San Pedro Garza García, Nuevo León, a 22-veintidos de febrero de 2012-dos mil doce.- - - - - - - - - - -

VISTOS.- El oficio número DS/018/12 de fecha 17-diesiciete de febrero de 2012-dos mil doce, suscrito por el C. Ing. Manuel Medrano Martínez, Director de Sistemas adscrito a la Secretaría de Administración, mediante el cual solicita la abrogación del Manual de Políticas "Seguridad Integral de Informática" el cual se encuentra físicamente en archivos de la Secretaría de la Contraloría y Transparencia Municipal y publicado en el portal del sitio oficial del municipio, en virtud de que la Dirección de Sistemas ha determinado de manera conjunta con la Secretaría de la Contraloría y Transparencia Municipal la abrogación del Manual en comento; debido a que su contenido y su referencia tecnológica ha quedado fuera de los procesos que actualmente lleva a cabo la Dirección referida; por lo que con fundamento en lo establecido por los artículos 34 inciso C) fracciones II y III del Reglamento Orgánico de la Administración Pública Municipal de San Pedro Garza García, Nuevo León y 14 fracciones I y V del Reglamento Interior de la Secretaría de la Contraloría y Transparencia Municipal de San Pedro Garza García, Nuevo León, este Órgano de Control Interno tiene a bien dictar el siguiente **ACUERDO:** -

PRIMERO: Después de analizar la solicitud del Director de Sistemas, respecto a la abrogación del Manual de Políticas "Seguridad Integral de Informática" clave SSA-SI-22 con fecha de emisión febrero de 2003, ya que esta dependencia es la indicada para la aplicación u operación del mismo y en virtud de que las políticas y procedimientos plasmados en ese instrumento, a la fecha no encuentran sustento jurídico para lo cual fueron creados, por ser inaplicables a los programas que actualmente funcionan, en fecha **22-veintidos de febrero de 2012-dos mil doce,** se declara inoperante el **Manual de Políticas "Seguridad Integral de Informática**", declarándose su **abrogación**.- -

SEGUNDO: Notifíquesele el presente al C. Ing. Manuel Medrano Martínez, Director de Sistemas adscrito a la Secretaría de Administración, para su conocimiento y efectos conducentes. -

TERCERO: Publíquese el presente acuerdo en el portal oficial del municipio de San Pedro Garza García, Nuevo León, dentro del manual en comento. -

Así, administrativamente actuando y conforme a numerales 34 inciso C) fracciones II y III del Reglamento Orgánico de la Administración Pública Municipal de San Pedro Garza García, Nuevo León y 14 fracciones I y V del Reglamento Interior de la Secretaría de la Contraloría y Transparencia Municipal de San Pedro Garza García, Nuevo León, lo acuerda y firma el **C. C.P. ERUBIEL CÉSAR LEIJA FRANCO, SECRETARIO DE LA CONTRALORÍA Y TRANSPARENCIA MUNICIPAL DE SAN PEDRO GARZA GARCÍA, NUEVO LEÓN.** Conste. - - - - - - - - - - - - - - - - -

EL C. SECRETARIO DE LA CONTRALORÍA Y
TRANSPARENCIA MUNICIPAL DE
SAN PEDRO GARZA GARCÍA, NUEVO LEÓN

C. P. ERUBIEL CÉSAR LEIJA FRANCO

Secretaría de la Contraloría y Transparencia Municipal
Independencia No 316 esq. Corregidora 4° Piso, San Pedro Garza García, Nuevo León, México C.P. 66200
Tels. (81) 8400.4478 | 8400.4587 Fax (81) 8400.4439
www.sanpedro.gob.mx

SAN PEDRO
garza garcía

Oficio: DS/018/12

C.P. ERUBIEL CÉSAR LEIJA FRANCO
SECRETARIO DE LA CONTRALORÍA Y TRANSPARENCIA MUNICIPAL
PRESENTE.-

Asunto: Revisión y Abrogación de Manual actual de Políticas de Seguridad, de la Dirección de Sistemas.

Referente a la reciente revisión de Manual de Políticas y a su petición de actualización, se ha determinado conjuntamente con personal de su Secretaría, que lo mas viable es la **abrogación** de este Manual; debido a que su contenido y su referencia de tecnologías queda fuera de lo que actualmente en procesos de la Dirección de Sistemas se llevan a cabo.

Así mismo le informo que llevaremos a cabo la elaboración de un nuevo manual con las especificaciones actuales y alcances mayores, para ello contaremos con el apoyo de la Secretaria de la Contraloría Municipal.

Sin más por el momento y agradeciendo su apoyo, quedo a sus órdenes para cualquier duda o aclaración.

Atentamente,
San Pedro Garza García, N.L. 17 de febrero de 2012

ING. MANUEL MEDRANO MARTÍNEZ
DIRECTOR DE SISTEMAS

PRESIDENCIA MUNICIPAL
SAN PEDRO GARZA GARCIA, N.L.
20 FEB 2012
RECIBIDO
SECRETARIA DE LA CONTRALORÍA
Y TRANSPARENCIA MUNICIPAL

c.c.p. Archivo.

DIRECCIÓN DE SISTEMAS
Palacio de Justicia 2do. Piso, Corregidora No. 507 Nte.
San Pedro Garza García, N.L. C.P. 66200
Tel. 8400 4597
www.sanpedro.gob.mx

ADMINISTRACIÓN PÚBLICA MUNICIPAL

SAN PEDRO GARZA GARCÍA, N.L.

MANUAL DE POLÍTICAS

SEGURIDAD INTEGRAL DE INFORMATICA

INDICE

SISTEMAS
Seguridad Integral de Informática

INDICE

SISTEMAS
Seguridad Integral de Informática

INDICE

SISTEMAS
Seguridad Integral de Informática

SECRETARÍA DE SERVICOS ADMINISTRATIVOS
DIRECCIÓN SISTEMAS

Firmas de Autorización

Presidente Municipal de San Pedro Garza García N.L.
Ing. Gerardo Garza Sada

Secretario de Servicios Administrativos
C.P. Rigoberto Ponce Quezada

Secretario del R. Ayuntamiento
Lic. Ricardo Martínez Elizondo

Director de Sistemas
Ing. Manuel Medrano Martínez

Director Jurídico
Abog. Alejandro López Valdés

Contralor Municipal
C.P. Manuel Treviño Martínez

OBJETIVO:

A TRAVÉS DE LA DIRECCIÓN DE SISTEMAS, PROTEGER LOS ACTIVOS Y RECURSOS DE TECNOLOGÍA DE INFORMACIÓN, QUE SE ENCUENTRAN INSTALADOS Y OPERANDO ACTUALMENTE EN EL MUNICIPIO DE SAN PEDRO, GARZA GARCÍA BUSCANDO DE MANERA PERMANENTE, BRINDAR UN SERVICIO EN EL CAMPO DE SISTEMAS EFICIENTE Y SEGURO PARA LOS SAMPETRINOS, QUE RECIBEN LOS SERVICIOS ADMINISTRATIVOS Y OPERATIVOS CORRESPONDIENTES.

Los objetivos específicos:

- **A)** Identificar las áreas de riesgo que generan para el Municipio de San Pedro el uso de los sistemas de información, así como de los recursos de cómputo y telecomunicaciones.
- **B)** Enfrentar posibles contingencias y eliminar o minimizar los riesgos efectos negativos que afecten la continuidad de operación en los servicios prestados a la comunidad y áreas administrativas y operativas de la alcaldía.
- **C)** Prevenir y detectar los riesgos en las tres líneas de acción establecidas por la Dirección de Sistemas, que son: Servicios inherentes a la administración de la función de sistemas, Seguridad Física y Seguridad Lógica.
- **D)** Mediante un Plan de Implantación formal poder liberarse de manera formal acciones que minimicen y enfrenten las posibles contingencias que genera hoy en día y en el mediano plazo el medio ambiente de software, cómputo y telecomunicaciones

ALCANCE:

Las políticas descritas en el presente Manual se diseñaron para su observancia general y aplicación estricta en la **ADMINISTRACIÓN PÚBLICA MUNICIPAL DE SAN PEDRO GARZA GARCÍA, N.L.** tomando como base las características y necesidades propias de la Administración Municipal.

NIVEL DE APLICACIÓN:

Estas políticas y procedimientos serán de aplicación para las Direcciones de Sistemas, de Adquisiciones, de Recursos Humanos y para todos los usuarios que tengan acceso a equipo de cómputo y a la red.

Únicamente el C Alcalde podrá autorizar las excepciones a estas políticas.

MISIÓN DE LA DIRECCIÓN DE SISTEMAS

San Pedro Garza García: Punta de lanza en tecnología y desarrollo de soluciones informáticas a los procesos Municipales en beneficio del sampetrino.

VISIÓN DE LA DIRECCIÓN DE SISTEMAS

La Dirección de Sistemas ha emprendido el desarrollo de un Manual de Seguridad Integral Proveer y mantener una plataforma de tecnología avanzada, mediante herramientas informáticas, apoyando todas las Dependencias del Municipio, para eficientizar y optimizar los procesos, trámites y desarrollos municipales.

I. SERVICIOS DE LA DIRECCIÓN DE SISTEMAS

ADMINISTRACIÓN DE SERVICIOS DE LA DIRECCIÓN DE SISTEMAS		Servicios
La Dirección de Sistemas debe proporcionar oportunamente a los usuarios los recursos de cómputo, sistemas de información y herramientas de productividad personal para el desempeño de sus labores		
Política No.: MSPser001	**Páginas: 2**	**Vigente a partir de: 2003**

PROCEDIMIENTO

1. La Dirección de Sistemas proporcionará los siguientes servicios al personal operativo y administrativo, según sus necesidades y debida solicitud y aprobación de sus superiores:

   - ❑ Sistemas de información
     - ⇨ Administrativos
     - ⇨ Servicio a la comunidad
   - ❑ Equipo de cómputo
   - ❑ Impresoras
   - ❑ Herramientas de Productividad Personal
     - ⇨ Internet
     - ⇨ Correo electrónico
     - ⇨ Paquete de oficina (hoja electrónica, procesadores de palabra, diagramadores, etc.).
     - ⇨ Control de proyectos
     - ⇨ Otras
   - ❑ Equipo de Cómputo:
     - ⇨ Móvil
     - ⇨ Escritorio
     - ⇨ Servidores
   - ❑ Capacitación:
     - ⇨ Sistemas
     - ⇨ Herramientas de productividad personal
   - ❑ Mesa de ayuda:
     - ⇨ Soporte vía telefónica
     - ⇨ Soporte en sitio
   - ❑ Seguridad

2. La Dirección de Sistemas establecerá los estándares para cada servicio prestado a los usuarios y a la comunidad.

CONTINUA PROCEDIMIENTO

3. El ingreso de un nuevo empleado y su perfil de usuario debe ser notificado formal y oportunamente a la Dirección de Sistemas por el área de Recursos Humanos con el fin de llevar a cabo el siguiente trabajo (únicamente aquellos que por su perfil de trabajo requieran de equipo de cómputo, para desempeñarse):

   - ❑ Definir el programa de capacitación correspondiente
   - ❑ Brindar capacitación requerida en sistemas de información y software
   - ❑ Definir el equipo de cómputo que deberá instalarse
   - ❑ Los sistemas de información que podrá utilizar para el desarrollo de sus funciones y los niveles de acceso correspondientes
   - ❑ Entregarle carta de responsabilidad y coordinarse con patrimonio para el resguardo del equipo de cómputo
   - ❑ Configurar las herramientas de productividad a las que tendrá acceso
   - ❑ Firma del usuario donde se comprometa a cumplir con las políticas de seguridad, antipiratería y buen uso del equipo.

4. Todas las bajas de empleados o cambios de departamento o dirección deben ser notificados por Recursos Humanos a la Dirección de Sistemas para realizar al menos las siguientes medidas preventivas:

   - ❑ Eliminar todos los accesos a sistemas de información y herramientas de productividad que les fueron asignados para desempeñar su trabajo.
   - ❑ Custodia del equipo de cómputo y accesorios mientras se lleva a cabo la reasignación correspondiente.
   - ❑ Inventariar internamente recursos de cómputo para su actualización en activos fijos a la Dirección de Patrimonio.

5. Todos los servicios podrán ser evaluados con base a una definición formal de niveles de servicio y a una encuesta anual de satisfacción de usuarios.

6. Cada solicitud de servicio se atenderá por personal de mesa de ayuda y el seguimiento a la misma quedará registrada en una bitácora formal.

7. Los empleados o personal externo que no cumplan con la presente política pueden provocar que se les retiren los privilegios, y en su caso estarán sujetos a medidas disciplinarias establecidas al respecto.

a) Responsable de su implantación: Dirección de Sistemas / Dirección de Patrimonio

b) Periodo sugerido de revisión: anual

c) Responsables de su cumplimiento: Recursos Humanos /Sistemas / Usuarios

Evidencia de Control Solicitud de Servicio, perfiles de usuarios, lista de

productos y servicios de informática, bitácora de servicios

INSTALACIÓN DE EQUIPO DE CÓMPUTO	Servicios

Los estándares de cómputo, así como la adquisición, instalación, monitoreo y reemplazo de equipo son responsabilidad de la Dirección de Sistemas

Política No.: MSPser002	Páginas: 3	Vigente a partir de: 2003

PROCEDIMIENTO

1. La Dirección de Sistemas es la responsable de definir los estándares de Tecnología:

   - ❑ Equipo de Cómputo Móvil
   - ❑ Equipo de Cómputo de Escritorio
   - ❑ Servidores

2. Todos los requerimientos de equipo de cómputo que sean adquiridos deben sujetarse al siguiente procedimiento:

   - ❑ Estar justificados por la función desempeñada
   - ❑ Tener presupuesto asignado
   - ❑ Tanto el presupuesto y compra autorizada por Director de Área deben seguir el flujo de operaciones y autorizaciones definidas por la políticas de adquisiciones establecidas
   - ❑ La adquisición del equipo se da por las siguientes razones
     - Personal de nuevo ingreso
     - Cambio de equipo por caducidad o reemplazo
     - Robo de equipo
     - Daño permanente en equipo a reemplazar
     - Implantación de un nuevo proyecto

3. El seguimiento a la compra debe realizarla adquisiciones, y el apoyo que brindará la Dirección de Sistemas consistirá en asegurarse que los modelos de cómputo a adquirir cumplan con los estándares establecidos formalmente.

4. El equipo de cómputo será configurado por personal de la Dirección de Sistemas para instalarle software de acuerdo al perfil administrativo y operativo del usuario correspondiente (a excepción de aquellos proyectos específicos o llave en mano que dependan de proveedores externos):

   - ❑ Aplicaciones (Alta, baja, cambios, generación de reportes, consultas, respaldos, etc.).

- ❑ Herramientas de Productividad Personal (Correo Electrónico, Internet, Procesadores de Palabra, Diagramadores, etc.).
- ❑ Software de uso específico (Diseño, Ingeniería, Auditoria, etc.).

CONTINUA PROCEDIMIENTO

5. La Dirección de Sistemas y el área de Recursos Humanos serán los responsables de definir el plan de capacitación (contenido del curso, calendario, método de evaluación, etc.), que recibirán los usuarios para utilización del equipo de cómputo y el software facilitado para sus labores:

   - ❑ Uso de los sistemas de información o aplicaciones
   - ❑ Uso de las Herramientas de Productividad
   - ❑ Procedimientos de Seguridad

6. La Dirección de Sistemas será la responsable de entregar e instalar el equipo de cómputo de escritorio, asegurándose de que se cumpla lo siguiente:

   - ❑ Instalación del equipo en el lugar del usuario
   - ❑ Prueba de arranque
   - ❑ Aclaración de dudas en la iniciación de cada paquete o aplicación
   - ❑ Firma del usuario donde se comprometa a cumplir con las políticas de seguridad, antipirateria y buen uso del equipo.
   - ❑ Activación de servicios de red

7. La Dirección de Sistemas será la responsable de entregar el equipo de cómputo móvil, asegurándose de que se cumpla lo siguiente:

   - ❑ Prueba de arranque
   - ❑ Aclaración de dudas en la iniciación de cada paquete o aplicación
   - ❑ Firma del usuario donde se comprometa a cumplir con las políticas de seguridad, antipirateria y buen uso del equipo.
   - ❑ Activación de servicios de red

8. El usuario es responsable del cuidado del equipo, así como de la resguarda de los datos alojados en su equipo

9. Los user-id y passwords de acceso a aplicaciones y servicios como internet y correo electrónico serán asignados inicialmente por la Dirección de Sistemas, y el cuidado y confidencialidad de los mismos depende del usuario directamente.

10. El soporte a los usuarios es responsabilidad de la Dirección de Sistemas

11. El reemplazo de equipo, control de fallas y la aplicación de garantías son responsabilidad de la Dirección de Sistemas.

12. El control de versiones de software para instalación en equipos de cómputo será realizado por la Dirección de Sistemas.

CONTINUA PROCEDIMIENTO

13. Los empleados o personal externo que no cumplan con la presente política pueden provocar que se les retiren los privilegios, y en su caso estarán sujetos a medidas disciplinarias establecidas al respecto.

a) Responsable de su implantación: Dirección de Sistemas/Dirección de Patrimonio

b) Periodo sugerido de revisión: Por evento (alta o baja de usuario)

c) Responsables de su cumplimiento: Usuarios

Evidencia de Control	**Bitácoras, carta de instalación, software de administración y monitoreo de equipos instalados, sistema operativo.**

COMPUTADORAS PORTÁTILES		**Servicios**
Todo el equipo de cómputo móvil deberá ser asignado y utilizado conforme a los criterios de administración y seguridad establecidos		
Política No.: MSPser003	**Páginas: 1 de 2**	**Vigente a partir de: 2003**

PROCEDIMIENTO

1. Los estándares de equipo de cómputo de escritorio y de equipo de cómputo móvil son definidos por la Dirección de Sistemas.

2. La Dirección de Sistemas solamente incluirá en el plan de adquisiciones de computadoras portátiles, aquellas que formen parte del presupuesto autorizado para cada dirección del municipio.

3. La asignación de equipo de cómputo se hará conforme al proceso de requisición y compra establecido en el Municipio de San Pedro.

4. Todas las computadoras portátiles deben ser asignadas a empleados que lo justifiquen por su puesto y función.

5. La Dirección de Sistemas podrá corroborar el detalle de cada solicitud de equipo de cómputo móvil con el usuario y jefes inmediatos si es necesario.

6. Los equipos de cómputo de escritorio y equipo móvil que sean reemplazados por equipo nuevo, deberán ser entregados a la Dirección de Sistemas y este lo canalizará conforme a las políticas del Municipio a donde sea más conveniente (Donación, venta, etc.), estableciendo comunicación con la Dirección de Patrimonio para la baja o cambio de esos activos, según sea el caso.

7. Los criterios establecidos para la asignación de cómputo móvil, para el personal del Municipio de San pedro son los siguientes:

    a. Funciones del empleado (Auditoria, Ingenieros de campo, etc.).
    b. Que el empleado requiera de manera cotidiana del uso de la computadora en su hogar, para desarrollar tareas de su puesto.

c. Brindar o procesar información en eventos que dan atención ciudadana en colonias o edificios municipales.

8. Las computadoras portátiles y el software que se entreguen a los usuarios, se asignarán de acuerdo al puesto y perfil del usuario.

CONTINUA PROCEDIMIENTO

PUESTO DEL SOLICITANTE	EQUIPO DE CÓMPUTO	SOFTWARE
Secretaria	Escritorio	Paquetes de oficina Correo electrónico Internet
Operador / auxiliar	Escritorio	Paquetes de Oficina Aplicaciones operativas (CxC / Inventarios/ etc) Correo Electrónico Internet
Coordinador / Jefe de área	Escritorio	Paquetes de oficina Internet Correo electrónico
Coordinador / Jefe de área (funciones de auditoria / empleados de frecuente desplazamiento)	Móvil	Aplicaciones Internet Correo Electrónico Firewalls (Seguridad)
Directores	Escritorio Móvil	Paquete de oficina Internet Correo Electrónico Aplicaciones
Secretarios	Escritorio Móvil	Paquete de oficina Internet Correo Electrónico Aplicaciones
Alcalde	Escritorio Móvil	Paquete de oficina Internet Correo Electrónico Aplicaciones

9. Los usuarios al recibir su computadora móvil o de escritorio firmarán carta de recepción donde se haga constar lo siguiente:

a. Harán buen uso del equipo (firma)
b. Respetarán las reglas de seguridad establecidas con relación al equipo

- Antipirateria
- Control de acceso físico
- Control de acceso lógico

CONTINUA PROCEDIMIENTO

10. Con relación a las computadoras portátiles, los usuarios deben cumplir con las siguientes acciones preventivas de seguridad:
    a. No deberá promover el uso de software pirata ni de instalarlo en su equipo
    b. No deberá revelar sus claves de acceso por ningún motivo
    c. No deberá utilizar el equipo para fines ajenos a los de sus funciones y responsabilidades con el Municipio
    d. Atender los cursos de capacitación que promueva la Dirección de Sistemas para los usuarios del Municipio.
    e. Cualquier robo o daño a su computadora debe ser inmediatamente reportado a la Dirección de Sistemas y a la Dirección de Patrimonio.
    f. Ser responsable del respaldo de datos oportuno y de la depuración de la información contenida en su equipo
    g. Instalar los accesorios de seguridad que le proporcione el municipio para salvaguarda del equipo
    h. Siempre estar alerta del equipo cuando se encuentre fuera de la oficina
    i. Otras que la Dirección de Sistemas o el Municipio consideren convenientes para la protección de este activo.

11. Ni la Dirección de Sistemas ni el Municipio se hacen responsables por el mal uso que se haga del equipo portátil, cuando esté se encuentre fuera de la red (conectada a un servidor) ni cuando este se transporte fuera de nuestras oficinas y se utilice de manera mal intencionada por el usuario o personal ajeno a nuestra institución.
12. El Municipio no es responsable de la administración ni salvaguarda de computadoras portátiles que traigan los empleados a nuestras oficinas.
13. Todas las computadoras portátiles que por proyectos con el Municipio, se conecten a nuestra red, seguirán nuestras políticas de seguridad.
14. Los reemplazos de equipo portátil serán programados por la Dirección de Sistemas y las excepciones no se contemplan en esta política.

a) Responsable de su implantación: Dirección Sistemas/Dirección de Patrimonio

b) Periodo sugerido de revisión: Permanente

c) Responsables de su cumplimiento: Usuarios

Evidencia de Control	**Solicitud de Servicio, perfiles de usuarios, lista de productos y servicios de informática, bitácora de servicios**

CORREO ELECTRÓNICO		Servicios
Los usuarios y administradores de sistemas deben cumplir los procedimientos establecidos para garantizar la seguridad y buen uso del correo electrónico		
Política No.: MSPser004	**Páginas: 3**	**Vigente a partir de: 2003**

PROCEDIMIENTO

1. La Dirección de Sistemas es la responsable de administrar los servicios de correo electrónico y para tal efecto tiene las siguientes tareas:

   - ❑ Configuración de los servicios
   - ❑ Altas y bajas de usuarios
   - ❑ Procedimientos relativos a Seguridad Lógica
   - ❑ Soporte a usuarios
   - ❑ Actualización de versiones
   - ❑ Depuración de correo masivo

2. Tanto al Alcalde como a Secretarios y Directores, se les asignará un correo electrónico y a los demás empleados la asignación deberá ser condicionada mediante un oficio que lo solicite, mencionado su número de nómina, nombre, puesto y dependencia; así como mencionar el porqué requiere de correo electrónico, enviado por el Alcalde, Secretario o Director que lo autoriza a la Dirección de Sistemas.

3. El uso del correo electrónico que de cada empleado se orienta de manera exclusiva a dar apoyo a las tareas asignadas por el Municipio, así mismo, como el preservar en secreto la contraseña (password) que les ha sido proporcionadas.

4. Es responsabilidad de los usuarios depurar y respaldar sus mensajes y archivos clave derivados del uso de correo electrónico.

5. Los administradores de Informática son los responsables para implantar las políticas de seguridad lógica inherentes a este servicio:

   - ❑ Control de accesos
   - ❑ Asignación del uso de correo electrónico
   - ❑ Detección y control de virus computacionales
   - ❑ Atención a incidentes que afecten la continuidad del servicio
   - ❑ Registro y seguimiento al mal uso del correo electrónico

CONTINUA PROCEDIMIENTO

6. Es responsabilidad de Recursos Humanos y de las direcciones que integran cada Secretaria notificarle a la Dirección de Sistemas de las altas, bajas y cambios de empleados para garantizar que se den los siguientes controles:

    a. Asignar acceso a servicios de correo electrónico a nuevos empleados
    b. Baja de empleados para cancelar privilegios de acceso al correo
    c. Resguardo de la información almacenada en los buzones de correo

7. La Dirección de Sistemas notificará de manera oportuna a las direcciones correspondientes de todas las acciones negativas que realicen los usuarios con el correo electrónico y que vayan en contra de las políticas de seguridad. Tales acciones pueden ser por ejemplo:

    - Mensajes de propaganda política / Amenazas
    - Mensajes de contenido sexual / Mensajes que promuevan el racismo
    - Mensajes con publicidad de negocios particulares
    - Ideas religiosas / Pornografía Infantil / Promover la Piratería de Software
    - Otros que afecten las políticas de comunicación establecidas por el Municipio

8. La intención primaría del correo electrónico es enviar y recibir mensajes, así como archivos electrónicos ligados con las actividades propias de la institución y los mensajes generados de correo electrónico se consideran propiedad del Municipio y pertenecen a las Direcciones correspondientes.

9. Los empleados cumplirán la seguridad que han tenido con los documentos escritos o con los servicios que les brinda el teléfono o el fax. (respaldo, confidencialidad, veracidad, actualización, clasificación, difusión, etc.).

10. Los mensajes indiquen a pie de página que la información en comunicados de los empleados no necesariamente reflejan la posición del Municipio.

11. Los empleados o personal externo que no cumplan con la presente política pueden provocar que se les retiren los privilegios, y en su caso estarán sujetos a medidas disciplinarias establecidas al respecto.

a) Responsable de su implantación: Dirección de Sistemas

b) Periodo sugerido de revisión: Semestral

c) Responsables de su cumplimiento: Usuarios

Evidencia de Control	Solicitud de Servicio, perfiles de usuarios, lista de productos y servicios de informática, bitácora de servicios

INTERNET	Servicios
Todos los usuarios deben acatar de manera permanente las políticas y procedimientos relacionadas con el uso de Internet	
Política No.: MSPser005	**Páginas: 3**	**Vigente a partir de: 2003**

PROCEDIMIENTO

1. Todos los servicios de Internet proporcionados por la Dirección de Sistemas a los empleados se limitaran al uso y condiciones establecidas por la Secretaria de Servicios Administrativos y el Municipio de San Pedro.

2. La Dirección de Sistemas instalará y actualizará de manera oportuna un firewall (apaga fuegos) y un detector de intrusos con el objetivo de minimizar o eliminar los riesgos de accesos no autorizados vía Internet.

3. Todos los empleados podrán utilizar Internet cuando las funciones que desempeña requieran de esta herramienta de trabajo, así mismo cuando haya cumplido previamente con los requerimientos de autorización de acceso.

4. La Dirección de Sistemas activará los accesos a Internet únicamente a aquellas personas autorizadas por su Director de Área o Secretario, mencionando su número de nómina, nombre, puesto y dependencia, y las funciones que justifiquen el uso de Internet, esto a través de un oficio dirigido a la Dirección de Sistemas.

5. Los usuarios de Internet cumplirán con las políticas descritas en este manual y en caso contrario podrán ser sujetas a las medidas disciplinarias administrativas y legales establecidas para estos casos.

6. Los usuarios no deben intentar acceder al Internet suplantando los privilegios de acceso de otra persona.

7. El empleado solamente puede utilizar el user id, el password, las direcciones de correo, los buzones de mensajes, y demás servicios de Internet para realizar investigaciones, consultas o intercambio de información relacionada con las funciones inherentes a su puesto.

8. Cuando los empleados requieran utilizar los servicios de Internet para propósitos personales deben hacerlo en su tiempo no laboral utilizando user id, passwords, software y proveedor de servicios particulares.

CONTINUA PROCEDIMIENTO

9. Los empleados tienen prohibido cambiar el contenido o estructura de la página del Municipio de San Pedro. Ya que los responsables son la Dirección de Sistemas y los representantes de comunicación e imagen de la alcaldía.

10. Lo usuarios no abrirán correos que se sospeche vengan de una fuente no confiable o que contengan archivos no solicitados previamente.

11. Las páginas de Internet del Municipio de San Pedro tendrán un respaldo de la última versión en una localidad diferente a donde se encuentra la original.

12. Las medidas de seguridad lógica fortalecerán el control de accesos y de monitoreo de actividades ligadas a los servicios de Internet.

13. Todas las páginas propiedad del Municipio tendrán advertencias legales para que empleados o terceros sean prevenidos de llevar acabo acciones malintencionadas (Disclaimers) con el diseño y contenido de dichas páginas.

14. El Municipio provee acceso a Internet a sus empleados, el uso y acciones que con esta herramienta se hagan son responsabilidad de los usuarios. A continuación se mencionan algunas actividades ilícitas:

    a. Violar los derechos de autor
    b. Accesar a sitios de Internet no autorizados
    c. Enviar comunicados de terceros a otros sin su autorización
    d. Enviar mensajes anónimos que atenten contra la moral desde equipos y enlaces proporcionados por el Municipio
    e. Dedicar tiempo a Internet que afecte la productividad de su trabajo.

15. Los objetivos del municipio son el facilitar a sus empleados el acceso a fuentes de información valiosas y útiles para el desempeño de su trabajo, e intentará con los medios y recursos disponibles evitar accesos a sitios que puedan contener material ilegal, pornográfico, difamatorio, inexacto o potencialmente ofensivo para menores o adultos por su contenido u orientación.

16. La Dirección de Sistemas tratará en lo posible de proteger la información de cada usuario de Internet, sin embargo esto no es una garantía, ya que el usuario debe cumplir con las políticas de confidencialidad, cuidado del equipo, respaldo de mensajes, entre otras cosas para tener una seguridad aceptable.

CONTINUA PROCEDIMIENTO

17. Los empleados o personal externo que no cumplan con la presente política pueden provocar que se les retiren los privilegios, y en su caso estarán sujetos a medidas disciplinarias establecidas al respecto.

a) Responsable de su implantación: Dirección de Sistemas

b) Periodo sugerido de revisión: Semestral

c) Responsables de su cumplimiento: Usuarios

Evidencia de Control	Bitácora de uso de los servicios de Internet, Políticas de Seguridad Lógica

INTRANET	Servicios

La administración de Intranet es responsabilidad de la Dirección de Sistemas, y los usuarios de su correcta utilización.

Política No.: MSPser006	Páginas: 2	Vigente a partir de: 2003

PROCEDIMIENTO

1. La Dirección de Sistemas es la responsable de llevar a cabo las siguientes tareas de administración y control de la Intranet

   - ❑ Desarrollo o adquisición de la solución Intranet
   - ❑ Altas, Bajas y Cambios de usuarios, con sus correspondientes privilegios
   - ❑ Soporte a usuarios y actualización de la solución
   - ❑ Integrador de requerimientos con comunicación y recursos humanos
   - ❑ Respaldos de los datos

2. El área de comunicación e imagen es responsable de verificar que tanto la estructura de navegación como el contendido cumplan con los requerimientos establecidos para transmitir información que no afecte los intereses u objetivos del Municipio.

3. Los objetivos de la Intranet son de difundir entre otros aspectos:

   - ❑ Políticas y comunicados de cada secretaria o dirección del Municipio
   - ❑ Políticas de Recursos Humanos
   - ❑ Políticas y procedimientos de seguridad en informática
   - ❑ Iniciativas o proyectos que benefician directamente a la comunidad
   - ❑ Boletines informativos / Circulares
   - ❑ Difusión de eventos internos

4. Las diferentes secretarias son responsables entre otras cosas de los siguiente:
   - ❑ Contenido de la información que desean exponer en Intranet
   - ❑ Solicitar modificaciones al contenido a la Dirección de Sistemas
   - ❑ Cumplimiento de las políticas de seguridad establecidas para Intranet

5. La Dirección de Sistemas y Recursos Humanos definirán y difundirán los roles y responsabilidades del personal de Sistemas, así como de las áreas usuarias involucradas en la administración de la Intranet del Municipio

6. Los datos de terceros que se difundan en Intranet tendrán un aviso preventivo de Derechos para evitar el uso indebido de los mismos.

7. Es importante reiterar a los usuarios que al navegar en Internet o Intranet es necesario respetar siempre los Derechos de Propiedad de Información.

CONTINUA PROCEDIMIENTO

8. Toda la información reflejada en Intranet que no contenga Derechos otorgados a terceros, se considera PROPIEDAD del Municipio de San Pedro.

9. Los administradores de Intranet podrán en todo momento y en medida de lo posible verificar el buen uso que se de a la información contenida en Intranet.

10. El password de acceso que se brinde a cada usuario para navegación y uso de la información de Intranet es confidencial y no debe compartirse con nadie.

11. La Dirección de Sistemas en Coordinación con las direcciones correspondientes y con el área de Recursos Humanos podrá desactivar los privilegios de acceso a todos aquellos usuarios que hagan mal uso de Intranet.

12. La Intranet no debe ser utilizada para promover negocios o actividades particulares, racismo, aspectos religiosos o propaganda política, pornografía infantil, difamación, entre otros.

13. La Dirección de Sistemas establecerá con el uso de herramientas de software y hardware todas las medidas necesarias para prevenir, detectar y bloquear accesos de terceros no autorizados.

14. La Dirección de Sistemas de manera inicial configurará los niveles de acceso mínimos (configuración primaria) para que los usuarios puedan consultar el contenido de la Intranet, conforme se justifique se darán más privilegios.

15. Recursos Humanos avisará a la Dirección de Sistemas de todas las altas, bajas o cambios de personal para que se eliminen accesos, se creen nuevas cuentas de usuario o se modifiquen privilegios.

a) Responsable de su implantación: Dirección de Sistemas

b) Periodo sugerido de revisión: Semestral

c) Responsables de su cumplimiento: Usuarios

Evidencia de Control	Bitácora de uso de los servicios de Intranet, Políticas de Seguridad Lógica

ATENCIÓN A REQUERIMIENTOS DE USUARIOS		Servicios
Todos los servicios que reciban los usuarios de la Dirección de Sistemas deberán ser registrados, atendidos y concluidos de manera formal y eficiente		
Política No.: MSPser007	**Páginas: 2**	**Vigente a partir de: 2003**

PROCEDIMIENTO

1. Todos los servicios proporcionados por las diferentes áreas que integran a la Dirección de Sistemas, serán registrados y controlados en una bitácora de servicios, asegurando que cada uno de ellos se atienda oportuna y eficientemente.
   - ❑ Los usuarios son los responsables de solicitar los servicios por los canales que se establecen en este procedimiento (Punto 3).
   - ❑ El personal de Sistemas es el responsable de registrar el servicio solicitado por el usuario, en el formato adjunto a esta política (Solicitud de Servicios de Sistemas **SolMSP1**)
   - ❑ Sin excepción, cada requerimiento notificado a sistemas y que genere un servicio, será registrado y controlado, hasta su oportuna satisfacción).

2. A continuación se mencionan los diferentes servicios que ofrece la Dirección de Sistemas, y los responsables de darle seguimiento:

TIPO DE SERVICIO	RESPONSABLE	COMENTARIOS
Adquisición de equipo	Operación	De acuerdo a presupuesto
Cambio de equipo	Operación	Por falla / Plan de cambio
Instalación de equipo	Operación	Se programa la fecha
Instalación de Sistema Operativo y Office	Operación	Se programa la fecha
Capacitación	Soporte a usuarios	Se da por calendario programado
Cambios o mejoras a los Sistemas de Información	Desarrollo	Se programa de acuerdo a la magnitud del cambio aprobado
Desarrollo de nuevos sistemas	Desarrollo	De acuerdo al plan de Sistemas
Correo electrónico	Operación	Se programa la fecha
Internet	Operación	Se programa la fecha
Herramientas de software de uso específico	Operación	Se programa la fecha
Asesoría para soportar proyectos del Municipio	Dirección de Sistemas	Por evento

CONTINUA PROCEDIMIENTO

3. Las diferentes alternativas para que cada solicitud de servicio de los usuarios, hacia la Dirección de Sistemas, son las siguientes:

SOLICITUD DE SERVICIO	REFERENCIA	HORARIOS
Vía Telefónica	Tel. Ext.	24 Horas x 7 días
Correo Electrónico	Email:	24 Horas x 7 días
Informal (en pasillo / oficina)	Se solicita verbalmente a Sistemas Esta solicitud informal deberá ser registrada por personal de sistemas antes de dar el servicio	Horarios de oficina

4. Todas las solicitudes de servicio serán entregadas al usuario al cumplirse con el requerimiento, para que se documenten los niveles de servicio correspondiente.
   - ❑ Fecha
   - ❑ Número de solicitud de servicio
   - ❑ Usuario solicitante del servicio de sistemas
   - ❑ Tipo de servicio
   - ❑ Responsable del servicio
   - ❑ Nivel de satisfacción del usuario del servicio recibido
   - ❑ Etc.

5. La Dirección de Sistemas actualizará la Bitácora de servicios ofrecidos a los usuarios a lo largo del año (**BitMSP1**).

a) Responsable de su implantación: Dirección de Sistemas

b) Periodo sugerido de revisión: anual

c) Responsables de su cumplimiento: Usuarios

Evidencia de Control **Solicitud de Servicio, Bitácora de control de servicios**

SECRETARÍA DE SERVICIOS ADMINSTRATIVOS

DIRECCIÓN DE SISTEMAS

REQUERIMIENTO DE USUARIO

SolMSP1

Fecha / /	**Folio No.**

Datos del solicitante del servicio: Nombre: Dirección en que trabaja:	Atendido por: Área de Sistemas: **(Operación, Desarrollo, Dirección)**

Marque con una X el tipo de servicio requerido por el usuario

Adquisición de equipo	
Cambio de equipo	
Instalación de equipo	
Instalación de Sistema Operativo y Office	
Capacitación	
Cambios o mejoras a los Sistemas de Información	
Desarrollo de nuevos sistemas	
Correo electrónico	
Internet	
Herramientas de software de uso específico	
Asesoría para soportar proyectos del Municipio	

TERMINACIÓN DEL SERVICIO DE LA DIRECCIÓN DE SISTEMAS	
Fecha en que se termina el servicio: / /	
Nombre y firma del usuario:	**¿Cómo califica el servicio?** a) Excelente ( ) b) Bueno ( ) c) Regular ( ) d) Malo ( ) Comentario del Usuario:

BitMSP1

BITÁCORA DE SERVICIOS DE LA DIRECCIÓN DE SISTEMAS

No. De Folio	Fecha de solicitud / /	Fecha de entrega / /	Responsable de sistemas

II. SEGURIDAD LÓGICA

LONGITUD DEL PASSWORD		Seguridad Lógica
Los passwords deben tener una longitud mínima para eliminar riesgos de que sean fácilmente detectados por gente no autorizada		
Política No.: MSPsl001	**Página: 1 de 1**	**Vigente a partir de: 2003**

PROCEDIMIENTO MSPSL001

1. La longitud de los passwords debe ser configurada y definida por los administradores del sistema operativo de red y Sistemas de Información Administrativos.
2. La longitud de passwords se revisará automáticamente por los sistemas operativos instalados por la Dirección de Sistemas cuando los usuarios activen tales passwords
3. Para usuarios de Windows la longitud mínima debe ser de 8 caracteres.
4. Para usuarios de soluciones Lotus Notes debe ser al menos de 8 caracteres.
5. Para usuarios del Sistema de Administración deben tener una longitud de 8 caracteres.
6. Los sistemas de alta seguridad deben considerar otros mecanismos para verificar la identificación de los usuarios, tal como passwords dinámicos, el cual cambia cada minuto o cada que el usuario inicia una sesión.
7. Los usuarios son responsables de cambiar sus passwords de manera frecuente (al menos cada tres meses)
8. Es necesario que los usuarios reciban un mail que describa la importancia de cambiar la longitud de los passwords para minimizar riesgos de accesos no autorizados. Este comunicado debe especificar la forma y tiempos de cumplimiento a esta política.
9. Este comunicado debe enviarse a más tardar treinta días antes de su implantación y debe ser respondida con un correo de aceptación de cada usuario.

a) Responsable de su implantación: Administradores de sistemas

b) Periodo sugerido de revisión: Semestral

c) Responsables de su cumplimiento: Administradores de sistemas da altas baja de user id y passwords.
usuarios cambian su password

Evidencia de Control	Sistema Operativo

DEFINICIÓN DEL PASSWORD		**Seguridad Lógica**
Todos los passwords seleccionados por los usuarios para las redes y computadoras deben ser difíciles de adivinar.		
Política No.: MSPsl002	**Página: 1 de 1**	**Vigente a partir de: 2003**

PROCEDIMIENTO MSPSL002

1. Al crear un password considerar el mínimo de caracteres requeridos así como las reglas que se dan para que este sea lo más difícil de adivinar posible. Además tratar de con cierta frecuencia cambiar todos los passwords. Por ejemplo términos técnicos y médicos pudieran prohibirse. Esta política y controles relacionados son particularmente importantes si los usuarios emplean el mismo password en varios sistemas.
2. Se pueden emplear métodos como: a) Juntar algunas palabras (se conocen como "passphrases"). b) Cambiar una palabra arriba, abajo, izquierda o derecha de la línea en el teclado. c) Cambiar caracteres en una palabra un cierto número de letras arriba o abajo del alfabeto. d) Combinar puntuación o números con una palabra regular. e) Crear acrónimos de palabras en una canción, un poema u otra secuencia de palabras conocidas. g) Combinar un número de factores personales como fechas de cumpleaños y colores favoritos.
3. Palabras en un diccionario, derivados de user-ids y secuencias de caracteres comunes tales como "123456" no se deben emplear. Así como detalles personales como el nombre de la esposa, placas del automóvil, rfc, número de seguro social, y cumpleaños no debe usarse a menos que se acompañe con caracteres no relacionados adicionales. Passwords que los usuarios seleccionan no deben ser parte de un discurso. Por ejemplo nombres propios, locaciones geográficas, acrónimos comunes, etc. No deben usarse.

a) Responsable de su implantación: Usuarios

b) Periodo sugerido de revisión: Frecuente (mínimo una vez cada 6 meses)

c) Responsables de su cumplimiento: Usuarios

Evidencia de Control	**Aplicar recomendaciones en la creación de passwords**

PASSWORDS CÍCLICOS		Seguridad Lógica
Los usuarios de Red y Sistemas no deben tener passwords cíclicos		
Política No.: MSPsl003	**Página: 1 de 1**	**Vigente a partir de: 2003**

PROCEDIMIENTO MSPSL003

1. Es responsabilidad de los administradores de sistemas garantizar que el Sistema Operativo valide automáticamente que los usuarios no usar passwords cíclicos, ya que la seguridad de la red y los sistemas conectados a la red se reduce.
2. Prohibir a los usuarios construir password fijos combinando caracteres determinados que no cambian o con cambios predecibles.
3. Usar un proceso automático que compare los passwords anteriores y nuevos para asegurarse que no se vuelvan a usar los mismos passwords.
4. En estos passwords prohibidos los caracteres con cambios se basan típicamente en el mes, un departamento, un proyecto, o algún otro factor fácil de adivinar. Por ejemplo, usuarios no deben emplear passwords como “Ene2002” en enero, o “Feb2003” en febrero, etc.

a) Responsable de su implantación: Administradores de Sistemas

b) Periodo sugerido de revisión: Frecuente (mínimo una vez cada 6 meses)

c) Responsables de su cumplimiento: Administradores de Sistemas

Evidencia de Control	Sistema Operativo Unix, Windows NT

PASSWORDS HISTÓRICOS		Seguridad Lógica
No se deben usar passwords que ya fueron seleccionados por usuarios o administradores anteriormente		
Política No.: MSPsl004	**Página: 1 de 1**	**Vigente a partir de: 2003**

PROCEDIMIENTO MSPSL004

1. Prohibir a los usuarios elegir passwords que hayan empleado anteriormente.
2. Debe buscarse que el sistema operativo pueda impedir o prevenir a los usuarios de emplear cualquiera de los últimos **9** passwords.
3. El número de passwords que no debe repetir lo define la Dirección de Sistemas.
4. En todas las maquinas multi-usuario, usar software de los sistemas o software desarrollado localmente para mantener un historial encriptador de los passwords fijos anteriores. Este archivo histórico se usara para prevenir a los usuarios de volver a usar los passwords fijos. El archivo histórico mínimo contendrá los últimos 13 passwords de cada user-id.

Nota: Volver a usar los passwords incrementa las posibilidades que el password se divulgue a personas no autorizadas que tomen ventaja de este conocimiento, además se incrementa las oportunidades de que se adivinen porque se van a usar en períodos considerablemente más largos.

a) Responsable de su implantación: Administradores de Sistemas

b) Periodo sugerido de revisión: Por evento (alta o cambio de password)

c) Responsables de su cumplimiento: Administradores de Sistemas

Evidencia de Control	Sistema Operativo Unix, Windows NT

PASSWORDS PROTEGIDOS		Seguridad Lógica
El desplegado e impresión del password debe ser enmascarado		
Política No.: MSPsl005	**Página: 1 de 1**	**Vigente a partir de: 2003**

PROCEDIMIENTO MSPSL005

1. El desplegado e impresión de passwords debe ser enmascarado, suprimido o de otra manera obscurecido por lo tanto partes no autorizados no serán capaces de observar o recobrar subsecuentemente a estos.
2. Es importante asegurar que cada usuario tenga un único password y user-id.
3. Los usuarios serán los únicos que conozcan sus passwords.
4. Ni el responsable de seguridad conocerá los passwords (con la excepción temporal de impresiones nuevas o reimpresiones justificadas por un requerimiento de usuario).
5. Todos los eventos donde el usuario requiera que el administrador o el sistema utilice sus datos para recuperar su password, deben ser registrados y guardados en una bitácora.
6. Siempre que un usuario teclee un password en el sistema, el password no será desplegado en el monitor o impreso en una copia de otra terminal.

a) Responsable de su implantación: Administradores de Sistemas

b) Periodo sugerido de revisión: Por evento (Recuperación de password)

c) Responsables de su cumplimiento: Administradores de Sistemas

Evidencia de Control	Sistema Operativo Unix, Windows NT, Bitácora de Cambios

LEGIBILIDAD DEL PASSWORDS		Seguridad Lógica
Los passwords no deben ser almacenados ni desplegados en forma legible		
Política No.: MSPsl006	**Página: 1 de 1**	**Vigente a partir de: 2003**

PROCEDIMIENTO MSPSL006

1. El administrador del sistema realizará las acciones necesarias para garantizar que los nombres de usuarios con sus correspondientes user id, passwords y perfiles de usuario estén debidamente protegidos contra accesos no autorizados.
2. Tanto usuarios como el administrador evitarán tener en reportes o papeles de trabajo los nombres con sus correspondientes user id y passwords.
3. Los passwords no se almacenarán en forma legible, en archivos batch, ini, scripts de login automático, macros de software, en computadoras sin control de accesos, o en otras facilidades donde personas no autorizadas puedan descubrirlas o usarlas.
4. Dar entrenamiento a los usuarios para que usen los paquetes de software sin almacenar sus passwords en documentos .doc, .xls, etc. Ya que algunos usuarios piensan que guardar sus passwords en forma legible les va a ayudar a recordar sus passwords pero esto indudablemente expone al sistema a accesos no autorizados.
5. Todos los eventos donde el usuario requiera que el administrador o el sistema utilice sus datos para recuperar su password, deben ser registrados y guardados en una bitácora.

a) Responsable de su implantación: Administradores de Sistemas

b) Periodo sugerido de revisión: Por evento (Recuperación / Cambio de password)

c) Responsables de su cumplimiento: Administrador del sistema / Usuarios

Evidencia de Control	Sistema Operativo Unix, Windows NT, Bitácora de Cambios

PASSWORDS DESCUBIERTOS		Seguridad Lógica
Los administradores de sistemas y los usuarios deben cancelar o hacer cambios a los passwords que se sospecha fueron descubiertos		
Política No.: MSPsl007	**Página: 1 de 1**	**Vigente a partir de: 2003**

PROCEDIMIENTO MSPSL007

1. Solamente el usuario conocerá su password. Si el password en cuestión ha sido descubierto por otras personas o solo se sospecha, entonces este se cambiará inmediatamente.
2. Los administradores tienen la facultad de notificar a los usuarios de la cancelación o cambio obligado de los passwords si existen sospechas fundadas de que estos han sido descubiertos por personal no autorizado (incluye personal interno).
3. Los usuarios deben notificar inmediatamente las actitudes sospechosas del personal que reiteradamente manifieste un interés de descubrir o conocer los passwords del personal usuario.
4. El usuario podrá cambiar sus passwords cuando las circunstancias lo requieran. Si esto no es posible por razones administrativas o técnicas, como vía alternativa, una persona de Informática podrá resetear los passwords de los user inmediatamente.
5. Si un sistema de cómputo multiusuario emplea passwords fijos para control de acceso primario, todos los passwords deben ser cambiados inmediatamente después de que se pruebe que el sistema ha sido descubierto, al mismo tiempo.
6. Los usuarios deben conocer un procedimiento emergente para cancelación y cambios de sus passwords.

a) Responsable de su implantación: Administradores de Sistemas

b) Periodo sugerido de revisión: Por evento (Cambio de password)

c) Responsables de su cumplimiento: Administrador del sistema / Usuarios

Evidencia de Control	Bitácora de Cambios / Registro de incidentes

IDENTIFICAR USUARIOS		Seguridad Lógica
Los avisos de los passwords nuevos o modificados por parte de los administradores a los usuarios serán revelados bajo identificación satisfactoria		
Política No.: MSPsl008	**Página: 1 de 1**	**Vigente a partir de: 2003**

PROCEDIMIENTO MSPSL008

1. El administrador dará al usuario su password hasta que cumpla con al menos dos características de evidencia definitiva que verifiquen su identidad.
2. El administrador podrá revelar un password por teléfono solamente cuando se haya provisto de una evidencia adecuada de identidad (el día de nacido, los nombres de sus dependientes o de sus padres, el RFC, número de nómina, etc.). Este método es conveniente, aunque es definitivamente menos seguro que requerir que el usuario se presente en persona.
3. Esta política necesita acompañarse de otras políticas relacionadas, y establecidas por la Dirección de Sistemas del Municipio de San Pedro.
4. El usuario podrá cambiar sus passwords cuando las circunstancias así lo requieran. Si esto no es posible por razones administrativas o técnicas, el administrador podrá reasignar los passwords de los user inmediatamente.
5. Los usuarios deben conocer un procedimiento emergente para cancelación y cambios de sus passwords.

a) Responsable de su implantación: Administradores de Sistemas

b) Periodo sugerido de revisión: Permanente

c) Responsables de su cumplimiento: Administrador del sistema / Usuarios

Evidencia de Control	Datos claves de los usuarios / Bitácora de asignación y control de cambios de passwords.

ACCESO A LA RED		Seguridad Lógica
Todos los usuarios de los sistemas y herramientas de productividad personal deben ser identificados satisfactoriamente antes de ingresar a la red.		
Política No.: MSPsl009	**Página: 1 de 1**	**Vigente a partir de: 2003**

PROCEDIMIENTO MSPSL009

1. Antes de usar cualquier sistema el usuario deberá ser identificado positivamente, una identificación ordinaria seria el user-id y passwords fijos, pero pudiera también incluir biometría, sistema de regreso de llamada, señales de password dinámicos o certificados digitales.
2. Cada usuario debe tener un único user-id y password secreto personal. Este user-id y password será requerido para acceder a las redes y computadoras multiusuario.
3. La exacta definición de identificación positiva está basada en la plataforma o tecnología, por ejemplo acceder a computadoras dentro de Internet, como firewalls, puede requerir passwords dinámicos además de passwords fijos. Mientras que usar una tarjeta de crédito telefónica requerirá solo passwords fijos.
6. Dependiendo de la confiabilidad de la información en algunos casos cuando el Personal de Sistemas lo defina se requerirá dos tipos de autentificación para acceder dichos sistemas, algo que el usuario conozca como el password, combinado con algo que el usuario tenga, tal como una señal de identidad.

a) Responsable de su implantación: Administradores de Sistemas

b) Periodo sugerido de revisión: Por evento (Cambio / Cancelación de password)

c) Responsables de su cumplimiento: Administrador del sistema

Evidencia de Control	Sistema de Control de Acceso

ACCESO A LOS SISTEMAS		Seguridad Lógica
Los usuarios que vayan a acceder a la Red y a los Sistemas instalados por la Dirección deben ser identificados satisfactoriamente al dar sus passwords		
Política No.: MSPsl010	**Página: 1 de 1**	**Vigente a partir de: 2003**

PROCEDIMIENTO MSPSL010

1. No se conectará un sistema remoto con un sistema de producción a menos que tenga un mecanismo de acceso aprobado.
2. Cada usuario debe tener un único user-id y password secreto personal. Este user-id y password será requerido para acceder a las redes y computadoras multiusuario.
3. Todas las computadoras las cuales tienen diálogos de tiempo real remoto, con sistemas de producción del Municipio deben correr un paquete de control de acceso aprobado por la Dirección de Sistemas.
4. Todos los sistemas multiusuario y redes tendrán un software de control de accesos el cual identificará y restringirá los privilegios de cada usuario. Estas facilidades de software además permiten monitorear el software que utiliza cada usuario.
5. Para limitar el uso de personas no autorizadas de los sistemas del Municipio (esto depende de Informática) queda prohibido utilizar el mismo password fijo en cada máquina del Municipio, aunque el mismo user-id si se puede usar.
6. El uso del mismo user-id en todas las computadoras y redes del Municipio es deseable porque esto hace el análisis o las actividades de log considerablemente más fácil.

a) Responsable de su implantación: Administradores de Sistemas

b) Periodo sugerido de revisión: Por evento (Cambio / Cancelación de password)

c) Responsables de su cumplimiento: Administrador del sistema

Evidencia de Control	Sistema de Control de Accesos

ACCESO A COMPUTADORAS AISLADAS		Seguridad Lógica
Se debe utilizar user-id y password para acceder a computadoras aisladas (stand alone)		
Política No.: MSPsl011	**Página: 1 de 1**	**Vigente a partir de: 2003**

PROCEDIMIENTO MSPSL011

1. Es necesario que para computadoras aisladas se configure a los usuarios la validación de password desde el arranque.
2. Los passwords de computadoras aisladas no aseguran la custodia de la información alojada en ellas, por lo que los usuarios son responsables de la custodia física del equipo y de los respaldos de la información ahí alojada.
3. Cada usuario es responsable de respaldar su información en algún medio magnético u óptico a menos que la información sobrepase las capacidades de estos medios se dará parte a sistemas para especifique un espacio de disco duro en alguno de los servidores de archivos para su respaldo frecuente en cinta magnética, dada su importancia y cantidad (esto no incluye archivos personales del usuario así como archivos de música y video en cualquier formato que no sea información del municipio)

a) Responsable de su implantación: Administradores de Sistemas

b) Periodo sugerido de revisión: Anual

c) Responsables de su cumplimiento: Usuarios

Evidencia de Control	Sistema de Control de Acceso

INTENTOS DE ACCESO	Seguridad Lógica

La Dirección de Sistemas establecerá un límite en intentos consecutivos fallidos de introducir un password

Política No.: MSPsl012	Página: 1 de 1	Vigente a partir de: 2003

PROCEDIMIENTO MSPSL012

1. Los administradores de sistemas definirán el número de veces que permitirá introducir un password equivocado antes de tomar acciones (suspenderlo, deshabilitarlo y / o desconectarlo) y si hay un limite de tiempo.
2. Para prevenir los ataques de adivinar los passwords, el número de intentos consecutivos para introducir un password incorrecto debe ser estrictamente limitado.
3. El número de intentos consecutivos será de tres y solo podrá ser desbloqueado por los Administradores de Sistemas

a) Responsable de su implantación: Administradores de Sistemas

b) Periodo sugerido de revisión: Trimestral

c) Responsables de su cumplimiento: Administradores de Sistemas

Evidencia de Control	Sistema de Control de Acceso

PROTECCIÓN EN ENVIÓ DE PASSWORDS		Seguridad Lógica
Cuando se asignen o transmitan passwords a los usuarios remotos se deberán proteger vía encriptación o cartas oficiales selladas.		
Política No.: MSPsl013	**Página: 1 de 1**	**Vigente a partir de: 2003**

PROCEDIMIENTO MSPSL013

1. El password inicial para un nuevo usuario remoto será enviado vía un canal de comunicación que asegure que no sea interceptado o conocido por terceros.
2. Para transmitir un password inicial a un usuario remoto, se pueden usar varios medios los cuales serán definidos por Administrador de Sistemas.
3. Un medio puede ser el servicio de mensajería tomando las precauciones debidas, ya que si este password es interceptado, no se conocerá el user-id y otra información necesaria para accesar los sistemas.
4. Otro mecanismo es enviar el password en un mensaje electrónico que vaya encriptado y que se facilite su lectura al empleado propietario de la contraseña.
5. La idea de esta política es distribuir la información con los métodos necesarios que hagan más difícil al intruso interceptar los passwords.

a) Responsable de su implantación: Administradores de Sistemas

b) Periodo sugerido de revisión: Permanente

c) Responsables de su cumplimiento: Administradores de Sistemas

Evidencia de Control	Sistema de Control de Acceso / Bitácora de entrega de passwords oficiales.

COMPOSICIÓN DEL PASSWORD		Seguridad Lógica
Los passwords deben contener caracteres alfabéticos y no alfabéticos, así como mayúsculas y minúsculas		
Política No.: MSPsl014	**Página: 1 de 1**	**Vigente a partir de: 2003**

PROCEDIMIENTO MSPSL014

a. Todos los passwords que los usuarios eligen deben contener al menos un carácter alfabético. Los caracteres no alfabéticos incluyen números (0-9) y puntuación.

b. El uso de los caracteres de control y otros caracteres no impresos se excluyen porque ellos pueden inadvertidamente causar problemas de transmisión de red o no intencionalmente invocar ciertas utilidades del sistema.

c. El Administrador de Sistemas debe recomendar sugerencias a los usuarios para construir sus passwords de manera que sean difíciles de adivinar. Por ejemplo:

   a. Usar caracteres mayúsculas y minúsculas en el mismo password
   b. Incluir caracteres alfabéticos y no alfabéticos si el sistema lo permite

a) Responsable de su implantación: Administradores de Sistemas

b) Periodo sugerido de revisión: Permanente

c) Responsables de su cumplimiento: Usuarios

Evidencia de Control	Sistema de Control de Acceso

CONFIDENCIALIDAD DEL PASSWORD		Seguridad Lógica
Los usuarios no deberán bajo ninguna circunstancia compartir su passwords y en excepciones esto será autorizado por directores de área		
Política No.: MSPsl015	**Página: 1 de 1**	**Vigente a partir de: 2003**

PROCEDIMIENTO MSPSL015

1. Bajo ninguna circunstancia los administradores de sistemas deberán conocer los passwords de los usuarios, a excepción de eventos donde se de la alta, cambio o baja de los mismos, previa autorización del usuario y del Director de Sistemas.
2. Los passwords nunca deben ser revelados y en los casos donde se comparta información y funciones comunes debe existir un acuerdo firmado por los directores de área (excepciones registradas y almacenadas en Informática)
3. La información utilizada y las funciones realizadas por el personal del municipio con los passwords otorgados son responsabilidad de los usuarios correspondientes y las acciones malintencionadas o que generen problemas operativos, administrativos o de imagen al Municipio serán enfrentadas conforme al reglamento interno y a las políticas de seguridad de informática.

a) Responsable de su implantación: Administradores de Sistemas

b) Periodo sugerido de revisión: Permanente

c) Responsables de su cumplimiento: Usuarios

Evidencia de Control	Sistema de Control de Acceso

PASSWORDS EXPIRADOS	**Seguridad Lógica**

Deben asignarse passwords iniciales *solamente para la primera sesión de acceso a los recursos de software*

Política No.: MSPsl016	**Página: 1 de 1**	**Vigente a partir de: 2003**

PROCEDIMIENTO MSPSL016

1. Los passwords iniciales editados por el responsable de seguridad debe ser válido solo para la primera sesión del usuario. A ese tiempo el usuario debe ser forzado para elegir otro password antes de que se ejecute cualquier otro trabajo.
2. Forzar a los administradores y usuarios finales a cambiar el password inicial antes de que ellos hagan cualquier otro trabajo.

a) Responsable de su implantación: Administradores de Sistemas

b) Periodo sugerido de revisión: Permanente

c) Responsables de su cumplimiento: Usuarios

Evidencia de Control	**Sistema de Control de Acceso**

CAMBIOS PERIÓDICOS DE PASSWORD		Seguridad Lógica
DEBEN SINCRONIZARSE INTERVALOS DE CAMBIOS DE PASSWORDS A TRAVÉS DE TODA LA PLATAFORMA		
Política No.: MSPsl017	**Página: 1 de 1**	**Vigente a partir de: 2003**

PROCEDIMIENTO MSPSL017

1. Los intervalos de cambios a los passwords fijos deben ser sincronizados a través de sistemas, computadoras y plataforma de red del Municipio.
2. Los usuarios pueden registrarse solo una vez, pero dentro de una sola sesión ellos pueden usar múltiples sistemas. El administrador de sistemas establecerá el plan para el uso de los servidores de seguridad a través de los cuales se pueden administrar múltiples plataformas.
3. Los usuarios podrán cambiar sus passwords cuando ellos lo deseen. Si el sistema operativo de la estación de trabajo lo permite y/o con apoyo del personal de sistemas

a) Responsable de su implantación: Administradores de Sistemas

b) Periodo sugerido de revisión: Permanente

c) Responsables de su cumplimiento: Usuarios

Evidencia de Control	Sistema de Control de Acceso

ACCESO A LA PLATAFORMA		Seguridad Lógica
LOS USUARIOS DEBEN REGISTRARSE UNA SOLA VEZ PARA INGRESAR A LOS DIFERENTES AMBIENTES QUE CORRESPONDEN A SU PERFIL		
Política No.: MSPsl018	**Página: 1 de 1**	**Vigente a partir de: 2003**

PROCEDIMIENTO MSPSL018

1. Los usuarios se identificarán ellos mismos sólo una vez y habrá un proceso, el cual comunicará transparentemente la identidad del usuario (user-id) a la(s) computadora(s) destino.
2. Habrá excepciones cuando un usuario tenga acceso a privilegios especiales o múltiples user-id. En estos casos múltiples passwords pueden ser necesarios para controlar los accesos con privilegios y registrar las actividades.
3. La información relacionada a la identidad del usuario será pasada transparentemente a otras computadoras, sistemas administradores de base de datos y aplicaciones.

a) Responsable de su implantación: Administradores de Sistemas

b) Periodo sugerido de revisión: Permanente

c) Responsables de su cumplimiento: Usuarios

Evidencia de Control	Sistema de Control de Acceso

ACCESO A ESTACIONES DE TRABAJO		Seguridad Lógica
TODAS LAS ESTACIONES DE TRABAJO DEBEN TENER PROTECCIÓN BASADA EN PASSWORD		
Política No.: MSPsl019	**Página: 1 de 1**	**Vigente a partir de: 2003**

PROCEDIMIENTO MSPSL019

1. El personal de Seguridad de Informática definirá quien usará los sistemas de control de acceso a las estaciones de trabajo, protegiendo cada máquina.
2. El personal de Seguridad de Informática aprobará que productos de protectores de pantalla se usarán, así como el número de minutos antes de que un protector de pantalla funcione.
3. En la mayoría de los casos esto involucra a protectores de pantalla con password fijos basado en protección junto con un tiempo fuera después de que no haya actividad.

a) Responsable de su implantación: Administradores de Sistemas

b) Periodo sugerido de revisión: Permanente

c) Responsables de su cumplimiento: Usuarios

Evidencia de Control	Sistema de Control de Acceso

SISTEMAS DE SERVICIO AL CLIENTE		Seguridad Lógica
LOS PASSWORDS FIJOS NO SE DESPLEGARÁN POR LOS SISTEMAS DE SERVICIO AL USUARIO DEL MUNICIPIO		
Política No.: MSPsl020	Página: 1 de 1	Vigente a partir de: 2003

PROCEDIMIENTO MSPSL020

1. Seleccionar cuidadosamente al personal que dará servicio a usuarios por teléfono ya que estos serán los responsables de teclear los passwords de estos, para las diferentes transacciones que realizarán.
2. Al teclear los passwords estos no se desplegarán por la pantalla sólo se confirmará si está correcto o no.

a) Responsable de su implantación: Administradores de Sistemas

b) Periodo sugerido de revisión: Permanente

c) Responsables de su cumplimiento: Usuarios

Evidencia de Control	Sistema de Control de Acceso

CONFIRMACIÓN DE CAMBIOS POR CORREO		Seguridad Lógica
DEBE EXISTIR UNA CONFIRMACIÓN DE CAMBIOS A PASSWORDS FIJOS POR CORREO REGULAR PARA DETECTAR ABUSOS		
Política No.: MSPsl021	**Página: 1 de 1**	**Vigente a partir de: 2003**

PROCEDIMIENTO MSPSL021

1. Siempre que se pida resetear o cambiar un password por teléfono se enviará una confirmación del cambio por correo regular incluso pudiera mandarse el nuevo password, si el personal de Seguridad de Informática lo autoriza. Esto es para reducir el riesgo de que una persona falsa use el teléfono, y de ciertos detalles de la persona y requiera el cambio o resetear el password.
2. Esta política es relevante para los pagos por teléfono y otros sistemas de respuesta automática. En cualquier caso si el usuario no inicia el cambio de password él o ella deberá contactar al responsable del sistema e informar que sospecha del engaño.
3. Los passwords deben ser enviados separados de los user-ids y en diferente tiempo. Esta correspondencia no debe tener marcas que indiquen la naturaleza de la carta. Los passwords deben estar ocultos dentro de un sobre opaco.

a) Responsable de su implantación: Administradores de Sistemas

b) Periodo sugerido de revisión: Permanente

c) Responsables de su cumplimiento: Usuarios

Evidencia de Control	Sistema de Control de Acceso

PASSWORDS OLVIDADOS		Seguridad Lógica
SE REQUIERE RE-REGISTRACIÓN PARA TODOS LOS USUARIOS QUE OLVIDARON LOS PASSWORDS FIJOS		
Política No.: MSPsl022	**Página: 1 de 1**	**Vigente a partir de: 2003**

PROCEDIMIENTO MSPSL022

1. Mejor que resetear o cambiar los passwords existentes, todos los usuarios que olvidaron o perdieron sus passwords deben registrarse otra vez y recibir el nuevo user-id y el nuevo password correspondiente.

a) Responsable de su implantación: Administradores de Sistemas

b) Periodo sugerido de revisión: Permanente

c) Responsables de su cumplimiento: Usuarios

Evidencia de Control	Sistema de Control de Acceso

HELP DESK	Seguridad Lógica
EL ADMINISTRADOR DE SISTEMAS DEBE REINICIAR UN PASSWORD QUE FUE DESACTIVADO POR INTENTOS DE ACCESO FALLIDOS	
Política No.: MSPsl023	**Página: 1 de 1**	**Vigente a partir de: 2003**

PROCEDIMIENTO MSPSL023

1. Cada usuario de los sistemas del Municipio que emplea passwords fijos para registrarse, debe tener un número de oportunidades definido por la Dirección de Sistemas para introducir el password correcto.
2. Si un usuario introduce su password erróneamente cierta cantidad de veces en un cierto tiempo, será desactivado automáticamente, hasta que el personal de help desk autentifique la identidad del usuario y resetee el password.
3. La cantidad de veces que podrá introducir el password así como el tiempo permitido lo definirá los Administradores de Sistemas.
4. El máximo de Intentos permitidos será de 3 veces después se bloqueará la cuenta del usuario y podar ser activada de nuevo solo por los Administradores de sistemas

a) Responsable de su implantación: Administradores de Sistemas

b) Periodo sugerido de revisión: Permanente

c) Responsables de su cumplimiento: Usuarios

Evidencia de Control	Sistema de Control de Acceso

PASSWORDS ENCRIPTADOS		Seguridad Lógica
LOS PASSWORDS DEBEN SER ENCRIPTADOS		
Política No.: MSPsl024	Página: 1 de 1	Vigente a partir de: 2003

PROCEDIMIENTO MSPSL024

1. Los passwords siempre serán encriptados cuando se mantienen almacenados por un periodo significante de tiempo o cuando son transmitidos a través de la red. Esto los prevendrá de ser descubiertos por personas que intervienen las redes, staff técnico que lee los registros de los sistemas y otras partes no autorizadas.
2. El método de encriptamiento a usar lo definirá el personal de Seguridad de Informática. La encriptación provee una de las pocas maneras de salvaguardar los passwords, llaves de encriptamiento, generador de semillero de números pseudo-random y otros parámetros de seguridad.
3. Sin encriptación estos parámetros pueden ser descubiertos inadvertidamente por personas quienes tienen acceso a buffers de sistemas de telecomunicaciones, la memoria que trabaja temporalmente dentro de la computadora, etc.
4. Basureros especiales de programas de cómputo pueden estar disponibles con registros de parámetros de seguridad no encriptados donde estos pueden ser recuperarlos subsecuentemente por personas no autorizadas.
5. Los diseñadores de sistemas siempre usarán encriptación para proteger los parámetros de seguridad tales como los passwords.

a) Responsable de su implantación: Administradores de Sistemas

b) Periodo sugerido de revisión: Permanente

c) Responsables de su cumplimiento: Usuarios

Evidencia de Control	Sistema de Control de Acceso

PASSWORDS EN EL SOFTWARE		Seguridad Lógica
LOS PASSWORD NUNCA DEBEN ESTAR INCORPORADOS EN EL SOFTWARE		
Política No.: MSPsl025	Página: 1 de 1	Vigente a partir de: 2003

PROCEDIMIENTO MSPSL025

1. Los passwords no se incorporarán al software desarrollado y / o modificado por el Municipio. Esto permite que los mecanismos de seguridad sean inflexibles lo cual no puede ser fácilmente modificado.
2. Parametrizar los sistemas, ya que esto permite a la administración hacer cambios a los passwords, llaves de encriptamiento, generador de números seudo-random, números de identificación personal (PINs), etc.
3. Los parámetros de seguridad son los caracteres string que controlan el proceso de seguridad, tales como los empleados cuando accesan un servidor de la red de área local.

a) Responsable de su implantación: Administradores de Sistemas

b) Periodo sugerido de revisión: Permanente

c) Responsables de su cumplimiento: Administradores de Sistemas

Evidencia de Control	Documentación de sistemas

RECUPERACIÓN DE PASSWORDS		Seguridad Lógica
SE DEBE PREVENIR LA RECUPERACIÓN DE PASSWORDS DE LOS SISTEMAS		
Política No.: MSPsl026	**Página: 1 de 1**	**Vigente a partir de: 2003**

PROCEDIMIENTO MSPSL026

1. Los sistemas de cómputo y de comunicación deben ser diseñados, probados y controlados para prevenir la recuperación, y el uso no autorizado de passwords almacenados, de cualquier forma que aparezcan estos ya sea en forma encriptada o no encriptada.
2. Cuando un password sea introducido por un usuario, este será encriptado usando una función única; este nuevo string encriptado será comparado con el string encriptado relevante en el archivo de passwords de la máquina destino.
3. Los string encriptados que aparecen en el archivo de passwords no deberán ser recuperados por los usuarios, esto permite que se monte un diccionario de ataque.
4. Un diccionario de ataque envuelve encriptación de entradas en un diccionario legible de cómputo y la comparación de estas cantidades a las entradas en el archivo de passwords, si coinciden, entonces se descubre un descriptamiento (limpiatexto) versión de un password. Este password limpiatexto puede entonces ser usado para comprometer la seguridad del sistema envuelto. Aún y aunque se usen funciones de encriptamiento únicas el diccionario de ataque puede ser montado.

a) Responsable de su implantación: Administradores de Sistemas

b) Periodo sugerido de revisión: Permanente

c) Responsables de su cumplimiento: Administradores de Sistemas

Evidencia de Control	Sistema de control de acceso

CONFIANZA EN EL SISTEMA OPERATIVO		Seguridad Lógica
SE DEBE TENER CONFIANZA EN EL PROCESO DE AUTENTIFICACIÓN DE USUARIO DEL SISTEMA OPERATIVO		
Política No.: MSPsl027	**Página: 1 de 1**	**Vigente a partir de: 2003**

PROCEDIMIENTO MSPSL027

1. Los desarrolladores de las aplicaciones de los sistemas deben confiar en los controles de accesos, passwords provistos por el sistema operativo o un paquete de control de accesos que realice el sistema operativo.
2. Los desarrolladores no deben construir mecanismos separados para colectar passwords o user-ids. Igualmente los desarrolladores no construirán o instalarán otros mecanismos para identificar o autentificar la identidad de usuario sin previo permiso del responsable de Seguridad de Informática.
3. Los sistemas del Municipio no tendrán internamente controles de accesos (passwords) ya que estos estarán en el sistema operativo. Esta política no solo hace el diseño de las aplicaciones de los sistemas más fáciles y menos caros, además logra que haya mas consistencia en el manejo de los datos de las aplicaciones.
4. Los desarrolladores no construirán o desplegaran user-ids secretos o passwords con privilegios especiales los cuales no están claramente cubiertos en la documentación del sistema.
5. Esta acción involucra la definición de user-ids especiales y passwords que nadie conoce acerca de ellos (excepto el personal técnico de alta jerarquía). A pesar que es relativamente fácil de codificar es difícil para otros descubrirlos (a menos que se revise línea por línea). Estos mecanismos pueden dar a los programadores acceso a funciones muy importantes, aunque estos programadores ya no trabajen en el Municipio.

a) Responsable de la implantación: Administradores Sistemas /Desarrolladores

b) Periodo sugerido de revisión: Permanente

c) Responsables de su cumplimiento: Administradores de Sistemas

Evidencia de Control	Controles de acceso del sistema operativo. Documentación de sistemas.

PASSWORDS INDIVIDUALES		**Seguridad Lógica**
EL CONTROL DE ACCESO A LOS SISTEMAS DEBE REALIZARSE MEDIANTE PASSWORDS INDIVIDUALES		
Política No.: MSPsl028	**Página: 1 de 1**	**Vigente a partir de: 2003**

PROCEDIMIENTO MSPSL028

1. Los controles de acceso a los sistemas de cómputo y comunicaciones se realizarán vía passwords que sean únicos por usuario.
2. Los controles de acceso a los archivos, base de datos, computadoras, y otros recursos de sistemas vía passwords compartidos (también llamados lockwords) están prohibidos.
3. Usar un sólo password por usuario y un user-id individualizado a través de toda la plataforma con los privilegios específicos de control de acceso, lo cual prevendrá de "diseminaciones secundarias".
4. Prohibir compartir los user-ids con los llamados "grupos de cuentas".

a) Responsable de su implantación: Administradores de Sistemas

b) Periodo sugerido de revisión: Permanente

c) Responsables de su cumplimiento: Administradores de Sistemas

Evidencia de Control	**Software de control de passwords**

PASSWORD POR DISPOSITIVO		Seguridad Lógica
DEBE HABER PASSWORDS ÚNICOS PARA CADA DISPOSITIVO DE LA RED INTERNA		
Política No.: MSPsl029	Página: 1 de 1	Vigente a partir de: 2003

PROCEDIMIENTO MSPSL029

1. Todos los dispositivos de la red interna del Municipio (routers, firewall, servidores de control de acceso, etc.) tendrán passwords únicos u otros mecanismos de control de acceso. Un compromiso en la seguridad de un dispositivo por lo tanto no conducirá automáticamente a un compromiso en otros dispositivos.
2. Usar un password único para cada dispositivo, restringe el daño a un dispositivo solamente, y a lo que el dispositivo puede hacer (quizá capturar otros passwords fijos que fluyen a través de éste) si se usa el mismo password en varios lugares esto dificulta más encontrar un hacker / cracker.
3. De otra manera el uso de un solo password para múltiples dispositivos de red restringe la habilidad de la administración para establecer una separación de tareas y para restringir el acceso basado en tareas de trabajo.

a) Responsable de su implantación: Administradores de Sistemas

b) Periodo sugerido de revisión: Permanente

c) Responsables de su cumplimiento: Administradores de Sistemas

Evidencia de Control	Software de control de passwords

PASSWORD CON ALARMA DE SEGURIDAD		Seguridad Lógica
PARA DATOS SENSIBLES DEBEN USARSE PASSWORDS QUE ACTIVEN LA ALARMA DE SEGURIDAD		
Política No.: MSPsl030	Página: 1 de 1	Vigente a partir de: 2003

PROCEDIMIENTO MSPSL030

1. Siempre que el acceso a un sistema con datos particularmente valiosos o sensitivos sea dado por un usuario, se deben emplear password de activación de alarma para cubrir las señales del sistema que este usuario ha sido presionado a introducir.
2. Los passwords de activación de alarma son passwords especiales usados solamente en esas circunstancias donde una señal debe ser accionada porque la seguridad del usuario pudiera ser amenazada.
3. Usar los passwords especiales solo cuando la seguridad del usuario esta amenazada ya que al introducir este password se activará una alarma para avisar al operador del sistema y a otra persona de seguridad que algo serio esta pasando.
4. Estos passwords limitan los privilegios de los usuarios, limitan la disponibilidad del balance, en ciertas cuentas de bancos automáticamente inician alguna acción relacionada con la seguridad.
5. Informática debe clasificar los datos sensibles del Municipio e identificar a los usuarios que tendrán estos passwords especiales.

a) Responsable de su implantación: Administradores de Sistemas/Jefatura de Desarrollo

b) Periodo sugerido de revisión: Permanente

c) Responsables de su cumplimiento: Jefatura de Desarrollo

Evidencia de Control	Software que valida passwords

PASSWORD DEFAULT		Seguridad Lógica
SE DEBEN CAMBIAR LOS PASSWORDS QUE EL PROVEEDOR DA POR DEFAULT		
Política No.: MSPsl031	Página: 1 de 1	Vigente a partir de: 2003

PROCEDIMIENTO MSPSL031

1. Todos los passwords por default proporcionados por el proveedor de software deben ser cambiados antes de que cualquier sistema de cómputo o comunicaciones sea usado en un ambiente de producción en el Municipio.
2. Cambiar todos los passwords que vienen por default del proveedor antes de que el sistema entre en producción, ya que una de las maneras más comunes de introducirse a los sistemas es empleando los passwords que usa el vendedor por default casi por todos conocidos.

a) Responsable de su implantación: Administradores de Sistemas

b) Periodo sugerido de revisión: Permanente

c) Responsables de su cumplimiento: Administradores de Sistemas

Evidencia de Control	Software que valida passwords. Documentación de sistemas.

PASSWORD PARA CADA SISTEMA		Seguridad Lógica
SE DEBE USAR UN PASSWORD DIFERENTE PARA CADA SISTEMA		
Política No.: MSPsl032	Página: 1 de 1	Vigente a partir de: 2003

PROCEDIMIENTO MSPSL032

1. Para prevenir que se comprometa la seguridad de múltiples sistemas, los usuarios deben emplear diferentes passwords en cada sistema al cual tengan acceso.
2. Para los ambientes donde se requiere alta seguridad se pide un password para cada sistema. Esta política previene que un intruso descubra un password que le permita acceder a una variedad de sistemas en lugar de un solo sistema.
3. Se requiere de un permiso para usar el mismo password en diferentes sistemas. Los usuarios evitarán usar el mismo password en múltiples sistemas de cómputo a menos que ellos sean informados por los Administradores de sistemas que si hacen eso no comprometen la seguridad indebidamente.
4. Se debe comprometer a los usuarios a no difundir los passwords mediante la firma de cartas de confidencialidad.

a) Responsable de su implantación: Administradores de Sistemas

b) Periodo sugerido de revisión: Permanente

c) Responsables de su cumplimiento: Administradores de Sistemas

Evidencia de Control	Software de seguridad. Cartas de confidencialidad.

CONSERVACIÓN DE PASSWORDS		Seguridad Lógica
NO DEBEN DEJARSE PASSWORDS ESCRITOS DONDE OTROS LOS PUEDAN DESCUBRIR		
Política No.: MSPsl033	Página: 1 de 1	Vigente a partir de: 2003

PROCEDIMIENTO MSPSL033

1. La administración alertará a los usuarios de no dejar sus passwords escritos en algún lugar donde puedan ser descubiertos por algún intruso.
2. Los usuarios no escribirán o grabarán passwords de forma legible y no los almacenarán cerca del dispositivo de acceso al cual pertenece.
3. Si se escriben los passwords se usarán técnicas secretas. Es decir los usuarios no deben escribir sus passwords a menos que:
    a. Los usuarios encubran los passwords en un número de teléfono o en otros caracteres que aparentemente no se relacionen.
    b. Se utilice un código de sistema para ocultar el password.

a) Responsable de su implantación: Administradores de Sistemas

b) Periodo sugerido de revisión: Permanente

c) Responsables de su cumplimiento: Usuarios

Evidencia de Control	Difusión de la política

ALMACENAMIENTO DE PASSWORDS		Seguridad Lógica
NO DEBEN ALMACENARSE PASSWORDS FIJOS EN PROGRAMAS DE MARCADO O BROWSERS DE INTERNET		
Política No.: MSPsl034	**Página: 1 de 1**	**Vigente a partir de: 2003**

PROCEDIMIENTO MSPSL034

1. Los usuarios no deben almacenar passwords fijos en programas de marcado de comunicaciones o browsers de Internet en ningún tiempo.
2. Prevenir a los usuarios de almacenar los passwords fijos para referencias futuras en programas de comunicaciones. Estos passwords son típicamente almacenados en forma encriptada y son enmascarados cuando se teclean en la pantalla, para que otras personas no autorizadas no puedan verlo, aún siguen siendo usados por personas no autorizados quienes tienen acceso a la computadora en la que reside este software de comunicaciones.
3. La única alternativa es prohibir a los usuarios de emplear esta característica que ellos pudieran de otra manera considerar conveniente y deseable.

a) Responsable de su implantación: Administradores de Sistemas

b) Periodo sugerido de revisión: Permanente

c) Responsables de su cumplimiento: Administradores de Sistemas

Evidencia de Control	Software de seguridad

UTILIZACIÓN DE "COOKIES"		Seguridad Lógica
LOS USUARIOS QUE CONTROLAN LAS MÁQUINAS NO DEBEN EMPLEAR "COOKIES" PARA DAR LOG-IN AUTOMÁTICO		
Política No.: MSPsl035	**Página: 1 de 1**	**Vigente a partir de: 2003**

PROCEDIMIENTO MSPSL035

1. Los usuarios de cómputo deben rehusar todas las ofertas del software de colocar "cookies" en su computadora para que ellos puedan automáticamente entrar la siguiente vez que ellos visiten un site particular de Internet.
2. No se permitirá a los usuarios utilizar "cookies", ya que esto podría mas tarde ser usado por personas no autorizadas para introducirse a los sistemas, otros productos, u obtener información restringida.
3. Los "cookies" son archivos pequeños que contienen información especifica de usuarios, se colocan en el disco duro, y pueden ser usados para identificar únicamente que usuario es el que se firma.
4. El uso de log-in con "cookies" simplifica y reemplaza el tradicional proceso de acceso, pero reduce la seguridad al reemplazar la información que el usuario conoce con solo aproximarse físicamente a una máquina remota.
5. Esta aplica en la administración de perfiles a cargo de la dirección de sistemas donde se seleccionara a que usuarios se les habilitará la opción de bajar o aumentar la seguridad del navegador de red, mediante el sistema operativo de red

a) Responsable de su implantación: Administradores de Sistemas

b) Periodo sugerido de revisión: Permanente

c) Responsables de su cumplimiento: Administradores de Sistemas

Evidencia de Control	Software que valida passwords

ALMACENAMIENTO DE PRUEBAS DE PASSWORD		Seguridad Lógica
LAS RESPUESTAS PARA RECUPERACIÓN DE PASSWORDS Y PRUEBAS DE PASSWORD NO DEBEN ALMACENARSE CERCA DE LAS COMPUTADORAS DEL USUARIO		
Política No.: MSPsl036	**Página: 1 de 1**	**Vigente a partir de: 2003**

PROCEDIMIENTO MSPSL036

1. Las respuestas para recuperar passwords no deben almacenarse en el mismo portafolio o maleta que las computadoras portátiles usadas para accesos remotos de redes.
2. No se deberán guardar las pruebas de passwords dinámicos en el mismo contenedor de la computadora a la que pertenece. En algunos casos estas pruebas no tienen passwords fijos, y esto significa que con poseer las pruebas y la computadora es suficiente para ganar acceso al sistema por personas no autorizadas.
3. Esta política adelanta la causa de autentificación del usuario “multi-factor” básicamente dice: que diferentes cosas son requeridas antes de obtener acceso al sistema (algo que el usuario conozca, algo que el usuario tenga, algo que el usuario pueda hacer, algo que el usuario sea (biometría), etc.)

a) Responsable de su implantación: Administradores de Sistemas

b) Periodo sugerido de revisión: Permanente

c) Responsables de su cumplimiento: Administradores de Sistemas

Evidencia de Control	Software que valida passwords

CONSTRUCCIÓN DE PINS	Seguridad Lógica
LOS NÚMEROS DE IDENTIFICACIÓN PERSONAL (PINS), DEBEN SER CONSTRUIDOS USANDO LAS REGLAS DE PASSWORDS	
Política No.: MSPsl037	**Página: 1 de 1**	**Vigente a partir de: 2003**

PROCEDIMIENTO MSPSL037

1. Todos los números de identificación personal (PINs) deben ser construidos con las mismas reglas que aplican para passwords fijos.
2. Solo por que los accesos a los sistemas son asistidos por una tarjeta magnética, una prueba de password dinámico, o alguna otra tecnología de autentificación del usuario, no elimina la necesidad de emplear PINs que sean difíciles de adivinar.
3. Tanto los usuarios finales como los administradores de sistemas no deben bajar la guardia cuando seleccionan o construyen números de identificación personal, también conocidos como PINs.
4. Porque los PINs son frecuentemente una parte de un esquema de autentificación del usuario (donde ambos un PIN y algo más se requiere para acceder a un sistema) la necesidad de que los PINs sean difíciles de adivinar es porque frecuentemente los PINs se componen solo de 4 caracteres lo que significa que no hay muchas combinaciones.
5. Es particularmente importante tener un mecanismo de cerradura que se active después de un cierto número de intentos fallido de acceso.

a) Responsable de su implantación: Administradores de Sistemas

b) Periodo sugerido de revisión: Permanente

c) Responsables de su cumplimiento: Administradores de Sistemas

Evidencia de Control	Software que valida passwords

NO COMPARTIR PASSWORDS		**Seguridad Lógica**
ESTÁ PROHIBIDO COMPARTIR PASSWORDS		
Política No.: MSPsl038	**Página: 1 de 1**	**Vigente a partir de: 2003**

PROCEDIMIENTO MSPSL038

1. A pesar de las circunstancias, los passwords nunca deben ser compartidos o revelados a alguien más además del usuario autorizado.
2. El usuario autorizado se responsabilizará por las acciones que otras partes ejecuten con su password.
3. Si los usuarios necesitan compartir datos residentes en la computadora, ellos deben usar correo electrónico, directorios públicos, o servidores de redes de área local, y otros mecanismos.
4. Cuando un usuario descubra sus passwords se hará responsable de las acciones de otros. Es importante que el usuario guarde el password exclusivamente para él mismo; ya que al exponerlo compromete los controles de acceso a los sistemas.

a) Responsable de su implantación: Administradores de Sistemas

b) Periodo sugerido de revisión: Permanente

c) Responsables de su cumplimiento: Administradores de Sistemas

Evidencia de Control	**Software que valida passwords. Difusión de la política**

RESPONSABILIDAD DE ACCIONES		**Seguridad Lógica**
LOS USUARIOS DEBEN SER RESPONSABLES DE TODAS LAS ACTIVIDADES QUE INVOLUCRAN LOS USER-IDS PERSONALES		
Política No.: MSPsl039	**Página: 1 de 1**	**Vigente a partir de: 2003**

PROCEDIMIENTO MSPSL039

1. Los usuarios son responsables de todas las actividades ejecutadas con sus user-ids personales.
2. Los user-ids no serán utilizados por cualquiera, solamente por las personas a quienes ellos han sido emitidos.
3. Los usuarios no permitirán a otros ejecutar cualquier actividad con sus user-ids. Similarmente los usuarios no podrán ejecutar cualquier actividad con IDs pertenecientes a otros usuarios (exceptuando user-ids anónimos como “guest”)
4. No se compartirán los user-ids y passwords asociados. Si los usuarios comparten sus user-ids y passwords, el log no va a reflejar la verdadera identidad de los usuarios, y acorde con esto no será útil para tomar acciones disciplinarias, demandas e investigaciones.

a) Responsable de su implantación: Administradores de Sistemas

b) Periodo sugerido de revisión: Permanente

c) Responsables de su cumplimiento: Administradores de Sistemas

Evidencia de Control	**Software que valida passwords. Difusión de la política**

SEGURIDAD DEL SISTEMA COMPROMETIDA		Seguridad Lógica
DEBE HABER CAMBIOS FORZOSOS DE TODOS LOS PASSWORDS DESPUÉS DE COMPROMETER EL SISTEMA		
Política No.: MSPsl040	**Página: 1 de 1**	**Vigente a partir de: 2003**

PROCEDIMIENTO MSPSL040

1. Siempre que un sistema haya sido comprometido por una persona no autorizada, los administradores del sistema deben inmediatamente cambiar cada password en el sistema involucrado. Aún si solo se sospecha, se requiere que todos los passwords se cambien inmediatamente.
2. Bajo cualquier circunstancia, una versión verdadera del sistema operativo y toda la seguridad relacionada con el software debe también ser recargada. Similarmente bajo cualquiera de estas circunstancias, todos los cambios recientes para el usuario y privilegios del sistema serán revisados para validar modificaciones no autorizadas.
3. Restablecer un sistema operativo y sus controles de acceso “limpio” y “seguro” basados en passwords asociados después de una interrupción forzosa o algún comprometimiento de las medidas de seguridad, es decir cambiar los passwords inmediatamente después de que el sistema se comprometió o se sospecha de un comprometimiento.
4. Se requiere una respuesta inmediata porque entre mas se tarde esta medida, las personas no autorizadas tienen mas oportunidad de establecer user-ids no autorizados, privilegios no autorizados para los user-ids existentes, sobre los cuales ellos tienen control y puertas falsas que les puedan permitir futuros accesos al sistema.

a) Responsable de su implantación: Administradores de Sistemas

b) Periodo sugerido de revisión: Permanente

c) Responsables de su cumplimiento: Administradores de Sistemas

Evidencia de Control	**Software que valida passwords.**

INSTALAR UN DETECTOR DE INTRUSOS		Seguridad Lógica
LOS SERVIDORES Y COMPUTADORES CONECTADAS A INTERNET Y SISTEMAS EXTERNOS DEBEN TENER UN SOFTWARE PROBADO (NET SENSER) PARA DETECTAR INTRUSOS		
Política No.: MSPsl041	Página: 1 de 1	Vigente a partir de: 2003

PROCEDIMIENTO MSPSL041

1. Para permitir al Municipio de San Pedro responder rápidamente a los ataques, todas las computadoras conectadas y servidores conectados a Internet deben protegerse con un software que detecte intrusos y permita registrar datos relevantes de los mismos.

2. El software que adquiera la Dirección de Sistemas debe ser evaluado y seleccionado cuando se determine que cumpla con los requerimientos mínimos de seguridad y control de los mejores detectores de intrusos conocidos e instalados en el mercado y que son generalmente aceptados para cubrir tan importante tarea.

3. Todos los sistemas o soluciones de software que son alcanzables vía Internet deben ser protegidos con herramientas automáticas que detecten inmediatamente cualquier ataque.

4. La Dirección de Sistemas y su personal de operación evaluarán y determinarán cuales de estas herramientas son las mas apropiadas para el Municipio de San Pedro.

a) Responsable de su implantación: Administradores de Sistemas

b) Periodo sugerido de revisión: Semestralmente

c) Responsables de su cumplimiento: Dirección de Sistemas

Evidencia de Control	Software detector de intrusos

ACCESO A INTERNET PROTEGIDO CON FIREWALL (APAGA FUEGOS)		Seguridad Lógica
NO SE DEBE PERMITIR EL ACCESO A INTERNET SIN UN APAGAFUEGOS (FIREWALL)		
Política No.: MSPsl042	Página: 1 de 1	Vigente a partir de: 2003

PROCEDIMIENTO MSPSL042

1. Todos los accesos a Internet deben ser protegidos mediante un firewall que será instalado por el personal de operación de la Dirección de Sistemas.

2. Hasta que la Dirección de Sistemas del Municipio de San Pedro establezca un firewall aprobado, será cuando se permitan las conexiones a Internet.

3. Cuando una computadora utilizada por personal del Municipio en su casa o en ubicaciones fuera de las instalaciones de la alcaldía, esta no debe conectarse simultáneamente a Internet a menos que se emplee un firewall como protección.

4. Antes que los usuarios se conecten a Internet instalar un apagafuegos apropiado. La manera mas rápida y fácil de hacer esto es evaluar a la brevedad soluciones generalmente aceptadas en el mercado, seleccionando a los proveedores de software que vendan y den soporte del software apropiado para este propósito.

5. Los servidores web de Internet estarán protegidos mediante los ruteadores y firewalls para controlar los accesos y eliminar riesgos en el envío y recepción de archivos.

6. Los firewalls al igual que los detectores de intrusos estarán instalados en el municipio para garantizar a los usuarios de las diferentes soluciones de Internet, Correo Electrónico y Comercio Electrónico que los riesgos de accesos no autorizados y malintencionados serán enfrentados, minimizados y eliminados eficientemente.

   a) Responsable de su implantación: Administradores de Sistemas

   b) Periodo sugerido de revisión: Semestralmente

   c) Responsables de su cumplimiento: Dirección de Sistemas

Evidencia de Control	Firewalls

SERVIDORES DE INTERNET PÚBLICO		Seguridad Lógica
LOS SERVIDORES DE INTERNET PÚBLICO DEBEN ESTAR COLOCADOS EN REDES SEPARADAS A LAS DE SERVICIO INTERNO EN EL MUNICIPIO		
Política No.: MSPsl043	**Página: 1 de 1**	**Vigente a partir de: 2003**

PROCEDIMIENTO MSPSL044

1. Los ruteadores (routers) y - o apagafuegos deben ser empleados para restringir el tráfico de servidores de Internet público a las redes internas que operan en el Municipio de San Pedro.

2. Todos los apagafuegos de la organización conectados a Internet deben ser configurados ya que cada servicio de Internet (Telnet, ftp, http,etc.) por default está deshabilitado. Solamente aquellos servicios que hayan sido específicamente aprobados por escrito por el responsable de operación de sistemas o el Director de Sistemas puede ser habilitado.

3. Los apagafuegos deben correr en computadoras dedicadas.

4. Para hacer cambios a la configuración de los apagafuegos se requiere aprobación del Director de Sistemas o del responsable de la administración de sistemas.

5. Las instalaciones de sistemas y administradores no colocaran los servidores de Internet públicos (tales como las páginas web hosting) en la misma red donde se encuentran soluciones como las intranets.

a) Responsable de su implantación: Administradores de Sistemas

b) Periodo sugerido de revisión: Semestralmente

c) Responsables de su cumplimiento: Administradores de Sistemas

Evidencia de Control	**Firewalls y ruteadores.**

CERTIFICADOS DIGITALES Y ENCRIPTAMIENTO		Seguridad Lógica
LOS SERVIDORES DE COMERCIO ELECTRÓNICO DEBEN USAR CERTIFICADOS DIGITALES Y ENCRIPTAMIENTO		
Política No.: MSPsl044	**Página: 1 de 1**	**Vigente a partir de: 2003**

PROCEDIMIENTO MSPSL044

1. Para prevenir a los intrusos de interferir con actividades de comercio electrónico, todos los servidores web, servidores de bases de datos, servidores de transacciones electrónicas, servidores de seguridad, etc.) emplearán certificados digitales únicos y el encriptamiento para transferir información adentro y afuera de estos servidores

2. Se hace una excepción a los servidores web, servidores FTP, y cualquier otro servidor de la organización que soporte comunicaciones con clientes, prospectos, o ciudadanos que requieran intercambio de información con el Municipio.

   a) Responsable de su implantación: Administradores de Sistemas

   b) Periodo sugerido de revisión: Semestralmente

   c) Responsables de su cumplimiento: Administradores de Sistemas

Evidencia de Control	Certificados digitales y encriptamiento

FIREWALLS PARA ACCESOS INTERNOS		**Seguridad Lógica**
TODOS LOS INTENTOS DE ACCESOS INTERNOS A SERVIDORES DE RED O EQUIPOS AISLADOS DEL MUNICIPIO, DEBEN SIEMPRE PASAR POR EL APAGAFUEGOS		
Política No.: MSPsl045	**Página: 1 de 1**	**Vigente a partir de: 2003**

PROCEDIMIENTO MSPSL045

1. Todas las líneas de marcado de entrada conectada a las redes internas de la organización y/o los sistemas de cómputo deben pasar directo a un punto de control de acceso adicional (tal como un apagafuegos), antes de que los usuarios alcancen un conducto de entrada.

2. Como una alternativa para requerir dos niveles de passwords algunas organizacións permiten sistemas de autentificación de usuarios (tarjetas inteligentes con passwords dinámicos, por ejemplo). La ventaja de usar estas tecnologías es que los usuarios no tienen que dar login dos veces ni memorizar passwords complejos.

a) Responsable de su implantación: Administradores de Sistemas

b) Periodo sugerido de revisión: Semestralmente

c) Responsables de su cumplimiento: Administradores de Sistemas

Evidencia de Control	**Firewalls en servidores y equipo aislados**

FIREWALLS PARA ACCESOS EXTERNOS		**Seguridad Lógica**
LAS CONECCIONES DE RED EXTERNA EN TIEMPO REAL REQUIEREN DE APAGAFUEGOS Y DE UN MONITOREO PARA DETECCIÓN DE INTRUSOS PERMANENTE.		
Política No.: MSPsl046	**Página: 1 de 1**	**Vigente a partir de: 2003**

PROCEDIMIENTO MSPSL046

1. Todas las entradas de conexiones externas de tiempo real a las redes internas de la organización y/o sistemas de computo multiusuario debe pasar a través de un punto de control de acceso adicional

2. Instalar en los periféricos de las redes internas mecanismos de control de acceso fuertes.

3. Todas las conexiones de tiempo real externas tendrán un apagafuegos o un sistema de seguridad comparable.

4. Cada intento de acceso debe ser identificado por un detector de intrusos y será controlado y monitoreado cuando el origen intente romper las reglas de acceso configuradas en los servidores del Municipio de San Pedro.

a) Responsable de su implantación: Administradores de Sistemas

b) Periodo sugerido de revisión: Semestralmente

c) Responsables de su cumplimiento: Administradores de Sistemas

Evidencia de Control	**Firewalls y detectores de intrusos**

III. SEGURIDAD FÍSICA

ÁREAS CON INFORMACIÓN CONFIDENCIAL		Seguridad Física
Control de acceso físico para áreas que contienen información confidencial		
Política No.: MSPsf001	**Página: 1 de 1**	**Vigente a partir de: 2003**

PROCEDIMIENTO MSPSF001

1. El acceso a cada oficina, site y área de trabajo en la que se encuentre información confidencial, estará físicamente restringida.
2. El personal responsable de estas áreas de trabajo debe consultar al personal de sistemas para determinar el método de control de acceso más apropiado (recepcionistas, llaves de metal, tarjetas magnéticas para puertas, etc.)
3. El personal de sistemas asesorará a la administración para determinar que tipo de tecnología usar para el control de accesos
4. Se restringirá el acceso a todas las áreas en las que se encuentre información confidencial.
5. Todos los accesos de personal no autorizado, deben ser justificados y registrados en una bitácora de visitas. (ANEXO HOJA 74)

a) Responsable de su implantación: Administradores de sistemas

b) Periodo sugerido de revisión: Semestral

c) Responsables de su cumplimiento: Administradores de sistemas
Personal responsable de áreas de trabajo con información confidencial

Evidencia de Control	Tecnología de control de accesos

Municipio de San Pedro	**CONTROL DE ACCESO**

APLICA A ÁREAS QUE CONTIENEN INFORMACIÓN CONFIDENCIAL

				Fecha:	
Hora Entrada	**Hora Salida**	**Nombre**	**Empresa**	**Motivo**	**Firma**

PUERTAS CERRADAS EN EL CENTRO DE CÓMPUTO		Seguridad Física
El centro de cómputo debe ser un cuarto de puertas cerradas		
Política No.: MSPsf002	**Página: 1 de 1**	**Vigente a partir de: 2003**

PROCEDIMIENTO MSPSF002

1. Los centros de cómputo del Municipio son cuartos cerrados a los que no se permitirá el acceso a personas sin autorización incluyendo programadores, usuarios, y personas sin negocio.
2. Solo se permitirá el acceso a los operadores y personal debidamente autorizado.
3. Todos los accesos de personal no autorizado, deben ser justificados y registrados en una bitácora de visitas.

a) Responsable de su implantación: Administradores de sistemas

b) Periodo sugerido de revisión: Semestral

c) Responsables de su cumplimiento: Administradores de sistemas
Responsable del centro de cómputo

Evidencia de Control | **Mecanismos de seguridad**

PERSONAS TRABAJANDO SOLAS		Seguridad Física
Está prohibido que una persona que no sea la Dirección de Sistemas o personal de operación, trabaje sola en un área restringida		
Política No.: MSPsf003	**Página: 1 de 1**	**Vigente a partir de: 2003**

PROCEDIMIENTO MSPSF003

1. No permitir a los proveedores o empleados estén solos en un área restringida con información confidencial
2. En un área restringida que se encuentre información confidencial siempre deberá haber más de una sola persona en el lugar.
3. Todos los accesos de personal no autorizado, deben ser justificados y registrados en una bitácora de visitas (ver política de bitácora de acceso).

a) Responsable de su implantación: Administradores de sistemas

b) Periodo sugerido de revisión: Semestral

c) Responsables de su cumplimiento: Administradores de sistemas
Guardia

Evidencia de Control	Tecnología de control de accesos

PUERTAS DEL CENTRO DE CÓMPUTO		Seguridad Física
Cuando las puertas del centro de cómputo están abiertas se requiere la presencia de personal de operación que lo vigile		
Política No.: MSPsf004	**Página: 1 de 1**	**Vigente a partir de: 2003**

PROCEDIMIENTO MSPSF004

1. Cuando la puerta del centro de cómputo esta abierta (tal vez por algún movimiento del equipo de cómputo, muebles, materiales o algo similar) la entrada debe estar continuamente monitoriada por personal de operación de Sistemas.
2. Siempre que se requiera tener la puerta abierta del centro de cómputo un guardia vigilará la entrada para evitar el acceso a extraños y si están sacando equipo, muebles, o material asegurarse de que sea realmente lo que se autorizó para evitar un robo o una equivocación.
3. Todos los accesos de personal no autorizado, deben ser justificados y registrados en una bitácora de visitas.

a) Responsable de su implantación: Administradores de sistemas

b) Periodo sugerido de revisión: Semestral

c) Responsables de su cumplimiento: Administradores de sistemas
Guardias

Evidencia de Control	Tecnología de control de accesos

VISITANTES EN EL CENTRO DE DATOS		Seguridad Física
No se permiten visitantes en el centro de datos o al departamento de sistemas de información		
Política No.: MSPsf005	**Página: 1 de 1**	**Vigente a partir de: 2003**

PROCEDIMIENTO MSPSF005

1. Está prohibido que entren al centro de cómputo visitantes quienes no necesitan dar servicios relacionados con los equipos de cómputo y comunicaciones del Municipio
2. Clientes, directivos y demás visitantes pueden ver las actividades de los trabajadores a través de ventanas o puertas, si así se requiere.
3. Todos los accesos de personal no autorizado, deben ser justificados y registrados en una bitácora de visitas.
4. Para el personal de mantenimiento que tiene acceso físico se le asignara una escolta permanente durante toda su estancia en el área

a) Responsable de su implantación: Administradores de sistemas

b) Periodo sugerido de revisión: Semestral

c) Responsables de su cumplimiento: Administradores de sistemas
Personal de seguridad

Evidencia de Control	Tecnología de control de accesos

TOURS PÚBLICOS		Seguridad Física
Los tours públicos al Centro de Computo		
Política No.: MSPsf006	**Página: 1 de 1**	**Vigente a partir de: 2003**

PROCEDIMIENTO MSPSF006

1. Estas visitas debe ser supervisadas por los administradores de sistemas y deberán ser autorizadas por el Jefe de Redes del Municipio, tours educativos y los turísticos para evitar riesgos de sabotaje, daños, robos, etc., en los centros de cómputo.
2. Los tours para empleados, consultores, contratistas o para quienes tienen negocios con la alcaldía y necesitan saber más acerca de ella, así como de directores, o clientes importantes se llevarán a cabo con las debidas precauciones.
3. Estos accesos de personas deben ser justificados y registrados en una bitácora de visitas.

a) Responsable de su implantación: Administradores de sistemas

b) Periodo sugerido de revisión: Semestral

c) Responsables de su cumplimiento: Administradores de sistemas
Guardias
Encargado del centro de cómputo

Evidencia de Control	Controles de seguridad / Mecanismos de seguridad

ACCESOS CONTROLADOS		Seguridad Física
Cada individuo debe presentar su identificación para entrar a cualquier puerta que tenga acceso controlado		
Política No.: MSPsf007	**Página: 1 de 1**	**Vigente a partir de: 2003**

PROCEDIMIENTO MSPSF007

1. Cada persona presentará su identificación antes de entrar a cualquier puerta de acceso controlado.
2. Antes de entrar esperará hasta que se le indique que tiene permiso de entrar.
3. No se permite que una persona se identifique con una credencial que no sea la de él.
4. Es muy común que con una sola identificación pase otra persona o grupo de personas que vayan a entrar también. Por seguridad y para llevar una bitácora de accesos con fecha y hora de las personas que entran a centros de cómputo, es muy importante que cada cual muestre su identificación y justifique su ingreso.

a) Responsable de su implantación: Administradores de sistemas

b) Periodo sugerido de revisión: Semestral

c) Responsables de su cumplimiento: Administradores de sistemas
Personal responsable de áreas con información confidencial

Evidencia de Control	Tecnología de control de accesos

REGISTROS DE CONTROL		Seguridad Física
Sistema de registro de control de acceso al edificio		
Política No.: MSPsf008	**Página: 1 de 1**	**Vigente a partir de: 2003**

PROCEDIMIENTO MSPSF008

1. Para facilitar una evacuación de emergencia y para casos de investigaciones, el personal de seguridad mantendrá registros de las personas han entrado a las instalaciones del Municipio en los últimos 3 meses.
2. Fuera de Horario de oficina las vistas a estos lugares deben ser registrados en una bitácora aun que sean los responsables de las áreas.
3. En cada Centro de Cómputo o área con información confidencial se deberá de contar con un diario para registrar las personas y las actividades a realizar fuera de horario de oficina.

a) Responsable de su implantación: Administradores de sistemas

b) Periodo sugerido de revisión: Semestral

c) Responsables de su cumplimiento: Administradores de sistemas

Evidencia de Control	Tecnología de control de accesos / Registros de accesos a las instalaciones

REPORTE DE IDENTIFICACIONES PERDIDAS O ROBADAS		Seguridad Física
Reporte de identificaciones perdidas o robadas y tarjetas inteligentes de sistemas de acceso		
Política No.: MSPsf09	**Página: 1 de 1**	**Vigente a partir de: 2003**

PROCEDIMIENTO MSPSF09

1. Las identificaciones del Municipio y tarjetas de acceso físico que han sido perdidas o robadas –o se sospecha- deben ser reportadas al personal de seguridad de sistemas inmediatamente.
2. El trabajador que pierda o le roben –o que sospeche- reportará el robo o perdida inmediatamente al personal de seguridad de sistemas.
3. El personal de seguridad tomará las medida necesarias en casos de robos o pérdidas de identificación (bloquear privilegios y accesos etc.)
4. Tramitar inmediatamente otra identificación para el trabajador que realizó el reporte de pérdida o robo.

a) Responsable de su implantación: Administradores de sistemas

b) Periodo sugerido de revisión: Semestral

c) Responsables de su cumplimiento: Administradores de sistemas

Evidencia de Control	Identificaciones o gafetes / Reporte de robo o pérdida de identificación

REGISTRO DE VISITANTES		Seguridad Física
Proceso de identificación y firma requerida para todos los visitantes		
Política No.: MSPsf010	**Página: 1 de 1**	**Vigente a partir de: 2003**

PROCEDIMIENTO MSPSF010

1. Que todos los visitantes muestren identificación con foto y firmen antes de que se les conceda autorización para entrar a cualquier área restringida del Municipio.
2. Los visitantes serán admitidos en las instalaciones del Municipio sólo para propósitos específicos autorizados
3. Todos los visitantes e inclusive trabajadores de la compañía de diferentes ubicaciones muestren identificación y firmen en un libro de entradas y salidas con el guardia o en recepción.
4. En el caso de que solo se pida identificación sólo se permitirá el acceso a las personas que tengan cita con algún trabajador del Municipio. Pero es más conveniente pedir la firma y que quede registrada la hora de entrada y salida de la persona.

a) Responsable de su implantación:	Administradores de sistemas Recursos Humanos
b) Periodo sugerido de revisión:	Semestral
c) Responsables de su cumplimiento:	Administradores de sistemas Recursos Humanos Guardias

Evidencia de Control	Tecnología de control de accesos / Bitácora de entradas y salidas

INDIVIDUOS SIN IDENTIFICACIÓN		Seguridad Física
Individuos sin identificación dentro de un área restringida del Municipio deben ser interrogados		
Política No.: MSPsf011	**Página: 1 de 1**	**Vigente a partir de: 2003**

PROCEDIMIENTO MSPSF011

1. Individuos sin identificación propia del Municipio en un lugar visible serán cuestionados inmediatamente acerca de la falta de identificación. Si no se puede hacer una identificación valida pronto se le escoltara a recepción.
2. En áreas restringidas sin excepción todos portarán una identificación del Municipio en un lugar visible.
3. Si alguna persona se encuentra en instalaciones donde se encuentre equipo de cómputo e información relacionada con sistemas sin identificación visible llamar inmediatamente a seguridad, para escoltar a estas personas a recepción donde serán interrogadas

a) Responsable de su implantación: Administradores de sistemas

b) Periodo sugerido de revisión: Semestral

c) Responsables de su cumplimiento: Administradores de sistemas
Todos los trabajadores

Evidencia de Control	Tecnología de control de accesos / Identificaciones

GUARDAR IDENTIFICACIÓN AL SALIR		Seguridad Física
Guardar la identificación después de salir de las instalaciones del Municipio		
Política No.: MSPsf012	**Página: 1 de 1**	**Vigente a partir de: 2003**

PROCEDIMIENTO MSPSF012

1. Por seguridad de la persona y la alcaldía inmediatamente después de salir de las instalaciones del Municipio todos los trabajadores guardarán sus identificaciones en un lugar seguro y oculto de las miradas de otras personas.

a) Responsable de su implantación: Administradores de sistemas

b) Periodo sugerido de revisión: Semestral

c) Responsables de su cumplimiento: Administradores de sistemas
Todos los trabajadores

Evidencia de Control	Tecnología de control de accesos / Identificaciones

VISITANTES NO ESCOLTADOS		Seguridad Física
Cuando un visitante no esté escoltado en áreas restringidas debe ser interrogado		
Política No.: MSPsf013	**Página: 1 de 1**	**Vigente a partir de: 2003**

PROCEDIMIENTO MSPSF013

1. Siempre que un trabajador note que un visitante no esta escoltado dentro de un área restringida del Municipio, se le cuestionará el porqué está en ese lugar y para que.
2. El visitante será acompañado directamente a recepción a una estación de seguridad o con la persona que vino a ver.
3. Si el trabajador nota sospechoso al visitante o teme por su seguridad física, llamará al personal de seguridad para que ellos se hagan cargo del intruso.

a) Responsable de su implantación: Administradores de sistemas

b) Periodo sugerido de revisión: Semestral

c) Responsables de su cumplimiento: Administradores de sistemas
Todos los trabajadores
Personal de seguridad

Evidencia de Control **Tecnología de control de accesos / Identificaciones**

REVISIÓN AL EQUIPAJE	Seguridad Física

Los trabajadores deben mostrar el contenido de su equipaje al salir de las instalaciones del Municipio, si así lo solicita vigilancia

Política No.: MSPsf014	Página: 1 de 1	Vigente a partir de: 2003

PROCEDIMIENTO MSPSF014

1. Al salir de las instalaciones del Municipio el guardia, si lo requiere, revisará las bolsas, portafolios, o cualquier maleta que la persona traiga consigo.
2. Esta medida no asegura el robo de información, ya que esta puede estar impresa o en discos, pero si puede evitar robo de equipo.
3. En la puerta de salida es recomendable tener un letrero donde diga que toda persona al salir podrá ser requerido, de mostrar su equipaje (bolsas, portafolios, etc.) al guardia.
4. La medida anterior busca evitar que alguna persona se sienta agredida por el guardia al pedirle este que le muestre su equipaje.

a) Responsable de su implantación: Administradores de sistemas

b) Periodo sugerido de revisión: Anual

c) Responsables de su cumplimiento: Administradores de sistemas
Guardias

Evidencia de Control	Tecnología de control de accesos / Pases de autorización de salida de equipo

PERMISO PARA SACAR EQUIPOS DE LAS INSTALACIONES		**Seguridad Física**
Formato autorizado para sacar cualquier computadora y/o mecanismo de comunicación		
Política No.: MSPsf015	**Página: 1 de 1**	**Vigente a partir de: 2003**

PROCEDIMIENTO MSPSF015

1. Computadoras portátiles (excepto el personal que tenga asignado dicha portátil), módems, y otro equipo de cómputo y telecomunicaciones, no saldrá de las instalaciones del municipio, a menos que esté acompañado de un pase apropiado y aprobado por sistemas.
2. Para la reubicación de cualquier equipo de cómputo o comunicaciones instalado en algún edificio del Municipio, será necesario contar con un pase autorizado, ya que el guardia tendrá ordenes de no permitir la salida de cualquiera de ellos.

a) Responsable de su implantación: Administradores de sistemas

b) Periodo sugerido de revisión: Anual

c) Responsables de su cumplimiento: Administradores de sistemas
Personal de seguridad

Evidencia de Control	**Tecnología de control de accesos / Pases de autorización de salida de equipo**

FORMATO PARA SACAR MEDIOS DE ALMACENAMIENTO		Seguridad Física
Al sacar de las instalaciones del Municipio de San Pedro, cualquier medio de almacenamiento computacional deberá tener un formato autorizado		
Política No.: MSPsf016	**Página: 1 de 1**	**Vigente a partir de: 2003**

PROCEDIMIENTO MSPSF016

1. Todos los medios de almacenamiento (cintas de respaldo.) que salen del Municipio deben ser acompañados por un pase propiamente autorizado.
2. Las salidas de medios de almacenamiento se registrarán en recepción.
3. Se llevará un control de existencias de los medios de almacenamiento así como de sus entradas y salidas.
4. Responsabilizar a la persona que saque un medio de almacenamiento por la información que esta pudiera contener.

a) Responsable de su implantación: Administradores de sistemas

b) Periodo sugerido de revisión: Permanente

c) Responsables de su cumplimiento: Administradores de sistemas
Personal de seguridad

Evidencia de Control	Tecnología de control de accesos / Pases de autorización de salida de equipo

ÁREA DE SEGURIDAD INTERMEDIA		Seguridad Física
Establecimiento de un área de seguridad intermedia para restringir el acceso al centro de cómputo		
Política No.: MSPsf017	**Página: 1 de 1**	**Vigente a partir de: 2003**

PROCEDIMIENTO MSPSF017

1. Tener una antesala en el centro de cómputo para recibir toda la mensajería. Con esta área se evita abrir directamente las puertas del centro, se restringe el movimiento de materiales y controla aún mas los accesos al centro de cómputo en sí.
2. Este cuarto servirá para guardar la papelería y otros materiales que se encuentren en el centro de cómputo.
3. Con esto se disminuye el riesgo de fuego y de exponer los sistemas a sustancias peligrosas, polvo, derramamiento de algún liquido, etc.
4. Personal de mensajería no entrara directamente los cuartos que contienen facilidades de computación multiusuario.

a) Responsable de su implantación: Personal directivo

b) Periodo sugerido de revisión: Semestral

c) Responsables de su cumplimiento: Personal directivo
Diseñadores del centro de cómputo

Evidencia de Control — **Diseño y ubicación de las instalaciones**

ENCRIPTAMIENTO DE DATOS		Seguridad Física
Seguridad física o encriptamiento de datos requerida para toda la información confidencial		
Política No.: MSPsf018	**Página: 1 de 1**	**Vigente a partir de: 2003**

PROCEDIMIENTO MSPSF018

1. Todos los medios de almacenamiento de información (tal como disco duro, floppy disks, cintas magnéticas, cd-roms) que contengan información confidencial debe ser asegurada físicamente cuando no se usa. Una excepción pudiera hacerse si esta información es protegida por un sistema de encriptamiento (convertidor) aprobado por el personal de seguridad.
2. Todos los responsables de áreas implementarán medidas de seguridad física o encriptamiento para resguardar la información confidencial, esta política es particularmente relevante para PCs portátiles, laptop, palmtop, y otras pequeñas microcomputadoras (PCs). Cuando la seguridad física no puede garantizarse se requiere de un sistema de encriptamiento.

a) Responsable de su implantación: Administradores de sistemas

b) Periodo sugerido de revisión: Semestral

c) Responsables de su cumplimiento: Administradores de sistemas
Usuarios de la información

Evidencia de Control	Sistema de encriptamiento

PUERTAS DE ESTANTES CON EQUIPO		Seguridad Física
Las puertas de los estantes del equipo de comunicaciones y de cómputo deben estar cerradas		
Política No.: MSPsf019	**Página: 1 de 1**	**Vigente a partir de: 2003**

PROCEDIMIENTO MSPSF019

1. Todas las puertas de los estantes donde se encuentra el equipo de comunicaciones y de cómputo en site deben permanecer cerradas al menos que un técnico autorizado esté en alguna actividad de reparación, mantenimiento o actividades de reconfiguración.
2. Se debe establecer otro nivel de control de acceso físico sobre el equipo de cómputo localizado dentro del site, ya que en algunos casos se permite la entrada a un gran número de personas como por ejemplo: programadores que recogen sus reportes, operadores que ponen cintas, analistas que miden características de un sistema, etc.
3. Lo deseable es reducir al mínimo la cantidad de gente en el site, aunque algunas veces no es práctico y se permite la entrada a varias personas. Hay dos alternativas para esta política:
    a. Poner paredes adicionales o jaulas de metal con cerradura para segmentar el site en diferentes zonas, cada una con su propio nivel de seguridad
    b. Cerrar con llave los gabinetes con equipo de producción

a) Responsable de su implantación: Administradores de sistemas

b) Periodo sugerido de revisión: Semestral

c) Responsables de su cumplimiento: Administradores de sistemas
Jefe de centro de cómputo

Evidencia de Control | **Tecnología de control de accesos / Mecanismos de seguridad**

COMPUTADORAS MULLTIUSUARIO		Seguridad Física
Computadora multiusuario o sistema de comunicaciones dentro de cuartos cerrados		
Política No.: MSPsf020	**Página: 1 de 1**	**Vigente a partir de: 2003**

PROCEDIMIENTO MSPSF020

1. Todas las computadoras multiusuario y equipo de comunicaciones se colocarán en cuartos cerrados para prevenir usos no autorizados.
2. Todos los sistemas multiusuario de sites remotos deben localizarse tras puertas cerradas, incluyendo sistemas administradores y administradores de redes.
3. Los switches, PBXs, hubs, routers, apagafuegos, y otros equipos de red deben estar en cuartos cerrados. No importa cuan sofisticado sea el software de control de acceso, si se tiene acceso físico a los servidores y equipo similar entonces el software de control de acceso puede ser violado.

a) Responsable de su implantación: Administradores de sistemas

b) Periodo sugerido de revisión: Semestral

c) Responsables de su cumplimiento: Administradores de sistemas

Evidencia de Control	Tecnología de control de accesos

SISTEMAS AISLADOS FÍSICAMENTE		Seguridad Física
Sistemas de finanzas y comercio de internet deben estar físicamente aislados		
Política No.: MSPsf021	**Página: 1 de 1**	**Vigente a partir de: 2003**

PROCEDIMIENTO MSPSF021

1. Todas los servidores de comercio de Internet y equipo como apaga fuegos; así como los sistemas que manejan transferencias y otras actividades financieras, deben ser aislados físicamente, y asegurados en una manera que estén separados de otras computadoras que se encuentren en el mismo centro de cómputo.
2. Segregar y proteger separadamente las computadoras que manejan dinero digitalizado en un esfuerzo para reducir el riesgo de un fraude.
3. Al permitir el acceso a personas no autorizadas estas pudieran robar respaldos de cintas que contienen números de tarjetas de crédito, números de cuentas de cheques u otra información con la cual se cometen fraude.
4. Esta política supone además que el centro de cómputo esta cerrado con llave y solo un número restringido de personas tiene acceso a este.
5. El mecanismo a usar depende de la administración, en conjunto con el personal de sistemas responsable, un ejemplo es emplear jaulas de metal con cerradura para separar las maquinas o usar otro cuarto separado, etc.

a) Responsable de su implantación: Administradores de sistemas

b) Periodo sugerido de revisión: Semestral

c) Responsables de su cumplimiento: Administradores de sistemas
Encargado del centro de cómputo

Evidencia de Control	Tecnología de control de accesos / Mecanismos de se guridad

SISTEMAS EXTERNOS	Seguridad Física

Se debe aislar el equipo de los sistemas del Municipio de equipos utilizados por proveedores para actividades propias de su trabajo.

Política No.: MSPsf022	Página: 1 de 1	Vigente a partir de: 2003

PROCEDIMIENTO MSPSF022

1. El equipo computacional y de comunicaciones manejado por la alcaldía debe estar aislado físicamente del equipo manejado por terceras partes.
2. Colocar en cuartos separados o bien en jaulas separadas los equipos computacionales y de comunicaciones que son del Municipio de los equipos de otras partes.

a) Responsable de su implantación: Administradores de sistemas

b) Periodo sugerido de revisión: Semestral

c) Responsables de su cumplimiento: Administradores de sistemas
Encargado del centro de cómputo

Evidencia de Control	Tecnología de control de accesos

ACCESO A ESTACIONES DE TRABAJO		**Seguridad Física**
Se deben usar llaves de metal para controlar el acceso a todas las estaciones de trabajo		
Política No.: MSPsf023	**Página: 1 de 1**	**Vigente a partir de: 2003**

PROCEDIMIENTO MSPSF023

1. Todos los escritorios principales de las estaciones de trabajo tendrán una llave de metal para controlar el acceso a personas autorizadas.
2. Además de tener un software de control de accesos, se tendrá bajo llave los escritorios principales, ya que si alguien viola el control de accesos, habrá otra medida de seguridad, se deben incluir computadoras portátiles, como handhelds y palmtops.
3. El encargado de departamento tendrá una copia de las llaves de los escritorios principales, para en casos de que alguien olvide o pierda sus llaves.

a) Responsable de su implantación: Administradores de sistemas

b) Periodo sugerido de revisión: Semestral

c) Responsables de su cumplimiento: Administradores de sistemas
Encargados de departamento
Personal de seguridad

Evidencia de Control	**Tecnología de control de accesos / Llaves de escritorios principales**

CENTRALIZACIÓN DE DISPOSITIVOS		Seguridad Física
Centralización de todos los dispositivos de voz y datos		
Política No.: MSPsf024	**Página: 1 de 1**	**Vigente a partir de: 2003**

PROCEDIMIENTO MSPSF024

1. Todos los dispositivos críticos del negocio que soportan al Municipio como los sistemas de teléfonos, intranet, redes de área local y redes de área ancha, estarán centralizados y en cuartos dedicados con controles de acceso físico, circuito cerrado de televisión, sistema de monitoreo del medio ambiente y otras medidas de seguridad indicadas por el administrador de seguridad digital.

a) Responsable de su implantación: Administradores de sistemas

b) Periodo sugerido de revisión: Semestral

c) Responsables de su cumplimiento: Administradores de sistemas
Personal de seguridad de informática

Evidencia de Control	Controles de seguridad / Mecanismos de se guridad

ACCESO A DISPOSITIVOS DE ALMACENAMIENTO		Seguridad Física
Acceso restringido a cintas magnéticas, discos y librerías de documentación		
Política No.: MSPsf025	**Página: 1 de 1**	**Vigente a partir de: 2003**

PROCEDIMIENTO MSPSF025

1. Las cintas magnéticas, discos y librerías de documentación están en áreas controladas dentro del centro de cómputo.
2. El acceso estará restringido para los trabajadores a quienes sus responsabilidades de trabajo requieran de su presencia en esa área.
3. Restringir el acceso físicamente a las áreas que contienen información sensible, valiosa o crítica.

a) Responsable de su implantación: Administradores de sistemas

b) Periodo sugerido de revisión: Semestral

c) Responsables de su cumplimiento: Administradores de sistemas
Usuarios

Evidencia de Control	Controles de seguridad de informática / Mecanismos de seguridad

LISTA DE PERSONAL AUTORIZADO		Seguridad Física
La lista del staff autorizado para acceder al centro de cómputo debe ser revisada trimestralmente		
Política No.: MSPsf026	**Página: 1 de 1**	**Vigente a partir de: 2003**

PROCEDIMIENTO MSPSF026

1. La lista de los miembros del staff autorizados a quienes se les permite entrar al centro de cómputo debe ser revisado y actualizado trimestralmente por el responsable de operaciones computacionales.
2. Solo esos miembros que tienen realmente necesidad de estar dentro del site se les permitirá el acceso.

a) Responsable de su implantación:	Administradores de sistemas
b) Periodo sugerido de revisión:	Semestral
c) Responsables de su cumplimiento:	Administradores de sistemas Personal de operaciones computacionales

Evidencia de Control	Mecanismos de seguridad / Lista de personal autorizado para acceder al centro de cómputo

ACCESOS A ÁREAS CON EQUIPO DE COMUNICACIONES		Seguridad Física
Áreas con equipo de comunicaciones cerradas y acceso con escolta		
Política No.: MSPsf027	**Página: 1 de 1**	**Vigente a partir de: 2003**

PROCEDIMIENTO MSPSF027

1. Gabinete telefónico, cuartos de redes, ruteadores y hubs, cuartos de sistemas de correo de voz y áreas similares que contienen equipo de comunicaciones deben mantenerse siempre cerradas.
2. Está prohibido el acceso a estas áreas a visitantes, y en los casos que se autorice el acceso se asignará una escolta, que monitoreará todo el trabajo que se ejecute

a) Responsable de su implantación: Administradores de sistemas

b) Periodo sugerido de revisión: Semestral

c) Responsables de su cumplimiento: Administradores de sistemas
Guardias

Evidencia de Control	Controles de seguridad de informática / Mecanismos de seguridad

OFICINAS VACÍAS		Seguridad Física
Las puertas de oficinas vacías deben estas cerradas		
Política No.: MSPsf028	**Página: 1 de 1**	**Vigente a partir de: 2003**

PROCEDIMIENTO MSPSF028

1. Todos los trabajadores que tengan oficinas privadas deben cerrar las puertas cuando no se encuentren en ellas, además de otras medidas también necesarias, esta práctica ayudará a restringir accesos no autorizados a información confidencial.
2. Solo los responsables de áreas restringidas así como sus secretarias contarán con llaves maestras para en casos de emergencias puedan tener acceso a estas áreas cerradas.

a) Responsable de su implantación: Administrador de sistemas

b) Periodo sugerido de revisión: Semestral

c) Responsables de su cumplimiento: Administrador de sistemas
Personal de Sistemas
Personal con oficinas privadas

Evidencia de Control	Tecnología de control de accesos

RECEPCIONISTAS EN ÁREAS CON INFORMACIÓN CONFIDENCIAL		Seguridad Física
Debe haber guardias o recepcionista en áreas que contienen información confidencial		
Política No.: MSPsf029	**Página: 1 de 1**	**Vigente a partir de: 2003**

PROCEDIMIENTO MSPSF029

1. Los guardias, recepcionistas o personal del staff controlarán los accesos a las oficinas del Municipio, centros de cómputo, y otras áreas de trabajo que contienen información confidencial.
2. No se permitirá el acceso a visitantes u otras personas no autorizadas por la entrada de empleados u a otros caminos que conduzcan a las áreas de trabajo que contienen información confidencial.
3. Todas las áreas que contengan información confidencial estarán cerradas y solo el personal asignado previamente permitirá el acceso a visitantes o terceras personas al lugar.

a) Responsable de su implantación: Administradores de sistemas

b) Periodo sugerido de revisión: Semestral

c) Responsables de su cumplimiento: Administradores de sistemas
Guardias
Recepcionistas

Evidencia de Control	Tecnología de control de accesos

DESACTIVAR CÓDIGOS NO UTILIZADOS		**Seguridad Física**
Cambiar el código de control de acceso físico al salirse un trabajador		
Política No.: MSPsf030	**Página: 1 de 1**	**Vigente a partir de: 2003**

PROCEDIMIENTO MSPSF030

1. Cuando un trabajador termina su relación de trabajo con el Municipio, todos los códigos de acceso de seguridad física que tenga el trabajador deben ser cambiados o desactivados. Por ejemplo el password o clave para entrar al edificio.

a) Responsable de su implantación: Administradores de sistemas

b) Periodo sugerido de revisión: Semestral

c) Responsables de su cumplimiento: Administradores de sistemas
Recursos Humanos
Personal de Sistemas

Evidencia de Control	**Tecnología de control de accesos / Registros de accesos a las instalaciones**

NO PROBAR LOS CONTROLES DE ACCESO		Seguridad Física
Está prohibido probar los controles de acceso		
Política No.: MSPsf031	**Página: 1 de 1**	**Vigente a partir de: 2003**

PROCEDIMIENTO MSPSF031

1. Si un trabajador requiere entrar a un área restringida no debe intentar violar el control de acceso si no que ir por el canal correcto a pedir autorización
2. Si un trabajador intenta más de una vez de burlar los controles de acceso será motivo de una acción disciplinaria

a) Responsable de su implantación: Administradores de sistemas

b) Periodo sugerido de revisión: Semestral

c) Responsables de su cumplimiento: Administradores de sistemas
Personal responsable de áreas con información confidencial
Guardia

Evidencia de Control	Tecnología de control de accesos

HORARIOS DE TRABAJO		Seguridad Física
Solo se trabajará en las áreas restringidas durante horas normales de trabajo		
Política No.: MSPsf032	**Página: 1 de 1**	**Vigente a partir de: 2003**

PROCEDIMIENTO MSPSF032

1. Los trabajadores tendrán acceso a los recursos tecnológicos del Municipio únicamente durante horas de oficina.
2. Se restringirá el uso de los recursos tecnológicos a horas de oficina.
3. Si alguien requiere trabajar fuera de este horario se solicitara permiso con el responsable del área.

a) Responsable de su implantación: Administradores de sistemas

b) Periodo sugerido de revisión: Semestral

c) Responsables de su cumplimiento: Administradores de sistemas
Personal responsable de áreas con información confidencial
Guardias

Evidencia de Control	Tecnología de control de accesos / Control de entradas y salidas

RESPONSABLES DE AUTORIZACIÓN DE ACCESO		Seguridad Física
Mantenimiento de la lista que muestra al personal responsable de autorizar las concesiones a los accesos físicos		
Política No.: MSPsf033	**Página: 1 de 1**	**Vigente a partir de: 2003**

PROCEDIMIENTO MSPSF033

1. La dirección del Municipio designará a varias personas responsables (puede ser una por departamento o algunas personas del staff) para que estas sean las encargadas de autorizar los permisos para los accesos físicos.
2. Se hará una lista con los nombres de las personas responsables la cual será revisada periódicamente.

a) Responsable de su implantación: Personal directivo

b) Periodo sugerido de revisión: Semestral

c) Responsables de su cumplimiento: Personal directivo
Recursos Humanos

Evidencia de Control	Tecnología de control de accesos / Lista de personal responsable

REPORTES DE IDENTIFICACIONES		Seguridad Física
Reportes periódicos de identificaciones emitidos para los responsables de cada departamento		
Política No.: MSPsf034	**Página: 1 de 1**	**Vigente a partir de: 2003**

PROCEDIMIENTO MSPSF034

1. El personal de Sistemas emitirá un reporte por departamento con todo el personal, contratistas, consultores, temporales, etc., que laboren en el área o tienen una relación de trabajo con el Municipio.
2. El encargado del departamento revisará uno por uno al personal en la lista para determinar si la identificación sigue vigente o no, y dar aviso inmediatamente al personal de seguridad de las personas que se darán de baja en la lista, para que seguridad a su vez revoque los permisos y privilegios que esta persona pudiera tener.
3. En la lista vendrá nombre, clave de usuario y otros mecanismos de acceso

a) Responsable de su implantación: Administradores de sistemas

b) Periodo sugerido de revisión: Semestral

c) Responsables de su cumplimiento: Administradores de sistemas
Recursos Humanos
Responsables de departamento

Evidencia de Control	Tecnología de control de accesos / Lista del personal con identificación por departamento

SEGURIDAD PARA SISTEMAS DE COMUNICACIÓN		Seguridad Física
Medidas de seguridad física para computadoras y sistemas de comunicación		
Política No.: MSPsf035	**Página: 1 de 1**	**Vigente a partir de: 2003**

PROCEDIMIENTO MSPSF035

1. Edificios del Municipio que contienen computadoras y sistemas de comunicaciones deben ser protegidos con medidas de seguridad física que prevengan el acceso a personas no autorizadas
2. Esta política es particularmente relevante para microcomputadoras (PCs), estaciones de servicio, LANs y sistemas de cliente servidor, etc.

a) Responsable de su implantación: Administradores de sistemas

b) Periodo sugerido de revisión: Semestral

c) Responsables de su cumplimiento: Administradores de sistemas
Personal de Sistemas

Evidencia de Control	Mecanismos de seguridad

ACTIVIDADES CRÍTICAS		Seguridad Física
Las actividades críticas o sensibles se permiten solamente en áreas aseguradas físicamente		
Política No.: MSPsf036	**Página: 1 de 1**	**Vigente a partir de: 2003**

PROCEDIMIENTO MSPSF036

1. Todas las actividades que manejan información critica o sensitiva deben tomar lugar en áreas que estén físicamente seguras y protegidas contra accesos no autorizados, interferencias y daños.
2. Los centros de cómputo, área de conmutador, bodega de archivos y otros lugares donde se maneje información critica o sensible deben tener un control de acceso físico adecuado, la tecnología a usar la decidirán la administración del Municipio, junto con el personal de la Dirección de Sistemas y auditores internos. La tecnología de la seguridad física debe estar en función del valor, sensibilidad y lo critico de la información, así como de la localización del site.

a) Responsable de su implantación: Administradores de sistemas

b) Periodo sugerido de revisión: Semestral

c) Responsables de su cumplimiento: Administradores de sistemas
Personal responsable de departamento

Evidencia de Control	Mecanismos de seguridad

ÁREAS CON EQUIPO VACANTE		Seguridad Física
Áreas con equipo vacante deben estar cerradas y revisadas periódicamente		
Política No.: MSPsf037	**Página: 1 de 1**	**Vigente a partir de: 2003**

PROCEDIMIENTO MSPSF037

1. Todas las áreas con equipos de sistemas digitales que estén vacantes deben estar cerradas y revisarse periódicamente por algún sistema de monitoreo remoto y/o guardia de seguridad.
2. Revisar y confirmar que todas las puertas estén cerradas y que todo se vea seguro en el área. No solo en los centros de cómputo sino las oficinas con PCs, etc.
3. El Procedimiento de Referencia detallado y la frecuencia la establecerá el encargado de seguridad de informática y sistemas.

a) Responsable de su implantación: Administradores de sistemas

b) Periodo sugerido de revisión: Semestral

c) Responsables de su cumplimiento: Administradores de sistemas
Personal de seguridad de informática
Guardias

Evidencia de Control	Controles de seguridad de informática / Mecanismos de seguridad

EQUIPOS DE AUDIO O VIDES		**Seguridad Física**
Están prohibidos los equipos de audio o video y cámaras		
Política No.: MSPsf038	**Página: 1 de 1**	**Vigente a partir de: 2003**

PROCEDIMIENTO MSPSF038

1. Dentro del centro de cómputo y áreas donde se encuentren servidores que almacenen información integral del Municipio no se permiten las cámaras personales ni equipo de grabación de audio y video, a menos que esté autorizado por la Dirección de Sistemas a través de un oficio.
2. Si alguien trae alguna cámara o equipo, este se quedara en recepción o con el guardia hasta que la persona abandone las instalaciones, a menos que esté autorizado por la Dirección de Sistemas a través de un oficio.
3. Si esta política es violada el personal de seguridad quitará el rollo o cinta y la destruirá o bien confiscará el rollo, lo revelará y regresará solo el material que no sea del Municipio.

a) Responsable de su implantación: Administradores de sistemas

b) Periodo sugerido de revisión: Semestral

c) Responsables de su cumplimiento: Administradores de sistemas
Guardias

Evidencia de Control	**Reglamento de acceso a las instalaciones del Municipio**

AVISO DE NO INGRESO AL CENTRO DE CÓMPUTO		Seguridad Física
Todas las puertas de acceso a centro de cómputo y áreas de sistemas del Municipio tendrá avisos de advertencia para evitar ingresos no autorizados		
Política No.: MSPsf039	**Página: 1 de 1**	**Vigente a partir de: 2003**

PROCEDIMIENTO MSPSF039

1. Es política de la Dirección de sistemas que solamente personal de operación, proveedores de informática autorizados y el director de sistemas ingresen al centro de cómputo y a las áreas de sistemas de los edificios del municipio donde haya servidores y equipos de telecomunicaciones.
2. Todas las puertas de acceso deben tener colocado el letrero que se muestra en la página siguiente (ACCESO A PERSONAL AUTORIZADO).
3. Las personas que omitan esta advertencia e ingresen al centro de cómputo o áreas de sistemas sin autorización serán sujetas a las medidas correctivas que establezca el Municipio de San pedro.
4. El centro de cómputo y las áreas de sistemas donde exista equipo de cómputo y de telecomunicaciones contarán con controles de acceso para prevenir ingresos de personal no autorizado.
5. Un monitoreo permanente dentro de los centros de cómputo y de las áreas de sistemas se llevará a cabo, ya sea con supervisión directa del personal de sistemas, así como rondas del personal de seguridad de los edificios o cámaras de video.

a) Responsable de su implantación:	Administradores de sistemas
b) Periodo sugerido de revisión:	Anual
c) Responsables de su cumplimiento:	Administradores de sistemas Guardias Empleados y visitantes

Evidencia de Control	**Controles de acceso, filmación de actividades dentro de los centros de cómputo y áreas de sistemas, avisos.**

Municipio de San Pedro	**A V I S O D E A D V E R T E N C I A**	
APLICA A TODOS LOS VISITANTES Y EMPLEADOS AJENOS A LA OPERACIÓN		
Dirección de Sistemas	**Edificio:**	**Responsable de Operación:**

A V I S O

PROHIBIDO EL INGRESO A ESTA ÁREA. SOLAMENTE PUEDE INGRESAR PERSONAL AUTORIZADO POR LA DIRECCIÓN DE SISTEMAS

CUALQUIER INDIVIDUO QUE SE SORPRENDA INFRINGIENDO ESTA REGLA SE SOMETERÁ A LAS MEDIDAS CORRECTIVAS PERTINENTES