintos componentes conectados a él. Sin embargo la carcasa exterior de algunos componentes puede que no esté adecuadamente apantallada, dando lugar a interferencias entre los dispositivos. Es útil no olvidar que los problemas de incompatibilidad por ruido electromagnético aparecen de cuando en cuando, incluso con productos del mismo fabricante.

6.7. CONMUTACIÓN

Cuando se abren o cierran los conmutadores, algo de electricidad se escapa en forma de chispa, corto, sobretensión o pico. Si se conecta y desconecta un secador de pelo en una habitación oscura probablemente verá este fenómeno. Si desenchufa el secador mientras está funcionando probablemente verá una chispa en el enchufe.

Estas chispas pueden tener dos aspectos negativos sobre los sensibles equipos de las computadoras. En primer lugar el pico, la subida brusca de voltaje frente a la que nos protegen los protectores de picos.

El segundo efecto negativo de la conmutación es el tema mucho más complejo de los armónicos, frecuencias eléctricas sustancialmente más altas que la corriente que las ha producido.

La acción rápida del conmutador tiene el mismo efecto que el golpe con el dedo que produce armónicos en la cuerda de una guitarra. La generación de estas frecuencias no deseadas por un elemento del equipo, puede interferir con el funcionamiento de un elemento próximo.

Los buenos protectores ante sobretensiones y picos que suministran tensión a más de un elemento, ofrecerán algún tipo de aislamiento para cada elemento con el objetivo de evitar este problema, algunas veces descrito como ruido.

Reglas para evitar problemas de conmutación.

Se puede ayudar a evitar estos problemas siguiendo las siguientes reglas:

- No enchufar ni desenchufar aparatos eléctricos que estén encendidos
- No enchufar ni desenchufar especialmente las computadoras, impresoras y monitores. A menudo estos aparatos poseen alguna forma de protección en sus circuitos de conexión que no pueden actuar. Debido a que conectar por separado cada elemento del equipo puede ser una rutina desagradable, puede ser recomendable utilizar un centro de conexión, una unidad con protección ante sobretensiones y picos con diseño en forma de consola que alimenta a todos los elementos del sistema

6.8. SUMINISTRO ELECTRÓNICO

Las caídas, subidas de tensión y los picos tienen un impacto negativo en todo tipo de aparato electrónico, entre los que se incluyen las computadoras, monitores, las impresoras y los demás periféricos.
Un corte de la alimentación de la unidad principal puede:

- Hacer que desaparezca la información que hay en la RAM. Los datos recién introducidos o recién editados que no se hayan grabado, se pierden.
- Se interrumpe el proceso de escritura en el disco. Se puede perder información de importancia que necesita el sistema operativo, como puede ser la localización de un archivo, dando como resultado que pierdan o desorganicen archivos.
- Puede "aterrizar" un disco fijo. La cabeza de lectura -escritura de la mayor parte de los discos fijos se separa automáticamente del disco cuando se desconecta la unidad, pero puede ocurrir en algunos sistemas que la cabeza "aterrice" sobre la superficie del disco y la dañe, dando lugar a que se pierdan datos e incluso, resulte dañado físicamente el disco.
- Interrumpir impresión. Cuando vuelva la tensión se han de continuar los procesos de impresión. En algunos casos se ha de volver a comenzar el proceso de impresión.

- Se interrumpen las comunicaciones. Cuando vuelve la corriente, los datos que se estaban transfiriendo entre las computadoras deben de ser comprobados para tener exactitud, y los archivos que se estaban transmitiendo puede que haya que volver a transmitirlos.

- Detiene el trabajo.

- El sistema queda expuesto a picos y subidas de tensión cuando vuelve la tensión. Normalmente se desconectan los equipos cuando se va la corriente, pero esto no siempre es posible. Cuando la empresa de electricidad restaura el servicio, a menudo viene con picos que pueden dañar los aparatos que no se hubieran desconectado.

6.8.1. U.P.S o S.A.I. (Sistema de Energía Ininterrumpible)

Energía de seguridad para un sistema de computación, cuando la energía eléctrica de la línea se interrumpe o baja a un nivel de tensión inaceptable. El UPS suministra electricidad a una PC (estación o servidor) cuando falla el fluido eléctrico. Esta unidad hace transparente a las interrupciones de fracciones de segundo que inevitablemente detiene a los sistemas y le permite seguir trabajando durante varios minutos. **Los pequeños sistemas UPS proveen energía de baterías por sólo unos pocos minutos**. Los sistemas más sofisticados están conectados a generadores eléctricos y pueden proveer energía durante días enteros. Los sistemas UPS proveen generalmente protección contra sobrecarga y pueden proveer asimismo regulación de tensión.

Selección de un UPS. Al seleccionar un UPS se debe tener en cuenta los siguientes factores principales:

- Requerimientos de Potencia (actuales y futuros)
- Requerimiento de frecuencia
- Tiempo de respaldo requerido
- Futuras Expansiones
- Picos por corriente de arranque
- Servicio de Mantenimiento
- Soporte Técnico (antes, durante y después de la instalación)

6.8.2. Grupo Electrógeno

Son máquinas que generan energía eléctrica, aprovechando la energía máxima producida por máquinas de combustión interna.

Una planta generadora ideal, deberá tener el rendimiento y capacidad adecuada para alcanzar los requerimientos de carga que va a soportar. Esta hará que no tenga capacidad excesiva o funciones innecesarias que incrementarían el costo inicial y el costo de operación.

Para obtener el rendimiento y la confiabilidad adecuada, se debe declarar las especificaciones en términos de rendimiento deseado, en vez de intentar especificar un determinado tamaño, tipo o marca de equipo.

Es necesario mencionar que el circuito de generación eléctrica produce extraños voltajes y corrientes en el circuito de comunicación telefónica. Esto puede ser peligroso para las personas o puede dañar los aparatos o interferir las comunicaciones. Por eso, se debe evitar la proximidad de un grupo electrógeno con los circuitos telefónicos y proteger éstos con dispositivos que eviten los peligros y la interferencia.

Tablero de Control. El tablero de control debe ser diseñado de acuerdo al voltaje y corriente que se propone soportar, y debe ser equipado con los dispositivos necesarios de protección contra fallas para proteger al generador de daños, cuando hay fallas o sobrecargas en el sistema.

Mantenimiento. La limpieza con paño seco puede ser satisfactoria cuando los componentes son pequeños. Generalmente se debe soplar la suciedad con aire comprimido, especialmente en los lugares donde se ha juntado tierra y no se puede llegar con el paño.

El polvo y la tierra pueden quitarse con una escobilla de cerdas y luego aspirar. No usar escobilla de alambre.

Los componentes eléctricos, después de la limpieza, almacenamiento o embarque deben secarse antes de hacerlos funcionar.

Comprobar la zona alrededor de las aberturas de admisión y escape del aire estén limpias y sin obstrucciones.

Inspeccionar que no haya conexiones sueltas o contaminadas. Si durante la inspección se muestra que los revestimientos de barniz se han deteriorado, se les debe volver a cubrir con barniz de aislamiento.

Como regla general, los cojinetes deben relubricarse anualmente. Condiciones de operación muy severas, tales como ambientes muy calurosos y polvorientos, requerirán una lubricación más frecuente.

En caso que los grupos electrógenos sean usados sólo en emergencias, se debe establecer una política o procedimiento de puesta en funcionamiento para mantener operativo los equipos.

6.9. ACCIONES HOSTILES

6.9.1. ROBO

Los equipos de cómputo son posesiones muy valiosas de la Institución y están expuestas al "robo", de la misma forma que lo están las piezas de stock e incluso el dinero. Es frecuente que los operadores utilicen el computador de la institución en realizar trabajos privados para otras organizaciones y, de esta manera, robar tiempo de máquina. La información importante o confidencial puede ser fácilmente copiada. Muchas empresa invierten millones de soles en programas y archivos de información, a los que dan menor protección que la que otorgan a una máquina de escribir o una calculadora. El software, es una propiedad muy fácilmente sustraída, cintas y discos son fácilmente copiados sin dejar ningún rastro.

Cómo evitar el robo:

- Colocar plataformas de anclaje en los diferentes elementos del computador (monitor, cpu, impresora, etc.)
- Diseñar muebles para ordenadores de forma que se pueda asegurar fácilmente la máquina y los periféricos (Tapas con llave, puertas, etc.).
- Evitar que quiten la tapa del ordenador y se lleven la unidad y tarjetas adaptadoras.

Cómo prevenir los robos con computadora

- Adoptando un sistema operativo de última tecnología y que permita el acceso a los equipos de acuerdo a las funciones de cada usuario.
- Creación de un equipo con misión especial que establezca y compruebe técnicas de seguridad para la computadora. Este equipo deberá incluir representantes de los departamentos de procesamiento de datos, seguridad, auditoría y usuario
- Ejecución de un análisis de riesgos en los sistemas que abarquen pérdidas potenciales por accidentes, así como por delitos intencionados.
- Establecer inspecciones y entrevistas que abarquen:
  - Estado físico del local de la computadora y departamentos de usuarios.
  - Control de acceso.
  - Documentación.
  - Segregación de deberes. Separar (Planeamiento/Desarrollo, de Ejecución y de Verificación/Control).
  - Trabajo excesivo o innecesario del personal.
  - Entorno general personal.
  - Prestar atención especial a la información contable.

Evitar

- Depender de una sola persona para las funciones vitales.
- Repetición periódica de comprobaciones de seguridad. Emplear inspecciones ad-hoc.
- Trabajo no supervisado, especialmente durante el turno de noche. Malas técnicas de contratación, evaluación y de despido de personal.

6.9.2. FRAUDE

Cada año, millones de dólares son sustraídos de empresas y, en muchas ocasiones, *las computadoras* han sido utilizadas en dicho propósito.

En realidad, el potencial de pérdida a través de fraudes, y los problemas de prevención y detección del fraude, están en aumento en sistemas computarizados.

Sin embargo, debido a que ninguna de las partes implicadas (compañía, empleados, fabricantes, auditores, etc.), tienen algo que ganar, sino que más bien pierden en imagen, no se da ninguna publicidad a este tipo de situaciones.

Las tres principales áreas donde se produce el fraude son:

a. Manipulación de información de entrada, fácil de realizar y muy difícil de detectar, al ser los métodos de validación de entrada simples y, en general, conocidos por un gran número de personas de la empresa.
b. Alteración o creación de archivos de información. Se alteran los datos directamente del fichero o se modifica algún programa para que realice la operación deseada.
c. Transmisión ilegal. Interceptar o transferir información de teleproceso.

Entornos que conducen al fraude con computadoras

- Baja moral entre el personal. Los colaboradores en los departamentos de procesamiento de datos y usuarios de la computadora, muestran falta de disciplina respecto a las precauciones de seguridad y en mantener una operación ordenada y sistemáticamente realizada.
- Documentación deficiente. La documentación del sistema está incompleta, anticuada y desordenada. Sólo el diseñador del sistema tiene una idea verdadera de lo que hace el sistema.
- Falta de segregación de deberes. Se permite a los programadores ingresar datos, el personal de operaciones interviene en programación, etc.
- Deficiente administración de la operación. Falta de control de documentos y de procedimientos de autorización, regulando cambios del sistema y alteraciones a los ficheros de datos. Falta general de control del sistema.

6.9.3. SABOTAJE

El peligro más temido por los centros de Procesamiento de Datos, es el sabotaje. Empresas que han intentado implementar programas de seguridad de alto nivel, han encontrado que la protección contra el saboteador es uno de los retos más duros. Este puede ser un empleado o un sujeto ajeno a la propia empresa.

La protección contra el sabotaje requiere:

- Una selección rigurosa de los colaboradores.
- Buena administración de los recursos humanos.
- Buenos controles administrativos.
- Buena seguridad física en los ambientes donde están los principales componentes del equipo.
- Asignar a una sola persona la responsabilidad de la protección de los equipos en cada área.

El problema de la seguridad del computador debe ser tratado como un problema importante de dirección. Los riesgos y peligros deben ser identificados y evaluados, para conocer las posibles pérdidas y para que pueda ponerse en práctica los adecuados métodos de prevención.

Una mejora en la seguridad produce, a menudo, importantes beneficios secundarios. Por ejemplo, el cambio de metodología aplicada a determinadas operaciones conduce frecuentemente a una reducción del índice de errores, a una mejora en calidad, a una mejor planificación y a resultados más rápidos.

No existe un plan idóneo o una recomendación simple para resolver el problema de la seguridad. Realmente no es una situación estática o un

problema "puntual", sino que requiere un constante y continuo esfuerzo y dedicación.

Se menciona a continuación algunas medidas que se deben tener muy en cuenta para tratar de evitar las acciones hostiles:

- Ubicar los equipos en lugares más seguros en donde se prevea cualquier contingencia de este tipo.
- Mantener una lista de números telefónicos de las diferentes dependencias policiales a mano y en lugares donde se pueda hacer un llamado de emergencia.
- Siempre habrá de tomarse en cuenta las Políticas de Seguridad en caso como vandalismo y sabotaje. Son importantes la medida de ingreso de personas debidamente identificadas, marcación de zonas de acceso restringido, prevención para explosivo, etc.
- Mantener adecuados archivos de reserva (backups)
- Identificar y establecer operaciones críticas prioritarias cuando se planea el respaldo de los servicios y la recuperación de otras actividades.
- Montar procedimientos para remitir registro de almacenamiento de archivos y recuperarlos.
- Usar rastros de auditoría o registro cronológico (logs) de transacción como medida de seguridad.

CAPITULO VII

7. MEDIDAS DE PRECAUCIÓN

7.1. EN EL CENTRO DE DATOS

- Es recomendable que el Centro de Datos no esté ubicado en las áreas de alto tráfico de personas o con un alto número de invitados.
- Hasta hace algunos años la exposición de los Equipos de Cómputo a través de grandes ventanales, constituían el orgullo de la organización, considerándose necesario que estuviesen a la vista del público, siendo constantemente visitados. Esto ha cambiado de modo radical, principalmente por el riesgo de terrorismo y sabotaje.
- Se deben evitar, en lo posible, los grandes ventanales, los cuales además de que permiten la entrada del sol y calor (inconvenientes para el equipo de cómputo), puede ser un riesgo para la seguridad del Centro de Datos.
- Otra precaución que se debe tener en la construcción del Centro de Datos es que no existan materiales que sean altamente inflamables, que despiden humos sumamente tóxicos o bien paredes que no quedan perfectamente selladas y despidan polvo.
- El acceso al Centro de Datos debe estar restringido al personal autorizado, el personal de la Institución deberá tener su carné de identificación siempre en un lugar visible.
- Se debe establecer un medio de control de entrada y salida de visitas al centro de cómputo. Si fuera posible, acondicionar un ambiente o área de visitas.
- Se recomienda que al momento de reclutar al personal se les debe hacer además exámenes psicológicos y médico y tener muy en cuenta sus antecedentes de trabajo, ya que un Centro de Datos depende en gran medida, de la integridad, la estabilidad y lealtad del personal.
- El acceso a los sistemas compartidos por múltiples usuarios y a los archivos de información contenidos en dichos sistemas debe estar controlado mediante la verificación de la identidad de los usuarios autorizados.
- Deben establecerse controles para una efectiva disuasión y detección, a tiempo, de los intentos no autorizados de acceder a los sistemas y a los archivos de información que contienen.
- Se recomienda establecer políticas para la creación de los password y establecer la periodicidad de cambios de los mismos.
- Establecer políticas de autorizaciones de acceso físico al ambiente y de revisiones periódicas de dichas autorizaciones.
- Los controles de acceso, el acceso, en sí y los vigilantes deben estar ubicados de tal manera que no sea fácil el ingreso de una persona extraña. En caso que ingresara algún extraño al Centro de Datos, que no pase desapercibido y que no le sea fácil a dicha persona llevarse un archivo.
- Las cámaras fotográficas no se permitirán en ninguna sala de cómputo, sin permiso por escrito de la Autoridad.

7.2. EN LOS NIVELES DE CONTROL

Existen dos tipos de activos en un Centro de Datos. Los equipos físicos y la información contenida en dichos equipos. Estos activos son susceptibles de robo o daño del equipo, revelación o destrucción no autorizada de la información clasificada, o interrupción del soporte a los procesos del negocio, etc.

El valor de los activos a proteger, está determinado por el nivel de clasificación de la información y por el impacto en el negocio, causado por pérdida o destrucción del Equipo o información. Hay que distinguir los activos en nivel clasificado y no clasificado. Para los de nivel no clasificado, no será necesario control. Cualquier control debe basarse únicamente en el valor del equipo y servicios que ellos prestan.

En cambio tratándose de nivel clasificado, deben observarse además todas las medidas de seguridad de la información que estos equipos contengan.

7.3. EN LOS MEDIOS DE ALMACENAMIENTOS

7.3.1. Mantenimiento de Discos Duros

- Aunque el conjunto de cabezales y discos viene de fábrica sellado herméticamente, debe evitarse que los circuitos electrónicos que se encuentran alrededor se llenen de partículas de polvo y suciedad que pudieran ser causa de errores.
- El ordenador debe colocarse en un lugar donde no pueda ser golpeado, de preferencia sobre un escritorio resistente y amplio.
- Se debe evitar que la microcomputadora se coloque en zonas donde haya acumulación de calor. Esta es una de las causas más frecuentes de las fallas de los discos duros, sobre todo cuando algunas piezas se dilatan más que otras.
- Evitar mover la CPU conteniendo al disco duro cuando esté encendido, porque los cabezales de lectura-escritura pueden dañar al disco.
- Una de las medidas más importantes en este aspecto, es hacer que la gente tome conciencia de lo importante que es cuidar un microcomputador.

7.3.2. Mantenimiento de Discos Compactos (Cds/Dvds)

- Deben mantenerse en un rango de temperatura de 5°C a 55 °C.
- No exponer a humedad relativa superior a los 90%.
- Cuidar no tocar, rayar, escribir con lapiceros en la parte reflectiva del disco.
- No exponer al polvo y/o sol la parte reflectiva del disco.
- Proteger de caídas, manteniendo guardado en su envase.

CAPITULO VIII

8. FALLAS GENÉRICAS FUNCIONALES DE LOS SISTEMAS

8.1. FALLAS COMUNES

Se han encontrado varias fallas comunes a muchos sistemas de computación. Estos incluyen:

1. Autentificación

Llamamos autentificación a la comprobación de la identidad de una persona o de un objeto. En muchos sistemas, los usuarios no pueden determinar si el hardware y el software con que funcionan son los que se supone que deben ser. Esto hace fácil al intruso reemplazar un programa sin conocimiento del usuario. Un usuario puede inadvertidamente teclear una contraseña en un programa de entrada falso.

2. Cifrado

La lista maestra de contraseñas debe ser almacenada, cifrada, lo que a menudo no se hace.

3. Implementación

Un diseño bien pensado de un mecanismo de seguridad puede ser implementado de forma improcedente.

4. Confianza implícita

Un problema corriente, una rutina supone que otra está funcionando bien cuando, de hecho, debería estar examinando detenidamente los parámetros suministrados por la otra.

5. Compartimiento implícito

El sistema puede depositar inadvertidamente información importante del sistema, en un espacio de direcciones del usuario.

6. Comunicación entre procesos

El intruso puede usar un mecanismo de SEND/RECEIVE para probar varias posibilidades. Por ejemplo el intruso puede pedir un recurso del sistema y suministrar una contraseña. La información devuelta puede indicar "contraseña correcta", confirmando la contraseña adivinada por el intruso.

7. Verificación de la legalidad

El sistema puede no estar realizando una validación suficiente de los parámetros del usuario.

8. Desconexión de línea

En tiempos compartidos y en redes, cuando la línea se pierde (por cualquier razón), el sistema operativo debe inmediatamente dar de baja del sistema al usuario o colocar al usuario en un estado tal, que sea necesaria la

reautorización para que el usuario obtenga de nuevo el control. Algunos sistemas permiten que un proceso "flote" después de una desconexión de línea. Un intruso puede llegar a obtener el control del proceso y usar cualesquier recurso a los que tenga acceso el proceso.

9. Descuido del operador

Un intruso puede engañar a un operador y hacer que cargue un paquete de disco con un sistema operativo falso.

10. Paso de parámetros por referencia en función de su valor

Es más seguro pasar los parámetros directamente en registros, que tener los registros apuntando a las localidades que contienen los parámetros. El paso por referencia puede llevar a una situación en la cual los parámetros, pueden aún encontrarse en el espacio de direcciones del usuario después de una verificación de la legalidad. El usuario podría así suministrar parámetros legítimos, verificarlos, y modificarlos justo, antes de ser utilizados por el sistema.

11. Contraseñas

Las contraseñas son, a menudo, fáciles de adivinar u obtener mediante ensayos repetidos. Debiendo implementarse con número máximo (3) de intentos infructuosos.

12. Entrampamiento al intruso

Los sistemas deben contener mecanismos de entrampamiento para atraer al intruso inexperto. Es una buena primera línea de detección, pero muchos sistemas tienen trampas inadecuadas.

13. Privilegio

En algunos sistemas hay demasiados programas con muchos privilegios. Esto es contrario al principio del menor privilegio.

14. Confinamiento del programa

Un programa prestado de otro usuario puede actuar como caballo de Troya: puede robar o alterar los archivos del usuario que los prestó.

15. Residuos

A menudo el intruso puede encontrar una lista de contraseñas con sólo buscar en una papelera. Los residuos se dejan a veces en el almacenamiento después de las operaciones rutinarias del sistema. La información delicada debe ser siempre destruida antes de liberar o descargar el medio que ocupa (almacenamiento, papel, etc.). Las trituradoras de papel son algo corriente en ese aspecto.

16. Blindaje

Una corriente en un cable genera un campo magnético alrededor de él; los intrusos pueden de hecho conectarse a una línea de transmisión o a un

sistema de computación sin hacer contacto físico. Puede usarse el blindaje eléctrico para prevenir tales "intrusiones invisibles".

17. Valores de umbral

Están diseñados para desanimar los intentos de entrada, por ejemplo. Después de cierto número de intentos inválidos de entrar al sistema, ese usuario (o el terminal desde donde se intentan las entradas) debe ser bloqueado y el administrador del sistema, advertido. Muchos sistemas carecen de esta característica.

8.2. ATAQUES GENÉRICOS A SISTEMAS OPERATIVOS

Ciertos métodos de penetración se han utilizado efectivamente en muchos sistemas.

1. Asincronismo

Con procesos múltiples que progresan de forma asincrónica, es posible que un proceso modifique los parámetros cuya validez ha sido probada por otro, pero que aún no ha utilizado. Con esto, un proceso puede pasar valores malos a otro, aún cuando el segundo realice una verificación extensa.

2. Rastreo

Un usuario revisa el sistema de computación, intentando localizar información privilegiada.

3. Entre líneas

Se usa un terminal especial para conectarse a la línea de comunicación mantenida por un usuario dado de alta en el sistema, que está inactivo en ese momento.

4. Código clandestino

Se hace un parche en el sistema operativo bajo la pretensión de una depuración. El código contiene trampas que permiten realizar a continuación reentradas no autorizadas al sistema.

5. Prohibición de acceso

Un usuario escribe un programa para hacer caer al sistema, poner al sistema en un ciclo infinito, o monopolizar recursos del sistema. Lo que se intenta aquí es el negar el acceso o servicio a los usuarios legítimos.

6. Procesos sincronizados interactivos

Los procesos usan las primitivas de sincronización del sistema para compartir y pasarse información entre sí.

7. Desconexión de línea

El intruso intenta obtener acceso al trabajo de un usuario después de una desconexión de línea, pero antes de que el sistema reconozca la desconexión.

8. Disfraz

El intruso asume la identidad de un usuario legítimo, después de haber obtenido la identificación apropiada por medios clandestinos.

9. Engaño al operador

Un intruso inteligente puede, a menudo, engañar al operador del computador y hacer que realice una acción que comprometa la seguridad del sistema.

10. Parásito

El intruso utiliza un terminal especial para conectarse a una línea de comunicación. El intruso intercepta los mensajes entre el usuario y el procesador, modifica el mensaje o lo reemplaza por completo.

11. Caballo de Troya

El intruso coloca un código dentro del sistema que le permita accesos posteriores no autorizados. El caballo de Troya puede dejarse permanentemente en el sistema o puede borrar todo rastro de si mismo, después de la penetración.

12. Parámetros inesperados

El intruso suministra valores inesperados a una llamada al supervisor, para aprovechar una debilidad de los mecanismos de verificación de la legalidad del sistema.

A medida que la computación se hace más asequible, los problemas de seguridad aumentan. Las comunicaciones de datos y las redes suponen un gran aumento de la vulnerabilidad de los sistemas. El hecho de ser favorables al usuario, implica también un incremento de la vulnerabilidad.

La seguridad externa se ocupa de la protección del sistema de computación contra intrusos y desastres. La seguridad de la interfase del usuario se encarga de establecer la identidad del usuario antes de permitir el acceso al sistema. La seguridad interna se encarga de asegurar una operación confiable y sin problemas del sistema de computación, y de garantizar la integridad de los programas y datos.

La autorización determina qué acceso se permite a qué entidades. La división de responsabilidades da a la gente distintos conjuntos de responsabilidades. Ningún empleado trata con una gran parte de la operación del sistema, de modo que para comprometer la seguridad tienen que estar implicados varios empleados.

La vigilancia trata de la supervisión y auditoría del sistema, y de la autentificación de los usuarios. En la verificación de las amenazas, el sistema operativo controla las operaciones delicadas, en vez de darle el control

directo a los usuarios. Los programas de vigilancia realizan operaciones sensibles.

Cuando los programas de vigilancia han de tener un acceso mayor que los programas del usuario, para servir las peticiones del usuario, esto se denomina amplificación.

CAPITULO IX

9. SEGURIDAD EN REDES

9.1. PROBLEMAS BÁSICOS

En el intento de proteger una red de computadoras, existen varias funciones comunes a las cuales deben dirigirse. La siguiente es una lista de cuatro problemas básicos:

9.1.1. EL ANFITRIÓN PROMISCUO

a. El anfitrión promiscuo es uno de los principales problemas de seguridad y uno de los problemas más urgentes de cualquier red.

b. Si un intruso es paciente, él puede simplemente mirar (con una red debugger o anfitrión promiscuo) que los paquetes fluyen de aquí para allá a través de la red. No toma mucha programación el análisis de la información que fluye sobre la red.

c. Un ejemplo simple es un procedimiento de login remoto. En el procedimiento login, el sistema pedirá y recibirá el nombre y contraseña del usuario a través de la red.

9.1.2. AUTENTICACIÓN

a. El procedimiento de login remoto ilustra el problema de autenticación. ¿Cómo se presenta credenciales al anfitrión remoto para probar que usted es usted?

b. ¿Cómo se hace esto, de forma que no se repita el mecanismo simple de una jornada registrada?

9.1.3. AUTORIZACIÓN

Aun cuando se pueda probar que usted es quien dice ser, simplemente, ¿Qué información debería permitir el sistema local acceder a través de una red?. Este problema de autorización parecería ser simple en concepto, pero considerar los problemas de control de acceso, cuando todo el sistema tiene su identidad remota de usuario, el problema de autorización sería un problema de seguridad bastante serio, en donde intervienen los conceptos de funciones autorizadas, niveles de autorización, etc.

9.2. CONTABILIDAD

a. Finalmente, considerar el problema de contabilidad. Hay que recordar que nosotros debemos asumir que hay otros con un conocimiento mayor de sistemas.

b. ¿Cuánta contabilidad tiene que hacer el sistema para crear una pista de revisión y luego examinar?

9.3. COMPONENTES DE SEGURIDAD

Para un intruso que busque acceder a los datos de la red, la línea de ataque más prometedora será una estación de trabajo de la red. Debe habilitarse un

sistema que impida que usuarios no autorizados puedan conectarse a la red y copiar información fuera de ella, e incluso imprimirla.
El administrador de la red tal vez tenga que clasificar a los usuarios de la red con el objeto de adjudicarles el nivel de seguridad adecuado. A continuación se detallan un sistema de seguridad en tres niveles:

1. **Nivel de administración**
Aquellos que diseñan, mantienen o ponen en marcha la red. Este debe estar constituido sólo por el administrador o por un pequeño grupo de personal de soporte y administración.

2. **Usuarios fiables**
Aquellos usuarios que cumplen las normas y cuyo trabajo se puedan beneficiar de una mayor libertad de acceso a la red.

3. **Usuarios vulnerables**
Aquellos que muestran falta de competencia, son excesivamente curiosos o beligerantes, o los que por alguna razón no se puede confiar.

Estos niveles pueden tener un reflejo en el número de barreras que se establecen para el acceso al sistema y el tipo de derechos de acceso que se conceden, para cuando se ha obtenido la conexión, así como el nivel de supervisión y la frecuencia de las comprobaciones

9.4. CONTROL DE ACCESO A LA RED

1. Restringir el acceso a las áreas en que están las estaciones de trabajo mediante llaves, tarjetas de identificación, tarjetas inteligentes y/o sistemas biométricos.

2. Restringir la posibilidad de conectar estaciones mediante llaves, tarjetas de identificación, tarjetas inteligentes y sistemas biométricos.

3. Identificación para la red con clave de acceso.

4. Proteger con clave de todas las áreas sensitivas de datos y restricción de acceso a los programas, según su uso.

5. Registrar toda la actividad de la estación de trabajo.

6. Proteger con clave de acceso o bloqueo de todas las operaciones de copia a disquete en las estaciones de trabajo.

7. Monitorizar todas las operaciones de copia en disquete en las estaciones de trabajo.

9.5. PROTECCIÓN DEL SERVIDOR

La parte más importante de la red es el servidor. La concentración de los datos en el servidor, en términos de cantidad e importancia, hace que sea necesario protegerlo de todas las eventualidades.

La dependencia en que esté el servidor no debe ser accesible para nadie, excepto para el administrador de la red. No se debe permitir que personas que no han de utilizar el servidor estén cerca de él. Las impresoras y otros periféricos deben mantenerse alejados de ojos fisgones.

Dada la importancia del servidor y la cantidad de datos que pasan por él, es necesario efectuar copias de seguridad, del servidor. Cabe recordar que las copias de seguridad del servidor de archivos son un elemento especialmente valioso, debiéndose quedar guardados en un lugar cerrado, seguro y con las condiciones ambientales necesarias. Un conjunto de copias de seguridad se debe **trasladar** regularmente a otro lugar seguro (de preferencia otro local).

9.6. REDES Y TOLERANCIA A FALLAS

La tolerancia a fallas es la capacidad de la red de continuar funcionando, en el caso que se produzca un problema importante o una caída catastrófica, sin daño para los datos y sin que el funcionamiento cambie perceptiblemente.

Municipalidad Provincial de Canchis SUB GERENCIA DE TECNOLOGIAS DE INFORMACIÓN Y SISTEMAS SICUANI

Tolerancia a Fallas (TF) en una red significa que si ocurre una falla en uno de sus componentes, esta continuará funcionando, y se logra aplicando un conjunto de disposiciones que se explicarán posteriormente y deben ser aplicados a cada uno de los componentes de la red.

Las redes son Flexibles a Fallas, cuando al ocurrir alguna, esta deja de funcionar, pero al sustituir el componente afectado se restaura el servicio en un corto tiempo.

La tolerancia a fallas, se refiere no sólo a la redundancia, sino a la detección de errores. Por lo general, la tolerancia a fallas conduce a un elemento hardware redundante, que entra en funcionamiento de forma automática en el caso que el componente primario falle. Sin embargo la tolerancia a fallas puede ser algo como duplicar la FAT (tabla de localización de archivos) y las entradas de directorio en áreas distintas de un mismo disco, o una simple verificación de lectura tras escritura, con lo que se asegura que los datos nunca se escriben en un sector dañado del disco.

No todas las redes requieren el mismo grado de tolerancia a fallas.

Acciones para tener en cuenta:

- Disponer de UPS para todas las computadoras que considere críticas para la Municipalidad Provincial de Canchis.

- Instale doble tarjeta de interfaz a la red en cada una de las computadoras y conectarlas en segmentos separados de la red.

- No se debe desestimar lo obvio, un ratón o un teclado se pueden dañar y generar inconvenientes innecesarios. Se debe tener un Kit de componentes de las computadoras en stock.

- No se debe utilizar unidades de almacenamiento de pequeña capacidad como medio de respaldo, hay que emplear esquemas reales de respaldo. Realice el respaldo y verifíquelo. Certifique estos respaldos. Analice los Logs con los resultados de los respaldos.

CAPITULO X

10.IMPLEMENTACIÓN DE PROCEDIMIENTOS EN CASO DE EMERGENCIAS

10.1. EMERGENCIA FÍSICAS (CASOS)

10.1.1. Error Físico de Disco de un Servidor (Sin RAID)

Dado el caso crítico de que el disco presenta fallas, tales que no pueden ser reparadas, se debe tomar las acciones siguientes:

a. Ubicar el disco malogrado.
b. Avisar a los usuarios que deben salir del sistema, utilizar mensajes por red y teléfono a jefes de área.
c. Deshabilitar la entrada al sistema para que el usuario no reintente su ingreso.
d. Bajar el sistema y apagar el equipo.
e. Retirar el disco malo y reponerlo con otro del mismo tipo, formatearlo y darle partición.
f. Restaurar el último backup en el disco, seguidamente restaurar las modificaciones efectuadas desde esa fecha a la actualidad.
g. Recorrer los sistemas que se encuentran en dicho disco y verificar su buen estado.
h. Habilitar las entradas al sistema para los usuarios.

10.1.2. Error de Memoria RAM

En este caso se dan los siguientes síntomas:

a. El servidor no responde correctamente, por lentitud de proceso o por no rendir ante el ingreso masivo de usuarios.
b. Ante procesos mayores se congela el proceso.
c. Arroja errores con mapas de direcciones hexadecimales.
d. El servidor deberá contar con ECC (error correct checking), por lo tanto si hubiese un error de paridad, el servidor se autocorregirá.
e. Todo cambio interno a realizarse en el servidor será fuera de horario de trabajo fijado por la compañía, a menos que la dificultad apremie, cambiarlo inmediatamente.
f. Se debe tomar en cuenta que ningún proceso debe quedar cortado, y se deben tomar las acciones siguientes:

- Avisar a los usuarios que deben salir del sistema, utilizar mensajes por red y teléfono a jefes de área.
- El servidor debe estar apagado, dando un correcto apagado del sistema.
- Ubicar las memorias malogradas.
- Retirar las memorias malogradas y reemplazarlas por otras iguales o similares.
- Retirar la conexión del servidor con el concentrador, ésta se ubica detrás del servidor, ello evitará que al encender el sistema, los usuarios ingresen.
- Realizar pruebas locales, deshabilitar las entradas, luego conectar el cable hacia el concentrador, habilitar entradas para estaciones en las cuales se realizarán las pruebas.

- Probar los sistemas que están en red en diferentes estaciones.
- Finalmente luego de los resultados, habilitar las entradas al sistema para los usuarios.

10.1.3. Error de Tarjeta(s) Controladora(s) de Disco

Se debe tomar en cuenta que ningún proceso debe quedar cortado, debiéndose ejecutar las siguientes acciones:

a. Avisar a los usuarios que deben salir del sistema, utilizar mensajes por red y teléfono a jefes de área.
b. El servidor debe estar apagado, dando un correcto apagado del sistema.
c. Ubicar la posición de la tarjeta controladora.
d. Retirar la tarjeta con sospecha de deterioro y tener a la mano otra igual o similar.
e. Retirar la conexión del servidor con el concentrador, ésta se ubica detrás del servidor, ello evitará que al encender el sistema, los usuarios ingresen.
f. Realizar pruebas locales, deshabilitar las entradas, luego conectar el cable hacia el concentrador, habilitar entradas para estaciones en las cuales se realizarán las pruebas.
g. Al final de las pruebas, luego de los resultados de una buena lectura de información, habilitar las entradas al sistema para los usuarios.

10.1.4. Caso de Incendio Total

La mejor manera de **prevenir** un incendio es no provocarlo. Observe las prohibiciones de no fumar y las normas de prevención propias del local en que se encuentre, y con mayor razón en un centro de cómputo.

En presencia del fuego tenga en cuenta que:

- Puede tratar de apagar un fuego en una oficina siempre que tenga detrás una puerta que le permita salida.
- Si el fuego prende en sus ropas, no corra, tírese al suelo y ruede. Si el hecho ocurre a otra persona cúbrala con alguna prenda o con una toalla humedecida, si se encuentra próximo a un aseo. No se quite la ropa si tiene quemaduras.
- En presencia de aparatos eléctricos, no eche agua al fuego. Tampoco debe hacerlo ante líquidos inflamables (alcohol, aceite, gasolina, etc).
- Si hay mucho humo póngase un pañuelo en la boca y nariz, a ser posible mojado, y salga agachado o gateando. Respire profundamente para evitar desvanecimientos.
- Al salir de una dependencia, procure cerrar las ventanas y las puertas, pues las corrientes avivan el fuego.
- Si se encuentra aislado y no puede ponerse a salvo, diríjase a la habitación más alejada del fuego (pero no a un nivel superior a menos que esté seguro de que los equipos de rescate se encuentran muy cerca y provistos de escaleras largas u otro equipo.
- Si se ve obligado a huir a través de las llamas para ponerse a salvo, no se entretenga en recoger nada, cúbrase (incluyendo la cabeza) con una manta, una toalla, una cortina o un abrigo mojados si es posible, luego aguante la respiración y corra.
- Si tiene que desalojar el edificio siga las indicaciones del Plan de Evacuación de Defensa Civil.

Con respecto a los equipo de computo

En el momento que se dé aviso por los altavoces de alguna situación de emergencia general, se deberá seguir al pie de la letra los siguientes pasos, los mismos que están encausados a salvaguardar la seguridad personal, el equipo y los archivos de información que tenemos en discos externos.

a. Ante todo, se debe conservar la serenidad. Es obvio que en una situación de este tipo, impera el desorden, sin embargo, se debe tratar de conservar la calma, lo que repercutirá en un adecuado control de nuestras acciones.

b. En ese momento cualquiera que sea(n) el (los) proceso(s) que se esté(n) ejecutando en el (los) Servidor (es), se deberá enviar un mensaje (si el tiempo lo permite) de "Salir de Red y Apagar Computador", seguidamente digitar Down en el (los) servidor(es).

c. Se apagará (poner en OFF) la caja principal de corriente del departamento de sistemas.

d. Tomando en cuenta que se trata de un incendio de mediana o mayor magnitud, se debe tratar en lo posible de trasladar el servidor fuera del local, se abandonará el edificio en forma ordenada, lo más rápido posible, por las salidas destinadas para ello.

10.1.5. Caso de Inundación

a. Para evitar problemas con inundaciones se ha de instalar los servidores en racks, y a una altura mínima promedio de 20 cm para la ubicación de los servidores. De esta manera evitaremos inconvenientes como el referido.

b. En lo posible, los tomacorrientes deben ser instalados a un nivel razonable de altura.

c. Dado el caso de que se obvió una conexión que está al ras del piso, ésta debe ser modificada su ubicación o en su defecto anular su conexión.

d. Para prevenir los corto circuitos, asegurarse de que no existan fuentes de líquidos cerca a las conexiones eléctricas.

e. Proveer cubiertas protectoras para cuando el equipo esté apagado.

10.1.6. Caso de Fallas de Fluido Eléctrico

Se puede presentar lo siguiente:

a. Si fuera corto circuito, el UPS mantendrá activo los servidores y algunas estaciones, mientras se repare la avería eléctrica o se enciende el generador.

b. Para el caso de apagón se mantendrá la autonomía de corriente que el UPS nos brinda (corriente de emergencia (*)), hasta que los usuarios completen sus operaciones (para que no corten bruscamente el proceso que tienen en el momento del apagón), hasta que finalmente se realice el By-pass de corriente con el grupo electrógeno, previo aviso y coordinación.

c. Cuando el fluido eléctrico de la calle se ha restablecido se tomarán los mismos cuidados para el paso de grupo electrógeno a corriente normal (o UPS).

(*) Llámese corriente de emergencia a la brindada por grupo electrógeno y/o UPS.

Llámese corriente normal a la brindada por la compañía eléctrica.

Se contará con transformadores de aislamiento (nivelan la corriente) asegurando que la corriente que entre y salga sea 220v, evitando que los equipos sufran corto circuito por elevación de voltaje (protegiendo de esta manera las tarjetas, pantallas y CPU del computador).

10.2. EMERGENCIAS LÓGICAS DE DATOS (CASO)

10.2.1. Error Lógico de Datos

La ocurrencia de errores en los sectores del disco duro del servidor puede deberse a una de las siguientes causas:

a. Caída del servidor de archivos por falla de software de red.

b. Falla en el suministro de energía eléctrica por mal funcionamiento del UPS.

c. Bajar incorrectamente el servidor de archivos.

d. Fallas causadas usualmente por un error de chequeo de inconsistencia física.

En caso de producirse alguna de las situaciones descritas anteriormente; se deben realizar las siguientes acciones:

PASO 1: Verificar el suministro de energía eléctrica. En caso de estar conforme, proceder con el encendido del servidor de archivos, cargar el sistema operativo de red.

PASO 2: Deshabilitar el ingreso de usuarios al sistema.

PASO 3: Descargar todos los volúmenes del servidor, a excepción del volumen raíz, si fuese el caso.

De encontrarse este volumen con problemas, se deberá descargarlo también.

PASO 4: Cargar un utilitario que nos permita verificar en forma global el contenido del(os) disco(s) duro(s) del servidor.

PASO 5: Al término de la operación de reparación se procederá a habilitar entradas a estaciones para manejo de soporte técnico, se procederá a revisar que las bases de datos índices estén correctas, para ello se debe empezar a correr los sistemas y así poder determinar si el usuario puede hacer uso de ellos inmediatamente.

Si se presenta el caso de una o varias bases de datos no reconocidas como tal, se debe recuperar con utilitarios.

10.2.2. Caso de Virus

Dado el caso crítico de que se presente virus en las computadoras se procederá a lo siguiente:

Para servidor:

a. Contar con antivirus licenciado y actualizado para el sistema, el que aislara el virus que ingresa al sistema llevándolo a un directorio para su futura investigación.

b. El antivirus muestra el nombre del archivo infectado y la fecha del suceso.

c. Estos archivos (exe, com, ovl, nlm, etc.) serán reemplazados del disco original de instalación o del backup.

d. Si los archivos infectados son aislados y aún persiste el mensaje de que existe virus en el sistema, lo más probable es que una de las estaciones es la que causó la infección, debiendo retirarla del ingreso al sistema y proceder a su revisión.

Para computadoras fuera de red:

Se revisará las computadoras que no estén en red con antivirus licenciado y actualizado.

De suceder que una computadora se haya infectado con uno o varios virus ya sea en la memoria o a nivel disco duro, se debe proceder a realizar los siguientes pasos:

a. Utilizar un disco de arranque que contenga un sistema operativo igual o mayor en versión al instalado en el computador infectado y que tenga un antivirus actualizado. Reiniciar el computador con dicho disco de arranque.

b. Una vez cargado el sistema operativo en el computador anfitrión, activar el programa antivirus de tal forma que revise todos los archivos y no sólo los ejecutables. De encontrar virus, dar la opción de eliminar el virus. Si es que no puede hacerlo el antivirus, se borrará el archivo, tomar nota de los archivos que se borren. Si éstos son varios pertenecientes al mismo programa, reinstalar al término del escaneado. Finalizado el escaneado, reconstruir el Master Boot del disco duro si fuera necesario.

CONSIDERACIONES FINALES

1. El Plan de Contingencia y Seguridad de la Información contará con el apoyo correspondiente por parte de la Alta Dirección, para suministrar de recursos financieros, humanos y materiales a fin de su implementación y ejecución.

2. Realizar la conformación de un **Comité de Gestión de Seguridad de la Información**, el cual sea el encargado de planificar, implementar y supervisar la ejecución del Plan de Contingencia y Seguridad de la Información, que asegure la legalidad, consistencia, adecuado uso, seguridad, inviolabilidad y sostenibilidad de los Sistemas de Información, hardware y software.

3. Los Gerentes, Subgerente, Jefes, y colaboradores que laboren en la Municipalidad Provincial de Canchis, deben tomar parte de las actividades y están obligados a participar en la implementación y ejecución del Plan de Contingencia y Seguridad de la Información.

4. Contar con la colaboración de los organismos como: Policía Nacional del Perú, Defensa Civil, ESSALUD, Organizaciones Vecinales, e instituciones, como apoyo externo.

5. Definir políticas de seguridad, como una herramienta para el control permanente del cumplimiento del Plan de Contingencia y Seguridad de la Información.

6. Implementar un Plan de Capacitación y Entrenamiento a todos los colaboradores de la Municipalidad Provincial de Canchis, con la finalidad de mantener al personal debidamente entrenado para prevenir y enfrentar cualquier emergencia, así como, disponer de un plan de entrenamiento de todos los colaboradores en la solución de situaciones de emergencia a través de charlas periódicas en los que se describan los riesgos existentes.

7. Las medidas que debemos adoptar para protegernos son tantas como amenazas existen, es por ello que se debe difundir a todas las áreas de la Municipalidad copias del Plan, documentos resumen, carteles, afiches u otro tipo de documento para su información.

8. Realizar las acciones necesarias para cumplir y hacer cumplir los objetivos y funciones determinadas en el presente Plan de Contingencia y Seguridad de la Información, y así cumplir con las disposiciones legales vigentes dispuestas por la ONGEI.

9. Implementar un servidor de respaldo que haga de Backup a cualquiera de los servidores, reemplazando a uno u otro según se necesite, para ello se realizará las acciones necesarias para que el Centro de Datos de la Municipalidad Provincial de Canchis cuente con dicho servidor que cumpla a su vez con una gama de funciones como por ejemplo: Servidor de Archivo,

Servidor de Respaldo, Almacenamiento masivo, Servidor de usuarios y/o Workgroups, etc.

ANEXOS

1. Anexo N° 01 - Comité de Gestión de la Seguridad de la Información.
2. Anexo N° 02 - Equipo de Recuperación de Desastres – ERD.
3. Anexo N° 03 - Sistemas Informáticos de la Municipalidad Provincial de Canchis
4. Anexo N° 04 – Formato de inventario de equipos de computo
5. Anexo N° 05 - Equipos Operativos de los Sistemas de Información

ANEXO N° 01

COMITÉ DE GESTION DE SEGURIDAD DE LA INFORMACION

1. JUSTIFICACIÓN

La elaboración de un Plan de Contingencia y Seguridad de la Información implica disponer de personal con responsabilidades y recursos definidos que ayuden a suplir los sistemas de información afectados.

2. MIEMBROS

El Comité de Gestión de Seguridad de la Información acompaña y hace seguimiento a la marcha del Plan en función de los objetivos planteados. Los representantes de este Comité son:

Municipalidad Provincial de Canchis SUBGERENCIA DE TECNOLOGIAS DE INFORMACION Y SISTEMAS SICUANI

Conformación del Comité de Gestión de Seguridad de la Información

Área	Encargado
Alcaldía	El Titular de la entidad
Gerencia de Administración y Finanzas	Gerente de Administración y Finanzas
Gerencia de Planeamiento y Presupuesto	Gerente de Planeamiento y Presupuesto
Sub Gerencia de Tecnologías de Información y de las Comunicaciones	Sub Gerente de Tecnologías de Información y Sistemas
Oficina de Asesoría Jurídica.	Jefe de la Oficina de Asesoría Jurídica

3. FUNCIONES

Las funciones del Comité de Gestión de Seguridad de la Información serán:

a. Monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes.
b. Tomar conocimiento y supervisar la investigación y el monitoreo de los incidentes relativos a la seguridad.
c. Aprobar las principales iniciativas para incrementar la seguridad de la información.
d. Evaluar y coordinar la implementación de controles específicos de seguridad de información para nuevos sistemas o servicios.
e. Promover la difusión y apoyo a la seguridad dentro de La Municipalidad.
f. Coordinar el proceso de administración de la continuidad de los sistemas de información municipales frente a interrupciones imprevistas.
g. Realizar las actividades que sean necesarias para el cumplimiento de su objetivo.
h. Efectuar el monitoreo y la evaluación periódica de los resultados;
i. Gestionar recursos financieros para la ejecución del Plan de Contingencia y Seguridad de la Información.

4. REUNIONES

a. El Comité se reunirá ordinariamente por lo menos una vez al año. La asistencia a esta reunión es de carácter obligatorio. En el caso que algún miembro no pueda asistir, deberá nombrar a un representante o suplente de su Gerencia o Sub Gerencia.

b. En el curso de la reunión el Comité puede establecer los equipos de trabajo que considere necesario para facilitar las labores del Comité, designando un responsable por cada equipo de trabajo.

c. El quórum para las reuniones del Comité estará constituido por la mitad más uno de los representantes designados o de sus suplentes (en caso de ausencia de los respectivos titulares).

d. Si se presenta a consideración un asunto no incluido en la orden del día de cualquiera de las reuniones, se decidirá de inmediato, mediante el voto de la mayoría, si procede o no su deliberación sobre el nuevo asunto.

e. Las decisiones del Comité se tomarán por voto de la mayoría simple de los representantes presentes del Comité.

f. A las reuniones del Comité de Gestión de Seguridad de la Información podrán asistir en calidad de observadores, representantes de las diferentes áreas relacionadas con el tema de reunión y que hayan sido invitados a través del Coordinador del Comité.

g. Se elaborarán informes finales de cada reunión, los cuales serán comunicados a los integrantes del Comité. Cuando se solicite o el caso lo requiera, los documentos se publicarán en otros medios de información.

ANEXO N° 02

EQUIPO DE RECUPERACIÓN DE DESASTRE – E.R.D.

La Sub Gerencia de Tecnologías de Información y Sistemas ha conformado un equipo de recuperación de desastres que asegurará la continuidad de los procesos y servicios de la Entidad ante cualquier contingencia que se pueda presentar en la Municipalidad.

Este equipo se encuentra dividido de la siguiente manera:

A. Instalación del Hardware y Software.

1. En Servidores

Encargado	Dirección	Teléfono	Celular
Responsable de la SGTIS			
Personal de Soporte Técnico de la SGTIS			

2. En Equipo de Redes y Comunicaciones

Encargado	Dirección	Teléfono	Celular
Responsable de la SGTIS			
Personal de Soporte Técnico de redes de la SGTIS			

3. En Estaciones de Trabajo

Encargado	Dirección	Teléfono	Celular
Responsable de la SGTIS			
Personal de Soporte Técnico de la SGTIS			
Personal de Soporte Técnico de redes de la SGTIS			

B. Apoyo Administrativo

Encargado	Dirección	Teléfono	Celular
Secretaria de Gerencia Municipal			

ANEXO N° 03
SISTEMAS INFORMÁTICOS DE LA MUNICIPALIDAD PROVINCIAL DE CANCHIS

La Municipalidad Provincial de Canchis, a través de sus diferentes Unidades Orgánicas, cuenta con los siguientes sistemas informáticos:

1. SIAF

El Sistema Integrado de Administración Financiera permite registrar operaciones de gastos, ingresos y otras complementarias, y son contabilizadas utilizando la Tabla de Operaciones (TO SIAF), matriz que relaciona los Clasificadores Presupuestales con las Cuentas del Plan Contable Gubernamental. Estos registros son procesados por el Sistema, permitiendo la obtención de los Estados Financieros y Presupuestarios.

Contiene los siguientes módulos:

- Módulo de Conciliación de operaciones Siaf
- Modulo Contable
- Módulo de Deuda Publica
- Módulo de Control de pago de Planillas
- Módulo de Proceso Presupuestario
- Modulo Administrativo

Este sistema es empleado en las siguientes áreas:

- ✓ Gerencia Municipal.
- ✓ Gerencia de Planeamiento y Presupuesto.
- ✓ Gerencia de Administración y Finanzas
- ✓ Sub Gerencia de Contabilidad.
- ✓ Sub Gerencia de Tesorería.

2. SIGA

El Sistema Integrado de Gestión Administrativa permite la ordenación y simplificación de los procesos administrativos relacionadas con todas las fases del proceso logístico que va desde la generación de los requerimientos hasta la gestión de las órdenes de compra y/o servicios, además cuenta con una interface totalmente integrada con el SIAF. Actualmente está en fase de implantación y es utilizado por la Sub Gerencia de Control Patrimonial. Cuenta con los siguientes módulos:

- Módulo de Patrimonio – maneja todas las operaciones de los activos fijos y sus movimientos como altas y bajas.
- Módulo de Logística

3. SISTEMA DE ADMINISTRACIÓN TRIBUTARIA - RENTAS.

Este sistema fue implantado bajo convenio con la C.E.C Guamán Poma de Ayala en el año 2010, y consta de los siguientes módulos: Impuesto Predial, Cuentas Corrientes, Caja, Fiscalización, Impuesto de Alcabala, Licencias de Funcionamiento, Limpieza Pública, Cobranza Coactiva. Este sistema es utilizado por la Sub Gerencia de Administración Tributaria.

Impuesto Predial	Registro de contribuyentes	Valorización Predial
	Registro de Predios Urbanos y Rústicos	Cálculo de Impuesto Predial
	Generación de deuda	Órdenes de Pago de acuerdo al MEF
	Registro de Vías y Aranceles	Esquela de Liquidación
	Registro de TIM	Autoevaluó por contribuyente
	Registro de IPM	Reportes de deuda y recaudación
	Registro de exoneraciones	Orden de cancelación
	Registro de valores anuales (UIT, Exoneración de alcabala, Gastos Administrativos, etc.)	Reporte de porcentaje de morosidad por vías
	Registro de valores unitarios	Declaración jurada mecanizada
Cuentas Corrientes	Fraccionamiento	Estado de cuenta por contribuyente
	Administración de cuentas	Orden de cancelación por fraccionamiento
		Esquela de Liquidación
		Órdenes de Pago
		Resolución de determinación
Caja	Registro de contribuyentes	Recibos, facturas y boletas de pago
	Registro de cancelación directa con recibo	Recibo de Ingresos
	Registro de cancelación de órdenes de pago	Fascículo
	Registro de cancelaciones con documento (Facturas y Boletas)	Reporte de Ingresos presupuestales para el SIAF
	Administración de cancelaciones	Reporte de Ingresos patrimoniales
Fiscalización	Registro de Requerimiento de Fiscalización	Resolución de multa
	Registro de fichas técnica de contrastación	Resolución de determinación de acuerdo al MEF
	Registro de tasas de multas	Ficha de contrastación de acuerdo al MEF
	Generación de deudas por tributos omitidos	Actualización Predial
Impuesto de Alcabala	Registro de contribuyentes	Cálculo del impuesto de alcabala
	Registro de ventas de inmuebles	Comprobante de pago de Alcabala
		Orden de cancelación
Licencias	Registro de contribuyentes	Emisión de Licencia de Funcionamiento

de Funcionamiento	Registro de establecimientos	Solicitudes de Licencia (de licencias, paneles y ambulantes)
	Registro de Ambulantes	Reportes de ingresos por tipo de licencia
	Registro de Paneles publicitarios	Reportes de Licencias emitidas
	Registro de tasas de licencia	Orden de cancelación
Limpieza Pública	Registro de contribuyentes	Emisión de Recibos de Limpieza para reparto
	Registro de características de tipo de servicio de limpieza	Órdenes de Pago
	Registro de responsabilidad del servicio	Resolución de determinación
	Generación de deudas por: limpieza pública, parques y jardines	Orden de cancelación
	Registro de arbitrios(Espectáculos no deportivos, apuestas y juegos)	Reporte de estados de cuenta por contribuyente
Cobranza Coactiva	Captura de órdenes de pago para ejecución coactiva	Requerimiento de Pago
	Administración de expedientes en coactiva	Resolución de inicio
	Administración de cuentas vencidas, prediales y de limpieza publica	Resolución de retención
	Generación de costas procesales	Resolución de embargo
		Resolución de prescripción
		Notificaciones de proceso coactivo
		Resolución de archivamiento
		Orden de cancelación

4. SISTEMA DE REQUERIMIENTOS SV-Logística

El Sistema de Logística y Requerimientos SV-Logística permite registrar operaciones de los procesos de logística desde la creación del requerimiento hasta la generación de la orden de compra y/o servicio. Es utilizado por todas las áreas de la entidad incluida la Sub Gerencia de Logística y Servicios Generales. Contiene los siguientes módulos:

- Módulo de Logística: Incluye el registro y gestión de Cuadros de Adquisición, Solicitud de Cotización, Cuadros comparativos, Órdenes de compra, Ordenes de Servicio, Pecosas, Neas así como la gestión de consultas y reportes.
- Módulo de requerimientos: Permite registrar los requerimientos de bienes y/o servicios.

5. SISTEMA SV_PATRIMONIO.

Este software permite registrar los bienes de la Municipalidad Provincial de Canchis, el cual lleva control por oficina, tipo de bienes, estado y demás características. Así mismo, genera actas de verificación por responsables, reportes en general, detalles de depreciaciones y adquisiciones. Fue instalado por la propia empresa desarrolladora, la misma que brinda el soporte técnico respectivo. Este software es empleado por la Sub Gerencia de Control Patrimonial.

Este software consta de los siguientes módulos:

- Registro de Bienes.
- Reporte de Bienes (Oficina, Cuenta, Estado, Tipo de Documento).
- Reporte de Compras y Depreciación.
- Cálculo de Depreciación.
- Impresión de Etiquetas.
- Migración a Excel.

6. SISTEMA DE PLANILLAS DS-PLANILLAS.

Sistema que permite procesar los diferentes tipos de planillas empleados en la Sub Gerencia de Recursos Humanos, entre sus características cuenta con personalización de conceptos y fórmulas que maneja el sistema, permite definir y procesar diferentes tipos de planillas por mes, permite la transferencia de información a PDT SUNAT y permite realizar reportes de AFP, CTS, FONAFE y demás.

Este software consta de los siguientes módulos:

- Ingreso de personas.
- Importación de personas.
- Administración específica de gasto.
- Apertura de planillas.
- Reporte de planillas.
- Boletas de pago.
- Datos para AFP.

Este software es empleado por la Sub Gerencia de Recursos Humanos, Unidad de Remuneraciones.

7. SISTEMA DE CONTROL DE ASISTENCIA (LECTOR DE HUELLAS BIOMETRICO).

Sistema de control de personal, que permite registrar los ingresos y salidas de personal mediante control biométrico (huella digital).

Este software consta de los siguientes módulos:

- Registro de trabajadores, según modalidad.
- Asignación de horarios, a los trabajadores.
- Registro de permisos de los trabajadores.
- Registro de vacaciones.
- Generación de reportes (en Excel).
- Cálculo de faltas, tardanzas, etc.

Este software es empleado por la Sub Gerencia de Recursos Humanos, Unidad de Escalafón.

8. R-SOFT SISTEMA DE REGISTRO CIVIL.

Este sistema permite escanear, procesar e imprimir actas de nacimiento, matrimonio y defunción. Es un sistema automatizado para procesos informáticos de la Subgerencia de Registro Civil. Este sistema fue instalado por terceros, y es la misma quien brinda el soporte técnico. Sistema utilizado por la Sub Gerencia de Registro Civil.

ANEXO N° 04

FORMATO DE INVENTARIO DE EQUIPOS DE CÓMPUTO

Características	**Datos**
1. Código de control patrimonial de la CPU	
2. N° de serie de la CPU	
3. Fecha de Actualización de registro	
4. Tipo de Computadora	Servido☐ Computadora P☐rsonal ☐ Portátil
5. Marca	
6. Modelo	
7. Estado Actual	Operativa en u☐o Operativa☐in uso ☐ No operativa
8. Régimen de tenencia	Propi☐ Alqui☐do ☐estado ☐ Donado
9. Fecha de instalación	
10. Función que cumple	
11. Tipo de Procesador	
12. Cantidad de procesadores	
13. Velocidad de procesamiento (MHz)	
14. Tecnología de procesamiento	
15. Capacidad de Memoria Principal RAM (Mb)	
16. Capacidad Total de Almacenamiento	
17. Sistema(s) Operativo(s) instalado(s)	
18. Modelo de la Unidad de Disco	
19. Código de control patrimonial de la Unidad de Disco	
20. N° de Serie de la Unidad de Discos	
21. Conexión de red	Con conexión☐ Sin c☐nexión
22. Tipo de Tarjeta de Video	
23. Marca del Monitor	
24. Número de Serie del Monitor	
25. Código de Control Patrimonial del Monitor	
26. Otros dispositivos	

Instrucciones (I – COMPUTADOR)

1. **Código de Control Patrimonial de la CPU.-** En el recuadro correspondiente escriba el código de Control Patrimonial de la CPU de la computadora.
2. **Número de la serie de la CPU.-** En el recuadro correspondiente escriba el número de serie de la CPU.
3. **Fecha de Actualización de Registro.-** En el recuadro correspondiente escriba la fecha de la última actualización del registro.
4. **Tipo de Computadora.-** Marque con una X el tipo de computadora correspondiente.
5. **Marca.-** Escriba en el recuadro la marca de la computadora.
6. **Modelo.-** En el recuadro correspondiente escriba el modelo de la computadora.
7. **Estado Actual.-** Marque con una X el estado actual de la computadora

- Operativa en uso, si la computadora está en buenas condiciones y en funcionamiento.
- Operativa sin uso, si la computadora está en buenas condiciones pero no está siendo utilizada.
- No operativa, si la computadora no funciona debido a alguna falla o falta de recurso.

8. **Régimen de Tenencia.-** Marque con una X el régimen de tenencia de la computadora.
9. **Fecha de Instalación.-** En el recuadro correspondiente escriba la fecha de instalación de la computadora, expresado en mes y año 99/9999.
10. **Función.-** Escriba en el recuadro la función que cumple la computadora. Como por ejemplo:

- Servidor Web
- Servidor Correo
- Firewall
- Servidor Bases de Datos
- Servidor Aplicaciones
- Servidor Producción
- Servidor Impresión
- Servidor Comunicaciones
- Servidor PDC (Dominio)
- BDC (Backup)
- Estación de Trabajo
- Otro Servidor

11. **Tipo de Procesador.-** Escriba en el recuadro el tipo de procesador que tiene la computadora. Como por ejemplo:

- Pentium IV
- Pentium D
- Dual Core
- Core2Duo
- QuadCore
- Core I3/I5/I7
- AMD
- Otros procesadores

12. **Cantidad de Procesadores.-** En el recuadro correspondiente escriba el número de procesadores de cada Mainframe o Minicomputadora.
13. **Velocidad de procesamiento.-** En el recuadro correspondiente escriba la velocidad de procesamiento en Mhz (Megahercios) de la computadora.
14. **Tecnología de Procesamiento.-** (Para sistemas de computación paralela) Escriba en el recuadro la tecnología de procesamiento que utiliza el Mainframe o Minicomputadora. Como por ejemplo:

- MPS
- MPP
- NUMA
- Otros

15. **Capacidad de la Memoria Principal (Mb).-** En el recuadro correspondiente escriba la capacidad en megabytes de la memoria principal de la computadora.
16. **Capacidad total de almacenamiento.-** En el recuadro correspondiente escriba la capacidad de almacenamiento en GB de la computadora.
17. **Sistema Operativo Instalado.-** Escriba en el recuadro el sistema operativo que está instalado en la computadora. Como por ejemplo:

- Windows XP
- Windows Vista
- Windows 7
- Windows 8/8.1
- DOS
- Linux
- Otros

18. **Modelo de la Unidad de Discos.-** En el recuadro correspondiente escriba el modelo de la Unidad de Disco de la computadora.

19. **Código de Control Patrimonial de la Unidad de Discos.-** En el recuadro correspondiente escriba el código de Control Patrimonial de la Unidad de Discos de la computadora.
20. **Número de serie de la Unidad de Discos.-** En el recuadro correspondiente escriba el número de serie de la Unidad de Discos.
21. **Conexión a Red.-** Marque con una X si la computadora está o no con conexión a red.
22. **Tipo de Tarjeta de Video:** En el recuadro correspondiente escriba el tipo de tarjeta de video que tiene instalado el CPU. Como por ejemplo:

- VGA
- SuperVGA
- AGP
- PCI Express
- Otros

23. **Marca del Monitor.-** En el recuadro correspondiente escriba la marca del monitor de la computadora.
24. **Número de Serie del Monitor.-** En el recuadro correspondiente escriba la serie del monitor
25. **Código de Control Patrimonial del Monitor.-** En el recuadro correspondiente escriba el código de Control Patrimonial del Monitor.
26. **Otros dispositivos.-** En el recuadro correspondiente escriba con qué otros dispositivos cuenta la computadora.

ANEXO N° 05

EQUIPOS OPERATIVOS DE LOS SISTEMAS DE INFORMACIÓN

Nombre del Sistema	Ubicación del Sistema	Unidades que usan la Información	Integrantes del Equipo
SIAF	Servidor: Data Center (2do Piso) Clientes: Oficinas de Área Usuaria	• Gerencia Municipal. • Gerencia de Planeamiento, Presupuesto y Ordenamiento Territorial. • Gerencia de Administración y Finanzas. • Sub Gerencia de Contabilidad. • Sub Gerencia de Tesorería	• Gerente de Planeamiento, Presupuesto y Ordenamiento Territorial. • Sub Gerente de Contabilidad. • Sub Gerente de Tesorería
SIGA	Servidor: Data Center (2do Piso) Clientes: Oficinas de Área Usuaria	• Sub Gerencia de Control Patrimonial	• Sub Gerente de Control Patrimonial
SAT - Rentas	Servidor: Data Center (2do Piso) Clientes: Oficinas de Área Usuaria	• Sub Gerencia de Administración Tributaria. • Oficina de Caja	• Sub Gerente de Administración Tributaria. • Responsable de Caja
Sistema de Requerimientos SV_Logistica	Servidor: Data Center (2do Piso) Clientes: Oficinas de Área Usuaria	• Todas las Gerencias y Sub Gerencias	• Subgerente de Logística y Servicios Generales
Sistema SV_Patrimonio	Sub Gerencia de Control Patrimonial (4to Piso)	• Sub Gerencia de Control Patrimonial	• Sub Gerente de Control Patrimonial
Sistema DS-Planillas	Sub Gerencia de Recursos	• Sub Gerencia de Recursos Humanos	• Sub Gerente de Recursos

	Humanos (2do Piso)		Humanos
Sistema de Control de Asistencias (Lector de Huellas Biométrico)	Unidad de Escalafón (2do Piso)	• Sub Gerencia de Recursos Humanos	• Responsable de la Unidad de Escalafón
R-Soft Sistema de Registro Civil	Sub Gerencia de Registro Civil (1er Piso)	• Sub Gerencia de Registro Civil	• Sub Gerente de Registro Civil