MUNICIPALIDAD DISTRITAL DE ATE

Resolución de Gerencia Municipal N° 094

Ate, 10 OCT. 2016

VISTO; los Informes N° 057 y 077-2016-MDA/GPE-SGPMI, de la Sub Gerencia Planeamiento y Modernización Institucional; el Informe N° 740-2016-MDA/GAJ de la Gerencia de Asesoría Jurídica; el Proveído N° 1321-2016-MDA/GM de la Gerencia Municipal; y,

CONSIDERANDO:

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

Que, mediante Informe N° 057-2016-MDA/GPE-SGPMI, de fecha 30 de junio del 2016, la Sub Gerencia de Planeamiento y Modernización Institucional, presenta el Proyecto de **"Directiva para la Implementación de Lineamientos de Seguridad de la Información en la Municipalidad Distrital de Ate"**, señalando que la presente propuesta contiene las definiciones a ser aplicadas en su implementación, así como las disposiciones específicas siguientes: i) De medidas de seguridad, acciones de detección y de recuperación; ii) De las acciones de prevención con relación a las áreas de trabajo y a las aplicaciones utilizadas; iii) De los Sistemas de redes con relación a los sistemas de red local y de conectividad a internet, y con relación a la gestión del servidor web y servidor de correo electrónico; iv) De la seguridad física, recomendando mantenimiento preventivo y correctivo; v) De la documentación, teniendo en cuenta el nivel de importancia de la información; vi) Del respaldo de la información, para minimizar los daños y proteger la información; emitiendo su opinión técnica favorable sobre el proyecto, el mismo ha sido propuesto por la Gerencia de Tecnologías de la Información, derivando el proyecto final sugiriendo se eleve, de encontrarlo conforme a la Alta Dirección para su trámite de aprobación;

Que, mediante Resolución N° 246-2007-PCM, se aprueba el Uso Obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 17799: 2007 EDI Tecnologías de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2da. Edición, en todas las entidades integrantes del Sistema Nacional de Informática. La acotada norma establece que "La seguridad de la información protege a esta de un amplio rango de amenazas para asegurar la continuidad del negocio, minimizar los daños a la organización y maximizar el retorno de las inversiones y las oportunidades de negocios. La seguridad de la información se consigue implantando un conjunto adecuado de controles, que pueden ser políticas, prácticas, procedimientos, estructuras organizativas y funciones de software y hardware. Estos controles necesitan ser establecidos, implementados, monitoreados, revisados y mejorados donde sea necesario, para asegurar que se cumplan los objetivos específicos de seguridad y negocios de la organización";

Que, mediante Ordenanza N° 385-MDA, publicada en el diario oficial "El Peruano" con fecha 20-01-2016, se aprobó la nueva Estructura Orgánica y el Reglamento de Organización y Funciones – ROF de la Municipalidad de Ate, la cual establece en su artículo 19° inciso s)., que es función del Gerente Municipal, entre otras "Emitir Resoluciones de Gerencia Municipal en el ámbito de competencia, así como aquellos asuntos delegados por el Alcalde y aquellos que aprueban Directivas y Manuales de Procedimientos Administrativos";

Que, el Artículo 89° inciso f), del Reglamento de Organización y Funciones (ROF) establece que es función de la Sub Gerencia de Procesos y Modernización Institucional, entre otras, "Proponer proyectos de normas y directivas relacionadas con el desarrollo de la organización municipal y de gestión de la calidad total, así como brindar opinión técnica de acuerdo a su competencia a directivas y procedimientos formulados por las demás unidades orgánicas de la Municipalidad";

Que, mediante Informe N° 740-2016-MDA/GAJ, de fecha 15 de julio del 2016, la Gerencia de Asesoría Jurídica, indica que el proyecto de Directiva se encuentra acorde a la normatividad vigente sobre la materia, el mismo que tiene como objeto establecer las normas y procedimientos técnicos para garantizar la confidencialidad, integridad y disponibilidad de la información presentada al ciudadano a través de los diferentes medios, así como disminuir los riesgos en la gestión de la información por parte del usuario dentro de la Red Municipal. Por lo expuesto, la Gerencia de Asesoría Jurídica es de **OPINION** que es procedente la aprobación de la **"Directiva para la Implementación de Lineamientos de**

Seguridad de la Información en la Municipalidad Distrital de Ate", presentada por la Sub Gerencia de Planeamiento y Modernización Institucional, la cual deberá realizarse mediante Resolución de Gerencia Municipal;

Que, mediante el Proveído N° 1321-2016-MDA/GM, la Gerencia Municipal, señala se proyecte la Resolución de Gerencia Municipal correspondiente;

ESTANDO A LOS FUNDAMENTOS EXPUESTOS EN LA PARTE CONSIDERATIVA, EN ESTRICTA OBSERVANCIA DE SUS FUNCIONES Y LAS FACULTADES CONFERIDAS EN LA ORDENANZA N° 385-MDA QUE APRUEBA EL REGLAMENTO DE ORGANIZACIÓN Y FUNCIONES DE LA MUNICIPALIDAD DISTRITAL DE ATE Y EN VIRTUD A LO DISPUESTO EN LA LEY DEL PROCEDIMIENTO ADMINISTRATIVO GENERAL N° 27444;

RESUELVE:

Artículo 1°.- **APROBAR;** la Directiva N° 010-2016-MDA/GPE-SGPMI **"Directiva para la Implementación de Lineamientos de Seguridad de la Información en la Municipalidad Distrital de Ate"** que como anexo forma parte integrante del presente, en mérito a las consideraciones antes expuestas.

Artículo 2°.- **ENCARGAR;** el cumplimiento de la presente Directiva a la Gerencia Municipal, Gerencia de Administración y Finanzas, Gerencia de Planificación Estratégica, Sub Gerencia de Planeamiento y Modernización Institucional, y demás áreas pertinentes de la Corporación Municipal.

REGÍSTRESE, COMUNÍQUESE Y CÚMPLASE.

MUNICIPALIDAD DE ATE
Abog. ADALBERTO GUARDIAN RAMIREZ
Gerente Municipal

DIRECTIVA N° 010-2016-MDA/GPE-SGPMI

DIRECTIVA PARA LA IMPLEMENTACIÓN DE LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA MUNICIPALIDAD DISTRITAL DE ATE

1. OBJETIVO.

Establecer las políticas y procedimientos técnicos para garantizar la confidencialidad, integridad y disponibilidad de la información presentada al ciudadano a través de los diferentes medios, así como disminuir los riesgos en la gestión de la información por parte del usuario dentro de la Red Municipal.

1.1. OBJETIVOS ESPECÍFICOS.

1.1.1. Conservar, salvaguardar y proteger la información producida por los procesos que se realizan en la institución, evitando su posible pérdida mediante exposición a amenazas latentes en el entorno, como acceso no autorizado, manipulación o deterioro de la información en forma accidental o deliberada.

1.1.2. Comunicar al personal de la institución sobre las normas sobre seguridad de la información que se contemplan en la presente directiva.

1.1.3. Establecer las reglas a seguir y las responsabilidades de los usuarios sobre el uso de información.

1.1.4. Establecer políticas para el registro ordenado de la información en miras de formular las bases de gestión del conocimiento.

2. FINALIDAD.

Lograr niveles adecuados de integridad, confidencialidad y disponibilidad para toda la información institucional relevante, con el objeto de asegurar continuidad operacional de los procesos y servicios que desarrolla la Municipalidad Distrital de Ate, mediante el resguardo de los activos de información asociados a los procesos críticos del negocio y su soporte.

3. BASE LEGAL.

3.1. Constitución Política del Perú.
3.2. Ley N° 27972 Ley Orgánica de Municipalidades.
3.3. Ley N° 27444 Ley del Procedimiento Administrativo General y sus modificatorias.
3.4. Decreto Supremo N° 033-2005-PCM, Reglamento del Código de Ética de la Función Pública.
3.5. Resolución Ministerial N° 004-2016-PCM, Aprueba el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/ IEC 27001:2014 EDI Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos 2da Edición" en todas las entidades integrantes del Sistema Nacional de Informática.
3.6. R.M. Nº 246-2007-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana NTP-ISO/IEC 17799:2007 EDI Tecnologías de la Información. Código de Buenas Prácticas para la Gestión de la Seguridad de la Información. 2da. Edición en todas las Entidades integrantes del Sistema Nacional de Informática.
3.7. Ordenanza N° 385-MDA, aprueba la nueva Estructura Orgánica y Reglamento de Organización y Funciones – ROF de la Municipalidad Distrital de Ate.

4. DEFINICIONES.

4.1. Confidencialidad.- De acuerdo a la norma ISO/IEC 27001:2011, es aquella característica que permite garantizar que la información en cualquier medio sólo será vista y accedida por personas autorizadas.

4.2. Información.- Se le llama información al conjunto de elementos de contenido que dan significado a las cosas, objetos y entidades del mundo a través de códigos y modelos. Para la Informática, la información es el conjunto de datos organizados y procesados que constituyen mensajes, instrucciones, operaciones, funciones y cualquier tipo de actividad que tenga lugar en relación con un ordenador.
La información puede encontrarse en formato papel, almacenada electrónicamente, enviada por correo electrónico, en formato vídeo o a través de una conversación hablada personalmente, entre otros.

4.3. Sistema de Gestión de Seguridad de la Información (SGSI).- Es aquel que ayuda a proteger la información de un amplio rango de amenazas diferentes con el que asegurar la continuidad de las operaciones de la Entidad, disminuyendo cualquier daño que se haya generado en la organización.

4.4. Control.- De acuerdo a la NTP-ISO/IEC 17999:2007, es una herramienta de gestión del riesgo, que incluye normas, procedimientos, estándares, estructuras organizacionales, de naturaleza administrativa, técnica, gerencial o legal.

4.5. Disponibilidad.- De acuerdo a la norma ISO/IEC 27001:2011, es aquella característica que permite garantizar que la información en cualquier medio siempre estará disponible en el momento que se necesite consultar o acceder.

4.6. Integridad.- De acuerdo a la norma ISO/IEC 27001:2011, es aquella característica que permite garantizar que la información en cualquier medio sólo será modificada por personas autorizadas.

4.7. Propietario de la Información.- Es cualquier persona o entidad a la cual se le asigna la responsabilidad formal de custodiar y asegurar un activo de información o un conjunto de ellos.

4.8. Usuario.- Puede ser definido como aquella persona que interactúa con la computadora a nivel de aplicación. En Informática, un usuario es un individuo que utiliza una computadora, sistema operativo, servicio o cualquier sistema informático. Por lo general es una única persona.
Un usuario generalmente se identifica frente al sistema o servicio utilizando un nombre de usuario (login/nick) y a veces una contraseña, este tipo es llamado usuario registrado. Por lo general un usuario se asocia a una única cuenta de usuario, en cambio, una persona puede llegar a tener múltiples cuentas en un mismo sistema o servicio (si eso está permitido).

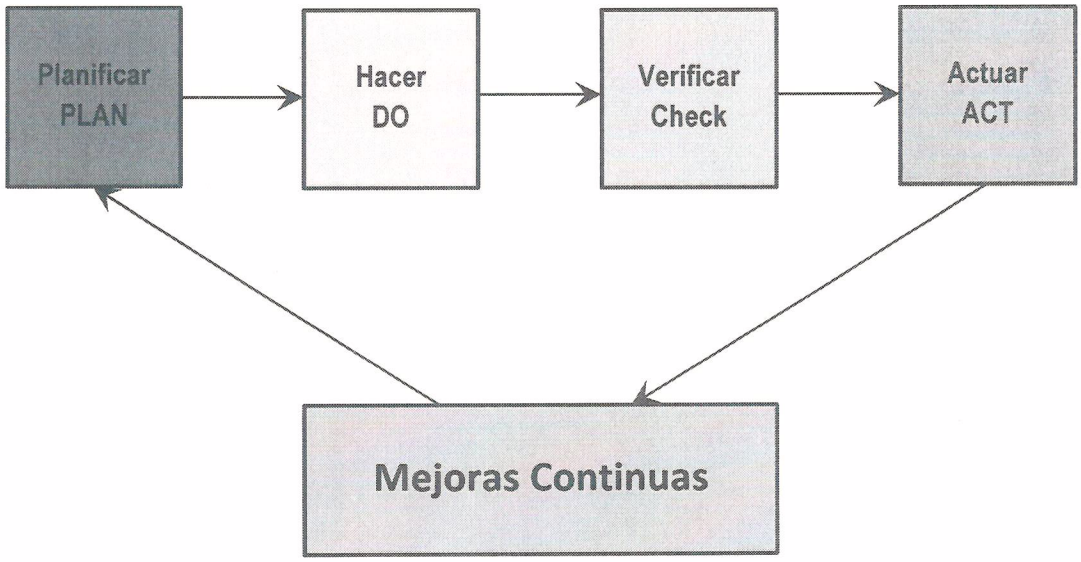
4.9. Clave de Acceso.- Una clave de acceso es una combinación de letras, números y signos que debe teclearse para obtener acceso a un programa o partes de un programa determinado, un terminal u ordenador personal, un punto en la red, etc. Muchas veces se utiliza la terminología inglesa "password" para referirse a la clave de acceso. Entre las recomendaciones más habituales a la hora de elegir una clave de acceso, está el no utilizar nombres pertenecientes a familiares o amigos, fechas concretas (nacimiento, aniversario),

nombres de mascotas, o palabras con significado (clave, acceso, etc.). Los expertos aconsejan utilizar una combinación de letras, números y signos («h+gy7/6t», por ejemplo) que debe cambiarse con relativa frecuencia.

4.10. Login.- Entrada de identificación, conexión. Sinónimo de nombre de usuario. Es una combinación de números y letras que sirve para identificar a un usuario dentro del sistema. Un proceso con el que se denomina el comienzo de una sesión en un sistema informático, usualmente compuesto por el pedido de un nombre de usuario (user name) y una clave (password), como medio fehaciente de autentificar la identidad del usuario.

4.11. Seguridad de la información (modelo PDCA).-Dentro de la organización el tema de la seguridad de la información es un capítulo muy importante que requiere dedicarle tiempo y recursos. La organización debe plantearse un Sistema de Gestión de la Seguridad de la Información (SGSI).
El objetivo de un SGSI es proteger la información y para ello lo primero que debe hacer es identificar los 'activos de información' que deben ser protegidos y en qué grado.
Luego debe aplicarse el plan PDCA ('PLAN – DO – CHECK – ACT'), es decir Planificar, Hacer, Verificar, Actuar y volver a repetir el ciclo.
Se entiende la seguridad como un proceso que nunca termina ya que los riesgos nunca se eliminan, pero se pueden gestionar. De los riesgos se desprende que los problemas de seguridad no son únicamente de naturaleza tecnológica, y por ese motivo nunca se eliminan en su totalidad.

Un SGSI siempre cumple cuatro niveles repetitivos que comienzan por Planificar y terminan en Actuar, consiguiendo así mejorar la seguridad.



* **PLANIFICAR (Plan):** Consiste en establecer el contexto en el que se crean las políticas de seguridad, se hace el análisis de riesgos, se hace la selección de controles y el estado de aplicabilidad.

* **HACER (Do):** Consiste en implementar el sistema de gestión de seguridad de la información, implementar el plan de riesgos e implementar los controles.

* **VERIFICAR (Check):** Consiste en monitorear las actividades y hacer auditorías internas.

* **ACTUAR (Act):** Consiste en ejecutar tareas de mantenimiento, propuestas de mejora, acciones preventivas y acciones correctivas.

4.12. Bases de la Seguridad Informática.- En general, un sistema será seguro o fiable si podemos garantizar tres aspectos:

- **Confidencialidad**: acceso a la información solo mediante autorización y de forma controlada.
- **Integridad**: modificación de la información solo mediante autorización.
- **Disponibilidad**: la información del sistema debe permanecer accesible mediante autorización.

5. ALCANCE.

Las normas y procedimientos establecidos en la presente Directiva son de cumplimiento obligatorio para todos los órganos y/o unidades orgánicas de la Municipalidad Distrital de Ate.

6. RESPONSABILIDAD.

Los Gerentes, Subgerentes, Secretario General, Procurador Público Municipal y demás funcionarios públicos de la Municipalidad Distrital de Ate, son los responsables de la implementación y cumplimiento de la presente Directiva.

La Responsabilidad recae también en todos los trabajadores independientemente del régimen laboral que tengan con la Corporación Municipal, tratándose de un mecanismo de seguridad de la información.

La Gerencia de Tecnologías de la Información es responsable de la implementación, aplicación, seguimiento y supervisión para el estricto cumplimiento de la presente Directiva.

7. DISPOSICIONES GENERALES.

7.1. Los Gerentes, Subgerentes, Secretario General, Procurador Público Municipal y demás funcionarios públicos de la Municipalidad Distrital de Ate, son los responsables directos del

buen uso de la información en sus respectivas unidades orgánicas.

7.2. La Municipalidad Distrital de Ate garantizará la aplicación de las medidas de seguridad de la información establecidas y optimizará su gestión mediante la conformación del Comité de Seguridad de la Información, el Oficial o Coordinador.

7.3. La Alta Dirección reconoce como activos de información estratégicos de la corporación municipal, la información contenida en cualquier medio y sistemas que la soportan. Por lo tanto las directivas de seguridad de la información es de aplicación obligatoria para todo el personal.

7.4. Cuando exista la necesidad de otorgar algún acceso lógico y físico a los servicios, tecnologías de la información u oficinas de la institución a personas o empresas que no tengan ningún vínculo directo y/o contrato, deberán ejecutarse medidas que garanticen la seguridad de la información, las cuales serán establecidas previamente por la Gerencia de Tecnologías de la Información y los responsables de las unidades orgánicas de la entidad.

7.5. En todos los contratos suscritos ya sea por prestación de servicios personales, servicios para la administración y control de los sistemas de información, redes y/o ambientes de procesamiento de información, consultorías, servicios entre otros, se deberá establecer la inclusión de términos relacionados a la seguridad de la información.

7.6. La Gerencia de Tecnologías de la Información es el órgano rector de las actividades informáticas y responsable de la administración de los sistemas implementados en la Entidad.

7.7. La Subgerencia de Recursos Humanos debe implementar dentro de su procedimiento de reclutamiento de personal, la firma por parte del nuevo personal de un acta de compromiso de conocimiento y aplicación de la presente directiva, así como de otros documentos que aseguren el correcto uso de la información de la Corporación Municipal.

8. DISPOSICIONES ESPECÍFICAS.

8.1. DE MEDIDAS DE SEGURIDAD.

8.1.1. Con relación a las medidas de seguridad presentadas en la Municipalidad.

a. La Gerencia de Tecnologías de la Información, en el marco de un plan de seguridad de la información, deberá implementar las medidas antes mencionadas, debiendo contar con la infraestructura adecuada.

b. La Gerencia de Tecnologías de la Información, debe informar periódicamente a los usuarios de las restricciones de seguridad implantadas en la institución, para proteger la información gestionada para los servicios.

c. La Gerencia de Tecnologías de la Información por lo menos una vez al año deberá realizar un inventario de los activos de la información en la cual indique el tipo de activo, clasificación, propietario el cual se le dará la responsabilidad respectiva en el uso adecuado del activo.

d. Crear las políticas e implementar los controles de la seguridad física, mediante la generación de perímetros de seguridad de protección de los activos informáticos.

e. La información que se procesa será respaldada por periodos, de acuerdo a la frecuencia de modificación de la información.

f. Una vez concluido el proceso de respaldo de la información, se realizará una prueba de funcionamiento utilizando el medio de respaldo, para comprobar que las copias se han realizado con éxito.
g. La información almacenada se mantendrá por un período que estime conveniente la institución, en concordancia con las normas establecidas por la autoridad competente.
h. La actividad de respaldo de la información, será supervisada por el responsable de la Seguridad de la Información de la Institución.
i. Las copias de respaldo (backup) se almacenarán en la caja fuerte de la municipalidad, en sobre lacrado. De ser posible se deberá contratar almacenamiento fuera de las instalaciones del Centro de Cómputo como medida de control de seguridad.

8.1.2. Acciones de Detección.

a. Revisar periódicamente las últimas actividades realizadas en la base de datos en busca de acciones sospechosas, efectuadas por usuarios externos o internos, mediante controles preventivos adecuados, como detectores de intrusos, registros de auditoria, entre otras.
b. Configurar el sistema y guardar periódicamente sus resultados en un medio confiable. Realizar comparaciones periódicas de la configuración operativa actual con la configuración inicial.
c. Comprobar periódicamente la integridad de los archivos importantes del sistema.
d. Verificar periódicamente los permisos de los archivos que se encuentren en los directorios de usuarios.
e. Asegurar que los eventos *y* debilidades en la seguridad de la información asociados con los sistemas de información, sean comunicados de manera que se tomen las acciones correctas a tiempo.

8.1.3. Acciones de Recuperación.

a. Disponer de procedimientos de contingencias, que permitan minimizar los daños y proteger la información del servicio a nivel bases de datos, aplicaciones, configuración de los sistemas operativos y de comunicaciones; para ello es necesario contar con un sistema de respaldo de información (backup).
b. Los procedimientos de contingencias, deberán ser debidamente documentados y difundidos entre el personal responsable y operativo de la Gerencia de Tecnologías de la Información.
c. La Gerencia de Tecnologías de la Información, deberá planificar el desarrollo de un plan de contingencia que incluya identificación de riesgo, identificación de soluciones, estrategias, documentación de procesos, realización de pruebas, implementación y mejoras.
d. Establecer periódicamente cursos de capacitación y simulacros, que permitan evaluar la respuesta del personal involucrado en la recuperación de contingencia, de sistemas completos (sistema operativo, aplicaciones, servicios y datos).

8.2. DE LAS ACCIONES DE PREVENCIÓN.

8.2.1. Con relación a las áreas de trabajo y a las aplicaciones utilizadas.

a. La Gerencia de Tecnologías de la Información, debe brindar a los usuarios acceso restringido, de acuerdo a sus funciones y responsabilidades asignadas al personal autorizado.
b. La información, servicios y procedimientos administrativos a proveer a la ciudadanía, deben administrarse por medios electrónicos con aplicaciones seguras.
c. Debe incorporarse un sistema de seguridad antivirus, a los servidores que gestionan las bases de datos, y en las estaciones donde se procesa la información.
d. Se recomienda incluir una herramienta de detección de intrusos y control de accesos, para proteger la información de carácter confidencial de la institución.
e. Disponer de copias completas de seguridad (backup) de la información, base de datos y aplicativos, con herramientas de respaldo en línea que evite interrumpir los servicios de los servidores.
f. Disponer de dispositivos para copias de respaldo (backup), Discos Duros de tecnología SCSI o SATA conforme a los Servidores, para un respaldo adecuado.
g. Resolver el problema de administración de cuentas y grupos para tener el absoluto control de quiénes son las personas autorizadas y con derechos en los recursos de almacenamiento. Debe existir un registro de usuarios con sus derechos y privilegios.
h. Tener una adecuada alimentación eléctrica, que involucra el estado de los pozos a tierra, estabilizador, UPS (Suministro de Poder Ininterrumpido), grupo electrógeno y redes de alimentación eléctrica independientes.

8.3. DE LOS SISTEMAS DE REDES.

8.3.1. Con relación a los sistemas de red local y de conectividad a Internet.

a. La red local y el sistema de conectividad a Internet deben contar con sistemas de seguridad.
b. Debe tenerse en consideración la aplicación de todas las técnicas de seguridad que se evalúen como convenientes: Cortafuegos, detección de intrusos, inspección de contenido, auditoria, filtrado, Proxy, criptografía o autenticación; que permitan controlar la seguridad de los usuarios de la red local y del sistema de conectividad a Internet.
c. Implementar políticas de restricción en la asignación de las direcciones IP, en los usuarios.
d. Se tener actualizado la estructura de la red de datos y comunicaciones, identificando locales, equipos utilizados, ips y demás información relevante para su supervisión.
e. Dadas las acciones de control en los equipos, sobre el bloqueo de programas como Facebook, twitter, youtube y otros que la entidad considere necesario limitar, se considerará como falta de parte del usuario, el vulnerar dichas configuraciones a fin de recuperar dichos accesos.

8.3.2. Con relación a la gestión del servidor web y servidor de Correo Electrónico.

a. Cerrar los servicios de comunicación del servidor, que no sean estrictamente necesarios y en especial los script CGI y los módulos de los aplicativos que soportan la identificación para acceso remoto (login remoto).
b. Minimizar el número de aplicaciones y archivos abiertos en los servidores.
c. Implementar políticas de control de acceso (deshabilitar las cuentas del sistema a usuarios que dejaron de laborar en la institución, personal con licencia,

control de horario en cuentas, deshabilitar las cuentas de usuarios que no se conecten al sistema durante un período de tiempo determinado por el administrador, etc.).

d. Implementar procedimientos de validación del servicio de datos y otros procesos, para garantizar los servicios de 7 días por 24 horas.

8.4. DE LA SEGURIDAD FÍSICA.

8.4.1. Se recomienda que los equipos donde se graba la información reciban mantenimiento preventivo y correctivo, con una frecuencia de acuerdo a las especificaciones técnicas del equipo o a un cronograma establecido.

8.4.2. Se deben desarrollar documentos normativos y guías de seguridad en el buen uso y tratamiento de los equipos, para poder brindar seguridad física de los activos más importantes de la Municipalidad.

8.4.3. Los ambientes donde se guardan los medios de almacenamiento de la información contarán con adecuadas condiciones de temperatura, humedad, entre otras.

8.4.4. Los ambientes donde se encuentran los medios de almacenamiento serán de acceso restringido, sólo estará autorizado el ingreso al personal responsable de la Seguridad de la Información.

8.5. DE LA DOCUMENTACIÓN.

8.5.1. La Gerencia de Tecnologías de la Información, planificará y organizará el proceso del respaldo de la información de la institución, teniendo en cuenta el nivel de importancia de la información. El procedimiento formará parte del Plan de Seguridad de la Información institucional.

8.5.2. La Gerencia de Tecnologías de la Información, especificará y documentará, en el Plan de Contingencias institucional, los procedimientos utilizados en el respaldo de la información, plan que debe considerarlo siguiente:

a. El respaldo de la configuración de los servidores y estaciones cliente, que permitan su puesta en marcha ante una eventual contingencia.

b. Los procedimientos para realizar el respaldo y la restauración de la información, a nivel de los servidores y estaciones cliente.

8.5.3. Se documentará las funciones y responsabilidades asignadas a las personas encargadas del proceso de respaldo de la información.

8.6. DEL RESPALDO.

8.6.1. La Gerencia de Tecnologías de la Información, dispondrá de un sistema de respaldo de información para minimizar los daños y proteger la información procesada, al nivel de base de datos, aplicaciones, configuración de los sistemas operativos y de comunicaciones.

8.6.2. Dependiendo de la importancia del servicio que preste la Municipalidad y con la finalidad de asegurar la continuidad de sus operaciones, ésta dispondrá de un sistema de respaldo de información en línea (dos sistemas de respaldo de información simultáneos), de acuerdo a su disponibilidad presupuestal.

8.6.3. Se realizarán copias de seguridad de la información en medios de almacenamiento cada vez que los archivos o bases de datos se actualicen, estas copias se podrán efectuar en tres formas:

a. ***Respaldo Total:*** copia completa de todos los archivos en un solo medio de almacenamiento.
b. ***Respaldo Incremental:*** copia de todos los cambios o adiciones que se realizan a determinados archivos cada día.
c. ***Respaldo Diferencial:*** copia de cambios o adiciones que se realizan a determinados archivos respectó al respaldo total, después de cierto período de tiempo.

8.6.4. Los usuarios que tienen asignada una computadora, son responsables de realizar el respaldo de la información local, de acuerdo al período establecido en el plan de respaldo de la información institucional, para lo cual la Gerencia de Tecnologías de la Información, facilitará los recursos necesarios y guardará la copia de los mismos. Para los casos de mayor riesgo, de acuerdo a la disponibilidad del servidor, podrán guardar su información en carpetas compartidas, en las cuales se realizarán las copias de respaldo adicional.

8.6.5. El disco duro será depurado permanentemente, eliminando o realizando una copia de los archivos que no volverán a ser utilizados en forma inmediata.

8.6.6. El responsable del respaldo proporcionará a los usuarios las copias de seguridad de la información, base de datos y aplicativos, en caso de pérdida o daño de la información residente en el medio local.

8.6.7. Se informará periódicamente a los usuarios, el cronograma de respaldo de información, asimismo, hará de conocimiento general las políticas de seguridad y respaldo de información.

9. ASPECTOS COMPLEMENTARIOS.

9.1. La Gerencia de Tecnologías de la Información brindará el asesoramiento y apoyo técnico correspondiente.

9.2. El traslado de información interno o externo debe ser autorizado por el funcionario responsable que genera la información o su inmediato superior de ser necesario.

9.3. Los archivos digitales cualquiera sea su origen (hoja de cálculo, procesador de texto u otros), no deben contener claves que restrinjan su visualización salvo orden o autorización expresa del funcionario responsable.

9.4. Los datos, registros y todo tipo de recolección o generación de información generada como parte de las labores que desempeña un trabajador que presta servicios a la entidad municipal, son parte del archivo digital de la misma; motivo por el cual debe proveer el acceso a dicha información en caso de vacaciones, permisos programados, suspensión, cese u otro tipo de ausencia.

9.5. Las unidades orgánicas quedan encargados de comunicar y formular las disposiciones complementarias a su personal para la implementación de la presente directiva.

10. DISPOSICIONES COMPLEMENTARIAS FINALES.

PRIMERA.- Para los aspectos no previstos en la presente Directiva, se aplicarán supletoriamente las normas legales vigentes sobre la materia. Adicionalmente se deberá tener en cuenta la adecuación a cualquier norma legal que se establezca con posterioridad a la fecha de aprobación de la presente Directiva.

SEGUNDA.- La Subgerencia de Recursos Humanos en coordinación con la Gerencia de Tecnologías de la Información efectuarán periódicamente eventos de capacitación al personal de la Municipalidad Distrital de Ate, referidos a la normatividad vigente para el cumplimiento de la presente Directiva y de las normas legales sobre la materia.

TERCERA.- La Gerencia de Tecnologías de la Información podrá emitir disposiciones específicas en el marco de las normas establecidas en la presente Directiva.

CUARTA.- El incumplimiento de las disposiciones contenidas en la presente Directiva, por parte de cualquier servidor de la Municipalidad Distrital de Ate, deviene en responsabilidad del servidor infractor y del funcionario a cargo del Órgano y/o Unidad Orgánica a la que pertenece, por lo que se les aplicará las sanciones correspondientes de acuerdo a lo establecido por las normas legales vigentes y normas internas de la Corporación Municipal de acuerdo al Régimen laboral al que pertenezca.

QUINTA.- La Presente directiva entrará en vigencia a partir del día siguiente de su aprobación a través del correspondiente acto administrativo. Asimismo, será publicada en el portal institucional de la Corporación Municipal.