ESTADO LIBRE ASOCIADO DE PUERTO RICO
MUNICIPIO AUTÓNOMO DE GUAYNABO
LEGISLATURA MUNICIPAL

ORDENANZA

Número: 109 Serie 2015-2016

Presentada por: Administración

PARA ADOPTAR LAS POLITICAS DE SEGURIDAD SOBRE EL USO DE DISPOSITIVOS MOVILES DEL MUNICIPIO DE GUAYNABO; DEROGAR LA ORDENANZA NÚM. 15, SERIE 2002-2003 Y LA ORDENANZA NÚM. 56, SERIE 2006-2007; Y PARA OTROS FINES.

Por Cuanto: La Ley de Municipios Autónomos del Estado Libre Asociado de Puerto Rico de 1991, reconoce la autonomía de todo municipio en el orden jurídico, económico y administrativo y establece que la misma comprenderá la libre administración de sus bienes, así como los asuntos de su competencia y jurisdicción. De igual manera, dispone que los municipios, tengan todos los poderes necesarios y convenientes para ejercer todas las facultades correspondientes a un gobierno local para lograr sus fines y funciones.

Por Cuanto: El Municipio de Guaynabo identifica la información como un componente o activo indispensable en la consecución de los objetivos establecidos, razón por la cual es necesario establecer un marco en el cual se asegure que la información es protegida de una manera adecuada independientemente de la forma en la que ésta sea manejada, procesada, transportada o almacenada mediante el uso de dispositivos móviles.

Por Cuanto: Los dispositivos móviles como iPhones, iPads, tabletas Android y otros similares se están convirtiendo en equipo estándar para la realización de negocios. Estas tecnologías ofrecen configuración para acceder información en tiempo real y a los recursos informáticos locales tales como correos electrónicos, calendarios, a la red y a los sistemas de información financiera de la entidad. No obstante, por su forma y tamaño son los más probables a ser perdidos o robados. En consecuencia, los datos almacenados en ellos se encuentran en riesgo de ser comprometidos.

Por Cuanto: El Municipio está obligado por imperativo constitucional a manejar los fondos públicos con los principios fiduciarios y éticos más altos. Como parte de estos deberes, los funcionarios y empleados son responsables del cuidado, la protección, la conservación y el uso adecuado de los bienes públicos bajo su dominio, control o custodia.

Por Cuanto: En el Artículo 2.004 se dispone que le corresponde a cada municipio ordenar, reglamentar y resolver cuanto sea necesario o conveniente para atender las necesidades locales y para su mayor prosperidad y desarrollo.

Por Cuanto: Se hace necesario derogar las Ordenanzas Núm. 15 y 56, Serie 2002-2003 y 2006-2007, respectivamente, toda vez que los controles que en ellas se establecen sobre las llamadas, uso, notificaciones en casos de pérdidas del teléfono celular y el rendir informes sobre las llamadas realizadas, estará ahora reglamentado en el Manual que se adopta por esta Ordenanza.

Por Cuanto: El Municipio Autónomo de Guaynabo, en su interés de proteger y ejercer un adecuado control de la información y el uso de los dispositivos móviles, desea establecer las políticas y procedimientos que regirán sobre los mismos.

Por Tanto: **ORDÉNASE POR ESTA LEGISLATURA MUNICIPAL DE GUAYNABO, PUERTO RICO, REUNIDA EN SESIÓN EXTRAORDINARIA, HOY, 8 DE JUNIO DE 2016:**

Sección 1ra.: Adoptar como por la presente se adopta el "MANUAL DE POLITICAS DE SEGURIDAD PARA DISPOSITIVOS MOVILES", el cual forma parte de esta Ordenanza.

Sección 2da.: Establecer las políticas y normas de seguridad para el uso de los dispositivos móviles provistos por el Municipio de Guaynabo a sus usuarios, así como los dispositivos móviles no adquiridos por el Municipio (BYODs) utilizados por los usuarios para lograr conexión o accesos remotos a la red del Municipio de Guaynabo, para uso oficial e institucional.

Sección 3ra.: Reglamentar las aplicaciones necesarias para realizar las funciones oficiales y acceso a Internet, así como la cantidad de "gigabytes" de data que se asignará a cada aparato móvil asignado a los funcionarios y empleados, según dispuesto en el "MANUAL DE POLITICAS DE SEGURIDAD PARA DISPOSITIVOS MOVILES DEL MUNICIPIO AUTÓNOMO DE GUAYNABO", el cual forma parte de esta Ordenanza.

Sección 4ta.: Se deroga la Ordenanza Núm. 15, Serie 2002-2003 y la Ordenanza Núm. 56, Serie 2006-2007.

Sección 5ta.: Esta Ordenanza comenzará a regir a los diez (10) días después de haber sido publicada en un periódico de circulación general del Estado Libre Asociado de Puerto Rico y copia de la misma le será enviada a las autoridades estatales y municipales que correspondan para los fines de rigor.

Javier Capestany Figueroa
Presidente

José A. Suárez Santa
Secretario

Fue aprobada por el Hon. Héctor O'Neill García, Alcalde, el día 9 de junio de 2016.

Alcalde

Estado Libre Asociado de Puerto Rico
Municipio Autónomo de Guaynabo
Legislatura Municipal

CERTIFICACIÓN

Yo, José A. Suárez Santa Secretario de la Legislatura Municipal de Guaynabo, Puerto Rico, por medio de la presente certifico que la que antecede es una copia fiel y exacta de la Ordenanza Núm. 109, Serie 2015-2016, aprobada por la Legislatura Municipal de Guaynabo, Puerto Rico, reunida en Sesión Extraordinaria el día 8 de junio de 2016.

CERTIFICO, ADEMÁS, que la misma fue aprobada por los miembros presentes en dicha sesión, los Honorables:

Javier Capestany Figueroa
Lilliana Vega González
Antonio O'Neill Cancel
Carmen Báez Pagán
Miguel A. Negrón Rivera
Luis C. Maldonado Padilla
Ángel O'Neill Pérez
Carlos M. Santos Otero
Luis A Rodríguez Díaz
Carlos J. Álvarez González
Guillermo Urbina Machuca
Natalia Rosado Lebrón
Andrés Rodríguez Rivera
Omar Llópiz Burgos

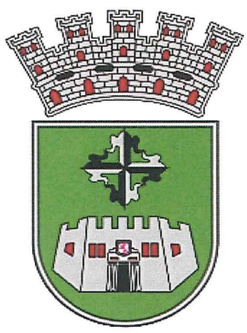
Excusados: Aída M. Márquez Ibañez, Carlos H. Martínez Pérez

Fue aprobada por el Alcalde, Hon. Héctor O'Neill García, el 9 de junio de 2016

EN TESTIMONIO DE TODO LO CUAL, libro la presente certificación bajo mi firma y el sello oficial de esta municipalidad de Guaynabo, Puerto Rico, el 13 de junio de 2016.

José A. Suárez Santa
Secretario

MUNICIPIO AUTONOMO DE GUAYNABO
DEPARTAMENTO DE INFORMATICA



MANUAL DE POLÍTICAS DE SEGURIDAD PARA DISPOSITIVOS MOVILES

Carmen Puig Marce
Director de Informática
MAYO 2016

Aprobado por la Ordenanza Núm. 109 Serie 2015-2016
el 8 de junio de 2016

I. INTRODUCCION

El Municipio de Guaynabo identifica la información como un componente o activo indispensable en la consecución de los objetivos establecidos, razón por la cual es necesario establecer un marco en el cual se asegure que la información es protegida de una manera adecuada independientemente de la forma en la que ésta sea manejada, procesada, transportada o almacenada mediante el uso de dispositivos móviles.

Los dispositivos móviles como iPhones, iPads, tabletas Android y otros similares se están convirtiendo en equipo estándar para la realización de negocios. Estas tecnologías ofrecen configuración para acceder información a tiempo real y a los recursos informáticos locales tales como correos electrónicos, calendarios, a la red y a los sistemas de información financiera de la entidad. No obstante, por su forma y tamaño son los más probables a ser perdidos o robados. En consecuencia, los datos almacenados en ellos se encuentran en riesgo de ser comprometidos.

Este documento describe las políticas y normas de seguridad para el uso de los dispositivos móviles provistos por el Municipio de Guaynabo a sus usuarios, así como dispositivos móviles no adquiridos por el Municipio (BYOD) utilizados por los usuarios para conexión a la red del Municipio de Guaynabo para uso oficial e institucional.

II. OBJETIVO

Este documento describe las políticas y normas de seguridad para accesos remotos al sistema o red del Municipio de Guaynabo a través de dispositivos móviles adquiridos por el Municipio de Guaynabo para uso de sus funcionarios y empleados, o a través de dispositivos móviles adquiridos o traídos por los usuarios ("BYOD") para conexión a la red del Municipio de Guaynabo para uso oficial. Todo dispositivo autorizado usado para acceder a la red del Municipio de Guaynabo deberá estar debidamente asegurado para prevenir accesos no autorizados, prevenir pérdida de información y reducir el riesgo de propagación de viruses y abuso o mal uso de la información y la red del Municipio de Guaynabo y la debida protección de activos.

III. ALCANCE

Las políticas de seguridad de la información cubrirán los aspectos administrativos y de control que deben ser cumplidos por los directores, funcionarios, empleados y terceros que laboren o tengan relación contractual con el Municipio de Guaynabo, para conseguir un adecuado nivel de protección de seguridad y calidad de la información. Las mismas serán de aplicación

a los dispositivos móviles autorizados y adquiridos por el Municipio de Guaynabo para uso de sus directores, funcionarios y empleados, así como aquellos no adquiridos por el Municipio (BYOD), usados por directores, funcionarios y empleados, para tener acceso a la red y los sistemas del Municipio de Guaynabo.

La revisión de esta política se realizará en una base anual, bajo la responsabilidad del Departamento de Informática, y en coordinación con la Oficina de Auditoría Interna, a fin de que la misma esté atemperada o actualizada ante los cambios y evolución de la tecnología.

IV. BASE LEGAL

En Puerto Rico existe una clara política pública dirigida a la protección de la propiedad y fondos públicos.

En lo pertinente, la Constitución del Estado Libre Asociado de Puerto Rico, en su Artículo IV, Sección nueve (9) dispone, expresamente, lo siguiente: *Sólo se dispondrá de las propiedades y fondos públicos para fines públicos y para el sostenimiento y funcionamiento de las instituciones del Estado, y en todo caso por autoridad de ley. (Énfasis y subrayado nuestro).* En armonía con este mandato constitucional, la Ley de Ética Gubernamental de 2011, Ley Núm. 1-2012, según enmendada, dispone en lo pertinente:

> (i) *un servidor público no puede utilizar los deberes y las facultades de su cargo ni la propiedad o los fondos públicos para obtener, directa o indirectamente, para él o para una persona privada o negocio, cualquier beneficio que no esté permitido por ley;*
>
> (ii) *un servidor público no puede revelar o usar información o un documento confidencial adquirido por razón de su empleo para obtener, directa o indirectamente, un beneficio para él o para una persona privada o negocio;*
>
> (iii) *Un servidor público no puede utilizar, en los bienes muebles o inmuebles del Gobierno, cualquier símbolo, lema, imagen, fotografía, pin, logo, pegatina, calcomanía, rótulo, insignia, aplicación tecnológica, mensaje escrito u otro distintivo que identifique o promueva, directa o indirectamente, los intereses electorales de cualquier partido o candidato político.*
>
> *(iv) Un servidor público no puede alterar, destruir, mutilar, remover u ocultar, en todo o en parte, la propiedad pública bajo su custodia.*

(v) Un servidor público no puede omitir el cumplimiento de un deber impuesto por ley o reglamento, si con ello ocasiona la pérdida de fondos públicos o produce daño a la propiedad pública.

(vi) Un servidor público no puede llevar a cabo una acción que ponga en duda la imparcialidad e integridad de la función gubernamental[1].

De las citadas disposiciones surge que el Estado está obligado por imperativo constitucional a manejar los fondos públicos con los principios fiduciarios y éticos más altos. Como parte de estos deberes, los funcionarios y empleados son responsables del cuidado, la protección, la conservación y el uso adecuado de los bienes públicos bajo su dominio, control o custodia. Asimismo, a tenor con Ley Núm. 96 de 26 de junio de 1964, según enmendada, se dispone el deber de notificar a la Oficina del Contralor de Puerto Rico en un término establecido, toda pérdida o irregularidad en el manejo de los fondos o de los bienes públicos.

Por su parte, el Código Penal de Puerto Rico contiene disposiciones que tipifican como delito varias conductas cuanto se utiliza medios tecnológicos. Las siguientes disposiciones resultan pertinentes:

Artículo 124: Toda persona que, a sabiendas, utilice cualquier medio de comunicación telemática para seducir o convencer a un menor para encontrarse con la persona, con el propósito de incurrir en conducta sexual prohibida por este Código Penal u otras leyes penales, será sancionada con pena de reclusión por un término fijo de ocho (8) años. Este delito no cualificará para penas alternativas a la reclusión."

Artículo 152: Toda persona que a sabiendas distribuya cualquier material obsceno a través de cualquier medio de comunicación telemática u otro medio de comunicación, incurrirá en delito menos grave. Cuando el material sea de pornografía infantil, la persona será sancionada con pena de reclusión por un término fijo de ocho (8) años. Si la persona convicta es una persona jurídica será sancionada con pena de multa hasta treinta mil dólares ($30,000)."

Artículo 168: Toda persona que sin justificación legal o sin un propósito investigativo legítimo utilice equipo electrónico o digital de video, con o sin audio, para realizar vigilancia secreta en lugares privados, o en cualquier otro lugar donde se reconozca una expectativa razonable de intimidad será sancionada con pena de reclusión por un término fijo de tres (3) años. Si la persona convicta es una persona jurídica será sancionada con pena de multa hasta diez mil dólares ($10,000)."

[1] Artículo 4.2, incisos (b), (f), (i), (p), (r), y (s) de la Ley Núm. 1-2012, citada.

Artículo 171: Toda persona que sin autorización y con el propósito de enterarse o permitir que cualquiera otra se entere, se apodere de los papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos de otra persona, o intercepte sus telecomunicaciones a través de cualquier medio, o sustraiga o permita sustraer los registros o récords de comunicaciones, remesas o correspondencias cursadas a través de entidades que provean esos servicios, o utilice aparatos o mecanismos técnicos de escucha, transmisión, grabación o reproducción del texto, sonido, imagen, o de cualquier otra señal de comunicación, o altere su contenido será sancionada con pena de reclusión por un término fijo de tres (3) años. Si la persona convicta es una persona jurídica será sancionada con pena de multa hasta diez mil dólares ($10,000). A los fines de este Artículo, el hecho de que la persona tuviere acceso a los documentos, efectos o comunicaciones a que se hace referencia dentro de sus funciones oficiales de trabajo no constituirá de por sí "autorización" a enterarse o hacer uso de la información más allá de sus estrictas funciones de trabajo."

Artículo 172: Toda persona que, sin estar autorizada, se apodere, utilice, modifique o altere, en perjuicio del titular de los datos o de un tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en discos o archivos informáticos o electrónicos, o en cualquier otro tipo de archivo o registro público o privado, será sancionada con pena de reclusión por un término fijo de tres (3) años. Si la persona convicta es una persona jurídica será sancionada con pena de multa hasta diez mil dólares ($10,000)."

Artículo 173: Toda persona que difunda, publique, revele o ceda a un tercero los datos, comunicaciones o hechos descubiertos o las imágenes captadas a que se refieren los Artículos 171 (Violación de comunicaciones personales) y 172 (Alteración y uso de datos personales en archivos), o que estableciere una empresa para distribuir o proveer acceso a información obtenida por otras personas en violación de los referidos Artículos, u ofreciere o solicitare tal distribución o acceso será sancionada con pena de reclusión por un término fijo de tres (3) años. Si la persona convicta es una persona jurídica será sancionada con pena de multa hasta diez mil dólares ($10,000)."

Artículo 174: Lo dispuesto en los Artículos 171 (Violación de comunicaciones personales), 172 (Alteración y uso de datos personales en archivos) y 173 (Revelación de comunicaciones y datos personales), será aplicable al que descubra, revele o ceda datos reservados de personas jurídicas, sin el consentimiento de sus representantes.

Artículo 175: Si los delitos que se tipifican en los Artículos 171 (Violación de comunicaciones personales), 172 (Alteración y uso de datos personales en archivos) y 173 (Revelación de comunicaciones y datos personales), se realizan con propósito de lucro por las personas encargadas o responsables de los discos o archivos informáticos, electrónicos o de cualquier otro tipo de archivos o registros; o por funcionarios o empleados en el curso de sus deberes será sancionada con pena de reclusión por un término fijo de ocho (8) años. Si la persona

convicta es una persona jurídica será sancionada con pena de multa hasta treinta mil dólares ($30,000). Lo dispuesto en este Artículo será aplicable también cuando se trate de datos reservados de personas jurídicas."

Artículo 186: Toda persona que use, altere, modifique, interfiera, intervenga u obstruya cualquier equipo, aparato o sistema de comunicación, información, cable televisión, televisión por satélite ("direct broadcast satellite"), o televisión sobre protocolo de Internet, con el propósito de defraudar a otra, incurrirá en delito menos grave, y convicta que fuere, será sancionada con pena de multa que no excederá de cinco mil dólares ($5,000), o pena de reclusión por un término fijo de seis (6) meses, a discreción del tribunal.

Artículo 203: Toda persona que con el propósito de defraudar y mediante cualquier manipulación informática consiga la transferencia no consentida de cualquier bien o derecho patrimonial en perjuicio de un tercero o del Estado, será sancionada con pena de reclusión por un término fijo de ocho (8) años. Si la persona convicta es una persona jurídica será sancionada con pena de multa hasta treinta mil dólares ($30,000).

Artículo 257: Todo funcionario o empleado público que esté encargado o que tenga control de cualquier propiedad, archivo, expediente, documento, registro computadorizado o de otra naturaleza o banco de información, en soporte papel o electrónico que lo altere, destruya, mutile, remueva u oculte en todo o en parte, será sancionado con pena de reclusión por un término fijo de tres (3) años. Cuando se produzca la pérdida de propiedad o fondos públicos, el tribunal también podrá imponer la pena de restitución.

En atención las disposiciones legales antes discutidas y en virtud de las facultades y poderes que confieren los Artículos 3.009, 6.003, 6.005 y 8.013, se adopta y promulga las Políticas de Seguridad y Uso de Dispositivos Móviles del Municipio.

V. DEFINICIONES

Acuerdo de Confidencialidad	Documento en que los funcionarios del Municipio de Guaynabo y contratistas (terceros) manifiestan su voluntad de mantener la confidencialidad de la información, comprometiéndose a no divulgar, usar

	o explotar la información confidencial a la que tengan acceso en virtud de la labor que realizan.
Autenticación	Procedimiento de comprobación de la identidad de un usuario o recurso tecnológico al tratar de acceder a un recurso de procesamiento o sistema de información.
Análisis de riesgos de seguridad de la información	Proceso sistemático de identificación de fuentes, estimación de impactos y probabilidades y comparación de dichas variables contra criterios de evaluación para determinar las consecuencias potenciales de pérdida de confidencialidad, integridad y disponibilidad de la información.
Cifrado (Encrypt)	Transformación de los datos mediante el uso de la criptografía para producir datos ininteligibles (cifrados) y asegurar su confidencialidad. El cifrado es una técnica muy útil para prevenir la fuga de información, el monitoreo no autorizado e incluso el acceso no autorizado a la información.
Confidencialidad	Garantía de que la información no está disponible o divulgada a personas, entidades o procesos no autorizados.
Dispositivo móvil	Teléfonos inteligentes tales como iphones y andoids, tabletas, ipads, USB, discos removibles, CDs, DVDs, accesos portátiles para internet, u otros dispositivos de computación portátiles. Ordenadores portátiles tales como "lap tops" no están en el ámbito de esta política.
Dispositivos de propiedad personal (BYOD)	Una política de permitir que los empleados usen sus dispositivos móviles personales en su lugar de trabajo para acceder a las aplicaciones e información privilegiada de la empresa.
Incidente de Seguridad	Evento adverso, confirmado o bajo sospecha, que haya vulnerado la seguridad de la información o que intente vulnerarla, sin importar la información afectada, la plataforma tecnológica, la frecuencia, la consecuencia, el número de veces ocurrido o el origen, sea interno o externo.
Información documento confidencial	Aquel así declarado por ley; el que está protegido por alguno de los privilegios de Derecho Probatorio; el que, si se revela, puede lesionar los derechos fundamentales de terceros o el derecho a la intimidad y a la vida privada de los servidores públicos; cuando revelarlos pueda constituir una violación del privilegio ejecutivo; cuando el documento o la información sea parte del proceso deliberativo en la formulación de la política pública y, cuando divulgarla, pueda poner en peligro la vida o la integridad física del servidor público o de otra persona, la seguridad del país o afectar transacciones de negocios o gestiones oficiales del Estado que están en

	proceso durante la solicitud. Incluye informes, memorandos o cualquier escrito preparado por un servidor público en el ejercicio de su cargo o empleo para su superior o para fines internos de las decisiones y de las actuaciones departamentales.
Perfiles de usuario	Grupos que concentran varios usuarios con similares necesidades de información y autorizaciones idénticas sobre los recursos tecnológicos o los sistemas de información a los cuales se les concede acceso de acuerdo con las funciones realizadas.
Registros de Auditoría	Son archivos donde son registrados los eventos que se han identificado en los sistemas de información, recursos tecnológicos y redes de datos del instituto. Dichos eventos pueden ser, entre otros, identificación de usuarios, eventos y acciones ejecutadas, terminales o ubicaciones, intentos de acceso exitosos y fallidos, cambios a la configuración, uso de utilidades y fallas de los sistemas.
Software malicioso	Variedad de software o programas de códigos hostiles e intrusivos que tienen como objeto infiltrarse o dañar los recursos tecnológicos, sistemas operativos, redes de datos o sistemas de información.
Vulnerabilidades	Debilidades, hoyos de seguridad o flaquezas inherentes a los activos de información que pueden ser explotadas por factores externos y no controlables por el instituto (amenazas), las cuales se constituyen en fuentes de riesgo.

VI. DISPOSICIONES APLICABLES A LOS DISPOSITIVOS MOVILES ADQUIRIDOS POR EL MUNICIPIO DE GUAYNABO

A. Los dispositivos móviles adquiridos por el Municipio, y provistos a sus funcionarios y empleados, serán utilizados para gestiones oficiales. Los mismos tendrán las aplicaciones necesarias para realizar sus funciones oficiales, incluyendo acceso a Internet móvil.

B. Las operaciones realizadas a través de los dispositivos móviles pueden generar responsabilidad por parte del Municipio. Por tanto, los usuarios que los tengan asignados no tienen expectativa de privacidad alguna con relación al uso y a los accesos realizados. El Municipio se reserva el derecho a intervenir, auditar y revisar sin previo aviso los accesos realizados por los usuarios a través de los dispositivos móviles provistos, el acceso a Internet y el contenido de lo accedido. El uso de un código para acceder (password) no impide que se audite el uso de los dispositivos móviles y no significa que el usuario albergue alguna

expectativa de intimidad relacionado con la información almacenada en éstos o en cualquier otro medio de almacenamiento.

C. Los dispositivos móviles adquiridos por el Municipio, y provistos a sus funcionarios y empleados, serán utilizados para gestiones oficiales. Los mismos tendrán las aplicaciones necesarias para realizar sus funciones oficiales, incluyendo acceso a Internet móvil.

D. Los usuarios mantendrán el sistema operativo original del dispositivo y con los parches de seguridad y actualizaciones del fabricante, los cuales previenen la instalación de software maliciosos ("malwares"). No se autorizará su uso ni acceso a la red del Municipio de Guaynabo a aquellos dispositivos cuya configuración haya sido alterada ni se podrán hacer cambios en los "Sim Cards" ni instalar "Sim Cards" personales.

1. Se prohíbe el uso del Internet móvil en los aparatos y dispositivos móviles para gestiones no oficiales. Entre las prohibiciones del uso del Internet móvil se encuentran las siguientes:
   - **a.** Realizar "video streaming".
   - **b.** Descarga de videos, películas, fotos y cualquier otro material no relacionado con las funciones oficiales del puesto, de índole profesional o educativo.
   - **c.** Acceso a páginas de contenido sexual.
   - **d.** Compras de carácter personal a través de "sites" de descuentos y cualquier otra.
   - **e.** Accesos a las cuentas personales de páginas de redes sociales tales como Facebook, Instagram, Twiter, entre otros.
   - **f.** Participar en encuestas, sistemas de opinión o "blogs".
   - **g.** Instalar juegos y otras aplicaciones no relacionadas con las gestiones oficiales en el Municipio de Guaynabo.
   - **h.** Conversaciones a través de "Messenger", "Chats Rooms" y otros similares tales como "Whatsapp".
   - **i.** Envío de fotos personales a través de mensajería de textos.
   - **j.** Enviar textos con vocabulario obseno y/o amenazante.
   - **k.** Envío o reenvío de imágenes no relacionadas con las gestiones oficiales tales como chistes, chismes, memes, etc.
   - **l.** Envío o reenvío de mensajes, fotos, memes, propaganda o cualquier otro material de índole político partidista.
   - **m.** Los usuarios de dispositivos móviles adquiridos por el Municipio, y provistos para sus funciones oficiales, no podrán realizar limpiezas ("wipe out") a los equipos.

2. El Municipio se reserva el derecho de controlar los accesos a las cuentas personales de Yahoo, Gmail, etc. para recibir y/o enviar información oficial y/o confidencial, relacionada con el Municipio de Guaynabo.

3. Se prohíbe el envío o el recibo de mensajes de texto o correo electrónico o de cualquier tipo entre el personal del Municipio y otras personas que no pertenezcan a la misma, en los cuales se divulguen, comenten o expresen hechos, opiniones o cualquier tipo de información relacionada con situaciones, controversias, problemas, malentendidos, funcionamiento, políticas, personas o cualquier otra situación o asunto interno del Municipio, aunque la información divulgada no sea de naturaleza confidencial.

4. Se autoriza a los empleados y funcionarios del Municipio de Guaynabo el uso del Internet en los dispositivos móviles para lo siguiente:
   a. Acceso a páginas de redes sociales tales como Facebook, Instagram, Twiter, entre otras, para propósitos institucionales y oficiales relacionadas con las funciones y operaciones de estos en el Municipio de Guaynabo.
   b. Llamadas y mensajes de textos ilimitados relacionados con las funciones y deberes del puesto y las operaciones del Municipio de Guaynabo.
   c. Acceso al Internet para búsquedas de información y gestiones oficiales, así como de carácter profesional y educativo. Recibir y enviar correos electrónicos a través de la red del Municipio de Guaynabo de carácter oficial.

3. No se adquirirán equipos que no sean compatibles con las soluciones de seguridad adoptadas por el Municipio.

4. Se requerirá la autenticación del usuario mediante un "pin code" o código de acceso, ya sea numérico o biométrico, en el dispositivo móvil como mecanismo de asegurar ("block") la pantalla para ocultar la información mientras el dispositivo continúa su operación. La aplicación de seguridad adoptada por el Municipio (Mobile Iron) podrá desconectar de la red el "BYOD" si no se establece un código de acceso al dispositivo.

5. Se asignará 5 gigabytes para uso de data a cada celular oficial asignado a funcionario o empleado. Se establece Access My Lan para evitar que los funcionarios se excedan del consumo. Para esto se crearán perfiles de los usuarios y se determinará, conforme a sus funciones, a cuáles aplicaciones se les autorizará acceso así como cualquier cantidad adicional de consumo de datos.

6. El Administrador de Access My Lan será el Departamento de Informática.

7. Todos los dispositivos IPhone tendrán acceso a "Apps@Work" que contiene las aplicaciones pre-autorizadas por el Municipio. La Gerencia podrá autorizar acceso a aplicaciones específicas a grupos según sus funciones o áreas de trabajo.

E. El personal no debe poner en peligro la información confidencial del Municipio de Guaynabo través del uso de los dispositivos móviles, por lo que no deberán permitir que otras personas (por ejemplo: familia, amigos, compañeros de trabajo) utilicen sus dispositivos adquiridos por el Municipio. Deberán supervisar el uso, en caso de surgir, en la medida necesaria para prevenir la divulgación accidental de información del Municipio.

F. En caso de surgir una pérdida o robo del dispositivo móvil, es necesario comunicarlo de inmediato al Municipio, a través del Director de Informática o Gerente de Proyecto de Informática, fin de que el Municipio pueda activar o realizar una búsqueda y localización a través de la aplicación de Mobile Iron. El Municipio, mediante dicha aplicación podrá intervenir con el dispositivo móvil obviando la contraseña de seguridad ("password") para acceder el mismo.

G. Si un dispositivo adquirido por el Municipio de Guaynabo es perdido o robado, o surge una terminación de empleo con el Municipio, o se identifica un problema de seguridad con el dispositivo, el personal de servicio del Departamento de Informática, previa autorización de la Directora o algún Gerente de Proyecto podrá limpiar remotamente la información y las aplicaciones del dispositivo.

VII. DISPOSICIONES APLICABLES A DISPOSITIVOS DE PROPIEDAD PERSONAL DEL USUARIO (BYODs)

A. El Municipio de Guaynabo podrá proveer acceso o conexión a la red del Municipio a aquellos empleados, funcionarios o contratistas a través de sus dispositivos móviles personales, siempre y cuando responda a la necesidad del servicio que realizan el Municipio. La opción de utilizar su dispositivo móvil personal será voluntaria y estará sujeta al cumplimiento de las provisiones o normas de seguridad:

1. Los directores de departamentos, a través "Help Desk" cumplimentará una solicitud al Departamento de Informática estableciendo en la misma necesidad del acceso. En la misma se deberá incluir entre otras cosas, la siguiente información:
    a. Nombre, puesto y departamento del usuario.
    b. Propósito de la solicitud.

c. Niveles de acceso en la red.
d. Período o tiempo que se le proveerá el acceso.
e. Descripción del dispositivo móvil a ser utilizado.

2. El personal de servicio del Departamento de Informática evaluará los diferentes tipos de dispositivos móviles de propiedad personal que serán utilizados para conectarse a la red del Municipio de Guaynabo, e informarán a la Director del Departamento de Informática para su aprobación final.

3. Los empleados, funcionarios y contratistas a los que se les autorice acceder a la red del Municipio de Guaynabo firmarán un acuerdo de confidencialidad comprometiéndose a no divulgar, usar o explotar la información confidencial a la que tengan acceso en virtud de la labor que realizan.

4. Se requerirá autenticación del usuario mediante un "pin code" o código de acceso, ya sea numérico o biométrico, en el dispositivo móvil como mecanismo de asegurar ("block") la pantalla para ocultar la información mientras el dispositivo continúa su operación. La aplicación de seguridad adoptada por el Municipio (Mobile Iron) podrá desconectar de la red el "BYOD" si no se establece un código de acceso al dispositivo.

5. Se requiere al usuario de un BYOD mantener el sistema operativo original del dispositivo y con los parches de seguridad y actualizaciones del fabricante, los cuales previenen la instalación de software maliciosos ("malwares"). No se autorizará su uso ni acceso a la red del Municipio de Guaynabo a aquellos dispositivos cuya configuración haya sido alterada.

6. Para los empleados y funcionarios del Municipio de Guaynabo que traigan sus dispositivos móviles se les proveerá acceso a su cuenta de correo electrónico de la red del Municipio.

7. En el caso de los BYOD se restringirá a siete (7) días la cantidad de correos electrónicos que podrán acceder a través del dispositivo móvil.

8. El personal no debe poner en peligro la información confidencial del Municipio de Guaynabo través del uso de sus dispositivos de propiedad personal. El personal que participa en el servicio "BYOD", y permiten que otras personas (por ejemplo: familia, amigos, socios de negocios) utilicen sus dispositivos de propiedad personal, deberán supervisar el uso en la medida necesaria para prevenir la divulgación accidental de información del Municipio.

9. El usuario, sea empleado, funcionario o contratista, utilizará su propio plan de data para acceso a Internet. En caso de que los empleados, funcionarios o contratistas soliciten acceso al "WiFi" del Municipio este se otorgará como visitantes entrando la contraseña autorizada para tales propósitos. Solo se autorizará dicho acceso para propósitos oficiales y relacionados con las labores que rinden en el Municipio de Guaynabo. El Municipio de Guaynabo, a través del Departamento de Informática, el Administrador de la Red y la Oficina de Auditoría Interna se reservan el derecho de monitorear los accesos al Internet móvil y "WiFi" provistos por el Municipio a fin de controlar su uso para propósitos oficiales.

10. El uso de su Internet personal o aplicaciones personales y contenido de los dispositivos móviles personales no se monitorearán, filtrarán, ni serán registrados o inventariados.[2]

11. El Departamento de Informática velará que la configuración de la aplicación de seguridad adoptada por el Municipio pueda controlar y proteger la información y la red del Municipio de Guaynabo.

12. Los datos propiedad del Municipio de Guaynabo serán cifrados o "encriptados".

13. El usuario de un dispositivo móvil personal estará sujeto a las normas y políticas de seguridad adoptadas por el Municipio para los BYODs. A tales efectos, se le proveerá (en formato de papel o electrónico) y se orientará sobre la normativa a fin de advertir sobre el cumplimiento de esta política.

14. El usuario de un BYOD se compromete a no transferir su dispositivo móvil o intercambiarlo sin notificar al Municipio de Guaynabo, a fin de evitar que la data propiedad del Municipio de Guaynabo pueda ser utilizada por terceras personas ajenos a la gestión municipal.

---

[2]En el caso Weber v ELA, 2014 TSPR 46 el Tribunal Supremo indico que existe una expectativa razonable de intimidad sobre los registros de llamadas telefónicas. Se reconoce que el teléfono se ha convertido en una herramienta esencial para llevar a cabo nuestros asuntos personales. La lista de números contenidas en una factura de teléfonos permite al Estado descubrir, con relativa facilidad, información privada de las personas incluyendo, por inferencia, el contenido de la conversación. Por vía de los registros de llamadas se puede conseguir: los lugares que la persona frecuenta; los bienes que adquiere; el partido al que contribuye; los periódicos y revistas que lee; la iglesia a la cual hace donaciones; las asociaciones a las cuales pertenece; las tiendas y establecimientos donde compra; los médicos que visita y otra información de naturaleza íntima.

VIII. OTROS DISPOSITIVOS MOVILES

A. Dispositivos para acceso a internet portátiles.

1. El control, registro y custodia de los dispositivos portátiles para acceso a internet estará a cargo del Departamento de Informática. Este mantendrá un registro electrónico sobre la prestación de los mismos que indique entre otras cosas lo siguiente:

   a. Nombre del funcionario o empleado que utilizará el mismo.
   b. Propósito del uso, lugar y fecha o período.
   c. Número de identificación del dispositivo.
   d. Declaración sobre el uso exclusivo del dispositivo móvil para propósitos oficiales y relacionados con las funciones de su puesto, así como la entrega inmediata una vez concluido el período del préstamo para uso.
   e. Firma del prestamista y del prestatario.

IX. PLATAFORMA DE SEGURIDAD MOBIL QUE ADOPTA EL MUNICIPIO

A. El Municipio adopta, como solución de seguridad la aplicación **"Mobile Iron"**. A través de la misma se podrán realizar los siguientes procedimientos:

1. El Municipio, a través del Departamento de Informática y el Administrador de la Red, y/o a través de la Oficina de Auditoría Interna, podrá intervenir con un teléfono inteligente, mediante la aplicación de Mobile Iron. Dicha intervención aplicará a los equipos adquiridos y provistos por el MAG.

2. Monitoreo y control del tráfico BYOD de dispositivos personales.

3. MAM (Mobile Application Management). A través de Mobile Iron, gestiona las aplicaciones a partir de listas negras y blancas, aplica políticas, entre otras funcionalidades.

4. MDS (Mobile Data Security). Mecanismo encargado de la seguridad de los datos, la protección de los puertos Wi-Fi, Bluetooth y mini USB del dispositivo.

X. RESPONSABILIDADES DEL DEPARTAMENTO DE INFORMATICA SOBRE LOS DISPOSITIVOS MOVILES

A. El personal de servicio del Departamento de Informática establecerá un mecanismo de Administración de Dispositivos Móviles **(Mobile Device Management)** orientado a la gestión y control centralizado de los dispositivos móviles adquiridos por el Municipio de Guaynabo y los personales que se conectarán a la red del Municipio. Este mecanismo permitirá contar con toda la información referente al dispositivo, monitoriarlo, configurar las políticas de seguridad, las aplicaciones que tiene y mantener un historial de cada equipo, entre otras funcionalidades. Estas incluirán entre otras las siguientes:

1. Mantener un inventario de los dispositivos móviles adquiridos por el Municipio que incluya la marca y modelo, versión del sistema operativo, número de serie, MAG address del WiFi, fecha de registración, aplicaciones o licencias instaladas en los dispositivos, entre otras cosas. Tal inventario será mantenido a través de la plataforma de seguridad Mobile Iron.

2. Supervisar la actividad de los dispositivos móviles para el cumplimiento de los estándares definidos.

3. Terminar servicios a dispositivos perdidos y robados, si el Municipio de Guaynabo es el suscriptor del servicio.

4. Hacer un análisis de las ofertas de dispositivos que hay en el mercado para saber cuáles son los más adecuados para manejar la información del Municipio.

5. Borrar todos los datos del Municipio del dispositivo móvil en caso de:
   a. terminación del usuario en el Municipio;
   b. si el dispositivo será reasignado a otro usuario;
   c. si el dispositivo será descartado y/o sustituido.

6. En coordinación con la Oficina de Auditoría Interna, monitoreará las métricas establecidas de uso de data de los dispositivos móviles.

7. Informará a la Gerencia y a la Oficina de Auditoría Interna sobre las incidencias o irregularidades o pérdidas observadas sobre el uso de los dispositivos móviles para investigación.

B. Dispositivos móviles que no hayan sido autorizados para conectarse a la red del Municipio, independientemente de su dueño, estará prohibido de conectarse a la red y no podrá almacenar, contener o transmitir información del Municipio de Guaynabo.

C. Si el Municipio provee un dispositivo móvil a un usuario que utilizaba un dispositivo de propiedad personal ("BYOD") autorizado, en sustitución de éste, el Departamento de Informática removerá la autorización de su uso y cancelará el acceso a la red.

D. La Gerencia y el Departamento de Informática del Municipio de Guaynabo son responsables de asegurarse, mediante divulgación adecuada, que los usuarios sean debidamente advertidos del entendimiento de estas políticas de seguridad para el uso de los dispositivos móviles, así como las expectativas de privacidad sobre el uso de los mismos.

E. En coordinación con la Oficina de Auditoría Interna, podrá realizar evaluaciones periódicas para corroborar que las políticas, procesos y procedimientos se están siguiendo. Actividades de evaluación pueden ser pasivas, por medio de revisión de registros, o activas mediante análisis de vulnerabilidad de los equipos y aplicaciones.

XI. EXPECTATIVAS DE PRIVACIDAD SOBRE LOS DISPOSITIVOS MOVILES

A. El Municipio no mantendrá expectativa de privacidad por el uso de dispositivos móviles adquiridos y provistos por el MAG. A tales efectos, el usuario será apercibido, mediante acuse de recibo, de que el equipo podrá ser monitoreado cuando el MAG lo considere.

B. En el caso de dispositivos de propiedad personal del usuario (BYOD), se mantendrá expectativa de privacidad conforme se establece en el Artículo VII de este Reglamento.

C. Las comunicaciones a través de la red del Municipio de Guaynabo y su sistema de correo electrónico, así como las comunicaciones a través de cualquier aplicación del sistema de información del Municipio de Guaynabo, no se considerará privada.

1. DISPOSITIVOS ADQUIRIDOS POR EL MUNICIPIO

a. Los correos electrónicos y uso del Internet cómo herramientas de trabajo son instrumentos para comunicar, procesar, organizar y recolectar información útil para los empleados, supervisores y jefes de departamentos al igual que para las entidades públicas y privadas. Toda la información contenida en algún equipo adquirido por el Municipio es propiedad del Municipio según lo dispuesto en el Reglamento para el Uso, Control y Custodia de las Computadoras y Accesos al Internet del Municipio.

b. El Municipio, a través del Departamento de Informática, el proveedor del servicio móvil y la Oficina de Auditoría Interna, se reserva el derecho de intervenir con cualquier dispositivo móvil provisto, incluso de manera remota para propósitos investigativos y para propósitos de monitoreo. A tales efectos, se podrán realizar los siguientes procedimientos:

    1. Bloqueo de sitios en Internet por categoría, tales como, pero no limitado a sitios de contenido sexual.
    2. Verificación de "logs" de llamadas realizadas en caso de investigaciones que así lo requieran, solicitados a través del Tribunal a la compañía de servicio.
    3. Verificación de mensajes de texto enviados y recibidos en caso de investigaciones que así lo requieran, solicitados a través del Tribunal a la compañía de servicio.
    4. Monitoreo en presencia del usuario de las aplicaciones contenidas en los dispositivos.
    5. Monitoreo remoto sobre el uso de los dispositivos a través de la aplicación de seguridad "Mobile iron".
    6. Suspensión o inactivación de cualquier aplicación instalada no autorizada.
    7. Suspensión de servicio de data de determinarse uso no adecuado del mismo o que se exceda de la cantidad autorizada para su uso.

c. Los procedimientos de monitoreo preventivos o rutinarios serán documentados por el personal a cargo e informados los resultados a la Gerencia. El Departamento de Informática y la Oficina de Auditoría Interna mantendrá un archivo, electrónico o manual, de las monitorias realizadas como evidencia de hacer cumplir las políticas de seguridad.

d. El Municipio podrá, de considerarlo necesario, implementar servicios o instalar aplicaciones de geolocalización en los dispositivos adquiridos por el Municipio, para propósitos de seguridad y necesidades administrativas. Se dispone que estos servicios o aplicaciones no podrá ser modificadas o desconectas por los usuarios. La

implementación de estos servicios o aplicaciones será determinada por la Gerencia del Municipio para los dispositivos móviles que así lo considere necesario.

2. **DISPOSITIVOS DE PROPIEDAD PERSONAL ("BYOD")**

a. La opción de uso de un BYOD es voluntaria, por lo que no se requerirá a un usuario utilizar su dispositivo personal para propósitos oficiales del Municipio, a no ser por acuerdo y aceptación previa. No obstante, todo usuario de un BYOD autorizado deberá, a solicitud del Municipio, proveer el dispositivo móvil cuando un incidente de seguridad ocurra y/o para instalar algún programa o aplicación para proteger la integridad de la información y el sistema del Municipio de Guaynabo.

b. La opción de uso de un BYOD incluirá la posibilidad de que el número telefónico del usuario pueda ser de conocimiento público, por lo que será apercibido de esto al momento del acuerdo de uso.

c. Si una necesidad legítima surge como respuesta a investigaciones internas, incidentes de seguridad o descubrimiento o solicitudes derivadas de los procedimientos judiciales y administrativos, civiles o penales, podrá requerirse el contenido del inventario o copia de los datos del dispositivo de propiedad personal. En estos casos, los requerimientos se llevarán conforme a las reglas de evidencia que rigen los procesos judiciales a través del Tribunal.

d. El Municipio no será responsable de ningún programa, aplicación, información personal o problemas con el equipo, o la pérdida, daño o robo del dispositivo de propiedad personal ("BYOD"). El Municipio no proveerá reembolso alguno por el plan de voz y data del dispositivo de propiedad personal.

XII. SANCIONES

1. Además de cualquier otra penalidad provista, se podrá cancelar o suspender cualesquiera autorizaciones y permisos de accesos otorgados para el uso de red del Municipio de Guaynabo.

2. Si como parte de un proceso de auditoría o investigación se determina que algún empleado o funcionario municipal no cumplió con las disposiciones contenidas en esta política podrá ser causa para las medidas disciplinarias correspondientes conforme a lo establecido en el Manual de Medidas Disciplinarias para los empleados y funcionarios del Municipio.

3. Cualquier empleado, funcionario o contratista que observe alguna vulnerabilidad o brecha de seguridad, violación a esta política, robo, pérdida, daño o uso indebido de la información privilegiada del Municipio de Guaynabo, deberá informarla inmediatamente mediante un informe de incidente al director de departamento, Departamento de Informática y la Oficina de Auditoría Interna. El no hacerlo, podrá ser causa para las medidas disciplinarias correspondientes conforme a lo establecido en el Manual de Medidas Disciplinarias para los empleados y funcionarios del Municipio.

XIII. CLÁUSULA DE SEPARABILIDAD

1. Las disposiciones de este Reglamento son separadas e independientes entre sí. Cualquier sección, párrafo, oración o cláusula que fuere declarada constitucional o nula por cualquier tribunal con jurisdicción, no afectará la validez de las restantes disposiciones del Reglamento que sean compatibles con dicha decisión judicial.

XIV. VIGENCIA

Este Reglamento comenzará a regir una vez aprobado por esta Legislatura Municipal, firmado por el Alcalde y se haya cumplido con el requisito de publicación dispuesto en la Ley de Municipios Autónomos de Puerto Rico.

Aprobado en Guaynabo, el día 9 de junio de 2016.

_____
Hon. Héctor O'Neill García
Alcalde