GOBIERNO DE PUERTO RICO
MUNICIPIO AUTÓNOMO DE GUAYNABO
LEGISLATURA MUNICIPAL

ORDENANZA

Ordenanza Número 42 **Serie 2024-2025**
(Proyecto Núm. 105)
Presentada por: Administración

PARA DEROGAR EL REGLAMENTO PARA EL USO, CONTROL Y CUSTODIA DE LAS MICROCOMPUTADORAS, COMPUTADORAS PORTÁTILES, CORREO ELECTRÓNICO Y ACCESO AL INTERNET, DEL MUNICIPIO AUTÓNOMO DE GUAYNABO, SEGÚN APROBADO MEDIANTE LA ORDENANZA NÚMERO 157, SERIE 2001-2002, Y ADOPTAR EL REGLAMENTO DE POLÍTICAS Y PROCEDIMIENTOS PARA EL USO, MANEJO Y SOPORTE DE RECURSOS TECNOLÓGICOS DEL DEPARTAMENTO DE INFORMÁTICA, DEL MUNICIPIO AUTÓNOMO DE GUAYNABO; Y PARA OTROS FINES RELACIONADOS.

Por Cuanto: A medida que los avances en la tecnología continúan se hace necesario que las instituciones se mantengan actualizadas. Dichos avances traen consigo riesgos inherentes que deben ser considerados a fin de mitigar los mismos, mediante la adopción e implementación de políticas y procedimientos.

Por Cuanto: Cónsono con dichos avances en la era de la informática, el Gobierno de Puerto Rico ha adoptado leyes, políticas y procedimientos para establecer, desarrollar y coordinar la política pública del Gobierno sobre la innovación, información y tecnología.

Por Cuanto: La utilización de los fondos y la propiedad pública del Municipio Autónomo de Guaynabo debe regirse por normas de sana administración pública y de la reglamentación vigente.

Por Cuanto: El Artículo 1.018 de la Ley 107-2020, según enmendada, conocida como Código Municipal de Puerto Rico, establece, entre otras disposiciones, que el Alcalde será la máxima autoridad de la Rama Ejecutiva del gobierno municipal y en tal calidad le corresponderá su dirección, administración y la fiscalización del funcionamiento del municipio. Además, el Artículo 1.018(c), dispone que, entre las facultades, deberes y funciones del Alcalde, se encuentra el promulgar y publicar las reglas y reglamentos municipales. De igual forma, la Legislatura Municipal tendrá la facultad de aprobar aquellas ordenanzas, resoluciones y reglamentos sobre asuntos y materias de la competencia o jurisdicción municipal, según lo establece en el Artículo 1.039 (m) de la referida la Ley.

Por Cuanto: El Artículo 2.005 del referido Código Municipal establece los deberes generales de los directores de unidades administrativas, entre los cuales se encuentra el establecer sistemas de control que permitan verificar el cumplimiento cuantitativo y cualitativo de los programas, proyectos y actividades de la unidad administrativa.

Por Cuanto: Conforme a una disposición similar de la derogada Ley de Municipios Autónomos, Ley Núm. 81-1991, se aprobó, mediante la Ordenanza Número 157, Serie 2001-2002, el Reglamento Para el Uso, Control y Custodia de las Microcomputadoras, Computadoras Portátiles, Correo Electrónico y Acceso al Internet del Municipio Autónomo de Guaynabo.

Por Cuanto: Es necesario actualizar las normas fundamentales que deben regir los controles básicos a ser establecidos para garantizar el uso adecuado de los recursos relativos a los sistemas de información y velar por el cumplimiento de estas por parte de todo usuario de los sistemas de información del Municipio Autónomo de Guaynabo, incluyendo los empleados y contratistas autorizados a tal uso.

Por Cuanto: Procede derogar el Reglamento Para el Uso, Control y Custodia de las Microcomputadoras, Computadoras Portátiles, Correo Electrónico y Acceso al Internet del Municipio Autónomo de Guaynabo, aprobado Mediante la Ordenanza Número 157, Serie 2001-2002 y adoptar un nuevo Reglamento de Políticas y Procedimientos para el Uso, Manejo y Soporte de Recursos Tecnológicos del Departamento de Informática, que se adapte a las necesidades tecnológicas actuales.

Por Cuanto: Una Comisión Especial analizó las disposiciones y el Reglamento propuestos en esta ordenanza, habiendo rendido un informe de fecha 21 de mayo de 2025.

POR TANTO: **ORDÉNESE POR ESTA LEGISLATURA MUNICIPAL DE GUAYNABO, PUERTO RICO, LO SIGUIENTE:**

Sección 1ra.: Derogar, como por la presente se deroga el Reglamento Para el Uso, Control y Custodia de las Microcomputadoras, Computadoras Portátiles, Correo Electrónico y Acceso al Internet del Municipio Autónomo de Guaynabo, aprobado Mediante la Ordenanza Número 157, Serie 2001-2002, y adoptar un nuevo Reglamento de Políticas y Procedimientos para el Uso, Manejo y Soporte de Recursos Tecnológicos del Departamento de Informática, del Municipio Autónomo de Guaynabo, el cual forma parte de esta pieza legislativa como si en ella estuviera transcrito.

Sección 2da.: Toda Ordenanza, Resolución, acuerdo o parte de los mismos que estén en conflicto con las disposiciones de esta Ordenanza quedan por la presente derogadas.

Sección 3ra.: Esta Ordenanza comenzará a regir inmediatamente después de su aprobación. Copia de la misma le será enviada a la Oficina de Servicios Legislativos (OSL) de la Asamblea Legislativa, según lo dispuesto en el Articulo 1.045(s) de la Ley Num.107-2020, según enmendada, así como a toda aquella dependencia gubernamental estatal y/o municipal pertinente, para su conocimiento y acción correspondiente.

Aprobada por la Legislatura Municipal de Guaynabo, Puerto Rico, reunida en Sesión Ordinaria el día 22 de mayo de 2025.

Luis Carlos Maldonado Padilla
Presidente

Lillian Amado Sarquella
Secretaria

Aprobada por el Hon. Edward A. O'Neill Rosa, Alcalde, el día 27 de Mayo de 2025.

Edward A. O'Neill Rosa
Alcalde

CERTIFICACIÓN

Yo, Lillian Amado Sarquella, Secretaria de la Legislatura Municipal de Guaynabo, Puerto Rico, por medio de la presente CERTIFICO que la que antecede es copia fiel y exacta de la **Ordenanza Número 42, Serie 2024-2025**, intitulada:

"PARA DEROGAR EL REGLAMENTO PARA EL USO, CONTROL Y CUSTODIA DE LAS MICROCOMPUTADORAS, COMPUTADORAS PORTÁTILES, CORREO ELECTRÓNICO Y ACCESO AL INTERNET, DEL MUNICIPIO AUTÓNOMO DE GUAYNABO, SEGÚN APROBADO MEDIANTE LA ORDENANZA NÚMERO 157, SERIE 2001-2002, Y ADOPTAR EL REGLAMENTO DE POLÍTICAS Y PROCEDIMIENTOS PARA EL USO, MANEJO Y SOPORTE DE RECURSOS TECNOLÓGICOS DEL DEPARTAMENTO DE INFORMÁTICA, DEL MUNICIPIO AUTÓNOMO DE GUAYNABO; Y PARA OTROS FINES RELACIONADOS".

CERTIFICO, además, que la misma fue aprobada por la Legislatura Municipal, en la Sesión Ordinaria del día 22 de mayo de 2025, con los votos afirmativos de los siguientes miembros presentes en dicha sesión, los honorables:

Aida M. Márquez Ibáñez
Ángel L. O'Neill Pérez
Carlos M. Santos Otero
Gabriela M. Alonso Ribas
Guillermo Urbina Machuca
Juan Reyes Nieves
Miguel A. Negrón Rivera
Niurka Del Valle Colón
Patricia S. Martínez Reyes
Rafael Ruiz Comas
Joaquín Rosado Morales
Luis C. Maldonado Padilla

Excusados: Honorables Gabriel A. Báez Lozada, Jorge R. Marquina González-Abreu, Wilma I. Pastrana Jiménez y María Elena Vázquez Graziani.

Fue aprobada por el Hon. Edward A. O'Neill Rosa, Alcalde, el día 27 de mayo de 2025.

En testimonio de lo cual firmo la presente certificación, bajo mi firma y el sello oficial de esta municipalidad de Guaynabo, el día 27 de mayo de 2025,

Lillian Amado Sarquella
Secretaria

Reglamento de Políticas y Procedimientos para el Uso, Manejo y Soporte de Recursos Tecnológicos del Departamento de Informática

NÚMERO: 2525

Fecha: 28 de mayo de 2025

Narel W. Colón

Aprobado: *Narel W. Colón*

Secretaria de Estado Interina

Departamento de Estado

DOCUMENTO ELABORADO POR EL DEPARTAMENTO DE

INFORMÁTICA

MUNICIPIO AUTÓNOMO DE GUAYNABO

CIUDAD CINCO ESTRELLAS

APROBADO MEDIANTE ORDENANZA NÚMERO 42, SERIE 2024-2025

Reglamento de Políticas y Procedimientos para el Uso, Manejo y Soporte de Recursos Tecnológicos del Departamento de Informática

DOCUMENTO ELABORADO POR EL DEPARTAMENTO DE

INFORMÁTICA

MUNICIPIO AUTÓNOMO DE GUAYNABO
CIUDAD CINCO ESTRELLAS

APROBADO MEDIANTE ORDENANZA NÚMERO 42, SERIE 2024-2025

Tabla de Contenido

I. DISPOSICIONES GENERALES

1. Introducción

Este documento establece las Políticas y Procedimientos para el uso, manejo y soporte de recursos tecnológicos (equipos, programas, datos e información) propiedad del Municipio Autónomo de Guaynabo (MAG) y de dispositivos no adquiridos por el MAG (BYOD) que los usuarios emplean para conectarse a los sistemas de información del MAG.

2. Objetivo

El objetivo del documento es establecer las pautas para la utilización adecuada de los fondos y la propiedad pública en el Municipio Autónomo de Guaynabo. Además, se busca regular el uso de herramientas tecnológicas, con el propósito de procesar, organizar y recolectar información útil para empleados, supervisores, jefes de departamentos y entidades públicas y privadas. Las normas establecidas en este reglamento buscan garantizar el uso apropiado de estas herramientas en beneficio del MAG y sus ciudadanos. Asimismo, las políticas de uso y seguridad de los sistemas computadorizados tienen como objetivo proteger la confidencialidad, integridad y disponibilidad de los datos y activos tecnológicos, basándose en una identificación previa de los riesgos a los que está expuesta la información y considerando todos los procesos, sistemas y personal involucrado.

3. Alcance

Las políticas y procedimientos establecidos en este documento abarcan todos los recursos tecnológicos (equipos, programas y sistemas) autorizados y adquiridos por el Municipio Autónomo de Guaynabo y su Departamento de Informática, así como los equipos tecnológicos BYOD, que son utilizados por funcionarios, empleados, contratistas y proveedores para acceder a la red, programas y sistemas municipales. Estas políticas y procedimientos se aplican a toda persona que utilice los mencionados recursos informáticos, incluyendo funcionarios, empleados, contratistas y proveedores.

4. 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.* 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

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

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 cuando 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)."*
>
> *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.

La Ley 122-2019, conocida como la Ley de Datos Abiertos del Gobierno de Puerto Rico, promulgada el 1 de agosto de 2019. Esta ley establece como principio de política pública la gestión efectiva de los datos gubernamentales para apoyar los procesos de innovación en todos los sectores de Puerto Rico y promueve la transparencia fiscal y administrativa, facilitando el acceso público a los datos gubernamentales.

La Ley 40–2024, conocida como la Ley de Ciberseguridad del Estado Libre Asociado de Puerto Rico, fue aprobada el 18 de enero de 2024. Esta ley busca fortalecer la infraestructura de seguridad cibernética del gobierno y proteger los datos sensibles contra amenazas y ataques cibernéticos.

En atención a las disposiciones legales antes discutidas y en virtud de las facultades y poderes que nos confieren los Artículos 3.009, 6.003, 6.005 y 8.013, se adopta y promulga el Reglamento de Políticas y Procedimientos Tecnológicos: Uso, Manejo y Soporte de Recursos.

II. EQUIPOS INFORMÁTICOS

Los equipos informáticos (computadoras, teléfonos celulares y de escritorio, impresoras, '*tablets*', multifuncionales, otros), de ahora en adelante llamados *equipo* o *equipos*, son responsabilidad de todos los que laboran en el municipio. Sin embargo, cada usuario que tenga un *equipo* asignado para su operación diaria deberá velar con mayor énfasis por el buen uso de este.

1. Adquisición

1.1. No se adquirirán *equipos* que no sean compatibles con las soluciones de seguridad adoptadas por el MAG.

1.2. Se prohíbe la adquisición de aquellas tecnologías (equipo y/o programas) que la Comisión Federal de Comunicaciones (FCC) clasifique como restringido por representar un riesgo para la seguridad nacional.

2. Uso

2.1. Los *equipos* adquiridos por el MAG, y provistos a sus funcionarios y empleados, serán utilizados para gestiones oficiales.

2.2. La utilización de los *equipos* se limita exclusivamente a las funciones y tareas asignadas a cada empleado en relación con su departamento. Queda estrictamente prohibido el uso de estos *equipos* para fines personales. No deberán ser proporcionados a personas ajenas.

2.3. Los *equipos* tendrán instaladas las aplicaciones necesarias para realizar sus funciones oficiales.

2.4. Las operaciones realizadas a través de los *equipos* pueden generar responsabilidad por parte del MAG. Por tanto, los usuarios que los tengan asignados no tienen expectativa de privacidad alguna con relación al uso y a los accesos realizados. El MAG se reserva el derecho a intervenir, auditar y revisar sin previo aviso, los accesos realizados por los usuarios a través de los *equipos* 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 *equipos* 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.

2.5. Los usuarios mantendrán el sistema operativo original de los *equipos*, con los parches de seguridad y actualizaciones del fabricante, los cuales previenen la instalación de programas maliciosos ("malwares"). No se autorizará su uso ni acceso a la red del MAG a aquellos *equipos* cuya

configuración haya sido alterada.

2.6. No se podrá hacer cambio de "Sim Card", ni instalar "Sim Cards" personales en los equipos del Municipio.

2.7. ANTIDISCRIMEN

a. Se prohíbe la utilización de los *equipos* para enviar, recibir o crear documentos de contenido discriminatorio por razón de raza, género, credo, ideas políticas, u organización social o nacional. También se prohíbe terminantemente cualquier contenido que pueda catalogarse como hostigamiento sexual.
b. Se prohíbe la divulgación por cualquier medio de opiniones específicas con relación a raza, origen nacional, sexo, orientación sexual, edad, ideas o creencias religiosas o políticas, así como opiniones sobre personas con impedimento físico o mental.

3. Instalación de Equipos

3.1. Las instalaciones de *equipos* y periféricos serán realizadas por el personal del Departamento de Informática. De ser necesario, se podrá delegar dicha tarea con la previa autorización del Director del Departamento de Informática. Los motivos son:

a. Mantener la consistencia.
b. Minimizar el tiempo y la productividad perdida debido a fallas en los equipos.
c. Asegurar el cumplimiento con las normas y políticas de este documento o cualquier otro que aplique debidamente.
d. Implantar controles adecuados.

3.2. La instalación de *equipos* se hará observando las siguientes guías:

a. Los *equipos* para uso interno de las oficinas del MAG se instalarán en lugares adecuados, lejos de polvo y tráfico de personas.
b. En las áreas de atención directa al público, los *equipos* se instalarán en lugares adecuados, que no atenten contra la seguridad humana.
c. Se le hará disponible al Departamento de Informática, así como las áreas operativas un plano actualizado de las instalaciones eléctricas.
d. Las instalaciones eléctricas y de comunicaciones, estarán de preferencia fija o en su defecto resguardadas del paso de personas o máquinas, y libres de cualquier interferencia eléctrica o magnética.
e. Las instalaciones cumplirán con los requerimientos de los *equipos*, cuidando las especificaciones del cableado y de los circuitos de protección necesarios.

f. En ningún caso se permitirán instalaciones improvisadas o sobrecargadas.
g. Cuando en la instalación se alimenten elevadores, motores y maquinaria pesada, se deberá tener un circuito independiente, exclusivo para el equipo y/o red.

4. Dispositivos de escritorio

Un dispositivo de escritorio, también conocido como "desktop", es un tipo de computadora diseñada para ser utilizada en un lugar fijo y no está diseñada para ser transportada con facilidad. Estos *dispositivos* suelen ser más grandes que los *dispositivos* móviles y tienen componentes separados, como la torre o cpu, monitores, teclado y el ratón o "mouse".

4.1. Encendido

Al comienzo del día toda computadora deberá ser encendida en el siguiente orden:

a. Monitor
b. Impresora

4.2. Otros periféricos

a. Unidad Central de Procesamiento (CPU)

4.3. Precauciones

Las siguientes guías deberán ser observadas y seguidas con el propósito de proteger las computadoras de posibles daños físicos:

a. El consumo de comidas, bebidas y/o fumar no está permitido por lo menos a tres (3) pies alrededor de cualquier *equipo* electrónico.
b. Las computadoras no podrán ser movidas de su área sin previa autorización del Departamento de Informática. En dicho caso, el Departamento de Informática enviará un técnico para ofrecer apoyo.
c. Está prohibido abrir o desmantelar (parcial o completamente) el *equipo*. El único personal autorizado a tales efectos son recursos autorizados del Departamento de Informática.
d. Está prohibido la instalación o conexión de cualquier tipo de *equipo* o aditamento a las computadoras. El único personal autorizado a tales efectos es el correspondiente al Departamento de Informática.
e. No está permitido golpear los *equipos*.
f. Siempre que se vaya a apagar los *equipos* es necesario verificar que:
    i. Todas las aplicaciones (programas) estén cerradas.
    ii. No haya archivos abiertos.

g. Está prohibido que cualquier persona desconecte la electricidad de cualquier equipo sin la debida autorización del Departamento de Informática. La única excepción a esta norma será en casos de Emergencia donde se deberá identificar alguna persona dentro del área correspondiente que sepa realizar esta tarea.
h. Se prohíbe la utilización de "screensavers" con fotos personales, de artistas, modelos, deportistas ni mucho menos fotos de calendarios desnudos y/o semidesnudos.

4.4. Monitor

El monitor representa la manera de visualizar los trabajos, documentos, aplicaciones, etc. El mismo deberá recibir sumo cuidado por la relevancia que tiene. Para prevención se deberá observar lo siguiente:

a. Se debe evitar el contacto con él lo más posible.
b. No deberá ser golpeado con nada.
c. No se limpiará el monitor con aerosoles ni líquidos.

4.5. Teclado

El teclado nos permite ejecutar comandos, apoya la creación de documentos, y otros. El mismo no debe ser golpeado con fuerza excesiva. No debe ser limpiado con aerosoles y/o líquidos.

4.6. Ratón (Mouse)

Al igual que el teclado, el ratón permite ejecutar comandos en la computadora. El mismo no debe ser abierto ni golpeado y podrá ser utilizado en conjunto con un 'mouse pad'.

4.7. Web Cam y Bocinas

Estos nos permiten tener reuniones virtuales o llamadas a traves de las herramientas de Microsoft Teams. De esta manera podemos ser mas eficientes y colaborativos en nuestras tareas diarias. De igual manera estos equipos no pueden ser abierto ni golpeados y podran ser utilizando en conjunto con los demas componentes de la computadora.

4.8. Documentación

a. Toda documentación del equipo y/o programas permanecerá en el Departamento de Informática.
b. En aquellos casos en que sea necesario efectuar el proceso de mantenimiento de equipos y/o programas se documentará en un boleto del sistema que maneja el HelpDesk.

4.9. Localización de los *equipos*

Ningún empleado municipal está autorizado a mover *equipos* sin autorización del Departamento de Informática. El procedimiento

establecido para estos propósitos es el siguiente:

a. El usuario que necesite el movimiento de un *equipo* de computadoras o impresoras deberá notificarlo a su supervisor inmediato mediante la creación de una solicitud de servicio.
b. El usuario completará la forma "*Formulario de Ayuda al Helpdesk*" solicitando el servicio de mudanza donde describirá clara y detalladamente las razones para la solicitud.
c. El Director del Departamento o personal autorizado correspondiente aprobará el formulario previo a ser remitido al Director del Departamento de Informática para su aprobación y acción.
d. El Director del Departamento de Informática o su representante autorizado será responsable de:
    i. Asignar a un técnico para que ofrezca apoyo en el movimiento del equipo correspondiente, de ser necesario.

5. Dispositivos móviles

Un dispositivo móvil, está diseñado para ser transportado fácilmente y suelen tener integrado todos los componentes necesarios. Algunos ejemplos de los dispositivos móviles adquiridos por el MAG son: Laptops, Tablets, Teléfonos móviles o celulares, equipo móvil de acceso a internet (Hotspot) y otros.

5.1. General

a. Los funcionarios y empleados no deben poner en peligro la información confidencial del MAG a través del uso de los *dispositivos* móviles, por lo que no deberán permitir que otras personas (por ejemplo: familia, amigos, compañeros de trabajo) utilicen los *dispositivos* asignados a usted y adquiridos por el MAG.
b. Será ilegal y una violación el uso de dispositivos móviles para asuntos que no sean inherentes a su trabajo o asignación especial para el cual fue otorgado.
c. Ningún funcionario o empleado podrá trasladar, transferir, prestar o de otro modo disponer de la propiedad pública sin la autorización previa del Director del Departamento de Informática.
d. La Oficina de Auditoría Interna coordinará con el Departamento de Informática para intervenir en auditorias de dispositivos móviles para velar por el uso apropiado.
e. Los funcionarios y empleados deberán supervisar el uso de su dispositivo móvil para prevenir la divulgación accidental de información

del MAG.

f. De determinarse que el funcionario o empleado ha hecho uso indebido de un dispositivo móvil asignado, se le solicitará la entrega inmediata del equipo y éste podrá ser sancionado.
g. Todo equipo bajo la custodia de un empleado debe estar a la vista en todo momento cuando este se encuentre fuera de alguna facilidad municipal.
h. Todo funcionario o empleado será responsable personalmente por el valor de la propiedad bajo su custodia en caso de daño o pérdida, si la causa de la pérdida o el daño fue su culpa o negligencia inexcusable.
i. En caso de surgir una pérdida o robo del *dispositivo* móvil, debe abrir una querella Policíaca y comunicarlo de inmediato al Director o representante autorizado del Departamento de Informática, a fin de que el MAG pueda activar o realizar una búsqueda y localización a través de sistemas de rastreo. El MAG, mediante dichos sistemas podrá intervenir con el dispositivo móvil obviando la contraseña de seguridad ("password") para acceder el mismo.
j. Si la pérdida de la propiedad fue debido a fuerza mayor como fuego, inundación, robo, huracán, terremoto u otro accidente análogo, el funcionario a cargo de la propiedad así lo hará constar y notificará al Director del Departamento de Informática, quién designará a una persona para que realice una investigación, quién no podrá ser la persona que tenía a cargo la propiedad perdida.
k. Si se determinara que hubo culpa, falta o negligencia de parte del funcionario o empleado que tenía bajo su custodia la propiedad, dicho empleado pagará el valor de la referida propiedad. Si no satisface el valor de la propiedad de su propio peculio, se le descontará el mismo del sueldo.
l. En caso de que un *dispositivo* propiedad del MAG se extravíe, sea robado, ocurra un cese laboral con el MAG, o se detecte una amenaza de seguridad en el mismo, el equipo técnico del Departamento de Informática, con el permiso previo del Director, podrá borrar a distancia los datos y aplicaciones contenidos en el dispositivo.
m. Los usuarios de dispositivos adquiridos por el MAG, y provistos para sus funciones oficiales, no podrán realizar limpiezas ("wipe out") a los equipos.
n. 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. Las aplicaciones de seguridad adoptadas por el MAG podrán desconectar de la red los dispositivos y "BYOD" si no se establece un código de acceso.

5.2. Laptop / Computadora portátil

a. Transportación

i. Siempre que la computadora portátil sea trasladada de un lugar a otro, independientemente de la distancia, la misma deberá ser apagada, desconectada y transportada de manera segura, para que proteja adecuadamente la unidad.

b. Precauciones Adicionales

i. Si no contiene pantalla táctil, no tocar la pantalla.

ii. No se limpiará la pantalla con aerosoles ni líquidos.

iii. No se utilizará ningún cable de corriente eléctrico o suplidor de energía (power supply) que no sea el que trajo la máquina o un reemplazo del manufacturero. Utilizar un suplidor de energía erróneo pudiera ocasionar que los circuitos de la máquina se quemen, haciéndola inservible y desestimando la garantía.

iv. En caso de tormentas eléctricas y/lo fluctuaciones en el servicio eléctrico, se deberá desconectar el equipo del tomacorriente. Si es necesario continuar su uso y la batería está agotada, tenga la precaución de conectarlo a una unidad de batería de resguardo ("UPS").

v. Siempre mantenga la computadora configurada con un salvador de pantalla ("screensaver") que se active a no más de cinco (15) minutos al detectar que no hay actividad.

vi. Nunca guarde su computadora portátil encendida. Las computadoras portátiles generan mucho calor y necesitan ventilación. Podrían dañarse los componentes internos o generar un incendio si están confinadas encendidas en su bulto.

5.3. Nunca se pondrá nada sobre la computadora portátil, esté abierta o cerrada.

5.4. Tablet

a. Debe mantener la Tablet en su funda o cubierta protectora para evitar rayones y daños por caídas. La cubierta protectora puede reducir la entrada de polvo en los puertos del dispositivo.

b. Mantenga la tablet alejada de líquidos, ya que pueden causar daños graves al dispositivo.

c. Evite la acumulación de polvo y suciedad, ya que pueden afectar el rendimiento de la Tablet y ayude a mantener el dispositivo en buenas condiciones.

5.5. Teléfono Móvil / Celular

a. Mantén el teléfono bloqueado. Utilice un PIN, huella digital o reconocimiento facial para evitar accesos no autorizados.
b. Protege el dispositivo móvil de caídas y golpes con un protector resistente.
c. Evite exponerlo a temperaturas extremas. No deje el teléfono en lugares muy calientes o fríos, ya que puede dañar la batería y los componentes internos.
d. Evite conectarte a redes Wi-Fi abiertas o públicas.
e. Evite el contacto con líquidos. Aunque existen teléfonos resistentes al agua, debe evitarse la exposición a líquidos para prevenir daños.

5.6. Dispositivos de propiedad personal del usuario (BYOD)

a. El MAG podrá proveer acceso o conexión a la red del MAG a aquellos empleados, funcionarios o contratistas a través de sus dispositivos móviles personales, siempre y cuando responda a la necesidad del servicio que realizan en el MAG.
b. La opción de utilizar su dispositivo móvil personal será voluntaria.
c. El usuario de un dispositivo móvil personal estará sujeto a las normas y políticas de seguridad adoptadas por el MAG en el reglamento de BYOD, aprobado mediante Ordenanza Núm. 109, Serie 2015-2016. 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.
d. El usuario de un BYOD se compromete a notificar al MAG sobre la transferencia o intercambiarlo de su dispositivo móvil, a fin de evitar que la data propiedad del MAG pueda ser utilizada por terceras personas ajenos a la gestión municipal.

5.7. Puntos de acceso a Internet portátil (Portable hotspots)

a. El control y registro de los dispositivos portátiles para acceso a internet será responsabilidad del Departamento de Finanzas.
b. Deberá mantenerse un registro electrónico sobre la prestación del dispositivo de internet portátil que indique entre otras cosas lo siguiente:
    i. Nombre del funcionario o empleado al que se le asigne.
    ii. Propósito del uso.
    iii. Número de identificación del dispositivo.

iv. Firma del prestamista y del prestatario.

6. Multifuncionales

6.1. Las impresoras multifuncionales están diseñadas para operar de manera óptima en el lugar específico asignado por el MAG, y solo personal autorizado puede cambiar su ubicación.

6.2. Es crucial que las impresoras se mantengan únicamente en las zonas que han sido previamente aprobadas para su uso. Estos equipos se instalan en áreas estables, alejadas de cualquier fuente de calor o humedad, garantizando así un espacio adecuado para su correcta ventilación.

6.3. La conexión eléctrica de las impresoras multifuncionales debe seguir estrictamente las especificaciones proporcionadas por el fabricante, por lo cual no se pueden conectar a adaptadores o extensiones eléctricas no autorizados, para asegurar tanto el funcionamiento eficiente del equipo como la seguridad en el lugar de trabajo.

6.4. Únicamente se pueden utilizar toners y papeles que hayan sido autorizados explícitamente por el MAG. El uso de materiales no autorizados puede resultar en daños al equipo y en una disminución en la eficiencia de los recursos municipales.

6.5. Está prohibido utilizar los equipos multifuncionales para imprimir, escanear, copiar o enviar documentos que no estén relacionados con las actividades oficiales del MAG. Esto incluye, pero no se limita a, documentos personales, correspondencia privada, y cualquier otro tipo de material no relacionado con las funciones del departamento.

7. Servidores

7.1. La instalación y/o configuración de todo servidor conectado a la red municipal será responsabilidad del Departamento de Informática.

7.2. Durante la configuración del servidor se debe autorizar/controlar el uso de los recursos del sistema y de la red, principalmente la restricción de directorios, permisos y programas a ser ejecutados por los usuarios.

7.3. Los servidores que proporcionen servicios a través de la red e Internet deberán:

a. Funcionar 24 horas del día los 365 días del año.
b. Recibir mantenimiento preventivo según sea necesario.
c. Recibir mantenimiento semestral que incluya depuración de “logs”.
d. Recibir mantenimiento anual que incluya la revisión de su configuración.
e. Ser monitoreados por el personal técnico de MAG.

7.4. Los servidores deberán ubicarse en un área física que cumpla las normas para un centro de telecomunicaciones:
   a. Acceso restringido.
   b. Temperatura adecuada al equipo.
   c. Protección contra descargas eléctricas.
   d. Mobiliario adecuado que garantice la seguridad de los equipos.

8. Seguridad

8.1. El MAG ha adoptado varios mecanismos y soluciones de seguridad por los cuales se podrán realizar los siguientes procedimientos:
   a. Intervenir con teléfonos inteligentes. Dicha intervención aplicará a los equipos adquiridos y provistos por el MAG.
   b. Monitoreo y control del tráfico BYOD de dispositivos personales.
   c. Gestionar aplicaciones a partir de listas negras y blancas, aplicar políticas, entre otras funcionalidades.
   d. Implementar seguridad de los datos, la protección de los puertos Wi-Fi, Bluetooth y mini USB de un dispositivo.

8.2. Informática hará uso de aplicaciones de seguridad para la administración de dispositivos móviles (MDM, por sus siglas en inglés) que le permite gestionar y proteger dispositivos móviles que se utilizan para acceder a la red.

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

8.4. Los datos propiedad del MAG serán cifrados o "encriptados" utilizando los siguientes métodos de encriptado.
   a. TLS (Transport Layer Security): Es un protocolo de seguridad que se utiliza para cifrar los datos transmitidos a través de la red. TLS asegura que la comunicación entre dos puntos, como un navegador web y un servidor, sea segura y privada.
   b. AES-256 (Advanced Encryption Standard): Es un algoritmo de cifrado simétrico que se utiliza para proteger los datos almacenados. AES-256 utiliza una clave de 256 bits para cifrar y descifrar la información, lo que lo hace extremadamente seguro y resistente a ataques.

III. ACCESOS

El control de acceso es un componente crucial para garantizar la seguridad y protección de los datos, equipos y dispositivos del MAG. Permite que solo los usuarios autorizados accedan a la información. Al restringir el acceso a equipos y dispositivos, se previene el uso indebido o el daño. Solo aquellos con permisos adecuados pueden utilizarlos. Se reducen los costos asociados con incidentes de seguridad, al evitar el acceso no autorizado o el uso inapropiado de recursos. Los accesos permiten a los empleados acceder rápidamente a los recursos necesarios y esto mejora la eficiencia y la productividad.

1. Autenticación Multifactorial

El MAG ha adoptado la política de autenticación multifactorial (MFA). El MFA es una medida de seguridad que requiere que los usuarios completen múltiples formas de verificación antes de acceder a aplicaciones en la nube. Esto incluye la autenticación mediante la validación de un dato que el usuario sabe (como una contraseña) y que el usuario tiene (como un dispositivo móvil). La implementación de MFA ayuda a proteger la confidencialidad, integridad y disponibilidad de la información, reduciendo así el riesgo de accesos no autorizados y posibles vulnerabilidades. Su objetivo es mitigar riesgos de seguridad derivados del uso de contraseñas comprometidas o accesos no autorizados y fortalecer la infraestructura de seguridad cibernética de la organización.

1.1. Informática revisará periódicamente los accesos otorgados a fin de identificar cambiados organizacionales que impacten los acceso y/lo roles otorgados.

2. Cuentas de Usuario

Las cuentas de usuario creadas en el MAG son una identificación creada en un sistema informático que permite a una persona iniciar sesión en su computadora, red o servicio de información. Estas cuentas tienen asignado un nombre de usuario y una contraseña para proteger el acceso. Estas cuentas de usuarios ayudan a mantener la seguridad y la privacidad de la información a la vez que facilitan la gestión de recursos y la administración del sistema.

2.1. Toda cuenta de usuario deberá estar protegida por contraseña.

2.2. Está estrictamente prohibido compartir el acceso a la cuenta de usuario que se le ha otorgado.

2.3. Cada usuario será responsable de cualquier uso que se le dé a alguna de sus cuentas, así como el uso indebido ésta.

2.4. Cada usuario será responsable por las transacciones efectuadas con su nombre de usuario y contraseña.

2.5. Solicitud de Cuenta de usuario.

a. El director de cada departamento o representante autorizado deberá realizar una solicitud formal, para la creación de toda nueva cuenta de usuario para el personal que labora en su área (ver Formulario Solicitud de Ayuda Helpdesk en el portal interno del Municipio). En dicha solicitud se indicará los accesos que debe tener el nuevo usuario. Dicha solicitud deberá estar aprobada por el director o su representante autorizado.

b. El director evaluará la solicitud de acuerdo con las necesidades del MAG y recursos disponibles. De ser aprobada la solicitud, éste se enviará al director del Departamento de Informática para su aprobación.

c. El director del Departamento de Informática, evaluará la solicitud y emitirá recomendación a tono con lo solicitado.

2.6. El Help Desk del MAG es el encargado de asignar las cuentas a los usuarios para el uso de los sistemas, observando las políticas para la creación de cuentas de usuarios.

2.7. A cada cuenta de usuario se le asigna un nivel de seguridad. Se prohíbe intentar o lograr evadir dicho nivel de seguridad para lograr acceso a objetos para los cuales el usuario no tenga permiso.

2.8. Las cuentas de usuario permiten acceso a los sistemas y recursos de cómputo y son propiedad de MAG. Se usarán exclusivamente para actividades relacionadas al MAG.

2.9. Las cuentas de usuario son personales e intransferibles. Se permite su uso única y exclusivamente durante la vigencia de derechos del usuario.

2.10. Recursos Humanos reportará al personal de Informática cuando un usuario deje de tener una relación de laboral con el MAG o cuando toma una licencia de más de 30 días consecutivos.

2.11. El Helpdesk procederá a inactivar los accesos físicos y lógicos (sistemas, oficinas, etc) una vez reciba la notificación para que sea de cese de labores.

2.12. En el momento en que se desee reactivar una cuenta de usuario, el director de Departamento o designado deberá aprobar este servicio. Esto aplica a toda cuenta de empleado que esté inactiva por razón de licencia a largo plazo, o a consultores/asesores del MAG que hayan renovado su contrato.

2.13. Nombre de Cuentas. El nombre de una cuenta deberá estar conformado por la primera letra del nombre y primer apellido del usuario y su contraseña asignada. La sintaxis de la cuenta será napellido@guaynabocity.gov.pr. La regla puede variar si la combinación ya está asignada a otro usuario.

3. Contraseñas

Una **contraseña** es una combinación secreta de caracteres (letras, números y símbolos) que se utiliza para proteger el acceso de una cuenta, dispositivo o sistema. La función principal de una contraseña es garantizar que solo las personas autorizadas puedan acceder a la información o recursos protegidos. Las contraseñas proporcionan protección contra el acceso no autorizado. Ayudan a mantener el registro de accesos y la confidencialidad a la información.

3.1. Las contraseñas permiten acceso a las computadoras y programas que están provistas en los sistemas MS Office, correo electrónico, internet y otras aplicaciones necesarias para el desempeño de una labor.

3.2. Se concede acceso sólo a empleados del MAG o personal externo realizando tareas especiales.

3.3. Cada usuario será responsable de su contraseña y su uso. Está terminantemente prohibido:

a. Divulgar su contraseña.
b. Prestar su contraseña a cualquier persona.
c. Anotar su contraseña en un lugar visible o de fácil acceso.

3.4. Después de crear una cuenta de usuario, se le notificará por teléfono al usuario para que acceda al sistema y establezca su contraseña privada. Esta contraseña provisional expira en 24 horas, si la cuenta no es accedida.

3.5. Como parte de la política para cambio de contraseñas el sistema le exigirá a cada usuario que cambie su clave de acceso cada noventa (90) días calendario, de manera que se pueda prevenir el acceso sin autorización pero el usuario puede cambiarla antes si lo considera necesario.

3.6. En caso de olvido de la contraseña o bloqueo de la cuenta por parte del usuario, podrá solicitar asistencia al Help Desk para el cambio de contraseña.

3.7. La contraseña debe tener un *largo mínimo de 8 caracteres*. Tener al menos una *letra mayúscula, una minúscula o un símbolo* y, además, debe incluir *al menos un dígito numérico*. No se permite utilizar ninguna de las *5 contraseñas anteriores*. La implementación de estas reglas está condicionada a la capacidad de la aplicación de soportar dicha

complejidad.

3.8. Las cuentas de Administrador deberán tener al menos 16 caracteres.

4. Tarjetas de acceso

Una tarjeta de acceso es una tarjeta física que contiene puede contener un chip, una banda magnética o tecnología RFID (Identificación por Radiofrecuencia). Esta tarjeta almacena información que identifica al usuario ante un sistema de control de acceso. Se utiliza para permitir o denegar el acceso a un lugar o sistema. Los sistemas que utilizan tarjetas de acceso llevan un registro de cuándo y quién accede a las áreas o sistemas restringidos.

4.1. Los usuarios no deben perder de vista la tarjeta de acceso y deben guardarla en un lugar seguro cuando no la estés utilizando.

4.2. Las tarjetas de acceso son asignadas individualmente y no deben ser compartidas con otras personas.

4.3. Si el usuario pierde su tarjeta de acceso o cree que ha sido robada, debe notifícalo de inmediato a la seguridad y al Help Desk para que puedan desactivarla y evitar un uso no autorizado.

4.4. Las tarjetas de acceso no deben se dobladas, rayes o expuestas a campos magnéticos fuertes.

5. Acceso No Autorizado

La implementación de cuentas de menor privilegio (*Least Privilege*) ayuda a proteger la confidencialidad, integridad y disponibilidad de la información, reduciendo así el riesgo de accesos no autorizados y posibles vulnerabilidades.

5.1. Se observará el principio de menor privilegio. Este enfoque busca limitar el acceso de los usuarios, a solo aquellos recursos y funciones que son esenciales para su trabajo y no más de lo necesario.

5.2. El uso o aceptación de información obtenida por medios ilegales constituye una violación a los derechos de los otros y está sujeta a acción disciplinaria.

5.3. Cualquier usuario que encuentre “una puerta” o falla de seguridad en cualquier sistema de información del MAG está obligado a reportarlo a los administradores del sistema.

5.4. No se puede hacer uso de “fallas de seguridad” o contraseñas especiales para dañar los sistemas o ganar acceso no autorizado.

5.5. Los usuarios no deberán crear o ejecutar sistemas o mecanismos tendientes a alterar o evitar la contabilidad o auditoria implementada.

5.6. Los accesos serán monitoreados como parte de la estructura de control y seguridad del sistema. El MAG a través de la Oficina de Auditoría Interna y el Administrador del Sistema se reserva el derecho de auditar, vigilar y fiscalizar los sistemas y de acceso.

6. Monitoreo No Autorizado

6.1. No se permite el uso de los recursos de cómputo para realizar monitoreo no autorizado de comunicaciones electrónicas.

IV. PROGRAMAS INFORMÁTICOS

Los programas informáticos son aplicaciones o software diseñado para realizar tareas específicas en los equipos. Estos programas pueden variar desde simples herramientas de procesamiento de texto hasta aplicaciones complejas de diseño gráfico, de planos, bases de datos, navegadores web y más. Ejemplos de programas informáticos utilizados en MAG incluyen: Navegadores web, Procesadores de texto como Microsoft Word, Hojas de cálculo como Microsoft Excel, Sistemas operativos como Windows, macOS o Linux, Bases de datos como Microsoft SQL Server, herramientas de producción como SAP y Kronos. Cada programa tiene su propósito específico y contribuye a una variedad de tareas y servicios entro de la operación diaria del MAG.

1. Uso

1.1. Los programas informáticos, así como el sistema de correspondencia interna (e-mail), el acceso al Internet y los documentos que existen en los mismos son propiedad del MAG; y solo podrán utilizarse para propósitos lícitos, prudentes, responsables y dentro de las funciones o poderes de este MAG. Los sistemas son para uso exclusivo de los empleados, funcionarios y contratistas que laboran para el MAG y para los cuales existe un acceso autorizado para ello.

2. Instalación de programas

2.1. La instalación de programas en dispositivos y en el ámbito de la red de comunicaciones será controlada por el director del Departamento de Informática.

2.2. Está prohibido instalar cualquier aplicación o programa que no haya sido legalmente adquirido y no sea propiedad del MAG.

2.3. Se le prohíbe a los usuarios la instalación de aplicaciones destinadas al acceso a redes sociales (como Facebook, Instagram, Twitter, etc.) en los dispositivos del MAG. Esto incluye tanto las aplicaciones preinstaladas como las descargadas posteriormente.

2.4. No está permitido crear ni mantener programas que recolecten de manera secreta y oculta información acerca de los usuarios ni de sus comunicaciones.

2.5. Solamente el personal del Departamento de Informática está autorizado a la instalación y remoción de programas en los dispositivos del MAG.

2.6. Todos los programas instalados por el MAG tienen licencia de uso. Durante

el proceso de instalación, los programas podrían requerir la siguiente información:

a. Nombre del Usuario (Municipio de Guaynabo)
b. Entidad o Compañía (Gobierno de Puerto Rico)
c. Número de Licencia: (número de licencia correspondiente)
d. No se permite utilizar:
    i. Nombres de Usuarios o nombres de compañías distintas a Gobierno de Puerto Rico. (Esto se debe hacer claro a los proveedores de sistemas).
    ii. Utilizar números de Licencia incorrectos o que no correspondan al producto siendo instalado.
    iii. Repetir números de Licencia (excepción: Licencias adquiridas en grupo).

2.7. Se prohíbe la reproducción, sustitución o modificación de cualquier programa adquirido o desarrollado por Departamento de Informática sin la autorización de su autor o del director del Departamento de Informática. Sea para beneficio personal de sus usuarios o terceras partes, tal acción va en contra de los mejores intereses del MAG, ya que viola la Ley de Propiedad Intelectual y/o Derechos de Autor.

2.8. Cualquier copia de resguardo o reemplazo de medio que sea necesario podrá ser realizado solamente por el Departamento de Informática. Se mantendrá un archivo detallando la fecha, el medio y la razón para el resguardo o transferencia, cada transacción en dicho archivo deberá estar autorizada por el director del Departamento de Informática o su subalterno.

2.9. Será responsabilidad del Departamento de Informática cumplir con todos los requerimientos legales de las instalaciones y asegurarse de que no existan más copias instaladas que licencias.

3. Internet

3.1. Normas generales al uso del Internet

a. El servicio de Internet se utilizará como un instrumento suplementario para la búsqueda de información oficial a través del gobierno federal, universidades, corporaciones y compañías privadas sobre tecnología, leyes y procedimientos relacionados con las operaciones del MAG y las encomiendas asignadas a sus funcionarios y empleados. Otros usos que justifiquen el acceso al Internet son: Comunicación, intercambio de información e identificación de fondos o programas disponibles para el desarrollo profesional, cultural, deportivo, comunitario, de

infraestructura y mejoras.

b. El uso de Internet es un privilegio especial y no un derecho inherente. La aprobación para su uso debe ser concedida por el director del departamento y el Director de Informática, quienes actuarán basándose en una recomendación y petición formal.
c. Los servicios hacia internet solo se podrán proveer a través de los equipos y servidores autorizados por el Departamento de Informática.
d. El uso de Internet más allá del horario de trabajo está permitido exclusivamente para investigaciones vinculadas a las funciones del MAG llevadas a cabo por los directores de departamentos. Estos privilegios pueden ser revocados en cualquier momento y por cualquier razón de peso que requieran su inmediata cancelación. El abuso de estos privilegios puede ser causa suficiente para el inicio de una acción disciplinaria.
e. Los usuarios del Internet deben tener claro que todas las transacciones que se efectúan mediante el uso de este sistema pueden ser grabadas y almacenadas para futuras auditorias de la Oficina de Auditoría Interna del MAG y la Oficina del Contralor de Puerto Rico. Dichas auditorias podrán realizarse en cualquier momento que la Oficina de Auditoría Interna estime necesario, por solicitud del Alcalde o por intervenciones regulares de la Oficina del Contralor.
f. Los supervisores de los usuarios que tienen acceso al Internet serán responsables de asegurarse que éstos conocen y cumplen con las normas establecidas por el MAG.
g. Cada usuario que utilice el Internet deberá identificarse correctamente con su nombre real y de su cuenta con el MAG.
h. Todo usuario será responsable por sus acciones y conducta al acceder el Internet. En ninguna circunstancia se realizarán actos o transacciones que puedan considerarse ilegales, inmorales u ofensivas.
i. Cualquier violación a estas normas podrá ser causa suficiente para ser sancionado como parte de un proceso disciplinario.

3.2. Guías para el uso de Internet

a. El Internet se utilizará única y exclusivamente para asuntos relacionados con las operaciones oficiales del MAG.
b. Todo usuario del Internet deberá seguir las normas de seguridad y control establecidas por el MAG.
c. Todo usuario deberá solicitar autorización de acceso al Internet siguiendo los siguientes pasos:

i. Realizar una solicitud formal por escrito, dirigida al director del departamento para utilizar el Internet. En dicha solicitud se indicará el uso que le dará a ese servicio. Dicha solicitud deberá estar aprobada única y exclusivamente por el director o su representante autorizado.
ii. El director evaluará la solicitud y de ser aprobada por éste se enviará la solicitud al director del Departamento de Informática para su aprobación.
iii. Una vez autorizado por el director de Informática o su representante autorizado se procederá a registrar como un incidente para otorgar los permisos necesarios.

3.3. Ejemplos de usos no permitidos

a. El Internet no será utilizado para propósitos de negocios o asuntos personales.
b. El Internet no deberá ser utilizado para efectuar gestiones de compras de productos o servicios, excepto aquellos departamentos que por su naturaleza requieran dicho acceso y que estén autorizados para ello.
c. El Internet no deberá ser utilizado para actividades ilegales, ilícitas, en violación a la ética profesional.
d. El Internet no deberá ser utilizado para ningún tipo de actividad que afecte la imagen y reputación del MAG y de sus integrantes.
e. El Internet no deberá utilizarse para acceder información, páginas, fotografías y mensajes de audio de contenido sexual.
f. El uso del Internet no deberá, en ninguna circunstancia, afectar las operaciones normales del MAG ni los servicios que se brindan al pueblo.
g. Los usuarios a los que se le otorgue la autorización de acceso al Internet no se suscribirán a servicios de propósitos privados como: correos, redes sociales, servicios de dialogo o "chat", programas de compartir datos, programas de acceso de multimedios (audios, imágenes y videos) y programa de llamadas de larga distancia. Todos estos programas tienen un impacto severo en la capacidad de la red local y su salida a la Internet.

3.4. Internet móvil

a. Se prohíbe el uso del Internet para gestiones no oficiales en los aparatos y dispositivos móviles provistos por el MAG. Entre las prohibiciones del uso del Internet móvil se encuentran las siguientes:
i. Realizar "video streaming".
ii. Descarga de videos, películas, fotos y cualquier otro material no

relacionado con las funciones oficiales del puesto, de índole profesional o educativo.

iii. Acceso a páginas de contenido sexual.
iv. Compras de carácter personal a través de "sites" de descuentos y cualquier otra.
v. Accesos a las cuentas personales de páginas de redes sociales tales como Facebook, Instagram, Twitter, entre otros.
vi. Participar en encuestas, sistemas de opinión o "blogs".
vii. Instalar juegos y otras aplicaciones no relacionadas con las gestiones oficiales en el MAG.
viii. Envío de fotos personales a través de mensajería de textos.
ix. Enviar textos con vocabulario obsceno y/o amenazante.
x. Envío o reenvío de imágenes no relacionadas con las gestiones oficiales tales como chistes, chismes, memes, etc.
xi. Envío o reenvío de mensajes, fotos, memes, propaganda o cualquier otro material de índole político partidista.

b. Se autoriza a los empleados y funcionarios del MAG el uso del Internet en los dispositivos móviles para lo siguiente:
    i. Acceso a páginas de redes sociales tales como Facebook, Instagram, Twitter, entre otras, para propósitos institucionales y oficiales relacionadas con las funciones y operaciones de estos en el MAG.
    ii. Llamadas y mensajes de textos ilimitados relacionados con las funciones y deberes del puesto y las operaciones del MAG.
    iii. 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 MAG de carácter oficial.

3.5. Supervisión del uso del Internet

a. Al solicitud Acceso al Internet, el usuario acepta que se supervise sin previo aviso el uso del servicio de Internet por los auditores de la Oficina de Auditoría Interna. También podrá ser examinado el uso de dicho servicio por los auditores de la Oficina del Contralor de Puerto Rico en sus intervenciones. Estos funcionarios podrán examinar las bitácoras del uso del Internet y el correo electrónico y cotejar que se estén cumpliendo las normas de uso de los sistemas de información adoptados por el MAG. Los usuarios tendrán el deber de informar al Alcalde, Director de Operaciones y Director de Auditoría Interna si han

hecho uso indebido de Internet, según las normas establecidas en este documento.

b. Se considerará que aquellos usuarios que hagan uso indebido del servicio de Internet habrán incurrido en una violación, por lo que podrán ser objeto de los procedimientos disciplinarios dispuestos por Reglamento.
c. Cada usuario es responsable por sus acciones y conducta al acceder a la Internet. Deberá tener siempre en mente que su uso debe ser correcto y según las políticas establecidas. Actos que pueden ser considerados ilegales, ofensivos o inmorales, no deberán ser llevados a cabo, en ninguna circunstancia.

4. Correo Electrónico (eMail)

4.1. Administración

a. El Help Desk se encargará de asignar las cuentas a los usuarios para el uso de correo electrónico en los servidores que administra.
b. Para asignar un buzón de correo a un usuario, el Departamento donde trabaja debe tramitar una solicitud autorizada por el director o representante autorizado al director de Informática. La solicitud puede ser electrónica mediante el uso del Formulario de ayuda al Helpdesk, o mediante un comunicado formal del Director.

4.2. Uso

a. Su correo electrónico puede ser accedido directamente a través de navegadores de internet y programas autorizados por el MAG.
b. El correo electrónico es sólo para uso oficial y en materias que sean pertinentes a la oficina asignada y su funcionamiento.
c. La información en los correos electrónicos será divulgada solamente a los oficiales autorizados.

4.3. Restricciones

a. Ninguna información deberá entrar en el sistema de correo electrónico no relacionado a las funciones municipales.
b. El correo electrónico no se deberá usar para envío masivo, materiales de uso no institucional o innecesarios (entiéndase por correo masivo todo aquel que sea ajeno al MAG, tales como cadenas, publicidad y propaganda comercial, política o social, etc.)
c. Se prohíbe el envío o recibo de mensajes de correo electrónico entre el personal del MAG y otras personas particulares que no pertenezcan al mismo en los cuales se divulgue información confidencial o de

transacciones en curso, opiniones, controversias políticas, o cualquier otra situación que pueda poner en entredicho la reputación o imagen del MAG.

d. Se prohíbe que se emitan opiniones relacionadas a raza, origen nacional, sexo, orientación sexual, edad, ideas o creencias religiosas o políticas, así como opiniones sobre personas con impedimento físico o mental.
e. Se prohíbe y no se tolerará la utilización del sistema de correo electrónico para enviar, recibir o crear mensajes de contenido discriminatorio, pornográfico o que pueda ser catalogado como de hostigamiento sexual, chistes, para la comisión dé cualquier delito o conspirar para cometer el mismo.
f. Está prohibido el manejo o transmisión de material obsceno, profano u ofensivo, a través del sistema de correo electrónico. Esto incluye acceso a materiales eróticos, bromas de cualquier forma y/o cualquier comentario o chiste que pueda violar la política de discrimen del MAG o su política de hostigamiento sexual.
g. Se prohíbe el uso de correo electrónico para propósitos y asuntos personales de los usuarios, de recreo, manejo de negocios, problemas o malentendidos. Tampoco tendrá acceso a juegos, compras ni páginas de entretenimiento o cualquier servicio ajeno a lo autorizado o correspondiente a sus funciones de su puesto.
h. Los empleados y/o funcionarios no tendrán el derecho a la intimidad con relación a cualquier información o mensaje creado, recibido o enviado a través del sistema de correo electrónico.

4.4. Correos Personales

a. El MAG 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 MAG.
b. Se prohíbe el envío o el recibo de mensajes de texto o correo electrónico o de cualquier tipo entre el personal del MAG 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 MAG, aunque la información divulgada no sea de naturaleza confidencial.

4.5. Políticas

a. El MAG se reserva el derecho de auditar, vigilar y fiscalizar los sistemas

de correspondencia electrónica para garantizar que la propiedad está siendo utilizada para los propósitos y gestiones relacionadas a fines públicos.

b. El MAG se reserva el derecho de realizar auditoria periódicamente y/o al azar, y/o cuando, exista una investigación sobre una situación en particular.
c. No se enviarán anejos más grandes de diez megabytes (10 MB). De requerir el envío de documentos que sobrepasan este tamaño deberá mediar autorización al Departamento de Informática.

5. Apps

5.1. Aplicaciones

La seguridad y el uso adecuado de los sistemas son cruciales para garantizar la integridad de los datos, la privacidad de la información y la eficiencia de los procesos en el MAG.

a. No está permitido el acceso a áreas o módulos de los sistemas que administra Infromática para los cuales no se haya otorgado acceso explícito.
b. Queda prohibido ingresar datos o realizar transacciones que puedan afectar la integridad del sistema o los procesos.
c. No se permite la carga de información maliciosa o que pueda causar daños.
d. No está permitida la omisión de registros ni la alteración de datos.

6. Antivirus

6.1. El sistema de antivirus instalado en las computadoras del MAG es una pieza medular en los Sistemas de Información, para asegurar la protección adecuada de los datos y archivos en nuestra organización. Está en contra de las políticas del MAG eliminar o desactivar la protección contra virus.

7. Copilot

7.1. En el MAG buscamos fomentar el uso de herramientas tecnológicas como la inteligencia artificial (IA) con el propósito de obtener un grado alto de productividad y calidad de trabajo, al tiempo que garantizamos la protección de datos y la seguridad. Es por esto que solo se permitirá el uso de herramientas de IA aprobadas por el MAG.

7.2. Los usuarios deben obtener la aprobación explícita antes de utilizar herramientas de IA.

7.3. Los usuarios deben utilizar las herramientas de IA de manera responsable y ética. No se permite el uso de herramientas de IA para actividades ilegales o maliciosas.

7.4. Se prohíbe el envió, transmisión o contenido de datos a cualquier sistema de inteligencia artificial en los cuales se incluya información confidencial, de transacciones en curso, o cualquier otra información que pueda exponer datos de los ciudadanos o poner en entredicho la reputación o imagen del MAG.

8. Juegos

8.1. Es política del MAG el remover los programas de juegos incluidos en los Sistemas Operativos de los dispositivos del MAG. Los juegos están prohibidos, aún fuera de horas laborables. Cualquier juego que sea encontrado en una máquina será removido sin previo aviso y se le notificará al director del área adonde dicho equipo reside.

9. Desarrollos internos

9.1. Propiedad y Almacenamiento del Código Fuente

a. Todo código fuente desarrollado internamente es propiedad exclusiva de MAG.
b. El código fuente debe almacenarse en el sistema de control de versiones que utilza el Departamento de Informática.
c. Se debe mantener un registro actualizado de los cambios realizados en el código fuente y observar el procedimiento para el control de cambios.

9.2. Documentación

a. Para cada desarrollo de software interno, se debe generar documentación técnica que incluya:
    i. Descripción general del proyecto.
    ii. Diagramas de arquitectura.
    iii. Diagramas de flujo.
    iv. Especificaciones técnicas.
    v. Manual de usuario.
b. La documentación debe estar disponible para todo el equipo de desarrollo y ser actualizada conforme se realicen cambios.

9.3. Responsabilidades

a. Equipo de Desarrollo Interno:
    i. Desarrollar software siguiendo las mejores prácticas y estándares establecidos.

ii. Mantener el código fuente y la documentación actualizados.
iii. Cumplir con las políticas de seguridad y propiedad intelectual.

b. Entidades Subcontratadas:
   i. Entregar el código fuente y la documentación completa a MAG al finalizar el proyecto.
   ii. Es importante validar si el contratista de sistemas de informática, posea las certificaciones adecuadas que demuestren su competencia y experiencia en el campo.
      1. Entre las certificaciones se sugieren:
         - Certificaciones en Cloud Computing: AWS, Azure, Google Cloud debido a la expansión de soluciones en la nube.
         - Certificaciones en Ciberseguridad: CISSP, CEH, CompTIA Security+ para roles relacionados con la seguridad informática.
      2. Las certificaciones no solo demuestran la capacidad técnica del contratista, sino también su compromiso con el desarrollo profesional continuo y la adaptación a las nuevas tecnologías.

c. Soluciones SaaS - Software as a Service
   i. Para entidades que ofrecen SaaS establecerán controles mínimos como el cumplimiento con SOC 2 / ISO 27001.

9.4. Auditoría y Cumplimiento

a. Se realizarán auditorías periódicas para verificar el cumplimiento de esta política.
b. El incumplimiento de esta política puede resultar en sanciones disciplinarias o según establecidas en el contrato.

V. DATOS / INFORMACIÓN

1. General

1.1. Todo dato, información, imagen, audio o video contenido en algún equipo de MAG (PC, laptop, tabletas, teléfonos móviles, disco o memoria externa, discos o memoria compartida, servidores, etc.) es propiedad del MAG.

1.2. El Departamento de Informática no es responsable por el contenido de datos ni por el tráfico que en ella circule, la responsabilidad recae directamente sobre el usuario que los genere o solicite.

1.3. Los datos se clasificarán para garantizar la seguridad y protección de la información, así como para cumplir con las normativas legales y políticas internas.

a. Clasificación de Datos
    i. Confidencial: Información que, si se divulga, podría causar un daño significativo a la organización o a individuos. Ejemplos incluyen datos personales sensibles información financiera no pública.
    ii. Restringido: Información que, si se divulga, podría causar un daño moderado. Ejemplos incluyen datos internos de la organización que no son de dominio público.
    iii. Interno: Información que es accesible solo para empleados y contratistas de la organización. Ejemplos incluyen políticas internas y procedimientos operativos.
    iv. Público: Información que puede ser divulgada sin restricciones. Ejemplos incluyen comunicados de prensa y material promocional.

1.4. Controles Asociados a la Clasificación de Datos

a. Confidencial: Requiere cifrado en tránsito y en reposo, acceso limitado a personal autorizado, y autenticación multifactorial (MFA).
b. Restringido: Requiere cifrado en tránsito, acceso limitado a personal autorizado, y autenticación fuerte.
c. Interno: Requiere controles de acceso basados en roles y monitoreo de acceso.
d. Público: No requiere controles estrictos, pero debe ser revisada antes de su divulgación.

1.5. Retención de Datos

a. Confidencial: Retención mínima de 7 años o según lo requiera la ley.

b. Restringido: Retención mínima de 5 años.
c. Interno: Retención mínima de 3 años.
d. Público: Retención según sea necesario.

2. Uso

2.1. Los *datos e información* utilizados en el MAG, y provistos a sus funcionarios y empleados, serán utilizados para gestiones oficiales.

2.2. La utilización de los *datos e información* se deberá limitar exclusivamente a las funciones y tareas asignadas a cada empleado en relación con su departamento.

2.3. El Administrador de Bases de Datos tendrá acceso a la información de la Base de Datos únicamente para:
a. realizar respaldos de la base de datos,
b. solucionar problemas que el usuario no pueda resolver,
c. diagnóstico o monitoreo.

3. Restricciones

3.1. Se prohíbe terminantemente reproducir distribuir o ceder la información contenida en los sistemas del MAG a personas particulares o entidad alguna sin la autorización del Alcalde o su representante autorizado o para fines ajenos a las funciones y poderes del MAG.

3.2. No se permite el acceso no autorizado a datos, recursos, objetos, sistemas de información o redes. El lograr acceso a recursos y/u objetos no disponibles al público o el ingresar de manera no autorizada o ilegal a los sistemas de información o redes constituye una violación a las reglas y políticas establecidas mediante este Reglamento y estará sujeto a acción disciplinaria según dispuesto en el Reglamento de Normas de Conducta y Acciones Disciplinarias.

3.3. Los administradores no deben eliminar información de cuentas individuales del sistema, a menos que dicha información sea ilegal o ponga en riesgo el buen funcionamiento de los sistemas, o se sospeche que un intruso está utilizando una cuenta ajena.

3.4. El mal uso, intencional, acceso no autorizado, destrucción, alteración, desmantelamiento, desconfiguración o deshabilitación de cualquier programación, banco de datos o cualquier sistema de información, mediante la propagación de virus, o la utilización para ataques, insultos o acoso a otros usuarios, se consideran actividades dañinas o perniciosas.

3.5. El mal uso de los sistemas de información del MAG incluye: la intención y/o realización de un crimen o actividad ilegal.

3.6. El Administrador de la Base de Datos no deberá eliminar ninguna información del sistema, a menos que la información esté dañada o ponga en peligro el buen funcionamiento del sistema.

4. Protección

4.1. Para mantener la seguridad de la información de su cuenta, el usuario deberá utilizar el método de almacenamiento asignado (al momento de la creación de este documento llamado "One Drive") para todos sus documentos. Cualquier información que guarde en algún otro medio no será resguardada por el Departamento de Informática y será responsabilidad del usuario hacer los resguardos que considere.

4.2. Para reforzar la seguridad de la información de los usuarios, bajo su criterio, deberá hacer resguardos de la información.

4.3. Resguardos ("backups")

a. La información de los servidores deberá ser respaldada de acuerdo con las políticas de frecuencia y medios establecidos:
    i. servidores y bases de datos: diario, semanal, mensual, y anual
    ii. correos en Office 365 tienen una retención máxima de 7 años
    iii. en año eleccionario, se tomará un "full backup" en septiembre 30 y se guardarán las copias según dispone el Código Municipal de Puerto Rico, Ley 107 del 14 de agosto de 2020 Artículo 2.094 — Disposición Especial para Años de Elecciones

4.4. Las Base de Datos de MAG serán resguardadas periódicamente en forma automática y manual tomando en consideración lo siguiente:

a. Respaldo completo (full backup) - A todas las bases de datos se les hará un respaldo completo al menos una vez a la semana, durante la noche.
b. Resguardo Incremental - A todas las bases de datos se les hará un respaldo incremental todas las noches en las que no tengan un respaldo completo.
c. Resguardo Transaccional – A todas las bases de datos que tengan modo de recuperación completo (recovery mode full) se les harán respaldos de las bitácoras transaccionales (transaction log backups) durante el horario de trabajo del Municipio, tantas veces como el Administrador de Bases de Datos considere necesario.
d. Resguardos Especiales – copia de la base de datos SAP a diciembre 31, junio 30 y 30 de septiembre (en año eleccionario) con una retención de

180 días.

4.5. El backup que se hace en Azure de cada servidor debe incluir el disco donde se hagan los respaldos de SQL Server.

a. Los resguardos de MAG deberán ser almacenados en un lugar seguro y distante del sitio de trabajo. A partir de enero 2020, los resguardos del MAG se harán en Microsoft Azure Cloud, región este. Esto incluye resguardos de los servidores virtuales, así como resguardos de las bases de datos de SAP. Una copia de los resguardos está disponible en la región oeste del Cloud ya que están disponibles en caso de que se active un desastre. Los detalles de esta configuración se encuentran en el documento MAG Disaster Recovery and Continuity Plan.

4.6. El Director del Departamento de Informática podrá autorizar el registro y seguimiento de sesiones de usuarios y autorizar la búsqueda de archivos en el entorno de un usuario sospechoso de violación de las políticas del Departamento de Informática.

4.7. Se realizará periódicamente ensayos / pruebas de recuperación para los sistemas críticos para revisar que ésos funcionen cuando haya alguna emergencia.

5. Archivos personales

5.1. Todos los archivos que no se relacionen con las operaciones municipales serán eliminados sin previa notificación al usuario del equipo y el mismo podrá estar sujeto a acciones disciplinarias.

6. Privacidad

6.1. El MAG 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.

6.2. En el caso de dispositivos de propiedad personal del usuario (BYOD), se mantendrá expectativa de privacidad conforme se establece el Reglamento de BYOD.

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

a. DISPOSITIVOS ADQUIRIDOS POR EL MAG

i. 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 MAG es propiedad del MAG según lo dispuesto en este reglamento.

ii. El MAG, 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.

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

iv. El MAG podrá, de considerarlo necesario, implementar servicios o instalar aplicaciones de geolocalización en los dispositivos adquiridos por el MAG, 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 MAG para los dispositivos móviles que así lo considere necesario.

b. DISPOSITIVOS DE PROPIEDAD PERSONAL ("BYOD")
    i. 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 MAG, a no ser por acuerdo y aceptación previa.
    ii. 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.
    iii. 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.
    iv. El MAG 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 MAG no proveerá reembolso alguno por el plan de voz y data del dispositivo de propiedad personal.

VI. INFRAESTRUCTURA DE RED INFORMÁTICA

La infraestructura de red informática del MAG comprende de componentes de hardware y software, sistemas y dispositivos los cuales permites la informática y la comunicación entre usuarios, servicios, aplicaciones y procesos. Todo lo que está involucrado en esta red de informática, desde servidores, cableados, antenas, hasta enrutadores (routers), se unen para formar la infraestructura de red del MAG. La red de MAG tiene como propósito principal servir en el intercambio y transformación de información dentro de la entidad entre usuarios, técnicos, departamentos, oficinas y hacia afuera del MAG.

1. Seguridad Física

1.1. No está permitido utilizar los servicios de la red del MAG para actividades que no estén directamente relacionadas con las tareas laborales que los usuarios realizan para el MAG.

1.2. Acceso Físico a la red de MAG

a. Todos los componentes principales estarán debidamente protegidos con la infraestructura apropiada de manera que ninguna persona no autorizada tenga acceso físico directo.

b. El acceso de terceras personas debe ser identificado plenamente, controlado y supervisado durante el acceso.

c. Las visitas internas o externas podrán acceder a las áreas restringidas siempre y cuando se encuentren acompañadas cuando menos por un técnico o con permiso del Director de Informática o representante autorizado.

1.3. Protección Física

a. Los usuarios deberán cuidar, respetar y hacer un uso adecuado de los recursos de cómputo y red de MAG, de acuerdo con las políticas que en este documento se mencionan.

b. El resguardo de los equipos de comunicaciones deberá quedar asignado a la persona que los usa o administra, permitiendo conocer siempre la ubicación física de los equipos.

c. El Director de Informática o su representante son responsables de autorizar para mover, cambiar o extraer equipo de la red de MAG. El Departamento de Informática llevará un registro de recibo y entrega del equipo y las normas que rigen su uso.

d. El Departamento de Informática, así como las áreas que cuenten con programas informáticos y sistemas tecnológicos que desempeñan un

papel fundamental en el funcionamiento esencial y sin interrupciones, deberán contar con vigilancia y/o algún tipo de sistema que ayude a evidenciar los accesos físicos a las instalaciones.

e. Las puertas del Departamento de Informática, así como sus almacenes y cuartos de datos y comunicaciones, deben contar con controles de acceso.
f. El cuarto de servidores de MAG debe:
    i. Recibir limpieza al menos una vez por semana, que permita mantenerse libre de polvo.
    ii. Ser un área restringida.
    iii. Estar libre de contactos e instalaciones eléctricas en mal estado
    iv. Contar por lo menos con un extintor de incendio adecuado para equipo electrónico y cercano al centro de telecomunicaciones.
g. El cuarto de servidores deberá seguir los estándares vigentes para una protección adecuada de los equipos de telecomunicaciones y servidores.
h. Los sistemas de "ground", sistemas de protección e instalaciones eléctricas del Site deberán recibir mantenimiento periódico con el fin de determinar la efectividad del sistema.
i. Cada vez que se requiera conectar equipo adicional de cómputo, se deberá comprobar la carga de las tomas de corriente.
j. El Departamento de Informática deberá disponer de un plan o esquema que garantice la continuidad del servicio.

1.4. El Departamento de Propiedad establecerá procedimientos para el inventario físico, basándose en los procedimientos definidos por el MAG.

2. Seguridad Lógica

2.1. El uso de analizadores de red, SIEM (Security Information Event Management) es permitido única y exclusivamente por el personal de Informática, para monitorear la funcionalidad de la red de MAG, contribuyendo a la consolidación del sistema de seguridad bajo las políticas y normas del MAG.

2.2. No se permitirá el uso de analizadores para monitorear o censar redes ajenas al MAG y no se deberán realizar análisis de la red de MAG desde equipos externos al MAG.

2.3. Cuando se detecte un uso no aceptable, se desconectará temporal o permanentemente al usuario, red involucrada o se cancelará la cuenta de usuario, dependiendo de la norma. La reconexión se hará en cuanto se

considere que el uso no aceptable se ha suspendido. Se podrá notificar al Director del usuario, Auditoría Interna y/o Recursos Humanos según sea el caso.

2.4. No se permite interferir o interrumpir las actividades de los usuarios por cualquier medio o evento salvo que las circunstancias así lo requieran, como casos de contingencia, los cuales deberán ser reportados en su momento a sus superiores correspondientes.

2.5. Si un usuario o departamento viola las políticas vigentes de uso de la red de MAG, los administradores de la red lo aislarán de la misma.

2.6. Será responsabilidad de Informática monitorear y responder a amenazas en dispositivos finales, como computadoras, teléfonos móviles y tablets. Para esto, hará uso de herramientas de detección y respuesta en endpoints (EDR, por sus siglas en inglés). Esta herramienta proporciona protección avanzada contra amenazas, detección y respuesta automatizada, y análisis de seguridad en tiempo real. Ayuda a proteger los dispositivos finales contra ataques cibernéticos y permite a los administradores de TI monitorear y gestionar la seguridad de los dispositivos de manera eficiente.

2.7. Informática será responsable de llevar a cabo o contratar a tales efectos evaluaciones periódicas a los sistemas. Las evaluaciones periódicas ayudas en caso de cambios significativos en la infraestructura, incidentes de seguridad, o nuevas amenazas emergentes.

a. Tipos de Evaluaciones.

i. Pruebas de Penetración: las pruebas pueden ser internas o externas para identificar vulnerabilidades en la red y sistemas

ii. Análisis de Vulnerabilidades: se realizará análisis de periódicos para detectar y corregir debilidades en los sistemas

iii. Evaluaciones de Riesgo: se llevará a cabo una evaluación de riesgo tanto para sistemas de TI como para la seguridad de la información.

VII. SERVICIOS DE TECNOLOGÍA

Los servicios de tecnología del MAG son provistos por el Departamento de Informática del MAG. El Departamento de Informática del MAG contribuye a mejorar la eficiencia operativa, la comunicación, la seguridad y la innovación tecnológica. Además, permite que la organización se adapte a los cambios tecnológicos y aproveche al máximo las ventajas que la tecnología ofrece. Se encarga de administrar y mantener la arquitectura de sistemas, cumplir con el protocolo de licenciamientos, actualizaciones, así como la resolución de problemas tecnológicos. Proporciona asistencia a los usuarios en temas relacionados con hardware, software y conectividad; asistencia en caso de fallos; implementación de medidas para proteger la infraestructura tecnológica, evalúa las necesidades de recursos, nuevos programas o equipos a adquirir, así como la continuidad de las operaciones.

1. Apoyo Técnico (Help Desk)

1.1. El Departamento de Informática del MAG será la entidad principal para brindar apoyo tecnológico a los empleados y usuarios del MAG.

1.2. Los usuarios deberán solicitar apoyo al Departamento de Informática, a través del Help Desk, ante cualquier duda en el manejo de los recursos de cómputo del MAG.

1.3. Todo servicio brindado a los usuarios a través del Help Desk deberá ser registrado y actualizado en la aplicación de Help Desk del MAG.

1.4. El Help Desk podrá ingresar de forma remota a computadoras única y exclusivamente para la solución de problemas y bajo solicitud explícita del usuario de la computadora.

1.5. El Help Desk debe actualizar la información de registro de los recursos de cómputo del MAG, cada vez que adquiera e instale equipo o software.

1.6. El Help Desk debe registrar cada máquina en el registro de control de equipo de cómputo y red del MAG.

1.7. A partir del 2018 la nomenclatura para el "*computer name*" será en formato Identificador-Tipo de Activos-Numero de Propiedad

a. Identificador – una letra que identifique el tipo de equipo
    i. A – All in One
    ii. D – Desktop
    iii. L – Laptop
    iv. TC-Thin client

b. Número de Propiedad (Asset Number) – El número de propiedad es

autoasignado por el sistema financiero. Para el *"computer name"* se utilizará los primeros dos dígitos del número de propiedad, indicativo del tipo de activo y los dígitos consecutivos omitiendo los ceros que preceden al consecutivo. Ejemplo de laptop con número de propiedad 120000018932: L-12-18932

1.8. El Help Desk deberá auditar periódicamente y sin previo aviso los sistemas el tráfico de la red, para identificar el mal uso de las comunicaciones, configuraciones no válidas o permisos extra que pongan en riesgo la seguridad de la información.

1.9. El Help Desk deberá realizar la instalación o adaptación de sus sistemas de cómputo de acuerdo con los requerimientos en materia de seguridad.

1.10. Es responsabilidad del Help Desk revisar periódicamente las bitácoras ("logs") de los sistemas a su cargo.

1.11. El Help Desk reportará al Director de informática, o representante autorizado los incidentes de violación de seguridad, junto con cualquier experiencia o información que ayude a fortalecer la seguridad de los sistemas de cómputo.

1.12. El Help Desk deberá utilizar los analizadores previa autorización del usuario o Director encargado y bajo la supervisión de éste, informando de los propósitos y los resultados obtenidos.

1.13. El Help Desk deberá cancelar o suspender las cuentas de los usuarios previa notificación, cuando se le solicite mediante un documento explícito en los siguientes casos:

a. Si la cuenta no se está utilizando con fines institucionales.
b. Si pone en peligro el buen funcionamiento de los sistemas.
c. Si se sospecha de algún intruso utilizando una cuenta ajena.

2. Gestoría Tecnológica

2.1. El Departamento de Informática debe llevar un control total y sistematizado de los recursos de cómputo.

2.2. Los encargados del área de informática son los responsables de calendarizar y organizar al personal encargado del mantenimiento preventivo y correctivo de los equipos de cómputo.

2.3. El Departamento de Informática debe mantener informados a los usuarios y poner a disposición de estos el software que refuerce la seguridad de los sistemas de cómputo.

2.4. El Departamento de Informática tiene la responsabilidad de verificar la instalación, configuración e implementación de seguridad, en los servidores

conectados a la Red.

2.5. El Departamento de Informática es el encargado de suministrar medidas de seguridad adecuadas contra la intrusión o daños a la información almacenada en los sistemas, así como la instalación de cualquier herramienta, dispositivo o software que refuerce la seguridad en cómputo.

2.6. El Departamento de Informática es el único autorizado para monitorear constantemente el tráfico de paquetes sobre la red, con el fin de detectar y solucionar anomalías, registrar usos indebidos o cualquier falla que provoque problemas en los servicios de la Red.

3. Control de Cambios

El Departamento de informática mantendrá y controlará los cambios relacionados a la infraestructura tecnológica y de aplicativos. Será responsable de: diseñar y planificar, implementar y mantener los sistemas, garantizar la seguridad y disponibilidad de los servicios tecnológicos.

3.1. Todo cambio de sistema conlleva una solicitud de cambios. Esta podrá generarse mediante un formulario de Ayuda al Help Desk, verbal, como consecuencia de un contrato o que surja como una necesidad inmediata.

3.2. La solicitud será documentada a través del sistema y clasificado según el impacto del cambio o nivel de urgencia (bajo, medio, alto). La misma deberá incluir los siguientes detalles: descripción del cambio, área de impacto (infraestructura, aplicativos).

a. Criterios de Clasificación:

i. Bajo Impacto: Cambios menores que no afectan significativamente las operaciones del MAG.

ii. Medio Impacto: Cambios que tienen un impacto moderado y requieren coordinación entre varios departamentos.

iii. Alto Impacto: Cambios críticos que pueden afectar significativamente las operaciones y requieren aprobación de la alta gerencia.

3.3. Los cambios de alto impacto deben ser aprobados por la alta gerencia.

3.4. Toda solicitud será evaluada para determinar la viabilidad del cambio, estimado de tiempo, su alineación con los objetivos y asignada a un recurso para ser trabajada.

3.5. Se registrará un incidente para documentar los cambios. Este incluirá las aprobaciones, las fechas de aprobación, el responsable del cambio, y los detalles del cambio.

3.6. Los cambios serán revisados por los departamentos afectados (Recursos

Humanos, Compras, Finanzas, Informática, etc.), puestos a prueba y aprobados para ser llevados a Producción.

3.7. Toda aplicación de cambio que afecte el uso de los sistemas o infraestructura será notificado a los usuarios mediante ventana de mantenimiento. La notificación deberá incluir el detalle del sistema que será afectado por el cambio, el tipo de cambio (Periódico, Planificado, Crítico) y la duración del evento.

3.8. Exclusión de Control de Cambio. Quedará excluido del proceso formal de manejo de cambios, incidentes que están fuera de nuestro control. Ejemplo de esto son cambios/actualizaciones impuestas por sistemas de terceros, que son aplicados sin nuestra intervención.

4. Marco de Resiliencia

4.1. Plan

a. El Departamento de Informática mantendrá un plan de resiliencia que revisará anualmente. Este plan tiene como objetivo garantizar la continuidad de los servicios tecnológicos en caso de eventos que puedan afectarlos. Este plan de resiliencia informática incluye:

   i. Evaluación de riesgos: Identifica y evalúa los posibles riesgos que podrían afectar los servicios tecnológicos. Esto incluye desastres naturales, ciberataques, fallos de hardware o software, entre otros.

   ii. Procedimientos de respuesta: Define procedimientos claros para abordar situaciones de crisis. Esto incluye cómo comunicarse con el personal de informática y usuarios, cómo restaurar sistemas y cómo garantizar la continuidad de los servicios.

   iii. Backup y recuperación: Establece políticas para realizar copias de seguridad regulares de datos críticos y sistemas. Además, define procesos de recuperación en caso de fallos.

   iv. Capacitación y concienciación: Asegura de que el personal esté capacitado para actuar en situaciones de emergencia. La concienciación sobre la importancia de la resiliencia también es fundamental.

   v. Pruebas y simulacros: Define pruebas periódicas para verificar la efectividad del plan. Esto podría incluir simulacros de ciberataques o pruebas de recuperación de datos.

   vi. Actualización constante: Dado que las amenazas cambian con

el tiempo, es importante revisar y actualizar el plan de resiliencia anualmente.

4.2. Infraestructura

a. El Departamento de Informática tomará las siguientes medidas para mantener una infraestructura resiliente

i. Utilizará múltiples circuitos de servicios de Internet y rutas de comunicación para minimizar el riesgo de falla de alguno de estos.

ii. Mantendrá soluciones de balanceo de carga y failover para distribuir el tráfico entre diferentes enlaces y garantizar la continuidad del servicio.

iii. Utilizará dispositivos de red redundantes, como routers y switches, para evitar puntos únicos de falla

iv. Asegurará que los empleados puedan trabajar de forma remota utilizando herramientas como Red Privada Virtual (VPN) o escritorios virtuales (Virtual Desktops).

v. Utilizará, en la medida que mejor aplique, arquitecturas de servidores como clústeres, balanceadores de carga y replicación de datos para distribuir la carga y garantizar la disponibilidad.

vi. Implementará servidores en la nube o infraestructura como servicio (IaaS) para aprovechar la escalabilidad y la redundancia proporcionada por los proveedores de nube.

vii. Tendrá servidores de respaldo listos para activarse en caso de falla.

viii. Debe mantener relaciones sólidas con los proveedores de servicios de comunicaciones.

ix. Implementará sistemas redundantes para el PBX y la infraestructura telefónica.

x. No dependerá exclusivamente del PBX o sistema telefónico tradicional. Implementará alternativas como VoIP (Voz sobre IP) a través de comunicaciones basadas en la nube como Microsoft Teams.

xi. En caso de un evento:

1. proporcionará información relevante a los llamantes y redirigirlos a canales alternativos (correo electrónico, números de manejo de emergencias, chat en vivo, etc.),
2. proporcionará a los empleados teléfonos móviles con

acceso a la red celular,

3. configurará el reenvío ("forward") de llamadas desde líneas fijas críticas a números móviles.

5. Manejo de Incidentes de Seguridad

5.1. El Departamento de Informática del MAG seguirá el siguiente proceso para manejar incidentes de seguridad:

a. Identificación del incidente.
    i. El Help Desk será el responsable de detectar y reconocer la incidencia a través del Protocolo para el Manejo de Riesgo establecido y notificarlo a su supervisor. Esto puede incluir actividades inusuales, alertas de seguridad o comportamientos sospechosos.
    ii. El usuario deberá reportar por cuenta propia algún comportamiento irregular en su sistema siguiendo la Guía para Reportar Incidentes de Ciberseguridad publicada en el portal interno del Municipio.
b. Clasificación y Documentación del incidente.
    i. Se evaluará la gravedad y el impacto del incidente y se clasificará como un ataque menor o una amenaza grave con el apoyo del Administrador de redes.
c. Priorización del incidente:
    i. Se priorizará según la criticidad y el riesgo del evento.
    ii. Si se identifica que es un incidente grave que requiera la intervención de niveles superiores.
d. Respuesta al incidente:
    i. Actúa según el tipo de incidente:
        1. Contención: Detén la propagación del incidente.
        2. Erradicación: Elimina la causa raíz.
        3. Recuperación: Restaura los sistemas afectados.
        4. Investigación: Analiza cómo ocurrió y qué se puede mejorar.
        5. Comunicación: Informa a las partes interesadas internas y externas.
        6. Documentación: Registra todos los detalles relevantes incluyendo las acciones tomadas, los resultados y las lecciones aprendidas.

e. Cierre del incidente:
    i. Una vez que se ha resuelto la incidencia, se documentará las acciones tomadas y realizará una revisión post-incidente para recoger las lecciones aprendidas y mejorar.

6. Campañas de Concienciación

6.1. Se llevarán a cabo campañas de concienciación sobre ciberseguridad periódicamente.

6.2. Las campañas estarán dirigidos a todos los usuarios, destacando la importancia de la seguridad y las mejores prácticas.

6.3. Se difundirán comunicaciones sobre los procedimientos a observar en respuesta a incidentes.

6.4. Se coordinarán charlas y orientaciones a los usuarios periódicamente.

7. Licenciamiento

7.1. Cada uno de los programas adquiridos por el MAG deberá ser registrado debida e inmediatamente de acuerdo con las indicaciones en su contenido. Se deberá mantener un archivo de dichos registros.

7.2. El Departamento de Informática deberá mantener un registro de todos los programas adquiridos y partes incluidas (medio, manuales, equipo, etc.)

8. Administración de Dispositivos Móviles

8.1. 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 MAG y los personales que se conectarán a la red del MAG. Este mecanismo permitirá contar con toda la información referente al dispositivo, monitorearlo, 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:

a. Mantener un inventario de los dispositivos móviles adquiridos por el MAG 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.

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

c. Terminar servicios a dispositivos perdidos y robados, si el MAG es el suscriptor del servicio.
d. 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 MAG.
e. Borrar todos los datos del MAG del dispositivo móvil en caso de:
    i. terminación del usuario en el MAG;
    ii. si el dispositivo será reasignado a otro usuario;
    iii. si el dispositivo será descartado y/o sustituido.
f. En coordinación con la Oficina de Auditoría Interna, monitoreará las métricas establecidas de uso de data de los dispositivos móviles.
g. 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.

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

8.3. Si el MAG 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.

8.4. La Gerencia y el Departamento de Informática del MAG 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 estos.

8.5. 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.

8.6. Se asignará una cuota de consumo para uso de data a cada celular oficial asignado a funcionario o empleado y se monitoreará para evitar que los funcionarios se excedan del consumo.

8.7. Todos los dispositivos iPhone tendrán acceso a "Company Portal" que contiene las aplicaciones preautorizadas por el MAG. La Gerencia podrá autorizar acceso a aplicaciones específicas a grupos según sus funciones o áreas de trabajo.

VIII. SANCIONES

De determinarse que el funcionario o empleado ha hecho uso indebido de la computadora portátil asignada, se le solicitará la entrega inmediata del equipo.

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 MAG.

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 MAG.

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 MAG, 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 MAG.

IX. CLÁUSULA DE SEPARABILIDAD

Si un tribunal declara ilegal o inconstitucional cualquier disposición de este Reglamento, dicha declaración no afectará las otras disposiciones del Reglamento por considerarse cada una por separado.

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.

X. DEFINICIONES

Acuerdo de Confidencialidad	Documento en que los funcionarios del Municipio Autónomo 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 "laptops" 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.

XI. VIGENCIA

Este reglamento comenzará a regir una vez aprobado y firmado por el Honorable Alcalde mediante ordenanza a esos efectos.

Aprobado en Guaynabo, el día 27 de Mayo de 2025.

Hon. Edward O'Neill Rosa
Alcalde