



Migración a Outlook Oficina de Sistemas de Información

10 de septiembre de 2020

Universidad de
Puerto Rico
Oficina del Presidente

La Universidad de Puerto Rico (UPR) ha iniciado un proyecto piloto a fines de cambiar su sistema de correo electrónico de *Gmail* a *Outlook* por razones de seguridad y economía, principalmente. El proceso comenzó en la Administración Central y hubo que agilizar el mismo de forma escalonada durante el verano de 2020 por motivos y razones que exponemos en el presente informe.

Igual que otras entidades, la Universidad de Puerto Rico ha sido objeto de ataques cibernéticos que fueron incrementando en la medida en que aumentó el uso del Internet y otras plataformas tecnológicas. La mayoría de los ataques se reciben a través del sistema de correo electrónico. Esto ha provocado gastos adicionales a la institución que sobrepasan el millón de dólares. Uno de los ataques fue el secuestro de información en el Recinto de Ciencias Médicas en julio de 2019. La compañía proveedora de la póliza de seguridad cibernética tuvo que desembolsar una cantidad significativa de dinero para solucionar la situación y evitar la exposición de información sensible.

Oficina de
Sistemas de Información

Estos incidentes, además, provocaron que se detuviera el proceso de contratación de la póliza de seguridad cibernética, ya que se requirieron elementos de seguridad adicionales a los que ofrece el *G Suite for Education*. No hemos encontrado una aseguradora en Puerto Rico que asuma el riesgo hasta que la UPR demuestre la implementación de medidas más estrictas de seguridad. Hasta el momento la institución tiene una extensión parcial de la póliza que vence el 1 de noviembre de 2020.

La póliza actual tiene un costo de \$32,000 y cubre un máximo agregado de \$1 millón, y lo siguiente (copia textual en inglés):

- *Privacy Liability: The insurer will pay damages and claims expenses by reason of a claim first made against the insured during the policy period and reported to the insurer pursuant to section VII. Notice, for any wrongful acts taking place after the retroactive date and prior to the end of the policy period.*
- *Data Breach Fund: The insurer will pay data breach expenses incurred by the insured during the policy period by reason of a claim reported to the insurer pursuant to Section VIII. Notice, for any wrongful acts taking place after the retroactive date and prior to the end of the policy period.*
- *Network Security Liability: The insurer will pay damages and claims expenses by reason of a claim first made against the insured during the policy period and reported to the insurer pursuant to Section VIII. Notice, for any failure of network security place after the retroactive date and prior to the end of the policy period.*

Para cumplir con estos requerimientos y salvaguardar la seguridad de los datos institucionales y la información que comparten nuestros estudiantes y empleados, la Oficina de Sistemas de Información de la Administración Central (OSI) evaluó las alternativas disponibles, tomando en

Jardín Botánico Sur
1187 Calle Flamboyán
San Juan PR 00926-1117
787-250-0000 Ext. 5400
Fax 787-763-6760

consideración las necesidades del sistema universitario, costos, entre otros aspectos técnicos y de implementación.

Luego de realizar la evaluación, la OSI recomendó la implementación de *Outlook*. Esta plataforma ya estaba disponible para la Universidad, sin costo adicional, por virtud de un contrato entre la institución y *Microsoft* para servicios indispensables para la operación y funcionamiento de la UPR incluyendo: servidores para bases de datos y proyectos, licenciamiento y herramientas de seguridad robustas, plataformas de servicios para proyectos en la nube, garantía de una operación segura, y en cumplimiento con requisitos locales y federales establecidos para instituciones de educación superior. Estos servicios, sin los cuales la Universidad no podría operar, redundan en un costo de aproximadamente \$3.3M renovados cada tres años.

Desde el 1999, la UPR contrata con *Microsoft* bajo diferentes modelos de licenciamiento. En el año 2013, los contratos se centralizaron para reducir costos y trabajar en forma integrada, en lugar de mantener contratos individuales por unidad dentro del sistema.

Microsoft ofrece el programa de *Outlook* a la UPR como parte del paquete de servicios bajo el contrato vigente. *Outlook* ofrece los mecanismos de seguridad que se necesitan para proteger los datos institucionales y de los usuarios.

La UPR tiene su cuenta de *G Suite for Education* desde el 2007, cuando se adquirió para mejorar y uniformar la mensajería electrónica para el principal centro docente de la isla. Para poder añadir los controles de seguridad y análisis avanzados óptimos, como los que ofrece *Outlook*, *G Suite for Education* requiere incurrir en un costo aproximado desde \$240,000 - \$2.88M anuales¹ adicionales, dependiendo de la negociación con *Google* y el total de cuentas. Esta cantidad no incluye los servicios esenciales requeridos para la operación antes mencionados.

El personal de Sistemas de Información de la Administración Central de la UPR, al igual que consultores, evaluaron los servicios. Ante el costo adicional que implicaría *G Suite for Education* para cumplir con requisitos de seguridad rigurosos, se determinó utilizar *Outlook* debido a varios factores: 1. Cumple con los requisitos de seguridad que necesita la UPR urgentemente; 2. No implica costo adicional; 3. Sólo requiere migración de cuentas de *Gmail* a *Outlook*; 4. *Microsoft* ofrece mediante su representante en Puerto Rico apoyo técnico y adiestramientos sin costo adicional; 5. El contrato vigente con *Microsoft* cubre los servicios descritos anteriormente evitando que los usuarios actuales tengan que costear el uso de manera individual.

Cancelar el contrato con *Microsoft* no es una opción viable, ya que implicaría la pérdida de servidores y otros servicios indispensables, lo que pondrían en riesgo el sistema de informática de la UPR. El sistema provee diferentes programas que son utilizados ampliamente a través del sistema.

La OSI sostuvo reuniones con los directores de sistemas de información de las unidades sobre este tema durante la primera mitad del 2020. Se realizó un proceso de RFP que se hizo público y todas las unidades participaron en las determinaciones.

¹ \$48 por usuario por año para facultad y estudiantes si se adquieren licencias individuales; \$24 por usuario si se adquiere la licencia para facultad y personal. Según se desprende de la página electrónica de *G Suite Enterprise for Education*: https://edu.google.com/products/gsuite-for-education/enterprise/?modal_active=none

La OSI emitió un comunicado a los empleados de la UPR previo al inicio de la migración (comunicado enviado el 4 de junio de 2020) para informar sobre el proceso. Además, se encomendó a los directores de las unidades ir trabajando y orientando a su comunidad universitaria sobre el cambio, así como atendiendo las circunstancias o problemas que ocurriesen durante la migración.

Las cuentas que se determinó migrar fueron las de los estudiantes y empleados activos (60,000 cuentas) del total que tiene la UPR (sobre 400,000 incluyendo jubilados y exalumnos que permanecerán en *Gmail*). A la fecha sólo se han migrado 8,632 cuentas que pertenecen a empleados. Aún se evalúa la migración de las cuentas de los estudiantes. Es necesario que todas las cuentas se porten a *Outlook* para implementar todas las herramientas y políticas de seguridad disponibles, conforme al propósito principal del cambio de plataforma.

Con la migración de *Gmail* también se migró *Calendar*, debido a que está atado al correo electrónico. Las demás herramientas de *G Suite for Education* (versión adquirida desde el 2007) tales como *Google Drive*, *Meet*, *Classroom*, entre otros, continúan activas y no hay intención ni razón al presente para que sean desactivadas. Las plataformas de *Google* y *Microsoft* son compatibles y las futuras migraciones se harán con mayor rigurosidad y precaución, basándonos en la experiencia reciente.

Entre las cuentas que quedan pendientes de migración están las de estudiantes y las utilizadas para envío de correos en masa. Estas se llevarán a cabo luego de que se documente y se atienda lo sucedido y aprendido durante la primera fase de transición de un sistema a otro, según surgió con los empleados. El fin es evitar los problemas confrontados durante el verano. Esto implica que se estarán ofreciendo talleres y orientaciones a los usuarios para tener una transición más ordenada.

Elementos de Seguridad de Microsoft

Los elementos de seguridad que tiene el contrato con *Microsoft 365* que no se tiene con *G Suite for Education* incluyen:

- Restricción de acceso a la plataforma desde países con poca reputación y desde donde se observaron intentos de ataques (Acceso condicional– Regla de Bloqueo –Implementado)
- Reglas basadas en comportamiento de usuarios (Reglas en MCAS y de momento solo en monitoreo)
- Acceso a recursos de la UPR (correo electrónico) sólo desde aplicaciones permitidas (*Outlook Mobile*, *OWA*, *Outlook Desktop*) (No implementado)
- Doble factor de autenticación (No Implementado)
- *Self Service Password Reset* (No Implementado)
- Administración de Dispositivos (*Intune* – No Implementado)
- Protección contra malware y ataques de día 0 en correo electrónico (Implementado)
- Reglas de Protección de *Phishing* (Correo – Implementado en Monitoreo)

La plataforma cuenta con un sinnúmero de controles de seguridad adicionales y herramientas para el resguardo de la información que serán considerados en la próxima fase. Además, provee a los administradores la visibilidad para monitorear ataques cibernéticos y tomar acción de manera proactiva.

A modo de ejemplo de los avances a nivel de seguridad hasta la fecha, incluimos una muestra visual del comportamiento de las cuentas de UPR antes y después de aplicar la regla que bloquea el acceso desde sitios maliciosos o de no confianza.

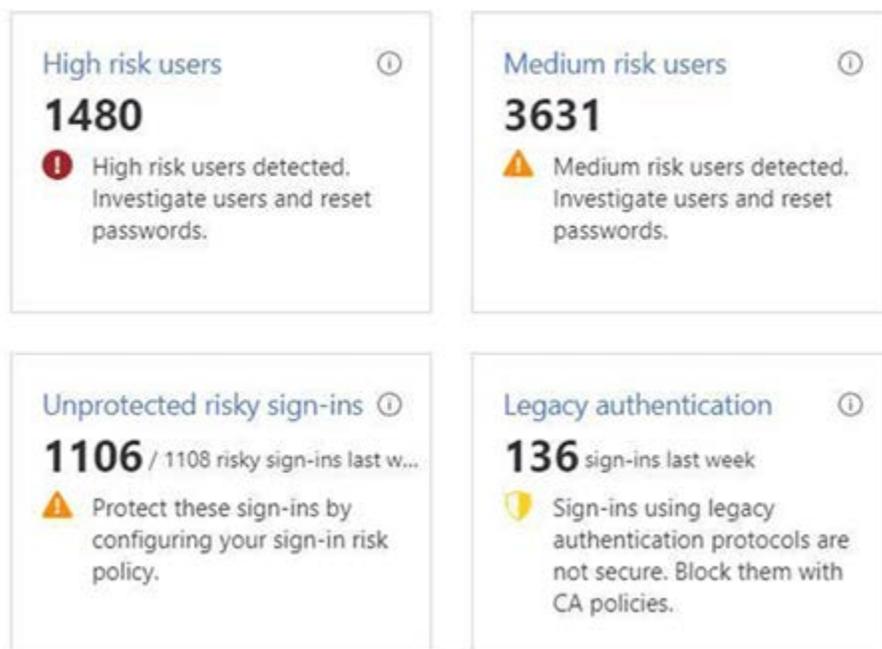
Esta imagen, que corresponde al 6 de julio de 2020, muestra evidencia de intentos de acceder a la plataforma de correo electrónico de la UPR desde otras jurisdicciones.



La siguiente imagen es del día 13 de julio de 2020, y demuestra la disminución de posibles accesos después de implementar la primera fase de migración a *Outlook* y las nuevas reglas de seguridad.



También se incluye a continuación un reporte de credenciales robadas que está detectando la plataforma *Outlook*. La herramienta detecta otras actividades tales como viajes imposibles, patrones anómalos, entre otros. Tanto así que la herramienta detecta hasta el momento 1,480 usuarios con un alto riesgo.



Es importante tomar en cuenta que estos controles están en monitoreo en este momento, pero la plataforma puede tomar acción si así lo deseamos, y en otros casos como, por ejemplo, cuando un usuario se trata de conectar desde un IP malicioso, bloquea la conexión.

En el tema de resguardo de los datos, toda actividad dentro de la plataforma es guardada en bitácoras que pueden ser auditadas en cualquier momento, así como todas las certificaciones de tercero que tanto *Microsoft 365* como *Azure* cumplen.

A continuación, compartimos el enlace donde se encuentran las certificaciones con las que cumplen las plataformas: <https://docs.microsoft.com/en-us/microsoft-365/compliance/offering-home?view=o365-worldwide>

Algunas de estas herramientas y certificaciones sí están incluidas en *G Suite Enterprise for Education*, pero conllevan un costo adicional; tal y como mencionamos previamente, pudieran rondar desde \$240,000 a \$2.88M anuales, dependiendo de los niveles de seguridad y la cantidad de cuentas asignadas.

Otros beneficios de Outlook

Las herramientas de productividad de *Microsoft* son las más utilizadas por nuestra comunidad universitaria y representan el estándar de la industria. *Office 365* ofrece las licencias de *Word*, *Excel*, *Power Point* y *Teams*, entre otras, que nuestros estudiantes y profesores pueden descargar hasta en cinco dispositivos.

Microsoft Teams es una oficina virtual que integra todas las herramientas de productividad y ha sido esencial para asegurar la continuidad de las operaciones y el trabajo remoto durante la emergencia provocada por la pandemia de COVID-19. Además, la plataforma de educación a distancia *Moodle* que contamos a nivel sistémico integra bien con *Microsoft 365*, incluyendo con *Teams*.

A continuación, se provee una lista de guías, manuales y sugerencias para temas de seguridad, accesibilidad entre otros.

- [Inicios rápidos de Office](#)
- [Ayuda y formación para las aplicaciones de Office](#)
- [Ayuda y formación para las aplicaciones de Office en el ámbito educativo](#)
- [Herramientas y funcionalidades de accesibilidad \(“accessibility”\) en Office](#)
- [Cambiar a SharePoint Online desde Google Sites](#)
- [Cambio de contraseña](#)
- [Activar componentes de seguridad para su cuenta](#)

Mediante la plataforma de *Microsoft Teams* todos los usuarios de la Universidad podrán tener un *hub* de colaboración que incluye herramientas que le permitirán ser más productivos desde un único lugar para realizar las siguientes acciones, a diferencia de otras soluciones:

- Establecer [conversaciones en tiempo real](#) con otros usuarios de la comunidad educativa y usuarios externos de ser necesario.
- Realizar videoconferencias en tiempo real con funcionalidades como la de registro de participación y traducción en vivo además de funcionalidades nuevas como “breakout rooms”, “[together mode](#)” y más.
- Realizar [eventos en vivo](#) en donde pueden participar hasta 10,000 usuarios concurrentes con un panel de Q&A para interactuar con los participantes y registrar su participación.
- [Canal de videos interno](#) con inteligencia artificial que provee transcripción y traducción en múltiples lenguajes proporcionando búsquedas avanzadas en base al contenido de las grabaciones.
- [Crear notas y apuntes digitales](#) con buscador para un acceso rápido y continuo a sus notas.
- Compartir una [pizarra virtual](#) durante llamadas en *Teams* para poder dibujar y escribir juntos en un lienzo digital compartido.
- Manejar y ver el progreso de sus tareas y las de su equipo en proyectos e investigaciones desde [Planner](#)
- Crear [encuestas, exámenes y cuestionarios](#).
- Integrar con [aplicaciones de terceros](#)
- [Almacenar documentos](#) y [manejar flujos de aprobación](#)
- [Realizar reportes](#) con su información para análisis y predicción
- Proveer un espacio de colaboración inclusivo tanto en el salón de clases como en el ambiente laboral con las [herramientas de accesibilidad](#) que ofrece *Microsoft*.

Otra herramienta muy útil es *Bookings* que podría utilizarse para coordinar citas y reuniones con oficinas de servicios a estudiantes y para que los estudiantes coordinen reuniones con sus profesores.

Problemas que se han presentado durante la migración a Outlook

1. Cuentas de empleados no migradas

Cada recinto y unidad compartió con la OSI una lista de cuentas de empleados para que fueran migradas a *Outlook*. Al momento de realizarse la migración, algunos empleados notificaron que sus cuentas de correo electrónico no funcionaban. Esto se debe a que algunas listas no estaban actualizadas y se quedaron empleados sin migrar apropiadamente. Inicialmente este proceso de activación de cuentas se realizaba en Administración Central, pero para acelerar el proceso, se le asignaron los accesos a los directores de sistemas de información de las unidades para atender los mismos. La mayoría de las cuentas de empleados han sido migradas exitosamente.

2. Regla de *forwarding* de *Outlook* a *Gmail*

Algunos empleados reportaron que dejaron de recibir correos electrónicos, y que *Microsoft* le enviaba un mensaje automático a la persona indicando que ese correo electrónico no estaba funcionando y requería contactar al administrador. Una de las razones principales que provocó esto fue que la regla de “forwarding” de *Outlook* a *Gmail* por medio de las cuentas “g2o.upr.edu”. Debido a la situación, algunos usuarios alegaron que la institución estaba censurando sus comunicaciones, lo que no es correcto. Al eliminar esta regla en el sistema de control de las cuentas, las personas pudieron recibir nuevamente sus correos. Se le exhorta a la comunidad universitaria a no utilizar esta regla y mantenerse usando *Outlook*, ya sea en la versión web o en la aplicación de preferencia para recibir correos electrónicos.

3. Envío de correos al *SPAM* de las cuentas de estudiantes

Los estudiantes comenzaron a reportar que no les estaban llegando los correos electrónicos de sus profesores. Igualmente, algunos profesores alertaron de la situación. Eventualmente se informó que los correos estaban llegando al *SPAM*. Esto también estaba ocurriendo con correos enviados por servidores en los recintos y unidades. Se detectó la causa y se corrigió.

4. Pérdida de documentos compartidos en *Google Drive* al copiarse a *Microsoft OneDrive*

Los archivos almacenados en *Google Drive* se emularon a *One Drive*, sistema de almacenamiento de *Microsoft*. Sin embargo, por razones de seguridad, los documentos compartidos fueron entregados al usuario que los originó. Estos tendrían que ser compartidos nuevamente. Se recomienda que los documentos nuevos sean creados en las aplicaciones de la plataforma *Microsoft 365*. Aclaremos que las personas podrán continuar usando *Google Drive* como de costumbre.

5. Eventos no relacionados a la migración pero que coincidieron durante las fechas

Se ha reportado *spoofing* o suplantación de identidad en correos electrónicos con contenido político-partidista, y esto fue atendido diligentemente por la administración. Esto se corrigió añadiendo reglas más restrictivas a nivel de nuestra infraestructura de telecomunicaciones y modificaciones a las reglas de *Office 365*. Reiteramos que para implementar todas las herramientas y políticas de seguridad cibernética disponibles es necesario que todas las cuentas se migren a la plataforma *Outlook*.

También se reportó una aparente exposición desautorizada de documentos o datos de los estudiantes o empleados por la migración. Las investigaciones preliminares realizadas indican que los casos reportados en el Sistema de Retiro como en algunas unidades se deben a usuarios que han permitido el acceso público (dentro de la red de la UPR) de documentos en plataformas de *Microsoft Teams* y *SharePoint*. Al momento en que la Administración Central tuvo conocimiento de esas situaciones, se contactó a los usuarios para que cambiaran los privilegios de acceso a esos documentos. Se exhorta a todos los directores y supervisores de oficinas a asegurar que el personal cuente con los adiestramientos correspondientes. La institución continuará orientando y ofreciendo capacitación a la comunidad universitaria.