Universidad de Puerto Rico
Oficina de Sistemas de Información
UPR Administración Central

Guía para Viajes Internacionales

Introducción

Los viajes internacionales pueden representar riesgos significativos para la información almacenada o accesible a través de computadoras, tabletas, teléfonos o cualquier otro dispositivo electrónico con los que accedemos servicios institucionales o personales. Parte del riesgo está asociado con las posibilidades de pérdida o robo, pero además nuestros dispositivos están en riesgo al utilizar redes que pueden ser administradas por entidades que monitorean y capturan el tráfico de la red con fines competitivos o maliciosos.

A tales efectos, la Universidad de Puerto Rico, en su objetivo de mantener un ambiente seguro en sus sistemas de información, define la siguiente guía para los miembros de la comunidad universitaria que viajan fuera del territorio de Estados Unidos y requieren acceso a los servicios electrónicos de la Universidad desde el extranjero.

Guía General para los Viajes Internacionales

1. Los viajeros internacionales deben limitar la cantidad de información confidencial almacenada o accesible en cualquier dispositivo móvil que se lleve durante el viaje, y evitar el contacto con la red de la Universidad en general, específicamente cuando viajan a países de alto riesgo (U.S. State Department's Alerts and Warnings). Si el viaje, por razones de trabajo requiere acceso a los sistemas de la universidad, es sumamente importante que se estudie cuidadosamente todo lo que se presenta en este documento.
2. Limite la cantidad de información confidencial que lleva en su viaje. La eliminación de datos confidenciales innecesarios de cualquier dispositivo reduce el riesgo de exposición para cualquier persona que obtenga acceso a la información.
3. Visite y siga las recomendaciones que se indican en el portal de itsecurity.upr.edu. Comprender y seguir estas prácticas lo ayudará a reducir el riesgo en sus viajes.
4. Revise de antemano las restricciones que los países imponen sobre dispositivos y/o software transportado para reducir la probabilidad de que sean confiscados o que su viaje se interrumpa. Estados Unidos restringe el transporte de ciertos tipos de dispositivos y software a países específicos (denominados "*export controls*"). Muchas otras naciones restringen el transporte de ciertos tipos de dispositivos o software a su país (denominados "*import controls*").

5. No utilice dispositivos públicos o de otras personas. Cuando usa una estación de trabajo que no está bajo su control, pudiera estar comprometida su seguridad y cualquier cosa que ingrese en el sistema (identificaciones, contraseñas, datos) puede capturarse. Limite su actividad desde sus propios dispositivos.
6. Identificaciones, contraseñas o información confidencial se puede ver comprometida simplemente al ver a la persona ingresar la información. Sea discreto al ingresar credenciales.
7. La mayoría de los casos en que los dispositivos móviles se pierden o son robados ocurren en las áreas donde las distracciones son mayores. Reconocer las situaciones de distracción y, cuando ocurren, prestar especial atención para mantener la concentración puede evitar que tenga que tomar las medidas necesarias para desactivar esos dispositivos o tomar otras acciones en caso de pérdidas.
8. En caso de pérdida o robo de una computadora portátil o dispositivo móvil, comuníquese con la Oficina de Sistemas de Información de su unidad para recomendaciones y acciones de prevención.

Recomendaciones al regresar de viajes internacionales

1. Al regresar de viajes internacionales, las contraseñas que haya utilizado durante el viaje deben ser cambiadas desde un dispositivo confiable. Cuando se viaja, especialmente en países de alto riesgo, la probabilidad de que sus credenciales hayan sido capturados es mayor. Cambiar rápidamente una contraseña comprometida ayuda a prevenir futuros ataques a esa cuenta.
2. Cuando los dispositivos se conectan a una red en un país de alto riesgo, existe una mayor probabilidad de que el dispositivo esté comprometido y tenga instalado software malicioso. Este software puede comprometer la información y otros dispositivos en la red cuando este se vuelve a conectar a la red de la Universidad. Ante dichas circunstancias, es altamente recomendable una reinstalación y limpieza el disco duro y otros componentes que almacenan datos y software para cualquier dispositivo que se haya usado durante el viaje.

Acceso a Servicios Institucionales Desde el Extranjero

Los sistemas de colaboración y mensajería institucionales, así como los sistemas de información administrativos y de educación a distancia requieren protecciones especiales para minimizar los riesgos de seguridad. Ante las circunstancias de un incremento en los incidentes de ciberseguridad a nivel mundial, se hace indispensable contar con mecanismos de prevención que en ocasiones requieren el control de acceso desde el extranjero.

- **Sistema de Colaboración y Mensajería – M365/Outlook**

  Los sistemas de colaboración y mensajería basados en la plataforma de Office 365 verifica de forma automática los lugares desde donde cada usuario intenta hacer una

conexión. Es muy saludable visitar la página https://mysignins.microsoft.com regularmente para verificar que los accesos a su cuenta son los correctos.
Aunque el acceso al correo electrónico y los recursos de M365 cuentan con el requisito de *Multifactor Authentication*, el acceso fuera de Puerto Rico y Estados Unidos está controlado. Esto significa, que en caso de que un usuario de la comunidad universitaria requiera el acceso desde el extranjero, deberá notificar a la Oficina de Sistemas de Información de su unidad para que se haga el arreglo correspondiente durante el período del viaje.

Las medidas de control se evaluarán caso a caso basado en el destino y el tipo de acceso que se requiera. Existen países que, por su clasificación por el Departamento de Estado de los Estados Unidos, no se permite acceso en ninguna circunstancia.

Cabe señalar que es importante considerar que aquellos que optan por el uso de MFA mediante mensajes de texto a su dispositivo móvil, puede aplicar cargos adicionales de su proveedor de servicio. Es por esto por lo que recomendamos el uso del *Microsoft Authenticator* (disponible para iOS y Android) el cual utiliza notificaciones a la aplicación y no utiliza ni consume servicio de mensajes de texto de su teléfono.

- **Plataforma de Gestión de Aprendizaje – Moodle Institucional**

  La Plataforma de Gestión de Aprendizaje Institucional basada en Moodle (online.upr.edu) tiene restricciones de acceso desde el extranjero bajo condiciones normales de conectividad. Esto significa que, para poder acceder a esta plataforma desde fuera de Puerto Rico y Estados Unidos, es necesario coordinar una conexión segura, en particular mediante *Virtual Private Network* (VPN) provisto por la Universidad.

  En caso de existir la necesidad de que un usuario de esta plataforma requiera acceso desde el extranjero, deberá notificar a la Oficina de Sistemas de Información de su Unidad para que le provean el acceso via VPN y las instrucciones para conectarse.

- **Acceso mediante *Virtual Private Network* (VPN) Institucional para otros Servicios**

  Cualquier usuario puede acceder los recursos electrónicos de la Universidad mediante el servicio de *Virtual Private Network* (VPN) provisto por la universidad. Este servicio requiere la instalación de un programa cliente en el dispositivo y unas credenciales provistas por la institución para lograr el acceso. Las Oficinas de Sistemas de Información de todas las unidades pueden proveer este servicio.

  El uso de VPN no garantiza que sus credenciales puedan ser interceptadas y utilizadas para lograr acceso a los recursos institucionales. Por tal razón, el uso de VPN para acceder los servicios institucionales deberá limitarse a situaciones excepcionales.

Además, una vez concluido el viaje se procederá eliminar el acceso via VPN y/o cambiar las credenciales de acceso al servicio.

Por otra parte, el uso de VPN personales (no institucionales) que permiten hacerse pasar como si la conexión se genera desde Estados Unidos, aunque se encuentre en el extranjero, tiene un alto potencial de riesgo y en la mayoría de las ocasiones es detectado por las mismas plataformas que se desea acceder evitando que así se logre.

Referencias Recomendadas

1. The FBI's Travel Tips brochure
   https://www.fbi.gov/file-repository/business-travel-508.pdf/view
2. FCC Cybersecurity Tips for International Travelers
   https://www.fcc.gov/consumers/guides/cybersecurity-tips-international-travelers