

Universidad de Puerto Rico
Oficina de Sistemas de Información
Administración Central

Reglamento de Uso de Servicios y Comunicaciones Electrónicas
Marzo 2017

INTRODUCCIÓN

La Universidad de Puerto Rico reconoce la importancia del uso de las comunicaciones electrónicas como un servicio esencial del quehacer de la comunidad universitaria. Además promueve su uso para apoyar la gestión administrativa y la misión educativa, investigativa y de servicio. Para ello, la Universidad provee servicios y facilidades de comunicación electrónica.

Este documento complementa la *Política Institucional sobre el Uso Aceptable de los Recursos de la Tecnología de la Información en la Universidad de Puerto Rico* y no sustituye o contradice ninguna de sus partes.

OBJETIVOS

El Reglamento y Procedimiento para las Comunicaciones Electrónicas de la Universidad de Puerto Rico tiene como objetivo proveer principios, reglas y procedimientos para el uso eficiente, efectivo y seguro de los recursos electrónicos que se utilizan para intercambiar o publicar información como lo son el correo electrónico (e-mail), los servicios de mensajes instantáneos, foros electrónicos institucionales, grupos de discusión, notificaciones electrónicas, redes sociales y páginas web, entre otros.

ALCANCE

Este Reglamento y Procedimiento aplica a todos los usuarios de los sistemas de comunicación electrónica, entiéndase estudiantes, profesores y todo el personal con acceso a dichos recursos, además de personas externas quienes prestan o reciben algún servicio. Aplica a todos los recursos de comunicación electrónica que pertenecen o son manejados por la Universidad de Puerto Rico y sus Recintos, u otros recursos provistos por la Universidad a través de contratos o acuerdos.

DISPOSICIONES GENERALES

Los sistemas de comunicaciones electrónicos, ya sea de uso interno o externo, son para ser utilizados en apoyo al quehacer de la Institución en su misión educativa, administrativa, servicios y de investigación.

Las comunicaciones transmitidas a través de los sistemas debe tener un propósito legítimo relacionada con la Universidad. Las mismas son para ser utilizadas para propósitos legales, y de ninguna manera para cualquier propósito ilegal, amenazadora, abusiva, fraudulenta, difamatoria, obscena o pornográfica, o cualquier comunicación, transmisión o distribución de material que constituya o promueva una conducta ilegal o que viole cualquier ley o reglamento institucional, estatal, federal o internacional. El uso de de las comunicaciones electrónicas de la Universidad para propósitos privados o comercial personal está estrictamente prohibido.

Según se establece en la Certificación, la Universidad reconoce el uso ocasional personal, sin fines de lucro, siempre y cuando no interfiera con el desempeño en el trabajo, o viole alguna política, reglamento o ley vigente.

Además, se reconoce la plataforma de *G Suite* (antiguo *Google Apps for Education*) como el sistema de productividad y colaboración institucional, según la [Certificación 82 \(2008-2009\)](#).

CORREO ELECTRÓNICO INSTITUCIONAL

La plataforma del *G Suite* incluye el servicio de correo electrónico, por lo cual se considera este como el sistema de correo electrónico institucional oficial.

Cuando un usuario se hace parte de la comunidad universitaria, ya sea como estudiante, empleado, o como parte de algún proyecto o circunstancia especial, se le asigna unas credenciales institucionales que dan acceso a los servicios del *G Suite*, entre otros.

El correo electrónico institucional se reconoce como un método oficial de intercambio de información. Como documentos electrónicos oficiales, se espera que cualquier gestión, documento o comunicación oficial haciendo uso de correo electrónico utilice la cuenta oficial interna de la Institución. Por consiguiente, no se utilizará ni se hará referencia a cuentas de correo electrónico externas a la Institución para efectuar comunicaciones electrónicas oficiales.

Por otra parte, la trasmisión de documentos con información restricta y/o privada institucional a través del correo electrónico debe hacerse conforme a la *Guía para el Manejo de los Datos de la Universidad de Puerto Rico*.

Por otra parte, se espera que el usuario no utilice su cuenta de correo institucional (credenciales) para registros y servicios externos personales (ej. cuentas de bancos, tiendas en

línea, membresías, etc.). La Universidad no se hace responsable del contenido de correos electrónicos personales de esta índole, ni de posibles consecuencias al usuario como parte de algún servicio malicioso, ilegal, o con contenido confidencial del individuo.

Según la Certificación, la Universidad puede intervenir con los recursos de Tecnología de Información. Según el *Procedimiento General para el manejo de Incidentes de la Tecnología de Información en la UPR*, la Universidad podrá intervenir con el correo electrónico en caso de la pérdida de contacto con el usuario custodio de dicha cuenta, o cuando se requiera en el caso de una investigación en curso.

Además, las credenciales institucionales, las cuales incluyen el acceso al correo electrónico pueden ser desactivadas sin previo aviso al usuario en caso de una investigación o querella, o para proteger la integridad, seguridad y operación, o para protegerse de algún riesgo o responsabilidad.

Cuando un usuario que no es parte de la comunidad universitaria, pero en el desempeño de algún servicio o colaboración requiere credenciales institucionales, se procederá a solicitar mediante solicitud oficial dicho acceso, en donde se especifique razón para dicho otorgamiento, firmas de las personas que auspician y supervisará al usuario, y fecha de expiración para dichas credenciales.

Las credenciales institucionales son confidenciales y bajo ninguna circunstancia deben ser compartidas. Sin embargo, un usuario que en el desempeño de su labor requiera asistencia en la administración de los correos electrónicos puede utilizar el recurso de “delegación”, el cual puede ser configurado y utilizado a través de la herramienta en línea de correo electrónico del *G Suite*. Una cuenta delegada da la capacidad de leer, enviar y borrar correos electrónicos, y estos quedan identificados como que han sido tramitados por la persona a quien ha sido delegada.

La institución promueve el uso de cuentas genéricas que identifican una oficina, centro o posición administrativa, la cual puede ser utilizada por el administrador en turno de dicha oficina o centro, o por un personal clerical asociado a la unidad. Estas cuentas son creadas mediante solicitud. El personal administrativo en turno es responsable de estas cuentas, con la misma responsabilidad y disposiciones que rigen su cuenta de usuario oficial institucional. Cuando estas cuentas son delegadas a un nuevo administrador de la misma, este nuevo administrador se asegurará de cambiar la contraseña de dicha cuenta genérica y se asegurará que la misma no es accedida por personal no autorizado.

Es responsabilidad del usuario conservar todo correo electrónico de interés institucional y hacerlo disponible a la institución cuando sea requerido, o cuando se entienda necesario para dar continuidad los trabajos y actividades institucionales.

La *Ley para Regular el Proceso de Transición del Gobierno de Puerto Rico* (Ley Núm. 197 del 18 de agosto de 2002, enmendada), establece claramente la responsabilidad que tienen todo funcionario público de garantizar que la información y documentos que son parte de una administración deben ser conservados y puestos a disposición de administraciones subsiguientes. Además la Ley establece, en el *Artículo 19.- Sanciones y Penalidades*, lo siguiente:

“(B) Destrucción o Mutilación de información, archivos o expedientes, incluyendo aquellos electrónicos, con la intención de retrasar u obstaculizar el proceso de transición, o de evadir su responsabilidad en cualquier agencia, departamento o corporación pública del Estado Libre Asociado de Puerto Rico cometerá delito grave y convicto que fuera, será sentenciado a cumplir seis (6) años de cárcel. De mediar circunstancias agravantes la pena podrá ser aumentada.”

Además, el *Reglamento para la Administración, Conservación y Disposición de Documentos de la Universidad de Puerto Rico, Certificación 62 (2015-2016)*, establece claramente, entre otras cosas, en el artículo XII que:

“No se destruirá, enajenará, obsequiará, alterará o dispondrá de documentos de la Universidad de Puerto Rico, a menos que sea conforme a la Ley. Toda persona que realice o facilite la ejecución de una de estas acciones sobre cualquier documento de la Universidad estará sujeta a las sanciones dispuestas por las leyes y reglamentos aplicables.”

Otras Leyes y Reglamentos pueden aplicar de igual forma.

La plataforma del G Suite provee la capacidad de que la Administración Universitaria conserve de forma permanente los correos electrónicos y el contenido del G Drive, aunque estos hayan sido borrados por los usuarios. Dicha funcionalidad permite cumplir con el *Procedimiento General para el manejo de incidentes de la Tecnología de Información de la UPR* y la *Guía para la Intervención de Información en el Sistema de Productividad y Colaboración Institucional*.

DESACTIVACIÓN DE CUENTAS DE PERSONAL O ESTUDIANTES NO ACTIVOS

Todo personal y estudiante que por cualquier causa o razón deja de ser parte de la comunidad universitaria activa (renuncias, jubilados, exalumnos) pasa por un proceso de relevo de responsabilidad que incluye, entre otras cosas, la desactivación de acceso a cuentas de servicios administrativos y académicos.

Las credenciales institucionales que utilizó el usuario para acceder los servicios en la Universidad serán desactivadas, aunque no eliminadas. El contenido de los espacios virtuales y de los servicios que utilizó durante su relación con la institución se conservarán de forma permanente.

Accesos que requiera el usuario luego de ser separado de la relación con la Universidad, a la información contenida en los sistemas de información de la Universidad, deberá ser tramitado a través de la Oficina de Recursos Humanos y/o la Oficina de Sistemas de Información de la Unidad a la cual pertenecía.

Se recomienda que la información que desee conservar el usuario debe ser descargada antes de que sus credenciales sean desactivadas.

PORTAL DE SERVICIOS ELECTRÓNICOS (Portal UPR)

El servicio conocido como Portal (<http://portal.upr.edu>) es la plataforma primaria de servicios electrónicos de la comunidad universitaria. Esta plataforma permite a los usuarios acceder servicios de comunicación, autoservicio y trámite para estudiantes, profesores y empleados en general.

Las credenciales asignadas para acceder estos servicios en el Portal son las mismas credenciales institucionales oficiales.

Aunque se reconoce la existencia de otros sistemas electrónicos que ofrecen servicios a sectores de la comunidad universitaria las cuales utilizan sus propias credenciales, estas no son consideradas las credenciales institucionales oficiales. Estos otros servicios individuales son evaluados para determinar su legitimidad, uso no conflictivo y seguridad. La evaluación de la legitimidad, uso no conflictivo y seguridad de los servicios electrónicos en la Institución es responsabilidad del Principal Oficial de Informática y del Principal Oficial de Seguridad de la Institución.

El resultado de estas evaluaciones pueden resultar en el requerimiento de medidas de seguridad adicionales, o cualquier otro requerimiento que garantice que el servicio es provisto y atendido adecuadamente. Una evaluación que evidencie la prestación inadecuada de dichos servicios podrá requerir la suspensión de los mismos.

SOLICITUD DE ENVÍO DE CORREO ELECTRÓNICO A LA COMUNIDAD UNIVERSITARIA

El sistema de correo masivo es un mecanismo de correo electrónico para la difusión de anuncios y actividades a toda la comunidad universitaria de la Universidad de Puerto Rico. Este mecanismo de difusión se estableció con el propósito de llevar información sobre asuntos extraordinarios y relevantes a TODA la población en la Universidad.

Se crearán distribuciones separadas por temas con el propósito de segregar los mensajes según el grupo al que va dirigido (estudiantes, profesores, empleados, actividades, convocatorias, etc.). Además, se ha estableciendo que no se utilizará el mecanismo de Cartero

AC para difundir información dirigida principalmente a un sector limitado de la comunidad universitaria, o local (Recintos).

Los Recintos pueden utilizar los mecanismos de difusión masiva internos con los que cuentan para informar a la totalidad o a sectores específicos en sus unidades. Además, se debe evaluar siempre otras estrategias con el fin de tener medios ágiles alternos de difusión de información y no solo depender del correo electrónico.

Como procedimiento general, se establece las siguientes reglas:

- Es requisito que se identifique el grupo o grupos a quien se tiene destinada la comunicación, e información de contacto de los responsables del mensaje.
- Los mensajes de personas o grupos individuales, asociaciones no reconocidas a través de los procesos oficiales establecidos en la Universidad, o de carácter personal de individuos no serán considerados para su difusión a través de los mecanismos internos de la institución a menos que no tenga un interés institucional genuino y que cuente con el endoso de la Oficina de Prensa y Comunicaciones.
- El método primario de difusión de promoción de actividades y noticias será a través de la página principal de la Universidad o sus Unidades.
- No se garantiza la publicación o el envío de un mensaje a través del correo electrónico el mismo día de haberlo solicitado.
- Se espera además que el mensaje a ser publicado o enviado a través de correo electrónico sea sometido de forma electrónica y accesible, tal y como se desea que se publique. La Oficina de Sistemas de Información, o la Oficina a cargo de los envíos no se hace responsable de transcribir o editar la información que se desea enviar.
- Ningún mensaje será enviado más de una vez a través de correo electrónico masivo.
- De ser necesario, por el contenido que pueda tener la comunicación (imágenes, documentos grandes) se hará referencia en el mensaje a enlaces donde se encontrará la información deseada. Estos enlaces deberán estar accesibles en un servidor interno en la institución.

Todas estas consideraciones deberán ser aplicadas por aquellos individuos que poseen el acceso de enviar correo masivo ya sea haciendo uso de las herramientas provistas por la Universidad o por cualquier otro mecanismo.

MALWARE, CORREO MASIVO SIN SOLICITAR (SPAM) Y MENSAJES EN CADENA

El sistema de correo electrónico institucional cuenta con un sistema de filtrado de *malware* e identificación de potencial correo electrónico masivo sin solicitar conocido comúnmente como *spam*. Todo correo electrónico que positivamente es identificado con *malware* o como *spam* es rechazado o marcado como tal automáticamente.

Se espera que los usuarios no utilicen los sistemas de comunicación para enviar mensajes en cadena. Si un usuario recibe uno de estos mensajes en su cuenta de correo electrónico no deberá, como normalmente se pide en estos mensajes, reenviarlo. Además, ningún usuario deberá enviar mensajes de índole político, religioso, comercial, difamatorio o inmoral a otros individuos o a listas personales de distribución, ni mensajes de índole económico donde una de las partes se pueda beneficiar económicamente de las acciones solicitadas en los mensajes. Si un usuario desea enviar un mensaje que no es de interés institucional a destinatarios en listas personales, deberá asegurarse primero que el/los recipientes de la comunicación están de acuerdo en recibirlo.

CONFIGURACIÓN DE SERVICIOS ELECTRÓNICOS

Como regla general, todo servicio electrónico en el cual se accedan o transmitan datos restringidos, privados o confidenciales, incluyendo las credenciales institucionales, tendrá que hacerse mediante conexiones seguras (cifradas), según se establece en la *Guía para el Manejo de los Datos de la Universidad de Puerto Rico*.

Las Unidades institucionales deberán mantener un inventario de los servicios electrónicos habilitados, incluyendo una descripción del mismo, su propósito, versión del programado utilizado y puertos de conexión utilizados. Se requiere que los servicios se mantengan actualizados, en sus versiones más recientes y se apliquen los parches disponibles correspondientes a vulnerabilidades conocidas e identificadas.

La [Guía de Configuración de Servicios Electrónicos](#) define los requisitos mínimos de configuración de los servicios más comunes.

REDES SOCIALES Y OTRAS REPRESENTACIONES

Las redes sociales se reconocen en nuestra institución como un mecanismo aceptable para complementar la misión de la Universidad, tanto en el área académica, administrativa y de investigación. Sin embargo, la proliferación y la facilidad del uso de estas plataformas propicia la falsa representación y el descontrol del contenido que se publica.

La Universidad delega el mantenimiento del inventario de la presencia de los organismos institucionales en las redes sociales a las respectivas Oficinas de Prensa y Comunicaciones de las Unidades. Estas serán responsables de hacer un inventario de forma periódica y exigirá responsabilidad a los Organismos que representan a la Universidad en estos ambientes. Tendrán la potestad de crear reglamentos y guías que ayuden a garantizar la continuidad, el mantenimiento y la imagen institucional correcta.

PUNTOS FINALES

Se ha creado una página informativa en donde se expone algunas de las mejores prácticas para minimizar los riesgos potenciales asociados con las comunicaciones y los sistemas de información. Esta página puede ser accedida en <http://seguridad.upr.edu> (en desarrollo).