Proveedores externos de correo electrónico y la Universidad Pablo de Olavide

Apreciado lector, si está leyendo este documento es porque se está encontrando con problemas para acceder a su proveedor de correo electrónico ajeno a la Universidad Pablo de Olavide.

Tal vez usted tenga una cuenta de correo personal *@gmail*, *@hotmail*, *@yahoo* o *@ono.com* (entre otras) y por conveniencia, le gustaría poder acceder a dicha cuenta con el mismo software de correo electrónico habitual (por ejemplo, *Thunderbird* u *Outlook*) con el que accede a su cuenta de correo de la Universidad Pablo de Olavide.

En la Universidad Pablo de Olavide la seguridad de la información es una prioridad. A fin de cuentas, se almacena y gestiona diariamente multitud de información de carácter reservado: calificaciones de asignaturas, datos económicos de trabajadores y matrículas, así como el correo electrónico de todos los integrantes de la Universidad, entre otros muchos activos.

Toda esa información ha de ser protegida contra ataques: accesos no autorizados, corrupción de datos, interceptación/espionaje, virus, troyanos, etc. Esta enorme cantidad de amenazas hace que la Universidad tome una serie de medidas tecnológicas y formativas para proteger a sus sistemas de información y usuarios.

Como organismo público, la Universidad Pablo de Olavide ha de velar por la seguridad de la información y de sus usuarios, cumpliendo y haciendo cumplir una serie de normativas y disposiciones legales como la *Ley Orgánica de Protección de Datos* (LOPD), la *Ley de Servicios de la Sociedad de la Información* (LSSI) o el *Esquema Nacional de Seguridad* (ENS), entre otras.

En base a esta exigencia normativa, en la Universidad Pablo de Olavide se han implantado múltiples medidas de seguridad, dispuestas en capas superpuestas (a modo de coraza), para en lo posible hacer lo más difícil posible que un atacante tenga éxito.

Una de esas medidas de seguridad consiste en impedir el acceso desde la red cableada a servicios de correo electrónico ajenos a la UPO empleando unos protocolos de red denominados *SMTP*, *POP3* e *IMAP*. Estos canales de comunicación son precisamente los que usan programas como *Thunderbird* u *Outlook* para acceder a proveedores de correo electrónico externos como *Yahoo*, *Gmail* o *Hotmail.*

El correo electrónico ha sido uno de los principales vectores de infección durante la última década: *virus*, *gusanos*, *troyanos* y otros tipos de *malware* (software malicioso) usan el correo electrónico como canal de propagación e infección.

El sistema de correo electrónico que da servicio a los dominios de correo *@*upo.es* cuenta con sus propias medidas de seguridad para proteger a nuestros usuarios de todas estas amenazas. A diario, se protege a todos nuestros usuarios de miles de ataques que llegan por correo electrónico, neutralizándolos antes de que lleguen a sus buzones de correo electrónico.

Por desgracia, no todos los proveedores de correo electrónico guardan con tanto celo la integridad de sus usuarios, y es por ello por lo que existe esta política de seguridad que impide el acceso desde la red cableada a proveedores de correo electrónico ajenos a la UPO empleando los protocolos SMTP, IMAP y/o POP3.

Entendemos que esta política puede ser una inconveniencia para algunos usuarios, pero se ha realizado un análisis cuidadoso del balance de coste/beneficio de tomar esta decisión y las ventajas superan a los inconvenientes: la cantidad de incidentes de seguridad se ha reducido y por tanto nuestros usuarios y datos están más seguros.

Por lo general, recomendamos a nuestros usuarios que usen sus cuentas de correo electrónico *@*upo.es* para todo lo relacionado con su actividad laboral, tanto académica como de gestión, y que use estos proveedores ajenos para sus cuestiones personales.

Si aún así usted tiene necesidad de acceder a estos servicios de correo electrónico y esta política restrictiva es inconveniente, hay varias alternativas:

- Acceder a estos servicios externos empleando la red *Eduroam*, que es una red inalámbrica aislada de la red cableada de la UPO.
- Usar un dispositivo móvil (como un *smartphone*) que conecta a Internet usando una conexión de datos tipo 3G o 4G.
- Usar un acceso web al correo (webmail) para acceder a su cuenta personal. En este caso, asegúrese que la conexión es cifrada (https).

Recuerde: la seguridad de la información en la Universidad Pablo de Olavide es responsabilidad de todos sus integrantes, PAS, PDI y alumnos no algo exclusivo del CIC[1].

1 Resolución rectoral disponible en https://www.upo.es/portal/impe/web/contenido/05039f80-eede-11e2-9bc8-3fe5a96f4a88?channel=a3645af1-2f47-11de-b088-3fe5a96f4a88