# REGLAMENTO DE SEGURIDAD INFORMÁTICA DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE GUAYAQUIL

M.I. MUNICIPALIDAD
DE GUAYAQUIL

**CONTENIDO**

# REGLAMENTO DE SEGURIDAD INFORMÁTICA DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE GUAYAQUIL

**OBJETIVO**

El presente reglamento tiene como finalidad establecer los principios, criterios y requerimientos de seguridad informática que garanticen la confidencialidad, integridad y disponibilidad de la información que se procesa, intercambia, reproduce y conserva mediante el uso de las tecnologías de información.

**RESPONSABLES**

**De su implementación:** Dirección de Informática
**De su cumplimiento:** Todo el personal del GADMG
**De su control:** Dirección de Informática
**De su seguimiento y evaluación:** Dirección de Desarrollo Institucional
**De su actualización:** Direcciones de Informática y de Desarrollo Institucional
**De su distribución y difusión:** Direcciones de Informática y de Desarrollo Institucional

## I. INTRODUCCIÓN

La base para que las organizaciones puedan operar de una forma confiable en materia de seguridad informática, comienza con la definición de normas que, en el caso de nuestra entidad, se definen en cuatro capítulos generales, a saber:

- Seguridad de Recursos Humanos
- Seguridad Lógica
- Seguridad Física
- Seguridad Legal

**Seguridad de Recursos Humanos**

Dentro de este capítulo se establecen los principios de seguridad de la tecnología de información que permiten asegurar que los empleados, contratistas y terceros, entiendan sus responsabilidades y sean idóneos para los roles que ejecutan, de tal forma que se reduzca el riesgo de robo, fraude y mal uso de los medios informáticos.

**Seguridad Lógica**

Establece e integra los mecanismos que permiten otorgar, controlar y monitorear el acceso a los programas y archivos de los sistemas de información automatizados.

**Seguridad Física**

En este nivel se identifican los límites mínimos que se deben cumplir respecto al control físico de los recursos tecnológicos, su acceso y la transferencia de información.

**Seguridad Legal**

Integra los requerimientos que deben cumplir los servidores municipales en relación a la normativa interna y externa en materia de seguridad informática.

## II. BASE LEGAL

El presente Reglamento de Seguridad Informática está fundamentado en las Normas de Control Interno emitidas por la Contraloría General del Estado. (*Publicadas en el Suplemento del Registro Oficial No. 87 del 14 de Diciembre del 2009, acuerdo N° 039-CG*) y, como referencia, se han considerado los dominios y objetivos de control de la norma internacional ISO/IEC 27002:2005.

## III. ÁMBITO DE APLICACIÓN

Es responsabilidad de todo usuario que tenga asignado un recurso tecnológico y que se encuentre en el ejercicio de sus funciones, ya sea personal interno o externo del GADMG, acatar lo indicado en el presente Reglamento.

## IV. CONTROL DEL REGLAMENTO

El Reglamento de Seguridad Informática ha tomado como referencia los objetivos de control de la Norma ISO/IEC 27002:2005; consecuentemente, las direcciones de Informática y de Desarrollo Institucional verificarán de manera oportuna y suficiente el cumplimiento de los mencionados controles, en el ámbito de sus competencias.

## V. ALCANCE

Establecer normas de seguridad de recursos humanos, lógicos, físicos y legales, para precautelar la integridad de los equipos de computación de la institución o de aquellos recibidos en comodato, así como garantizar la preservación de la información del GADMG.

Dotar de información a los usuarios del GADMG, respecto a las normas y mecanismos que deben cumplir y utilizar para proteger el hardware y software, así como la información que es almacenada y procesada en estos.

# M. I. CONCEJO MUNICIPAL DE GUAYAQUIL

## CONSIDERANDO

**QUE,** el artículo 238 de la Constitución de la República del Ecuador declara que, los gobiernos autónomos descentralizados gozarán de autonomía política, administrativa y financiera;

**QUE,** el artículo 425 del Código Orgánico de Organización Territorial, Autonomía y Descentralización, prescribe que es obligación de los gobiernos autónomos descentralizados velar por la conservación de los bienes de propiedad de cada gobierno y por su más provechosa aplicación a los objetos a que están destinados; y,

**QUE,** con la finalidad establecer los principios, criterios y requerimientos de seguridad informática que garanticen la confidencialidad, integridad y disponibilidad de la información que se procesa, intercambia, reproduce y conserva mediante el uso de las tecnologías de información, las Direcciones de Desarrollo Institucional y de Informática Municipal han elaborado un proyecto de reglamentación respecto de la seguridad informática de la Corporación Municipal.

En ejercicio de la facultad normativa que confiere el artículo 240 de la Constitución de la República, en armonía con lo previsto en los artículos 7 y 57 letra a) del Código Orgánico de Organización Territorial, Autonomía y Descentralización (COOTAD),

## EXPIDE

## EL REGLAMENTO DE SEGURIDAD INFORMÁTICA DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE GUAYAQUIL

## CAPÍTULO I

## SEGURIDAD DE RECURSOS HUMANOS

### 1.1 DE LA SEGURIDAD INFORMÁTICA RELACIONADA AL PERSONAL

**Art. 1** Los servicios de la red municipal de datos son de uso exclusivo para los usuarios del GADMG y de usuarios externos previamente autorizados por la autoridad competente.

**Art. 2** Es responsabilidad de los usuarios de bienes y servicios informáticos cumplir con lo establecido en el Reglamento de Seguridad Informática del GADMG.

**Art. 3** Se entregará al contratado toda la información necesaria para ejercer sus labores dentro de la institución, durante la vigencia de su contrato laboral.

**Art. 4** La información procesada, intercambiada, reproducida, almacenada y conservada en los computadores de la entidad, será considerada como municipal.

**Art. 5** Se consideran faltas graves el robo, daño, alteración de información de los sistemas automatizados de la entidad, el uso de los sistemas para ejecutar actos como piratería informática, penetración a otras redes, etc.; o que el usuario sea judicialmente declarado culpable de un delito informático.

**Art. 6** Cualquier acto negligente o ataque informático hacia los activos de información (redes, sitios, equipos, sistemas internos o externos) que cause o no daños a la información, será considerado como una falta grave y sancionado según lo establecido en la Ordenanza Reglamentaria del Talento Humano del GADMG.

## 1.2 RESPONSABILIDADES SOBRE ACTIVOS INFORMÁTICOS

**Art. 7** Todo equipo informático tendrá un custodio o responsable que velará por su cuidado y buen uso, debiendo responder en forma pecuniaria y directa en caso de cualquier pérdida o destrucción injustificada, de acuerdo con el Manual Específico para la Administración y Control de Bienes de Larga Duración que para el efecto emita la Municipalidad.

**Art. 8** Los administradores de sistemas (correo electrónico, intranet, internet, sistemas transaccionales y web, bases de datos y demás sistemas futuros), designados por la Dirección de Informática, serán los responsables de la seguridad de la información en el campo de sus competencias.

## 1.3 DE LA CAPACITACIÓN DE USUARIOS

**Art. 9** Todo funcionario, servidor o trabajador que ingrese a formar parte del GADMG, deberá recibir una inducción sobre el Manual de Políticas y Estándares de Seguridad Informática para Usuarios, donde se dan a conocer las obligaciones para los usuarios y las sanciones en caso de incumplimiento. Esta labor será realizada de manera coordinada entre las direcciones de: Recursos Humanos (Departamento de Capacitación), Informática (Departamento de Seguridad Informática) y Desarrollo Institucional (Departamento de Procesos Informáticos).

**Art. 10** Antes de realizar una capacitación al personal interno y externo de la institución, se tomarán las medidas de seguridad necesarias, tanto a nivel físico como lógico. La capacitación se llevará a cabo en equipos y programas del ambiente de pruebas.

## 1.4 DE LAS RESPUESTAS A INCIDENTES Y ANOMALÍAS DE SEGURIDAD INFORMÁTICA

**Art. 11** Las solicitudes de asistencia por parte de uno o más empleados, con problemas en las estaciones de trabajo, serán atendidas a través de la Mesa de Ayuda, de acuerdo a la disponibilidad de recursos o a las prioridades establecidas para el efecto.

**Art. 12** Cualquier situación anómala y contraria a la seguridad de la información, deberá ser tratada y documentada por un equipo de respuestas a

incidentes, con el objetivo de analizarla y dar una solución acorde al problema, ya sea esta en el ámbito técnico, legal o administrativo. Este equipo será designado por el director de Informática o la persona que él delegue para tal efecto.

## CAPÍTULO II

## SEGURIDAD LÓGICA

### 2.1 DE LAS POLÍTICAS Y ESTÁNDARES DE CONTROLES DE ACCESO LÓGICO

**Art. 13** Cualquier petición de información o servicios informáticos, provenientes de un determinado usuario o departamento, se deberá efectuar siguiendo los canales de gestión y niveles de autorización formalmente establecidos en la institución.

**Art. 14** Las direcciones de Informática y de Desarrollo Institucional mantendrán en la intranet la documentación relacionada a reglamentos, normas, guías, políticas y controles de Seguridad de Información, a la que tendrá acceso todo el personal del GADMG.

### 2.2 DE LA CLASIFICACIÓN DE LA INFORMACIÓN

**Art. 15** Las direcciones municipales deben considerar la clasificación de su información electrónica, de acuerdo a la importancia para la entidad y el cumplimiento de los requerimientos legales, a fin de establecer los parámetros para su acceso.

### 2.3 DE LA ADMINISTRACIÓN DE ACCESOS DE USUARIOS

**Art. 16** Son usuarios de la red municipal de datos todos aquellos a los que se les haya concedido los permisos correspondientes, siguiendo el procedimiento de Solicitud de Acceso al Sistema.

**Art. 17** Los usuarios tendrán acceso a sitios de la intranet una vez que se encuentren autenticados en la red municipal de datos y, de acuerdo a las funciones que desempeñen, se asignarán sus permisos correspondientes.

**Art. 18** Para el acceso a opciones consideradas como "restringidas", la Dirección de Informática solicitará que exista una autorización de la dirección propietaria de los datos, previo a otorgar el permiso correspondiente.

**Art. 19** Se considera usuario externo a cualquier persona natural o jurídica que tenga una relación con la institución fuera del ámbito de empleado, siempre que tenga una vinculación con los servicios de la red municipal de datos.

**Art. 20** El acceso a la red por parte de terceros es estrictamente restrictivo y permisible sólo mediante firma impresa de un acuerdo de confidencialidad hacia la institución, con el compromiso del uso exclusivo del servicio para el que fue provisto. Este tipo de acceso será autorizado por el director de Informática o su delegado.

**Art. 21** La contraseña de usuario de la red municipal de datos se establece siguiendo el procedimiento previsto en el Manual de Políticas de la Dirección de Informática.

## 2.4 DE LAS RESPONSABILIDADES DEL USUARIO

**Art. 22** El usuario será responsable exclusivo de mantener a salvo la privacidad de su contraseña.

**Art. 23** El usuario será responsable del buen uso de su cuenta de acceso a los sistemas o servicios.

**Art. 24** Es obligación del usuario cambiar la clave por defecto asignada por la Dirección de Informática.

**Art. 25** Se debe evitar guardar o escribir las contraseñas en cualquier papel o superficie, o dejar constancia de ellas.

**Art. 26** Las claves son individuales; está prohibido que los usuarios la compartan o revelen a terceros, siendo de su exclusiva responsabilidad el uso de la misma.

**Art. 27** Cuando a un usuario se le olvide, bloquee o caduque su contraseña, deberá solicitar a la Dirección de Informática el restablecimiento respectivo. Esta acción será realizada por el Departamento de Seguridad Informática tomando las medidas suficientes para evitar la suplantación de la identidad del empleado.

**Art. 28** El usuario deberá definir "contraseñas seguras", siguiendo los parámetros previstos en el Manual de Políticas de la Dirección de Informática.

**Art. 29** Cuando tengan que alejarse de sus estaciones de trabajo, los usuarios deberán bloquear, a través del sistema operativo, los equipos de computación a fin de proteger la información de accesos no autorizados.

**Art. 30** Cualquier usuario que encuentre una vulnerabilidad en la seguridad de los sistemas informáticos de la institución, sea porque la computadora que usa no tiene instaladas todas las actualizaciones del software de base, o su antivirus está desinstalado o deshabilitado, está obligado a reportarlo al Departamento de Seguridad Informática.

**Art. 31** El respaldo de la información que los usuarios mantengan en sus equipos de computación será de su exclusiva responsabilidad. La Dirección de Informática no se responsabilizará por la pérdida voluntaria o involuntaria de información en equipos.

**Art. 32** Será responsabilidad del jefe de Seguridad Informática deshabilitar del servicio de directorio de la red distribuida de computadores del GADMG, las cuentas de usuarios de los ex empleados municipales. En los casos de renuncia, se mantendrá un acceso limitado únicamente a las opciones que su jefe inmediato autorice durante el tiempo que la ley establece para la entrega definitiva de su cargo.

**Art. 33** Cuando exista la sospecha o el conocimiento de que alguna información haya sido revelada, alterada o borrada, sin la autorización respectiva, el usuario deberá notificar a la Dirección de Informática, que a su vez emprenderá el análisis correspondiente para determinar el origen, usuario y circunstancias de la actividad.

## 2.5 DEL USO DEL CORREO ELECTRÓNICO INSTITUCIONAL

**Art. 34** El correo electrónico es de uso exclusivo para los usuarios del GADMG; es personal e intransferible. A cada usuario se le creará su propia cuenta y está prohibido utilizar cuentas asignadas a otras personas para enviar o recibir mensajes de correo.

**Art. 35** El usuario será responsable de la información que sea enviada a través de su cuenta de correo electrónico.

**Art. 36** La Dirección de Informática podrá acceder y analizar los mensajes y archivos adjuntos enviados a través del correo institucional, al existir sospecha o denuncia de envío de información que comprometa la seguridad de la red, o cualquier otra acción no autorizada.

**Art. 37** Tanto los mensajes enviados y recibidos, así como los archivos adjuntos que salen y entran a los buzones institucionales, se consideran propiedad del GADMG.

**Art. 38** El usuario debe utilizar el correo electrónico exclusivamente para asuntos relacionados a las funciones que le fueron asignadas a su cargo, empleo o comisión. Se prohíbe utilizar el correo electrónico con fines personales para distribuir o reproducir información no relacionada a la institución.

**Art. 39** Queda prohibido suplantar, falsear o alterar la identidad de un usuario de correo electrónico.

**Art. 40** Queda prohibido el interceptar, ayudar a interceptar o revelar a terceros, las comunicaciones por correo electrónico.

**Art. 41** Se prohíbe utilizar en el correo institucional lenguaje inapropiado y/o palabras ofensivas que afecten la honra y estima de terceros.

**Art. 42** Para el envío de información reservada y/o confidencial, vía correo electrónico, se deberá utilizar la firma electrónica, y debe estar destinado exclusivamente a personas autorizadas y en el ejercicio estricto de sus funciones y atribuciones.

## 2.6 DE LA SEGURIDAD DE ACCESO A TERCEROS

**Art. 43** Todo usuario externo estará facultado a utilizar única y exclusivamente el servicio informático que le fue asignado, y asumir las responsabilidades de su uso.

**Art. 44** Los accesos a la red interna, por parte de terceros, contemplarán los mismos controles de acceso utilizados para los usuarios internos, además de los requisitos expuestos en sus contratos con el GADMG.

## 2.7 DEL CONTROL DE ACCESO A LA RED

**Art. 45** El acceso a la red interna será exclusivo a equipos de computación del GADMG; en caso de dispositivos particulares, se podrán conectar a la red excepcionalmente, siempre y cuando se justifique su propósito laboral y cumplan con los requisitos de seguridad y autenticación.

**Art. 46** Cualquier alteración del tráfico entrante o saliente a través de los dispositivos, será motivo de verificación y tendrá como resultado directo la realización de una auditoría a la red municipal de datos.

**Art. 47** Se registrará todo acceso a los dispositivos de red, mediante archivos de registro o archivos Log de sistemas.

**Art. 48** Será considerado como un ataque informático y una falta grave, cuando un usuario, con fines de detectar y explotar una posible vulnerabilidad, realice la exploración de los recursos informáticos o aplicaciones de la red municipal de datos.

**Art. 49** El director de Informática autorizará las restricciones de tiempo para las sesiones de trabajo de los usuarios, mientras que al jefe de Seguridad Informática le corresponderá verificar que el sistema lleve los registros de uso. Las restricciones de tiempo deben revisarse ante cualquier cambio del estado laboral del usuario, como ascenso, remoción o terminación de contrato.

**Art. 50** El director de Informática autorizará el acceso a la red inalámbrica interna, dependiendo de las características de seguridad del dispositivo con el que se desea conectar el usuario.

## 2.8 DEL CONTROL DE ACCESO AL SISTEMA OPERATIVO

**Art. 51** Los funcionarios del GADMG deberán tener en cuenta que la identificación del usuario y la contraseña, que les fueron asignados por la Dirección de Informática, son para el acceso al sistema operativo del computador y a otros servicios de información (tales como el e-Mas y SharePoint); por lo cual, tomarán las medidas de seguridad necesarias a fin de evitar accesos no autorizados por terceros.

## 2.9 DE LOS EQUIPOS SERVIDORES

**Art. 52** El acceso a la configuración del sistema operativo de los equipos servidores, es únicamente permitido a los administradores de sistemas designados por la Dirección de Informática.

**Art. 53** Los administradores de sistemas tendrán acceso único a los módulos de configuración de las respectivas aplicaciones que tienen bajo su responsabilidad.

## 2.10 DEL CONTROL DE ACCESO A LAS APLICACIONES

**Art. 54** La Dirección de Informática deberá definir y/o estructurar el nivel de permisos sobre las aplicaciones, de acuerdo a la ejecución o gravedad de las aplicaciones o archivos, y haciendo especial énfasis en los derechos

de escritura, lectura, modificación, ejecución o borrado de información. Para permitir el ingreso a los sistemas, la dirección solicitante deberá definir previamente los perfiles de acceso, de acuerdo a las funciones y jerarquías de los usuarios, así como rangos limitados de actividades (menús restringidos).

**Art. 55** La Dirección de Informática deberá habilitar un equipo servidor de prueba, en el que se realizará el control de calidad de cada programa, con el objetivo de evitar que en los sistemas de producción existan errores de fondo y forma.

**Art. 56** Se deberá llevar un registro mediante Log de aplicaciones, sobre las actividades de los usuarios en cuanto a accesos, errores de conexión, horas de conexión, intentos fallidos, terminal desde donde se conecta, entre otros, de manera que proporcionen información relevante y revisable posteriormente.

**Art. 57** Se prohíbe la instalación de software que no cuente con la licencia de uso; la responsabilidad que se origine en estos casos recaerá en el usuario que la realizó.

**Art. 58** Los usuarios que requieran utilizar un software que no sea propiedad del GADMG, deberán solicitarlo a la Dirección de Informática, justificando su uso e indicando el equipo de cómputo donde se instalará y el período de tiempo que permanecerá dicha instalación.

**Art. 59** Se considera una falta grave que los usuarios instalen cualquier tipo de programa (software), que no esté autorizado por la Dirección de Informática, en las computadoras a su cargo o cualquier equipo conectado a la red municipal de datos.

**Art. 60** La Dirección de Informática será la responsable de proveer las especificaciones técnicas ante la solicitud de adquisición o desarrollo de aplicaciones automatizadas que se requiera en la entidad, así como de evidenciar que la instalación del sistema nuevo no afecte adversamente la seguridad general ni los sistemas existentes.

**Art. 61** Todo sistema de información desarrollado o adquirido por el GADMG contará con programas, aplicaciones y procedimientos documentados, controles de acceso y seguridades, así como una segregación de funciones según el área y cargo competente, para salvaguardar la confidencialidad, integridad y disponibilidad de los datos.

## 2.11 DEL MONITOREO DE ACCESO Y USO DEL SISTEMA

**Art. 62** Se registrará y archivará toda actividad, procedente del uso de las aplicaciones, sistemas de información y uso de la red, mediante archivos de Log o bitácoras de sistemas.

**Art. 63** Los registros de Log almacenarán nombres de usuarios, nivel de privilegios, IP de terminal, fecha y hora de acceso o utilización, actividad desarrollada, aplicación implicada en el proceso, intentos de conexión fallidos o acertados, archivos a los que se tuvo acceso, entre otros, a fin de conocer las acciones que realizan los usuarios.

## 2.12 DE LA GESTIÓN DE OPERACIONES Y COMUNICACIONES

### 2.12.1 DE LAS RESPONSABILIDADES Y PROCEDIMIENTOS OPERATIVOS

**Art. 64** Las configuraciones y puesta en marcha de servicios de Tecnología de Información, son normadas por la Dirección de Informática.

**Art. 65** La Dirección de Informática es la responsable de mantener en óptimo funcionamiento los servicios informáticos del GADMG.

### 2.12.2 DE LA PLANIFICACIÓN Y ACEPTACIÓN DE SISTEMAS

**Art. 66** La Dirección de Informática establecerá una metodología para los procesos de: planificación, desarrollo, adquisición, implementación y/o adaptación de los sistemas automatizados necesarios para el GADMG.

**Art. 67** La Dirección de Informática es la responsable de actualizar las versiones de software, previo al análisis de los requerimientos técnicos necesarios.

**Art. 68** Cuando una de las direcciones del GADMG requiera un programa (software) específico (Autocad, Ms Project, etc.), deberá solicitar a la Dirección de Informática un informe técnico a fin de que se analice la factibilidad y parámetros de compatibilidad y seguridad acordes con los estándares técnicos municipales.

**Art. 69** La Dirección de Informática, a través de su Departamento de Producción, investigará programas (software) alternativos que pudieran beneficiar a la buena gestión de la institución en lo que se refiere a sistemas operativos, bases de datos, lenguajes de programación y otros propios de su ámbito de acción. Si otras direcciones requieren una aplicación automatizada para agilitar su trabajo, deberán solicitar asistencia a la Dirección de Desarrollo Institucional para definir y documentar los procesos de manera que la Dirección de Informática pueda programar o contratar el desarrollo respectivo.

**Art. 70** La aceptación y uso de los sistemas no impide que el Departamento de Seguridad Informática realice pruebas y controles sobre los sistemas a implementarse.

**Art. 71** El software desarrollado en la entidad debe cumplir con las normas internas de seguridad, por lo que antes de su implementación será revisado por el jefe de Seguridad Informática.

**Art. 72** Para la puesta en producción de un nuevo sistema, se deberá contar con la aprobación formal del área solicitante.

**Art. 73** Ningún usuario podrá realizar pruebas sobre sistemas en producción; por tanto, el testeo de aceptación por el área solicitante se lo realizará en el ambiente de control de calidad.

**Art. 74** Las solicitudes de modificación a los programas de un sistema automatizado que no signifiquen desarrollo de nuevos sistemas o subsistemas, pero que impliquen cambios en el proceso, serán

previamente evaluadas por la Dirección de Desarrollo Institucional; posteriormente, la Dirección de Informática será la responsable de la capacitación a los usuarios respecto a las modificaciones aplicadas en los sistemas.

### 2.12.3 DE LA PROTECCIÓN CONTRA SOFTWARE MALICIOSO

**Art. 75** Se adquirirá y utilizará software únicamente de fuentes reconocidas como confiables o referidas por sitios especializados en la evaluación de programas automatizados.

**Art. 76** La Dirección de Informática deberá contar con un equipo servidor dedicado exclusivamente para la gestión del software antivirus y sus funciones de actualización y protección de computadores en tiempo real.

**Art. 77** Es responsabilidad de cada usuario revisar, a través del software antivirus, todos los medios ópticos como discos compactos, discos de almacenamiento de datos, memorias USB, etc., para verificar que no tengan programas maliciosos, antes de usar esos dispositivos en su computadora.

**Art. 78** La Dirección de Informática será responsable de la instalación, configuración y actualización regular de los programas y sus últimas bases de datos, para la detección o reparación de códigos maliciosos.

**Art. 79** La Dirección de Informática configurará las herramientas de protección contra virus y códigos maliciosos, a fin de que los archivos adjuntos a los correos sean analizados previo a su descarga.

**Art. 80** El usuario que genere, compile, escriba, copie o propague programas o aplicaciones en cualquier código o lenguaje de computadora, que estén diseñados para auto-replicarse, dañar o borrar datos o impedir el funcionamiento de aplicaciones y programas autorizados o componentes del equipo computacional como memorias o periféricos, será sancionado como una falta grave de acuerdo a lo previsto en la Ordenanza Reglamentaria del Talento Humano del GADMG.

**Art. 81** Cualquier usuario que sospeche la infección de su equipo computacional con virus, troyano o cualquier otro código malicioso, no debe intentar erradicarlo por sí mismo, deberá dejar de usarlo inmediatamente y comunicar del particular a la Dirección de Informática, a través de la Mesa de Ayuda, para que se tomen las acciones respectivas de restablecimiento del equipo y eliminación del código malicioso.

**Art. 82** Los usuarios a quienes se les ha asignado equipos portátiles que no se conectan a la red municipal de datos, están en el deber de solicitar periódicamente a la Dirección de Informática la actualización del código antivirus.

**Art. 83** Queda prohibido a los usuarios modificar o eliminar la configuración de las consolas de antivirus instaladas en los equipos de computación.

**Art. 84** Ningún usuario, empleado o personal externo, podrá bajar o descargar software de sistemas, de mensajería instantánea y redes de

comunicaciones externas, sin la debida autorización de la Dirección de Informática.

### 2.12.4 DEL MANTENIMIENTO DEL SOFTWARE

**Art. 85** El mantenimiento de las aplicaciones y actualización de software de sistemas es de exclusiva responsabilidad del personal de la Dirección de Informática.

**Art. 86** Se llevará un registro global del mantenimiento efectuado sobre los equipos y cambios realizados desde su instalación.

### 2.12.5 DEL MANEJO Y SEGURIDAD DE MEDIOS DE ALMACENAMIENTO

**Art. 87** Es responsabilidad de los usuarios almacenar su información únicamente en la parte de disco duro identificada como "D:\Mis Documentos" ya que las otras están destinadas para archivos de programa y sistema operativo.

**Art. 88** Si un área desea bloquear los puertos de entrada (USB), solicitará a la Dirección de Informática que se implemente tales restricciones.

## 2.13 DEL SITIO WEB MUNICIPAL Y USO DEL INTERNET

**Art. 89** La Dirección de Informática será la responsable de la disponibilidad continua de los sitios web del GADMG.

**Art. 90** Los usuarios tendrán acceso a internet, siempre y cuando cuenten con la autorización del director del área en la que laboran, se cumplan con los requisitos mínimos de seguridad para acceder a este servicio y se acaten las disposiciones de conectividad de la Dirección de Informática.

Los usuarios con acceso a internet se sujetarán a las normas y políticas internas previstas en el documento de "Políticas de Uso del Internet del GADMG".

**Art. 91** El acceso a internet provisto a los usuarios del GADMG es exclusivamente para las actividades relacionadas con el puesto o función que desempeña y no para propósitos personales.

**Art. 92** Todos los accesos a internet tienen que ser realizados a través de los canales de acceso provistos por el GADMG. En caso de necesitar una conexión a internet especial, esta tiene que ser notificada y aprobada por la Dirección de Informática.

**Art. 93** Los usuarios con acceso a internet serán sujetos al monitoreo de las actividades que realizan.

**Art. 94** En lo relacionado al acceso a páginas web, los usuarios deberán acatar lo previsto en el Reglamento para la Utilización del Servicio de Internet en la Muy Ilustre Municipalidad de Guayaquil, Cap. V, "De las Restricciones".

### 2.14 DE LAS FIRMAS ELECTRÓNICAS

**Art. 95** Para las comunicaciones formales internas y externas se debe considerar el uso de la firma electrónica o firma digital.

**Art. 96** La Dirección de Informática debe tener actualizado el servicio de firmas electrónicas internas.

**Art. 97** La Dirección de Informática debe instalar la firma electrónica en cada computador con acceso al correo electrónico interno.

**Art. 98** En los casos de las firmas electrónicas otorgadas por otra entidad u organismo, el usuario titular es responsable del uso y actualización.

**Art. 99** Se debe hacer uso de la firma electrónica, según lo previsto en la Ley de Comercio Electrónico, firmas electrónicas y mensajes de datos Ecuatoriano (Título II, Capítulo I), para garantizar la legitimidad de la información del GADMG.

**Art. 100** La firma electrónica tendrá igual validez y se le reconocerán los mismos efectos jurídicos que a una firma manuscrita, en relación con los datos consignados en documentos escritos, y será admitida como prueba en juicios.

## CAPÍTULO III
## SEGURIDAD FÍSICA

### 3.1 DEL RESGUARDO Y PROTECCIÓN DE LA INFORMACIÓN

**Art.101** Será responsabilidad de la Dirección de Informática verificar que las áreas de trabajo cuenten con una adecuada instalación eléctrica.

**Art.102** La Dirección de Informática será responsable de analizar las áreas que requieran de una fuente de alimentación ininterrumpida (UPS), debido a la naturaleza de su información y los riesgos de pérdida de la misma, como por ejemplo cortes de energía.

**Art.103** La Dirección de Informática será responsable de analizar las áreas donde sea necesario la instalación de un regulador de voltaje para proteger máquinas de avanzada tecnología y alto costo, con la finalidad de que las mismas no sufran daños en el hardware o software.

**Art.104** La Dirección de Informática, a través de su Departamento Técnico, verificará que los medios de almacenamiento que contengan los equipos a dar de baja, no cuenten con ninguna información.

### 3.2 DE LOS CONTROLES DE ACCESO FÍSICO

**Art.105** Los equipos o activos críticos de información y procesamiento de datos deberán ubicarse en espacios aislados y seguros, protegidos con un nivel de seguridad verificable.

**Art.106** El espacio donde se ubican los equipos servidores debe tener un acceso restringido, contar con una puerta blindada, un sistema biométrico para su ingreso y un control de circuito cerrado de cámaras.

### 3.3 DE LA SEGURIDAD EN ÁREAS DE TRABAJO

**Art.107** El acceso durante la noche, fines de semana o feriados, hacia las áreas de procesamiento de información de la Dirección de Informática debe estar debidamente justificado. El guardia de seguridad debe verificar si el usuario cuenta con la debida autorización y en el horario señalado.

**Art.108** Los centros de cómputo son áreas restringidas, por lo que solo el personal autorizado por el director de Informática puede acceder a ellos.

### 3.4 DE LA PROTECCIÓN Y UBICACIÓN DE LOS EQUIPOS INFORMÁTICOS

**Art.109** Una vez instalados los equipos informáticos por personal autorizado, los usuarios no deben moverlos o reubicarlos, instalar o desinstalar dispositivos, ni retirar sus sellos de seguridad.

**Art.110** Mientras se utilizan los equipos informáticos, no se deberá consumir alimentos o ingerir líquidos.

**Art.111** No se debe colocar objetos encima de los equipos informáticos o cubrir sus orificios de ventilación.

**Art.112** Se deben mantener los equipos informáticos en un entorno limpio y sin humedad.

**Art.113** El usuario debe asegurarse que los cables de red no se encuentren presionados con objetos encima o contra ellos; en caso de que esta situación no se cumpla, debe solicitar la redistribución de los cables de red al Departamento de Soporte Técnico.

**Art.114** Cada usuario es responsable de los equipos informáticos, partes, piezas y accesorios, desde el momento en que el Departamento de Control de Bienes realiza la asignación correspondiente.

**Art.115** El usuario tiene la obligación de proteger las unidades de almacenamiento que se encuentren bajo su administración o custodia, aun cuando no se utilicen o no contengan información reservada/confidencial.

**Art.116** El suministro de energía eléctrica para los computadores debe hacerse a través de un circuito exclusivo, que debe contar con tomacorrientes a 120V polarizados (FASE-NEUTRO-TIERRA) y de tierra aislada. Para distinguir los tomacorrientes de los de servicio general, deben ser de color naranja y estar etiquetados con la nomenclatura "PC"; en ellos no deberán conectarse impresoras, cafeteras, microondas, aspiradoras ni cualquier dispositivo electrónico o aparato eléctrico, ya que estos equipos exceden la capacidad real del UPS, por lo que pueden provocar que este se apague y con el tiempo se dañe.

**Art.117** La Dirección Administrativa conjuntamente con el Departamento de Seguridad Industrial, de la Dirección de Recursos Humanos, verificará que las instalaciones eléctricas y de comunicaciones donde deban conectarse los equipos de cómputo cumplan las condiciones óptimas de seguridad (uso de canaletas, identificación con marcadores de cables y equipos), de forma que se prevenga el riesgo de incendios o accidentes de trabajo.

**Art.118** El cableado de red municipal se instalará físicamente separado de cualquier otro tipo de cables, llámese a estos de corriente o energía eléctrica, para evitar interferencias.

**Art.119** El Departamento de Seguridad Industrial identificará las áreas críticas para definir la ubicación y determinar el mantenimiento de detectores de humo y calor, alarmas, y extintores adecuados, que serán usados en la protección de las estaciones de trabajo y equipos especiales en casos de emergencia, lo que permitirá asegurar que los referidos dispositivos se encuentren en condiciones óptimas de funcionamiento.

**Art.120** La Dirección Administrativa, en todo lugar donde se encuentre instalado un equipo informático, deberá climatizarlo a fin de evitar el calentamiento de los mismos o daños por la humedad. Aquellos equipos que se encuentren disponibles al acceso del ciudadano, deberán tener características para esos ambientes. Es aconsejable que el equipo se utilice y almacene a una temperatura de 21 ± 1°C y una humedad relativa de 50% ± 5%.

### 3.5 DEL MANTENIMIENTO DE LOS EQUIPOS INFORMÁTICOS

**Art.121** Únicamente el personal autorizado por la Dirección de Informática podrá llevar a cabo los servicios de mantenimiento y reparación a los equipos informáticos.

**Art.122** La Dirección de Informática deberá ejecutar controles tanto para el mantenimiento preventivo como para el correctivo de los equipos informáticos.

**Art.123** Corresponde a la Dirección de Informática, a través del Departamento de Soporte Técnico, planificar, ejecutar y documentar el mantenimiento de los equipos informáticos.

### 3.6 DE LA PÉRDIDA O DAÑO DE LOS EQUIPOS INFORMÁTICOS

**Art.124** El usuario que tenga bajo su resguardo algún equipo de cómputo o accesorio, será responsable de su uso y custodia; en caso de desaparición, robo o extravío, deberá dar aviso inmediato al área de Control de Bienes de la Dirección Financiera, de acuerdo con el Manual Específico para la Administración y Control de Bienes de Larga Duración que para el efecto emita la Municipalidad.

**Art.125** En caso de que los equipos de cómputo o recursos de tecnología de información sufran algún daño por maltrato, descuido o negligencia por parte de su custodio, se aplicará lo previsto en el artículo 3 del Reglamento General Sustitutivo para el Manejo y Administración de Bienes del Sector Público.

### 3.7 DE LAS ACTIVIDADES PROHIBITIVAS

**Art.126** Se prohíbe a los usuarios utilizar los equipos informáticos provistos por el GADMG, para un objetivo distinto del que están destinados o para beneficiar a personas ajenas a la institución.

**Art.127** Queda terminantemente prohibido colocar stickers o cualquier otro material adhesivo a los recursos tecnológicos que son propiedad del GADMG.

# CAPÍTULO IV

# SEGURIDAD LEGAL

## 4.1 DEL LICENCIAMIENTO DE SOFTWARE

**Art.128** Todo software que se utilice en los equipos informáticos del GADMG y que no sea de propiedad municipal, deberá contar con la respectiva licencia de uso. Únicamente se utilizará software certificado o, en su defecto, software previamente revisado y aprobado por personal calificado en esta materia, designado por el director de Informática

**Art.129** Los sistemas desarrollados para el GADMG, por personal interno o externo, son de propiedad intelectual de la entidad municipal; por lo tanto, no podrán reproducirse sin el permiso de su autoridad máxima, respetando la Ley de Derecho de Autor y Propiedad Intelectual.

## 4.2 DE LOS CONTRATOS CON TERCEROS

**Art.130** Los contratos con terceros, en la gestión o prestación de un servicio, deberán especificar acuerdos de confidencialidad, medidas necesarias de seguridad, nivel de prestación del servicio, además del personal involucrado en tales procesos.

## 4.3 DE LAS VIOLACIONES DE SEGURIDAD INFORMÁTICA

**Art.131** Ningún usuario del GADMG debe probar o intentar probar vulnerabilidades en la seguridad de los sistemas, a menos que estas pruebas sean aprobadas y controladas por la Dirección de Informática.

**Art.132** No se debe intencionalmente escribir, generar, compilar, copiar, coleccionar, propagar, ejecutar o intentar introducir cualquier tipo de código (programa) conocidos como virus, gusanos o caballos de troya, diseñados para auto replicarse, dañar o afectar el desempeño o acceso a las computadoras, redes o información del GADMG.

# CAPÍTULO V

# CONSIDERACIONES GENERALES

## 5.1 DE LA VIGENCIA Y ACTUALIZACIÓN

El presente Reglamento de Seguridad Informática entrará en vigencia desde la aprobación de la máxima autoridad de la entidad.

Este reglamento deberá ser revisado y actualizado conforme a las exigencias del GADMG, o en el momento que existan cambios sustanciales en la infraestructura tecnológica de la red institucional.

# CAPÍTULO VI

# TÉRMINOS Y DEFINICIONES

**Archivos Log:** es un registro oficial de los eventos que ejecuta un sistema informático durante un rango de tiempo; sus datos permiten obtener quién, qué, cuándo, dónde y por qué ocurre una acción en una aplicación automatizada.

**Ataque informático:** es un método por el cual uno o varios individuos, mediante un sistema informático, intentan tomar el control, desestabilizar o dañar otro sistema o aplicación informática.

**Confidencialidad:** es garantizar que la información es accesible solo para aquellos autorizados a tener acceso.

**Cuenta:** es la identificación que se le otorga a un usuario y que, asociado a una contraseña, sirve para autenticarse e ingresar a un sistema informático.

**Disponibilidad:** es la característica o condición de que la información pueda ser accedida cuando sea requerida por las personas, procesos o aplicaciones de la entidad.

**Firma Electrónica:** es un mecanismo que permite al receptor de un mensaje firmado electrónicamente (o digitalmente), determinar la entidad originadora del mensaje y confirmar que no ha sido alterado desde que fue firmado por el originador.

**GADMG:** Gobierno Autónomo Descentralizado Municipal de Guayaquil.

**Integridad:** es mantener con exactitud la información tal cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados.

**Seguridad de la información:** son los mecanismos utilizados para la preservación de la confidencialidad, integridad y disponibilidad de la información.

**Seguridad Informática:** es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta, inclusive con los datos contenidos, a través de normas, procedimientos, métodos, técnicas, estándares, protocolos, reglas y herramientas relacionadas a la Tecnología de Información.

**Servicio:** en el contexto del presente reglamento, es el conjunto de aplicativos o programas informáticos y de comunicación de datos que apoyan la labor municipal.

**Riesgo:** es la probabilidad de que una amenaza determinada afecte a un activo que procese o maneje información.

**Terceros:** personas que proveen o realizan trabajos relacionados a la tecnología de información y deben acceder a las instalaciones municipales.

**Usuario:** define al servidor municipal que utiliza los servicios informáticos de la red del GADMG y tiene una vinculación laboral con la institución.

**Vulnerabilidad:** son puntos débiles del software que permiten que un atacante comprometa la confidencialidad, integridad y disponibilidad de la información.

El presente Reglamento entrará en vigencia a partir de su publicación en la Gaceta Oficial Municipal.

**DADO Y FIRMADO EN LA SALA DE SESIONES DEL M.I. CONCEJO MUNICIPAL DE GUAYAQUIL, A LOS NUEVE DÍAS DEL MES DE ENERO DEL AÑO 2014.**

Jaime Nebot Saadi
**ALCALDE DE GUAYAQUIL**

Dr. Vicente Taiano Basante
**SECRETARIO DE LA M.I. MUNICIPALIDAD DE GUAYAQUIL**

**CERTIFICO:** Que el presente **"REGLAMENTO DE SEGURIDAD INFORMÁTICA DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE GUAYAQUIL"**, fue discutido y aprobado por el M.I. Concejo Municipal de Guayaquil, en sesión ordinaria de fecha nueve de enero del año dos mil catorce.

Guayaquil, 09 de enero de 2014

Dr. Vicente Taiano Basante
**SECRETARIO DE LA M.I. MUNICIPALIDAD DE GUAYAQUIL**

De conformidad con lo prescrito en los artículos 323 y 324 del Código Orgánico de Organización Territorial, Autonomía y Descentralización, SANCIONO el presente **"REGLAMENTO DE SEGURIDAD INFORMÁTICA DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE GUAYAQUIL"**, y ordeno su PROMULGACIÓN a través de su publicación en la Gaceta Oficial del Gobierno Autónomo Descentralizado Municipal de Guayaquil.

Guayaquil, 10 de enero de 2014

Jaime Nebot Saadi
**ALCALDE DE GUAYAQUIL**

Sancionó y ordenó la promulgación a través de su publicación en la Gaceta Oficial, del presente **"REGLAMENTO DE SEGURIDAD INFORMÁTICA DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE GUAYAQUIL"**, el señor abogado Jaime Nebot Saadi, Alcalde de Guayaquil, a los diez días del mes de enero del año dos mil catorce.- LO CERTIFICO.-

Guayaquil, 10 de enero de 2014

Dr. Vicente Taiano Basante
**SECRETARIO DE LA M.I. MUNICIPALIDAD DE GUAYAQUIL**

**Secretaría Municipal.- Guayaquil, 24 de enero del 2014**

**El infrascrito Secretario Municipal, CERTIFICA: Que el presente "REGLAMENTO DE SEGURIDAD INFORMÁTICA DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE GUAYAQUIL", ha sido publicada para su vigencia y aplicación en la Gaceta Oficial No. 70, página 07, año 2 de fecha viernes 24 de enero del 2014.**

**Dr. Vicente Taiano Basante**
**SECRETARIO DE LA M. I. MUNICIPALIDAD DE GUAYAQUIL**