Oficina del Presidente

SISTEMA UNIVERSITARIO
ANA G. MÉNDEZ

PO Box 21345
San Juan PR 00928-1345
Tel (787) 751-0178, ext. 7200
Fax (787) 751-3305
www.suagm.edu

28 de septiembre de 2016

A TODA LA COMUNIDAD UNIVERSITARIA

José F. Méndez Méndez
Presidente

ORDEN EJECUTIVA NÚMERO 16-2016 SOBRE EL USO SEGURO Y RESPONSABLE DE LAS TECNOLOGÍAS DE INFORMACIÓN

Los sistemas de computadoras, las aplicaciones de mensajería, la utilización de la Internet, las redes sociales y otros recursos electrónicos se han convertido en herramientas necesarias e importantes para la operación institucional. El Sistema Universitario Ana G. Méndez provee a sus empleados y profesorado distintos recursos electrónicos con el propósito de optimizar los servicios que se ofrecen a la comunidad universitaria. Dichos recursos ayudan al desempeño de las funciones oficiales relacionadas a cada puesto, apoyan las distintas iniciativas y proyectos, y garantizan que el personal tenga a su alcance las herramientas tecnológicas necesarias para su operación.

El SUAGM, de igual manera, ofrece a nuestros estudiantes distintos servicios y recursos electrónicos con el propósito de apoyarles en su gestión académica durante el transcurso de su vida universitaria. A su vez, la comunidad en general tiene a su disposición el acceso a servicios electrónicos como parte del compromiso social del SUAGM.

La provisión y disponibilidad de estos recursos requiere que se establezcan normas y procedimientos para el uso adecuado de los sistemas tecnológicos disponibles, de forma tal, que la información y recursos tecnológicos se mantengan seguros y protegidos. La implantación de un sistema de seguridad redunda en beneficios tales como efectividad, productividad, integridad, confiabilidad y disponibilidad, lo cual es cónsono a nuestras metas institucionales.

Propósito

El Manual del Uso Seguro y Responsable de las Tecnologías de Información tiene como propósito:

- Recopilar en un solo documento las normas institucionales que gobiernan el buen uso y acceso de los recursos tecnológicos del SUAGM por parte de sus usuarios.
- Mantener los sistemas e información sensitiva protegida y libre de riesgos de seguridad.

Alcance

Este manual rige la utilización de los recursos tecnológicos, las redes de telecomunicaciones, el acceso a la Internet, los sistemas enlazados a la nube (*cloud*), el uso de redes sociales y otros dispositivos tecnológicos pertenecientes al SUAGM y/o servicios contratados, al igual que la información manejada a través de dichos sistemas. El mismo es aplicable a los empleados administrativos, profesorado, estudiantes y toda persona externa al SUAGM que de una manera u otra haga uso y acceda a cualquiera de los componentes de los recursos de información antes mencionados.

Esta Orden Ejecutiva núm. 16-2016 se rige por el Manual del Uso Seguro y Responsable de las Tecnologías de Información, en el cual se describen las normas para la protección, el buen uso de los recursos tecnológicos y la seguridad de la información.

Esta orden ejecutiva entró en vigor el 1 de octubre de 2016.

Sistema Universitario
Ana G. Méndez

Manual del Uso Seguro y Responsable de las Tecnologías de Información

1.0 Tabla de Contenido

Página

2.0 Introducción

Los sistemas de computadoras, las aplicaciones de mensajería, la utilización de Internet, las redes sociales y otros recursos electrónicos se han convertido en herramientas necesarias e importantes para la operación institucional. El Sistema Universitario Ana G. Méndez, Inc. (SUAGM) provee a sus empleados y profesorado distintos recursos electrónicos con el propósito de optimizar los servicios que se ofrecen a la comunidad universitaria. Dichos recursos ayudan al desempeño de las funciones oficiales relacionadas a cada puesto, apoyan las distintas iniciativas y proyectos, y garantizan que el personal tenga a su alcance las herramientas tecnológicas necesarias para su operación.

El SUAGM, de igual manera, ofrece a nuestros estudiantes distintos servicios y recursos electrónicos con el propósito de apoyarles en su gestión académica durante el transcurso de su vida universitaria. A su vez, la comunidad en general tiene a su disposición el acceso a servicios electrónicos como parte del compromiso social del SUAGM.

La provisión y disponibilidad de estos recursos requiere que se establezcan normas y procedimientos para el uso adecuado de los sistemas tecnológicos disponibles, de forma tal, que la información y recursos tecnológicos se mantengan seguros y protegidos. La implantación de un sistema de seguridad redunda en beneficios tales como efectividad, productividad, integridad, confiabilidad y disponibilidad, lo cual es cónsono a nuestras metas institucionales.

3.0 Propósito

El manual del uso seguro y responsable de las tecnologías de informacioón tiene como propósito: (1) recopilar en un solo documento las normas institucionales que gobiernan el buen uso y acceso de los recursos tecnológicos del SUAGM por parte de sus usuarios; y (2) mantener los sistemas e información sensitiva protegida y libre de riesgos de seguridad.

4.0 Alcance

Este manual rige la utilización de los recursos tecnológicos, las redes de telecomunicaciones, el acceso a la Internet, los sistemas enlazados a la nube (*cloud*), el uso de redes sociales y otros dispositivos tecnológicos pertenecientes al SUAGM y/o servicios contratados, al igual que la información manejada a través de dichos sistemas. El mismo es aplicable a los empleados administrativos, profesorado, estudiantes y toda persona externa al SUAGM que de una manera u otra haga uso y acceda a cualquiera de los componentes de los recursos de información antes mencionados.

5.0 Definiciones

1. Acuerdo de confidencialidad – documento firmado por todos los empleados del SUAGM y/o sub-contratistas donde se estipula la no divulgación y manejo de información confidencial privada y/o sensitiva.
2. Dispositivos externos o electrónicos/equipos periféricos – todo aquel dispositivo o equipo que al colocarse o conectarse a los recursos tecnológicos, éstos puedan enviar o recibir datos. Existe una gran variedad de éstos, entre los que se encuentran: usb, discos duros, impresoras, escáner, *hot spot*, memorias, DVD, entre otros.
3. Encriptación – método o proceso que se utiliza para proteger la información convirtiendo un texto legible en un texto no legible o codificado de forma tal que no pueda ser descifrado sin la debida autorización.
4. *Hot spot* – equipo que otorga acceso al internet a través de una red inalámbrica externa al SUAGM. Se utiliza para evitar la conexión a los puntos wifi autorizados por OCIT.
5. Información sensitiva – es aquella información que está protegida contra la divulgación indebida, bien sea por razones legales, éticas, derechos de autor, derecho a la intimidad, secretos comerciales, entre otros. Se trata de cualquier información que, al ser expuesta, pueda representar una pérdida financiera para el SUAGM, así como un daño a su imagen, una invasión al derecho a la privacidad de información conforme establecido en las leyes estatales y federales. Algunos ejemplos de información sensitiva lo son: el número de identificación de empleado o estudiante (SID), número de seguro social, número de licencia de conducir,

fecha de nacimiento, información socio-demográfica, firma original o rúbrica, cuenta de usuarios y contraseñas, datos financieros, planes de negocios, entre otros.

6. OCIT – Oficina Central de Informática y Telecomunicaciones en Administración Central. Esta oficina tiene responsabilidad directa con los sistemas y recursos tecnológicos del SUAGM.
7. *Phishing* – método utilizado, por lo general mediante correo electrónico, a través del cual se trata de obtener información sensitiva o confidencial de forma fraudulenta (nombre, contraseña, tarjetas de crédito, información bancaria, etc.).
8. Redes de telecomunicaciones – conjunto de infraestructuras tecnológicas conectadas entre sí para proveer comunicaciones de voz, de datos, conectividad a Internet, acceso y control de sistemas centralizados, sistemas de correo electrónico, aplicaciones de red, páginas web, y todos los archivos e información obtenida, accedida o archivada en los sistemas del SUAGM.
9. Recursos tecnológicos – aquellos equipos o dispositivos tecnológicos que utilizan los usuarios para realizar sus operaciones cotidianas. Estos pueden ser equipos fijos como computadoras y servidores, portátiles como laptops, tabletas y teléfonos inteligentes, o sistemas virtuales.
10. SUAGM – siglas de Sistema Universitario Ana G. Méndez y se refiere en todo momento a sus cuatro instituciones: la Universidad del Este (UNE), la Universidad Metropolitana (UMET), la Universidad del Turabo (UT), la Universidad Ana G. Méndez, Campus Virtual (UAGM) y sus centros universitarios a través de la Isla. Además, incluye a sus centros establecidos en los Estados Unidos, Sistema TV, Canal 40 y Administración Central.
11. Terceros – personas o entidades externas al SUAGM que pudieran o no tener un contrato con el SUAGM.
12. Usuarios – todo personal administrativo, profesorado, estudiantes, contratistas, consultores y cualquier otro que acceda o utilice nuestros sistemas o las redes de telecomunicaciones desde o fuera de nuestras facilidades.

6.0 Normativas

Según se desprende del Manual del Recurso Humano, los recursos tecnológicos utilizados en la Institución, y la información manejada a través de los mismos, son

propiedad del SUAGM y solamente pueden ser utilizados para propósitos debidamente autorizados y relacionados con la operación institucional. De igual forma el Reglamento de Estudiantes estipula que, el uso de los recursos y equipos tecnológicos de la Institución constituye un privilegio que requiere que el estudiante usuario actúe de acuerdo a la reglamentación de la Institución. Dicha utilización debe seguir las normas establecidas dentro de estos manuales. Sin embargo, el SUAGM se reserva el derecho de modificar los mismos en cualquier momento, adaptándolos a los cambios y a la evolución tecnológica, según sea necesario. Asimismo, el SUAGM se reserva el derecho de aprobar cualquier otra norma o política adicional relacionada a la operación de los recursos tecnológicos.

Debido a que los recursos tecnológicos y la información contenida en los mismos son propiedad del SUAGM, ambos pueden estar sujetos en cualquier momento a ser inspeccionados y/o monitoreados por cualquier agente o representante autorizado del SUAGM con o sin notificación previa. Por tal motivo, no existe una expectativa de privacidad por parte de los usuarios en cuanto a la utilización de los recursos tecnológicos, o con relación a la información contenida en los mismos, bien sea accedida u obtenida a través de estos recursos o en la realización de sus funciones.

Como parte del programa de auditorías periódicas, los sistemas de información serán monitoreados por el SUAGM, con o sin notificación previa, para cualquier propósito legítimo, incluyendo, pero sin limitarse, los siguientes: (1) garantizar que se estén utilizando los recursos antes mencionados únicamente para fines exclusivos del trabajo que se realiza en el SUAGM; (2) prevenir el mal uso del sistema; (3) reparar o corregir cualquier problema que tenga el mismo, ya sea de piezas o programación; (4) velar por el cumplimiento de las políticas y reglamentos de conducta y/o procedimientos establecidos por el SUAGM.

El incumplimiento con las normas y disposiciones contenidas en este manual, pueden dar lugar a acciones disciplinarias, incluyendo la terminación de empleo, suspensión o expulsión del SUAGM. Además, algunas violaciones pudiesen conllevar que se radique una acción legal en contra del usuario, conforme se disponga por ley.

OCIT se reserva la facultad de efectuar cambios, modificaciones y enmiendas a este Manual, en cualquier momento, con el fin de cumplir con cualquier norma o reglamentación estatal y federal, así como para reforzar la protección y seguridad de los recursos tecnológicos, de los datos y la información.

6.1 Divulgación del Manual

La divulgación de este Manual se realizará a través de los siguientes mecanismos:

1. Actividades de naturaleza educativa o de concienciación de la información
2. Envíos masivos de comunicaciones electrónicas
3. Publicación en la página web del SUAGM
4. Proceso de inducción de empleados y profesorado
5. Proceso de orientación de estudiantes de nuevo ingreso a todos los niveles

6.2 Uso de cuentas y contraseñas de sistemas

Los recursos tecnológicos del SUAGM deben ser accedidos utilizando la cuenta de usuario y contraseña asignada previamente a cada usuario. Su nombre de usuario (*username*) y contraseña (*password*) deben ser manejadas como información confidencial, ya que a través de ésta es que se puede obtener acceso a información privilegiada y/o sensitiva. Por tanto, todos los usuarios se comprometen a seguir las siguientes normas:

1. Utilizar de forma única e individual el nombre de usuario y contraseña asignada.
2. No compartir su nombre de usuario ni contraseña en ningún momento.
3. No dejar visible su nombre de usuario ni contraseña.
4. No escribir su contraseña en un papel de notas, libreta o pizarra donde pudiera estar comprometida.
5. Cambiar su contraseña si entiende que la misma ha sido expuesta o comprometida
6. Cambiar la contraseña en el periodo establecido por el sistema.

7. De sospechar de alguna situación comprometedora con su nombre de usuario y contraseña, deberá reportar el incidente según se indica en la sección 7.2 de este manual.
8. Registrarse en la plataforma provista por la unidad de Seguridad de Información de OCIT para auto-servicio de cambio de contraseña en caso de olvido o bloqueo de cuenta.
9. Seleccionar una contraseña de alta complejidad en todo momento tomando en cuenta los siguientes requisitos de complejidad:
    a. Contraseña debe tener al menos ocho (8) caracteres
    b. Debe incluir números y letras
    c. Debe incluir por lo menos una letra mayúscula
    d. Además debe incluir por lo menos un carácter especial, por ejemplo #,$,@
10. No utilizar sistemas de almacenamiento y manejo de contraseñas no autorizadas por el SUAGM.

Si usted tiene la responsabilidad de administrar una cuenta especial (cuenta de consultor o cuentas de visitantes) deberá cumplir con las siguientes normas para esas cuentas:

1. Mantener una bitácora del uso de estas cuentas.
2. Cambiar la contraseña en el período establecido por el sistema.
3. Especificar el tiempo mediante el cual se requerirá el uso de la cuenta.
4. No dejar visible el nombre de usuario ni la contraseña.
5. Orientar al consultor o visitante sobre el uso adecuado de esta cuenta y su contraseña, según se menciona en la sección anterior.

De usted ser responsable de administrar una cuenta de servicio deberá:

1. Registrar la información del nombre de usuario y su contraseña en la plataforma para resguardo de cuentas sensitivas, suministrada por la unidad de Seguridad de Información de OCIT.
2. Seguir todas las normas presentadas para los usuarios a excepción de la registración en auto-servicio, conforme se dispone en el primer párrafo, al inciso ocho (8) de esta sección.

6.3 Uso aceptable de recursos tecnológicos

El uso de los recursos tecnológicos del SUAGM debe ser uno apropiado, efectivo y eficiente; en cumplimiento con las leyes estatales y federales; y caracterizado por la ética profesional a tono con las funciones que el usuario desempeñe. Las siguientes disposiciones, entre otras, definen el uso aceptable de los recursos tecnológicos:

1. Los usuarios del SUAGM utilizarán los recursos tecnológicos con el propósito de manejar e intercambiar información y contenido de acuerdo a su perfil de usuario y sus funciones.
2. De contener información sensitiva de los empleados, profesorado y/o estudiantes debe ser encriptado, con la herramienta seleccionada por la unidad de Seguridad de Información de OCIT. Este proceso de encriptación debe ser certificado por los Analistas de Seguridad de OCIT.
3. Debe ser custodiado de forma segura en todo momento dentro y fuera del SUAGM. Es su responsabilidad el prevenir cualquier pérdida, robo o hurto del mismo. En caso de pérdida o robo de equipo deberá realizar una querella a la policía y a su vez ser notificado inmediatamente al Analista de Seguridad de Información de OCIT, según se indica en la sección 7.2 de este manual.
4. Tener instalado el antivirus sistémico autorizado por la unidad de Seguridad de Información de OCIT. Equipos del SUAGM que no requieran el antivirus sistémico tendrán que ser previamente autorizados y deberán permanecer fuera de la red de telecomunicaciones del SUAGM, entiéndase en ambiente aislado. Cualquier equipo personal conectado a la red inalámbrica debe tener instalado un antivirus y estar al día en cuanto a los parchos de sistema operativo publicado por el manufacturero.
5. Los programas o productos instalados deben ser las versiones más recientes o que aun tengan soporte estándar del manufacturero. Los parchos de los sistemas deben ser actualizados periódicamente, como mínimo cada tres (3) meses.
6. De ser decomisados, donados, cedidos, prestados a terceros o vendidos deben ser borrados de forma tal que su información no pueda ser accedida, recuperada o reconstruida.
7. Deben ser atendidos, configurados, arreglados o trabajados únicamente por personal de informática y telecomunicaciones del SUAGM. Queda enteramente

prohibido que dichas iniciativas sean realizadas por personas externas a esta unidad.

8. Todos los equipos tecnológicos tales como, computadoras, celulares y tabletas podrán conectarse a las redes inalámbricas provistas y deberán ser utilizados de acuerdo a las reglas que rigen estas redes.

Se considera uso prohibido de recursos tecnológicos, sin limitarse, lo siguiente:

1. La transmisión de información no autorizada o llevar a cabo acciones que vayan en contra de las reglamentaciones estatales y federales, misión y visión, políticas y normas que atenten contra la ética y moral del SUAGM o que vaya en detrimento de su imagen.
2. El envío, recepción o mantenimiento de lenguaje o imágenes obscenas, de acoso, acecho, hostigamiento, discriminatorias, incluyendo pornografía o material de contenido sexual, entre otros.
3. La utilización de recursos tecnológicos con fines personales, privados, políticos, religiosos, lúdicos, entretenimiento o de lucro para el usuario.
4. Obtener, transmitir o distribuir material de forma electrónica en violación de los derechos de propiedad intelectual.
5. Llevar a cabo acciones que causen congestión en los recursos tecnológicos o en las redes de telecomunicaciones como por ejemplo el mantener o bajar música o películas en los sistemas, hacer ataques de denegación de servicios o escaneos en la redes de telecomunicaciones.
6. La utilización de equipos o programas con el propósito de violentar los controles sistémicos implantados.
7. La instalación y/o utilización de programas no autorizados o no licenciados por el SUAGM.
8. La utilización de recursos tecnológicos personales para acceder a sistemas o aplicaciones internas del SUAGM que no son públicas en internet, sin previa autorización de la unidad de seguridad de información de OCIT.
9. Cualquier acto vandálico o en detrimento de los recursos tecnológicos.
10. Acceso o intento de acceder a sistemas, dispositivos, programas o secciones de programas para los cuales el usuario no está autorizado.

11. Burlar o dejar fuera del dominio del directorio activo (AD) recursos tecnológicos del SUAGM sin autorización previa de la unidad de Seguridad de Información de OCIT.
12. Todo y cualquier otro acto análogo o relacionado a lo antes descrito, o que guarde un fin de evadir o violentar la seguridad añadiendo así un riesgo a nuestros recursos.

6.4 Uso aceptable de otros equipos periféricos y dispositivos electrónicos

Además de los recursos tecnológicos mencionados anteriormente, el SUAGM puede requerir la utilización de otros equipos periféricos y dispositivos electrónicos como parte de la operación (refiérase a la sección 5.0 para definición). Dicha utilización se rige por las mismas normas mencionadas para los recursos tecnológicos, e incluye también las siguientes:

1. Solo se permite la instalación y utilización de equipos periféricos y otros dispositivos electrónicos que sean propiedad del SUAGM y que estén identificados con su número de propiedad.
2. La utilización de dispositivos de almacenamiento externo de datos e información es permitida únicamente en dispositivos que sean propiedad del SUAGM. Se prohíbe la copia o resguardo en dispositivos personales, así como el resguardo de asuntos personales en equipos del SUAGM.
3. Queda prohibido la utilización de impresoras, copiadoras, escáneres, USB, discos duros externos, otros equipos o dispositivos para propósitos personales o ajenos a las funciones oficiales.
4. Queda prohibido traer equipos periféricos personales tales como (pero no se limita a) impresoras, copiadoras, escáneres, *switches, routers*, *hubs*, *hotspots,* discos duros externos o cualquier otro medio electrónico externo y conectarlos a la red de telecomunicaciones del SUAGM sin previa autorización de OCIT.
5. Queda prohibido interceptar o acceder imágenes, en vivo o grabadas, de los sistemas de video vigilancia instalados en las facilidades del SUAGM; para cualquier fin que no sea las funciones oficiales de la Vicepresidencia Auxiliar de Seguridad y Salud Ocupacional.

El uso indebido de los dispositivos del SUAGM o el incurrir en violación a lo aquí establecido conllevará la aplicación de las acciones correctivas y disciplinarias correspondientes, conforme se dispone en los manuales, políticas, normas y reglamentos del SUAGM.

6.5 Uso aceptable de la información (data) por medio de los recursos tecnológicos

El uso y manejo de la información por medio de los recursos tecnológicos es una función esencial para toda labor en el SUAGM. Por tanto, el acceso a la información será de acuerdo al puesto o función que ejerce el usuario en el SUAGM y no para asuntos personales. Es responsabilidad del SUAGM y de toda su comunidad el mantener la data de sus usuarios de forma segura y protegida contra accesos indebidos. Es por ello que las siguientes normas rigen el buen uso de la información:

1. Todo usuario es responsable de toda la información que maneja para realizar sus funciones. Debe asegurar en todo momento que la información sensitiva o confidencial sea administrada bajo los mayores estándares de seguridad, entiéndase la encriptación o el acceso a través de contraseña.
2. Todo usuario debe asegurarse, antes de compartir información, que la persona a quien se le está proveyendo o enviando, es la persona correcta e indicada.
3. En aquellas instancias en que un usuario se encuentre bajo un proceso de investigación o que haya cesado sus funciones para el SUAGM, se le requerirá entregar de forma inmediata toda la información relacionada a sus funciones.
4. Los datos y archivos que contengan información que de alguna forma esté relacionada con la operación del SUAGM serán guardados únicamente en recursos tecnológicos del SUAGM.
5. Todo material que haya sido impreso con información sensitiva deberá ser triturado inmediatamente culmine su propósito. Cada oficina será responsable de proveer el equipo apropiado para este procedimiento.
6. Solo se permitirá compartir información sensitiva (encriptada) con terceros, cuando esté presente uno o varios de los siguientes escenarios:
    a. Para el cumplimiento de una orden judicial estatal o federal
    b. Como parte de un contrato o acuerdo de confidencialidad
    c. Cuando medie una autorización oficial

7. Está prohibida toda divulgación de información sensitiva y/o confidencial de estudiantes, empleados y profesorado del SUAGM, sin previa aprobación de la autoridad competente.
8. Está prohibida la retención, eliminación o difusión de información que esté relacionada a la operación del SUAGM sin la debida aprobación de la autoridad competente.
9. Está prohibida la extracción de información sensitiva mediante el uso de dispositivos externos sin encriptar o a través de material impreso. La extracción o portación de datos tendrá el único propósito de realizar gestiones autorizadas y relacionadas con la operación del SUAGM.
10. Está prohibido el uso de herramientas personales para el almacenamiento o publicación de la información del SUAGM.
11. Está prohibida la ubicación o publicación de información o documentos que sean propiedad del SUAGM en sitios o páginas web de terceros sin la recomendación del Gerente de Seguridad de Sistemas de Información y la aprobación del CIO. Esto incluye pero no se limita a: Dropbox, Google Drive, SkyDrive, iCloud, Dataprius, Box, Mega, Weebly, Spotidoc, GoDaddy, Amazon y cualquier otro de similar naturaleza.
12. Todo usuario deberá asegurarse que los permisos de sus documentos que residen en la nube suministrada o autorizada por OCIT sean los correctos y que no estén públicos.

De tener duda sobre qué información o documentos son propiedad del SUAGM puede referirse a la política de derechos de autor del Sistema Universitario Ana G. Méndez ubicada en la página web del SUAGM.

6.6 Uso de Office 365 o herramientas administrativas web

El SUAGM provee a todos sus empleados, profesorado y estudiantes cuentas de usuario para el uso de las herramientas de productividad Office y todas aquellas herramientas adicionales de servicio que incluye Microsoft. Este sistema es el recurso autorizado y suministrado por el SUAGM para la realización de las funciones administrativas y académicas. Además, se continúa aumentando el acceso a herramientas de forma web

para facilitar el conectarse remotamente a los sistemas del SUAGM. La utilización de las comunicaciones electrónicas y las herramientas web se rigen por las siguientes normas:

1. El usuario deberá utilizar discreción y juicio en el uso de estas herramientas, tomando en consideración el propósito, el contenido y la pertenencia del mismo.
2. La comunicación a través de las herramientas de Office deberá ser en cumplimiento con las normas del SUAGM.
3. El envío o transferencia de información sensitiva o confidencial requiere que el usuario utilice la herramienta de encriptación definida por la unidad de Seguridad de Información de OCIT.
4. El sistema de correo electrónico del SUAGM no constituye, de forma alguna, un método de almacenamiento de archivos. Toda información que requiera ser guardada, deberá almacenarse de forma segura a través de una herramienta autorizada que sirva como repositorio electrónico de documentación oficial, tales como, OneDrive, SharePoint o cualquier otro contratado que haya sido provisto o autorizado por OCIT.
5. Cada usuario es responsable de mantener niveles aceptables de utilización de los sistemas de almacenamiento provistos por el SUAGM, incluyendo hacer la limpieza y el mantenimiento.
6. No se permite la asociación de la cuenta de usuario o el correo electrónico del SUAGM a perfiles de redes sociales personales tales como Twitter, Facebook, Instagram, entre otros. Igualmente, no se debe utilizar esta información para asuntos personales donde se le solicite un correo electrónico como para recibir ofertas o descuentos (por ejemplo, “Groopanda”, “Groupon”, tiendas en general, entre otros).
7. Está prohibido el uso de los recursos de Office para fines comerciales personales del usuario y enviar virus o código de programación mal intencionado.
8. El acceso o intento de acceso por parte de un usuario a la cuenta de Office de otro usuario está prohibido a menos que no sea para propósitos legítimos de investigación y/o auditoría. Esta intervención debe contar con las debidas autorizaciones.
9. Se prohíbe la práctica de compartir cuentas y contraseñas de acceso a los sistemas.

10. El envío de correos electrónicos a grupos o en masa se realizará siguiendo las normas establecidas para dichos envíos.
11. Tabletas o celulares propiedad del SUAGM o personales que sean utilizados para conectarse a Office o a las herramientas web deben tener configurado una contraseña de seguridad ('PIN') y dichos dispositivos no deben estar desbloqueados (*jailbreak*). En caso de pérdida o robo se debe notificar inmediatamente a la Policía y al Analista de Seguridad de Información de OCIT para realizar una limpieza (*wipeout*) del dispositivo.
12. No se exige la utilización de una foto de perfil. Si usted desea colocar una foto de perfil en esta plataforma, solo se permite de su rostro y que muestre un estilo profesional, como por ejemplo, la foto de su tarjeta de identificación que provee la Vicepresidencia de Recursos Humanos.

Las normas aquí establecidas no sustituyen las reglas expuestas en la política para el uso adecuado de sistemas de correo electrónico, sino que complementan la misma.

6.7 Uso de la Internet

El SUAGM proporciona el acceso a la Internet para uso académico, investigativo y administrativo. El uso de la Internet conlleva el establecimiento de normas que estén relacionadas a su utilización. El SUAGM podrá monitorear y/o limitar el acceso de los usuarios al Internet utilizando recursos tecnológicos sistémicos a través de sus unidades de trabajo, esto con el fin de garantizar un servicio seguro y de calidad para nuestra comunidad universitaria. Dada la naturaleza de la Internet, el SUAGM no puede asegurar la disponibilidad, la exactitud, la accesibilidad o el uso apropiado de estos recursos. Cualquier violación o uso indebido del acceso a la Internet conllevará la aplicación de acciones correctivas o y disciplinarias correspondientes, conforme se dispone en los manuales, políticas, normas, y reglamentos del SUAGM.

Se considera uso indebido y, sin limitarse, las siguientes acciones:

1. Acceder a material pornográfico, actividades delictivas, ofensivas, difamatorias, discriminatorias o de cualquier naturaleza ilegal, que puedan ser consideradas ofensivas para otros o que afecten la imagen y seguridad del SUAGM.

2. Acceder, descargar o distribuir material a través de la Internet en violación a los derechos de propiedad intelectual o derechos de autor.
3. Interferir o evadir los sistemas de seguridad, control y monitoreo del acceso a la Internet.
4. Transmitir información sensitiva o confidencial del SUAGM de forma no autorizada.
5. Transmitir información sensitiva o confidencial que no esté debidamente protegida (encriptada).
6. Utilizar el acceso a Internet de forma que se cree congestión o degradación en la red. Para más información refiérase a la Sección 6.3, Inciso 5, Uso Prohibido de Recursos Tecnológicos.
7. Asumir falsa representación.
8. Utilizar las redes sociales de forma que interfiera directa o indirectamente con las funciones y la productividad del usuario.
9. Toda cuenta de redes sociales que se identifique con el nombre o logo de cualquiera de las instituciones del SUAGM debe estar asociada a un correo electrónico oficial. No se permite enlazar las cuentas oficiales a un correo electrónico personal. Dicha cuenta oficial tendrá más de un administrador asociado a la misma, quienes serán los responsables de su desarrollo de contenido, actualización y monitoreo. La creación de estos espacios debe tener la autorización de la Vicepresidencia de Mercadeo y Asuntos Estudiantiles del SUAGM.
10. La utilización de los recursos tecnológicos del SUAGM con fines no académicos y/o administrativos, como por ejemplo la descarga o acceso en línea de música, o el acceso a canales de transmisión (“streaming”) de audio y video.
11. El acceso a áreas de conversación o mensajería en línea (“chats”, “chat rooms”, “blogs”, “messenger”, etc.) utilizando recursos tecnológicos sistémicos, para gestiones personales, no académicas y/o administrativas.
12. La utilización de sistemas no autorizados para almacenar, compartir y distribuir archivos (*filesharing*, *peer-to-peer*, *cloud systems*, etc.). De ser necesario el uso de estos mecanismos debe mediar autorización de OCIT.
13. El acceso a páginas web que pueden comprometer la seguridad de la red del SUAGM.

14. Intentar cualquier ataque de seguridad dentro de los recursos tecnológicos del SUAGM con fines de exponer, experimentar, probar, dañar o afectar servicios dentro y fuera del SUAGM.
15. Cualquier otra acción análoga o relacionada a lo antes descrito, o que guarde un fin similar a poner en riesgo los sistemas o la imagen del SUAGM.

OCIT tiene la facultad de limitar el servicio de navegación al Internet bajo motivos que así lo requieran, como por ejemplo, el mal uso, infecciones por virus, navegación sospechosa y ataques cibernéticos, entre otros.

6.8 Información adicional

1. SUAGM provee sistemas de comunicación de tecnología avanzada, tales como, "*chat*" o "*messenger*", "audio conferencias" y "video conferencias", para poder apoyar la operación y entendiendo que la tecnología es una herramienta necesaria y, en ocasiones, un requisito. De requerir estos servicios puede comunicarse con la unidad de informática y telecomunicaciones de su institución.
2. OCIT ha evaluado y certificado algunos servicios ofrecidos a través de la nube (cloud) por terceros para el almacenamiento de documentos y publicación de páginas. Favor referirse a la página web de OCIT para conocer el listado de los sitios web que han sido autorizados por el SUAGM.
3. De requerir más información o tener duda en cuanto a cualquiera de las normativas aquí expuestas, le exhortamos a que se comunique con el personal de Seguridad de Sistemas de Información de OCIT.

7.0 Respuesta a incidentes de seguridad de información

La complejidad de las nuevas aplicaciones, la realidad de que los sistemas están conectados al Internet y el aumento en la actividad criminal cibernética hace que los incidentes de seguridad de información sean prácticamente inevitables. Por tanto, es indispensable tener un plan de manejo de estos incidentes de forma que se reduzca el impacto de los mismos y

se pueda reaccionar con la mayor rapidez y eficiencia. La comunicación efectiva a todos los niveles del SUAGM es esencial para limitar el impacto de los eventos de seguridad reportados. En consideración de lo cual, resulta imperante que nuestra comunidad sepa identificar incidentes de seguridad y conocer el proceso para reportar los mismos.

7.1 Identificación de incidentes de seguridad de información

Se exhorta a los usuarios a comunicar cualquier incidente de seguridad de información que pueda ser detectado y que presente, sin limitarse, las siguientes características:

1. Comportamiento errático e inexplicable de computadoras, servidores y las redes, como por ejemplo:
    a. Que el *mouse* se mueva solo y que comience a realizar acciones que usted no ha solicitado.
    b. Intermitencia exagerada en la conexión en un período corto, entiéndase de 5 a 10 minutos de tiempo.
    c. El sistema se presenta extremadamente lento.
2. Detección de cuentas que han sido bloqueadas concurrentemente sin ningún tipo de explicación.
3. Detección de acceso no autorizado a dispositivos electrónicos del SUAGM, como por ejemplo:
    a. Computadoras personales conectadas a la red administrativa (por cable).
    b. Personas que no son empleados del SUAGM utilizando computadoras del área administrativa.
    c. Pérdida o robo de equipos.
4. Robo de contraseñas.
5. Descubrimiento de sistemas inalámbricos no autorizados, como por ejemplo puntos de acceso de *wifi* (“*hot spot*”).
6. Email de *phishing* que ha sido accedido y credenciales han sido comprometidas.
7. Información confidencial o sensitiva ha sido distribuida inadvertidamente a personas no autorizadas o ha sido publicada en Internet.
8. Robo de información.
9. Comportamiento errático de algunas de nuestras páginas web, como por ejemplo:
    a. La página web contiene anuncios o imágenes con contenido no apropiado (pornográfico) o no representativo del SUAGM.

b. Si el escrito de la página web no es legible o entendible.
c. Si se encuentra fuera de servicio.
d. Si lo redirige a otra página que no es del SUAGM.

10. Amenazas de ataques cibernéticos dirigidas al SUAGM por cualquier medio de comunicación, entiéndase correo electrónico, correo regular, redes sociales, entre otros.
11. Prácticas de ingeniería social.

7.2 Cómo reportar incidentes de seguridad de información

No intente realizar ninguna otra acción que implique investigar lo sucedido, recolectar pruebas o solucionar el problema ocasionado por el incidente, sin la autorización previa de la unidad de Seguridad de Información de OCIT.

Todo usuario tiene la responsabilidad de reportar incidentes de seguridad de información a OCIT a través de los siguientes canales de comunicación:

- Email: servicedesk.suagm.edu o seguridadit@suagm.edu
- Teléfono: (787) 751-0178 extensión 7487, 7122
- Fax: (787) 751-3360
- Para someter un incidente de forma anónima utilice la siguiente dirección: https://humanresources.suagm.edu/sugerencias/ (tu opinión es importante).

7.3 Acta de seguridad cibernética en el campus

En armonía con los requerimientos de la Ley de Seguridad en el Campus, conocida como "*Jeanne Clery Act"* y con el propósito de ayudar a la prevención de un delito cibernético contra una persona o un delito particularmente amenazante contra los sistemas o la propiedad, el SUAGM mantendrá un informe anual de seguridad cibernética. En dicho informe estarán recopilados varios delitos del Código Penal y leyes especiales que tipifican ciertas conductas que pudieran entenderse como crímenes cibernéticos. Entre los delitos que se podrán reportar, siempre que exista evidencia sustancial de evidencia digital, se encuentran:

- Delitos contra la protección debida a los menores
- Delitos de obscenidad y la pornografía infantil

- Delito contra el derecho a la intimidad
- Delito contra la tranquilidad personal
- Delito contra los bienes y derechos patrimoniales
- Delitos relacionados con el fraude
- Delitos relacionados con la usurpación de identidad
- Delitos relacionados con las falsificaciones
- Delitos relacionados con la interferencia de los servicios públicos
- Violaciones a la Ley de regulación de programación de espionaje cibernético
- Violaciones a la Ley contra el acecho en Puerto Rico

Para más información sobre los delitos por favor refiérase al informe anual de seguridad cibernética que se encuentra en la página web de OCIT. Si usted es víctima de algún delito o requiere reportar alguno del cual tiene conocimiento, pero no quiere emprender ninguna acción dentro de la universidad o el sistema de justicia penal, le solicitamos que libre y voluntariamente considere someter el incidente de seguridad de sistemas de forma anónima según se indica en la sección 7.2. Todos los informes son manejados de forma confidencial. Los informes confidenciales y anónimos permiten recopilar registros precisos sobre el número de incidentes que ocurren en el SUAGM.

7.4 Referido de incidentes reportados a autoridades competentes

El SUAGM no se responsabiliza por acciones individuales de miembros de la comunidad universitaria que violenten las disposiciones del uso de los recursos tecnológicos. Si el SUAGM lo entiende pertinente, podrá referir cualquier incidente reportado a las agencias estatales y/o federales concernidas.

8.0 Historial de revisión de actualización

Versión	Descripción de la Actualización	Fecha
1.0	Versión original presentada	19/05/2015
1.1	Versión revisada por consultor experto Seguridad	25/09/2015
1.2	Versión revisada por Comité Políticas SUAGM	04/05/2016
1.3	Versión revisada por CIO, Rectores y Funcionarios	22/07/2016
1.4	Versión revisada por DESK Trial Lawyers & Counselors, LLC	09/09/2016

9.0 Autores

	Nombre	Fecha
Redactado Por:	Xohara Ayuso Vázquez	19 de mayo de 2015
Revisado Por:	Ricardo R. Reyes	12 de agosto de 2015
Revisado Por:	Abacode	25 de septiembre de 2015
Revisado Por:	Comité Revisión de Políticas SUAGM	4 de mayo de 2016
Revisado Por:	Kenneth Maldonado, CIO y Luis E. González, VP Asociado	27 de junio de 2016
Revisado Por:	Funcionarios y Rectores	22 de julio de 2016
Revisado Por:	DESK Trial Lawyers & Counselors, LLC	9 de septiembre de 2016