

DEPARTAMENTO DE TECNOLOGIA E INNOVACION**MANUAL DE POLITICAS Y PROCESMIENTOS DE LAS
TECNOLOGIAS DE INFORMACION Y COMUNICACION****SAN SALVADOR, MARZO DE 2023**

CONTENIDO

PRESENTACION.....	3
OBJETIVOS.....	4
OBJETIVO GENERAL.....	4
OBJETIVOS ESPECÍFICOS.....	4
ALCANCE.....	4
MARCO LEGAL.....	4
DISPOSICIONES GENERALES.....	5
POLITICAS.....	7
POLÍTICAS DE ADQUISICIÓN Y ASIGNACIÓN DEL EQUIPO INFORMÁTICO	
.....	7
POLÍTICAS DE SOFTWARE Y SISTEMAS DE INFORMACIÓN.....	8
POLITICAS DE USO ADECUADO DE RECURSOS DE HARDWARE Y SOFTWARE	
.....	9
POLITICAS MANTENIMIENTO PREVENTIVO Y CORRECTIVO DE LOS EQUIPOS	
INFORMÁTICOS	10
POLÍTICAS DE ADMINISTRACIÓN DE LAS BASES DE DATOS.....	11
POLITICAS ACCESO Y MANEJO DE LA INFORMACIÓN.....	12
POLÍTICAS DE CONTROL Y ACCESO A INTERNET (ACCESO A SITIOS Y CONTENIDO NO	
AUTORIZADO).....	13
POLÍTICAS DE DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN	
UTILIZADOS POR LA MUNICIPALIDAD.....	14
CONTINGENCIAS INFORMÁTICAS.....	15
MONITOREO.....	15
RESTRICCIONES.....	16
SANCIONES.....	16
GLOSARIO.....	17

Introducción

El presente manual está formulado en virtud de lo establecido en las **Normas Técnicas de Control Interno Específicas de la Municipalidad de San Martín** (NTCIE) aprobadas por la corte de cuentas de la república mediante Decreto N°05 el 30 de enero del 2023 “USO DE TECNOLOGIAS DE INFORMACION Y COMUNICACIÓN ART.63”

El consejo municipal a través del alcalde y al departamento de tecnología e información e innovación establecerá el manual de políticas y procedimientos de las tecnologías de información y comunicación que define los controles aplicables al procedimiento electrónico de datos con el propósito de salvaguardar el diseño, ciclo de operaciones y desarrollo de los sistemas. Así como la utilización de los sistemas operativos y equipos tecnológicos de información presentado en el siguiente manual y tiene el propósito fundamental de definir la base normativa para el adecuado uso de las tecnologías de información con el objetivo de que este se realice con racionalidad y eficiencia y a la vez mitigar los riesgos que generen su uso.

OBJETIVOS

OBJETIVO GENERAL

Definir políticas de TI, que simplifiquen la ejecución y control de las actividades tecnológicas en las diferentes unidades organizativas de la Municipalidad de San Martín.

OBJETIVOS ESPECÍFICOS

- Crear Políticas de TI para fortalecer el Control Interno de la Municipalidad.
- Definir responsabilidades en el uso de las TI.
- Establecer las diferentes restricciones y prohibiciones al utilizar TI dentro de la municipalidad.

ALCANCE

Todas las diferentes unidades organizativas que integran la Alcaldía Municipal de San Martín.

MARCO LEGAL

- Normas Técnicas de Control Interno Específicas de la Municipalidad de San Martín.
- Manual de Organización y Funciones de la Municipalidad de San Martín.

DISPOSICIONES GENERALES

El presente Manual de Políticas y procedimientos de las tecnologías de Información y comunicación Municipal fue formulado con el objetivo normar la utilización de los recursos de tecnologías de Información de la Alcaldía Municipal de San Martín no Específicas de la Municipalidad. El departamento de Tecnologías e innovación Municipal, es la autoridad competente.

Establecer y administrar los medios y técnicas para el tratamiento automatizado de la información que genere la institución.

- Proponer y solicitar las herramientas modernas y adecuadas para reforzar la capacidad institucional en la ejecución de las inversiones a las diferentes actividades que realiza.
- Realizar los servicios de mantenimiento preventivo y correctivo del equipo de computación de toda la comuna.
- Administrar la red y las bases de datos, asegurando la integridad, disponibilidad y confidencialidad de la información.
- Establecer la existencia de un plan de contingencia debidamente actualizado y verificar su cumplimiento.
- Proponer los sistemas de información que permitan adecuar el procesamiento de datos al desarrollo actual y futuro de la municipalidad.

- Identificar las necesidades de automatización a nivel institucional y de cada una de las dependencias municipales.
- Monitorear la eficiencia de la red de datos de la institución, garantizando el mantenimiento adecuado de la misma, la integridad, disponibilidad y confidencialidad de la información de los sistemas automatizados de la municipalidad.
- Establecer las normas y políticas relacionadas al uso de las diferentes herramientas de tecnologías de la información.
- Garantizar el funcionamiento adecuado del Sistema de Información, de los servicios de correo electrónico institucional y página Web Institucional.
- Establecer los criterios técnicos para la evaluación, selección y adquisición del equipo de computacional y programas necesarios para el funcionamiento de los sistemas de información de la institución, así como la instalación de los mismos.
- Llevar registros y estadísticas del trabajo realizado.

POLITICAS

POLÍTICAS DE ADQUISICIÓN Y ASIGNACIÓN DEL EQUIPO INFORMÁTICO

1. Toda solicitud de adquisición de equipo informático deberá estar sustentada por un análisis donde se demuestre los detalles y criterios por los que se requiere dicho hardware. El Análisis deberá ser realizado por el área usuaria que requiera el equipo y validado por el departamento de tecnología e innovación.
2. La Adquisición de equipos informáticos solo procederá por causa justificada, en caso sea por sustitución y/o renovación, el equipo sustituido deberá ser puesto a disposición del departamento de tecnología e innovación, quienes luego de un análisis técnico, coordinara conjuntamente con el Área de Contabilidad y activo fijo la baja del equipo de cómputo.
3. Toda decisión de adquisición de cualquier hardware requerirá la verificación por parte del departamento de tecnología e innovación, quien deberá corroborar que se cumpla con las características de la orden de compra.
4. Para la adquisición de computadoras que tengan el software instalado, el departamento de Tecnología e innovación y el Administrador de compras se aseguraran que el proveedor les entregue las licencias (Manuales, garantías, material de referencia, medios físicos o electrónicos originales, etc.). Esta información Quedará resguardada dentro de la oficina de dicho departamento para su custodia.
5. La responsabilidad y decisión de adquirir el “Hardware” es solamente del Concejo Municipal, siguiendo los debidos procedimientos administrativos de compras establecidos en la LACAP, tomando en cuenta las recomendaciones del departamento de tecnología e innovación.

6. El departamento de tecnología e innovación es el encargado de la distribución, traslados, control, entrega e instalación de los recursos tecnológicos a los usuarios de las diferentes unidades, dependiendo de las funciones a realizar. Estos recursos están asignados al usuario del puesto funcional de trabajo del área organizativa. Si el usuario es trasladado o promovido, este no está facultado a mover o trasladar el recurso tecnológico que utilizaba sin previa autorización del departamento de tecnología e innovación y el jefe de la unidad organizativa receptora deberá notificar al encargado de activo fijo y al departamento de tecnología e innovación el nuevo usuario a quien se le asignará el equipo.

7. Toda solicitud de traslado o reasignación de equipo tecnológico deberá de ser remitida por escrito o vía correo electrónico institucional al encargado de activo fijo y al departamento de tecnología e innovación quien evaluará la solicitud tomando en cuenta las mejores prácticas de distribución según el uso de los recursos tecnológicos dentro de la Municipalidad y las funciones a realizar; la solicitud podrá ser aceptada y ejecutada o podrá ser denegada y llevar una propuesta que resuelva la necesidad del traslado o reasignación.

8. Los empleados de la Municipalidad con Recurso Tecnológico asignado son responsables de:

- a. El cuidado y buen uso para realizar sus labores, siguiendo las recomendaciones establecidas en los manuales propios del fabricante
- b. Informar oportunamente el mal funcionamiento o necesidades de reparación.
- c. Entregar o devolver en buenas condiciones o con el normal desgaste de uso, el recurso tecnológico asignado, en caso que se le haya sido requerido o a su finalización de contrato.
- d. En caso de robo, pérdida o hurto deberá de interponer la denuncia policial ya su vez informar al departamento de tecnología e innovación y encargado de activo fijo sobre el hecho, para recibir instrucciones.
- e. Responder por los costos incurridos en caso de daño por negligencia y/o descuido.

POLÍTICAS DE SOFTWARE Y SISTEMAS DE INFORMACIÓN

9. El departamento de tecnología e innovación, definirá e instalará el software legalmente autorizado para utilizarse en los Recursos Tecnológicos de la Municipalidad.

10. El departamento de tecnología e innovación, será administrador de los proyectos de sistemas informáticos que se desarrollen con recursos internos o externos, con el propósito de garantizar soluciones de calidad.

11. Todo Sistema Informático antes de entrar a producción deberá contar con la correspondiente "Carta de Aceptación", donde la unidad organizativa usuaria garantiza que los datos que se registran, los procesos que contiene y los reportes que genera la aplicación son los requeridos según el Documento de Referencia del Proyecto.

12. Para todo sistema informático en producción se definirá como administrador el área organizativa usuaria principal.

13. Las usuarias o usuarios de los sistemas informáticos en producción, serán responsables de la calidad y veracidad de los datos que se ingresen u obtienen, con el propósito de asegurar la autenticidad y eficiencia de la información que estos generen.

14. Los sistemas de información que sean desarrollados por el departamento de tecnología e innovación serán propiedad de la Alcaldía Municipal de San Martín, y deberán ser usados para el propósito que fueron diseñados, quedando prohibido su uso para beneficio personal o ajeno a la institución.

POLÍTICAS DE SEGURIDAD

15. Todo usuario con acceso a un sistema de información dispondrá de una autorización de acceso, personal e intransferible, compuesta al menos de identificador de usuario y contraseña.

16. Las contraseñas tendrán plazo de vigencia, que en ningún caso podrá ser superior a los 6 meses.

17. Cada sistema informático de la Municipalidad deberá tener segmentados por roles a sus usuarios que permitan los cambios o modificaciones necesarias autorizadas.

18. Si los usuarios sospechan que su acceso autorizado (identificador de usuario y/o contraseña) está siendo utilizado por otra persona, deberá proceder a informar y solicitar una nueva contraseña.

19. Los usuarios no deben intentar obtener otros derechos de acceso al cual no están autorizados, ni utilizar ningún otro acceso autorizado que corresponda a otro usuario, aunque disponga de la autorización de éste. Salvo a la autorización dada por la autoridad competente.

20. En caso de traslado o cese del usuario del sistema, el jefe de la unidad deberá informar al departamento de tecnología e innovación para realizar la baja a las credenciales asignadas.

POLITICAS DE USO ADECUADO DE RECURSOS DE HARDWAREYSOFTWARE

21. El uso de los recursos informáticos debe ser única y exclusivamente para actividades relacionadas al propósito institucional y no deberá utilizarse para otros fines.

22. Los nombres de los equipos (PC) deberán identificar a la oficina a la que han sido asignados.

23. Ningún usuario podrá almacenar información personal o institucional en los servidores a menos que sea autorizado por el departamento de tecnología e innovación con el visto bueno del administrador del servidor.

24. Como parte de la responsabilidad por mantener constante la estabilidad de los sistemas informáticos, deberá monitorearse y optimizarse el correcto funcionamiento del

mismo por parte del departamento de tecnología e innovación, lo que puede involucrar compras de equipo o software para dicho monitoreo, y si se requiere, repuestos y/o servicios para su reparación o configuración, considerando para ello la disponibilidad financiera y presupuestaria.

25. El departamento de tecnología e innovación velará porque los recursos informáticos se mantengan en constante y óptimo funcionamiento, realizando para ello observaciones al uso y comportamiento de los mismos.

26. En caso de daños a los equipos Informáticos, la Unidad de Tecnologías de Información será la responsable de reinstalar los sistemas operativos, aplicaciones y acceso a los datos con el objeto que el servicio continúe habilitado y de forma oportuna para los usuarios de los sistemas.

27. El administrador de la red verificará periódicamente el crecimiento de la información o cualquier anomalía en los datos y directorios del servidor.

28. Toda instalación, reubicación y/o reasignación del equipo informático, deberá ser notificada al departamento de tecnología e innovación y al encargado de activo fijo.

POLITICAS MANTENIMIENTO PREVENTIVO Y CORRECTIVO DE LOS EQUIPOS INFORMÁTICOS

29. El departamento de tecnología e innovación comunicará el programa de mantenimiento preventivo a las diferentes unidades de la Alcaldía Municipal, informado a cada una de ellas la fecha de mantenimiento.

30. Con el objetivo de evitar pérdidas de datos o información relevante, antes de llevarse a cabo la actividad de mantenimiento, los usuarios deberán respaldar la información almacenada en la computadora.

31. Las oficinas deberán programar sus actividades de tal manera que el equipo esté disponible en la fecha indicada para ejecutarle el mantenimiento preventivo.

POLITICAS DE USO DE CORREO ELECTRÓNICO INSTITUCIONAL

32. El correo electrónico institucional no se deberá usar para envío masivo, materiales de uso no institucional o innecesario (entiéndase por correo masivo todo aquel que sea ajeno a la institución, tales como: cadenas, publicidad y propaganda comercial, política, social, etcétera).

33. El correo electrónico institucional permite a los usuarios de la municipalidad, el intercambio de mensajes, a través de una cuenta de correo electrónico institucional, que facilita el desarrollo de sus funciones, con el dominio propio de la municipalidad "sanmartin.gob.sv".

34. Cuando un funcionario, usuario o colaborador al que le haya sido autorizado el uso de una cuenta de correo electrónico y se retire de la Municipalidad, su cuenta de correo será desactivada.

35. Es responsabilidad de cada jefatura hacer las solicitudes vía correo electrónico o por nota escrita, para la creación de cuenta de correo institucional para su unidad o subalterno.

36. El tamaño del buzón de correo electrónico estará determinado por el rol desempeñado por el usuario en la Municipalidad.

37. Las cuentas de correo electrónico son propiedad la Municipalidad, las cuales son asignadas a personas que tengan algún tipo de vinculación laboral con la Municipalidad, ya sea como personal de planta o personal temporal, quienes deben utilizar este servicio único y exclusivamente páralas tareas propias de la función que desempeñan.

38. Queda prohibido para todos los usuarios el uso indebido del correo electrónico, utilizando mensajes con contenidos ofensivos o atentatorios a la dignidad humana. Asimismo, queda prohibido el envío deliberado de cualquier clase de programa o virus que pueda causar perjuicios en los sistemas de información de la Municipalidad o a terceros.

39. Los usuarios tienen prohibido el uso indebido del sistema de listas de correos para el envío de mensajes de forma masiva o piramidal.

40. Los correos electrónicos enviados a las unidades de la municipalidad u otra entidad serán tomados como documentos oficiales.

POLÍTICAS DE ADMINISTRACIÓN DE LAS BASES DE DATOS

1. El departamento de tecnología e innovación tendrá acceso información de la Base de Datos únicamente para:

a) La realización de los respaldos de la BD.

b) Solucionar, mediante memorando interno o acuerdo municipal, problemas que el usuario no pueda resolver.

c) Diagnóstico o monitoreo.

d) El Administrador de la Base de Datos no deberá eliminar ninguna información del sistema, a menos que la información esté dañada o ponga en peligro el buen funcionamiento del sistema; justificando posteriormente la acción realizada mediante un informe con copia a la Gerencia General y al departamento de tecnología e innovación.

e) El Administrador de la Base de Datos es el encargado de asignar las cuentas a los usuarios para el uso.

POLITICAS ACCESO Y MANEJO DE LA INFORMACIÓN

46. Toda información albergada en cualquier medio informático de la Municipalidad, o que circule a través de su red de datos o le haya sido confiada, tiene carácter confidencial.

47. Los usuarios están obligados a proteger la información, evitando la divulgación al exterior, incluyendo esta noción tanto el acceso como la visualización de la misma. Una especial consideración de confidencialidad corresponde a ficheros o información que contenga datos de carácter personal tanto de empleados como de contribuyentes, tal como lo establece la Ley de Acceso a la Información Pública, en el Capítulo III Art. 24. 48. Los usuarios están obligados a proteger la información y los datos a los que tienen acceso. Esta protección debe prevenir el empleo de operaciones que puedan producir una alteración indebida, inutilización o destrucción, robo, uso no autorizado o cualquier forma que pueda dañar los datos, aplicaciones informáticas y documentos electrónicos propios de la Municipalidad.

49. Los usuarios, conforme a las instrucciones que reciban, utilizarán los medios o carpetas de red que les facilite el departamento de tecnología e innovación, con la finalidad de garantizar la integridad y seguridad de los equipos informáticos, de las aplicaciones informáticas y de las informaciones que contengan.

50. Los usuarios están obligados a notificar al departamento de tecnología e innovación cualquier incidencia o anomalía en el uso de los medios informáticos que detecten: pérdida de información, DVD, dispositivos de almacenamiento externo o cualquier otro soporte físico y/o electrónico, acceso no autorizado, uso de su identificador de usuario o de su contraseña, introducción de virus, desaparición de soportes informáticos y, en general, toda situación que pueda comprometer el buen uso y funcionamiento de los sistemas de información.

51. Toda salida de información a terceros debe ser canalizado por la Unidad de Acceso de Información Pública acorde a la legislación vigente.

52. Queda prohibido el almacenamiento de cualquier tipo de fichero o información no perteneciente a la tarea encomendada, como pueden ser ficheros de música, videos, documentación no relacionada con la tarea no asignada, etc. El personal de la Unidad de Tecnología establecerá los parámetros necesarios para localizar, eliminar y dar cuenta al jefe de la unidad y/o la autoridad superior competente.

POLÍTICAS DE CONTROL Y ACCESO A INTERNET (ACCESOASITIOS Y CONTENIDO NO AUTORIZADO)

53. El acceso a Internet por los usuarios se realizará únicamente empleando los medios y a través de la red establecida a estos efectos por el departamento de tecnología e innovación. Por lo que no está permitido su acceso llamando directamente a un proveedor de servicio de acceso y usando un navegador, o con otras herramientas de internet conectándose mediante un módem.

54. El Internet es una herramienta de trabajo y su autorización se concederá exclusivamente para las actividades de consulta o transacción que están en relación con el trabajo desempeñado, según competencia y su uso será autorizado únicamente por Gerencia General durante el primer trimestre de cada año.

55. Las conexiones a Internet que se produzcan a través de la red institucional tendrán una finalidad profesional. En este sentido, cada usuario autorizado empleará estas conexiones exclusivamente para el ejercicio de las tareas y actividades que corresponden a las funciones de su puesto de trabajo.

56. No deberá accederse en ningún caso a direcciones de Internet que tengan un contenido de ocio, ofensivo o atentatorio de la dignidad humana. A estos efectos el departamento de tecnología e innovación podrá restringir el acceso a determinados servidores de contenido en Internet u otras direcciones que no se consideren de interés para el ejercicio de las actividades de esta administración.

57. Las autorizaciones de acceso a Internet se concederán acorde con las funciones del puesto que desempeñe el usuario, produciéndose una segmentación de perfiles que habilite las conexiones. Cualquier instalación de acceso a Internet ha de estar por el jefe de unidad, justificando por escrito el motivo de la necesidad del acceso, de esta forma se establecerán las configuraciones necesarias para el acceso a Internet según el perfil de la petición.

58. El departamento de tecnología e innovación regulará y controlará los accesos a Internet. Se procederá a monitorearse las direcciones de accesos y el tiempo de conexión de los usuarios a Internet, así como la limitación de su uso en razón de las funciones que ejerza, por motivos de seguridad o rendimiento de la red. Se emitirán informes regularmente al jefe de la unidad o departamento, de los accesos realizados desde sus dependencias.

59. Cuando se detecte el mal uso del servicio de internet, el departamento de tecnología e innovación podrá eliminar dicho acceso sin previo aviso.

60. Queda terminantemente prohibida la instalación de proxys y cualquier otro elemento electrónico que posibilite la conexión a Internet de usuarios no autorizados, o habilitar procesos que permitan al equipo anfitrión servir de pasarela de conexión a Internet a los usuarios. Por lo tanto queda prohibido la instalación de cualquier servicio en las redes de comunicaciones como son servidores WEB, DHCP, DNS, DNSS, VPN, etc.

POLÍTICAS DE DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN UTILIZADOS POR LA MUNICIPALIDAD

61. Cada sistema informático adquirido o desarrollado para la Municipalidad gozará intrínsecamente del derecho de propiedad y/o autoría institucional, por lo que se prohíbe terminantemente el uso de estos por parte de terceros. De igual manera, las herramientas de software utilizadas para el desempeño de labores institucionales, deberán estar actualizadas con sus respectivas licencias de autenticidad y registradas a nombre de la institución.

62. En los procedimientos de Desarrollo y Mantenimiento de Aplicaciones, se utilizará una metodología que sea compatible con las herramientas para la elaboración de sistemas usadas en la institución y que contenga lógica cronológica en sus respectivas fases, pero fundamentalmente, deberá incluir el acompañamiento de los usuarios.

63. El desarrollo de aplicaciones informáticas debe estar orientado al funcionamiento a largo plazo y bajo un principio que le permita adaptarse a múltiples operaciones y transacciones que mantendrán la integridad en la información, de tal manera que se reproduzca la historicidad, la prontitud y demás aspectos que reflejen la calidad de la información contenida en las Bases de Datos y así contribuir a los indicadores establecidos para la toma de decisiones.

64. Toda generación de información o reportes de las Bases de Datos, nuevos módulos informáticos y cambios en sistemas, debe ser solicitada por el responsable de la oficina interesada por escrito o correo electrónico al departamento de tecnología e innovación

CONTINGENCIAS INFORMÁTICAS

65. Ante cualquier riesgo que afecte o dañe sus datos, cada Unidad de Gestión deberá mantener un respaldo en dispositivos externos. Para tal medida puede solicitar apoyo al departamento de tecnología e innovación para ser almacenado en los servidores, cuando la capacidad de almacenamiento lo permita.

66. El departamento de tecnología e innovación contará con un Plan de Contingencias Informáticas (incluidas en este manual) que incluya al menos los siguientes puntos:

- a) Procedimientos alternos que garanticen la continuidad de las operaciones informáticas de cada Unidad de gestión.
- b) Garantizar los respaldos de información en un lugar seguro, fuera del espacio en el que se encuentran los Servidores.
- c) Fortalecer y continuar con el apoyo por medios de almacenamiento o en forma documental, de las transacciones diarias para reconstruir los archivos dañados.
- d) Contar con un servidor remoto para mantener un respaldo de datos y registro de transacciones fuera de la institución.

MONITOREO

67. El departamento de tecnología e innovación será la responsable de efectuar periódicamente la verificación del cumplimiento de estas Normas y Políticas. Cada eventualidad será sujeta a un registro en bitácora en una base de datos, de la gravedad y continuidad de la irregularidad esta se le informará por escrito al Jefe de Tecnología y al Gerente General para la aplicación de sanciones administrativas correspondientes.

RESTRICCIONES

68. Queda prohibido, a otras áreas distintas al departamento de tecnología e innovación:

- a) La manipulación o extracción de piezas internas de los equipos informáticos.
- b) La instalación de Software.
- c) Acceso al área de Servidores.

69. El presente documento es un marco de referencia para los usuarios de la Alcaldía Municipal de San Martín y en virtud de la imposibilidad de enumerar todos los elementos existentes en referencia a las Tecnologías de Información (TI), dejamos aquí constancia de que todo aquello que no se encuentra expresamente permitido se encuentra restringido.

SANCIONES

70. El inadecuado uso o incumplimiento de las políticas de Tecnologías de Información Municipal, será sancionado por el Concejo Municipal en los términos que establecen la normativa vigente y los procedimientos administrativos existentes en la Alcaldía Municipal de San Martín.

GLOSARIO

AMENAZA: es un evento que puede desencadenar un incidente dentro de la municipalidad, produciendo daños materiales o pérdidas inmateriales en sus activos.

AMSM: Alcaldía Municipal de San Martín.

CONTINGENCIA: interrupción de la capacidad de acceso a información y procesamiento de la misma a través de computadoras necesarias para la operación normal de un negocio.

FIREWALL: es español “Cortafuegos”, es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

POLITICA DE TI: conjunto de lineamientos, directrices, reglas y procedimientos, que se deben implementar por todos los empleados que hacen uso de la infraestructura tecnológica existente en la Alcaldía Municipal de San Martín, siendo responsabilidad de los Gerentes, Jefes, Supervisores y coordinadores, vigilar y hacer cumplir su estricta aplicación y observación en el ámbito de su competencia, tomando las medidas preventivas y correctivas que fuesen necesarias.

PLAN DE CONTINGENCIA: Conjunto de pasos o procedimientos necesarios para recuperar y estabilizar las operaciones informáticas en la Entidad, en caso de producirse una eventualidad que afecte la operación normal de los sistemas de información. Dicho plan contiene las medidas técnicas, humanas y organizativas necesarias para garantizar la continuidad de las operaciones de una compañía.

SEGURIDAD DE LA INFORMACIÓN: Es el conjunto de medidas preventivas y reactivas de las instituciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma.

TI: Tecnologías de Información.

UNIDAD DE GESTIÓN: Unidades operativas que realicen interacción con los sistemas informáticos.