Universidad de Puerto Rico
Oficina de Sistemas de Información
Administración Central

Normativa Sobre el Uso de Dispositivos Personales en el Ambiente Laboral (*Bring Your Own Device* – BYOD)

Revisado y aprobado por el Comité Institucional de Seguridad en los Sistemas de Información
Abril 2024

Introducción

La Universidad de Puerto Rico (UPR) reconoce que el uso de dispositivos personales en el ámbito laboral, conocido como la práctica "*Bring Your Own Device*" (BYOD) ofrece numerosos beneficios, tales como mayor flexibilidad en el uso de tecnologías para fines educativos y administrativos. Es crucial reconocer que esta libertad conlleva una gran responsabilidad por parte del usuario. Incluso cuando se trata de dispositivos personales, su uso en el contexto universitario debe adherirse a la *Política Institucional sobre el Uso y Acceso a los Recursos de la Tecnología de la Información en la Universidad de Puerto Rico* [1]. Esto implica una conciencia y diligencia constante para garantizar que la seguridad, la privacidad y la integridad de los datos y recursos institucionales se mantengan en todo momento. Los usuarios deben comprender y aceptar que, al integrar sus dispositivos personales en el entorno académico y administrativo de la universidad, se comprometen a seguir las directrices establecidas, asegurando que su uso esté alineado con los estándares de seguridad y ética dictados por la institución.

Esta normativa aplica a todo usuario de la Universidad de Puerto Rico que utilice el concepto de BYOD.

Definiciones

BYOD (*Bring Your Own Device*) – Se refiere a una normativa en la que instituciones permiten o fomentan a sus empleados utilizar sus propios dispositivos electrónicos para realizar actividades laborales conectados a la red institucional.

Dispositivos – Equipo tales como teléfonos inteligentes, tabletas, computadoras portátiles o equipo de comunicaciones que se conectan a la red institucional para acceder los servicios y recursos electrónicos.

VPN (*Virtual Private Network*) – Tecnología que permite establecer una conexión segura y cifrada a través de una red pública, garantizando la privacidad y seguridad de la información transmitida como si estuviera conectado directamente a la institución.

[1] https://www.upr.edu/itdocs/wp-content/uploads/sites/126/2023/02/9429_Pol_Inst_Uso_Acceso_Recs_Tec-1.pdf

Normativa

Cada miembro del personal es responsable de asegurar su dispositivo personal:

1. Utilizar contraseñas fuertes y únicas para todos los dispositivos y servicios. Las contraseñas deben incluir una combinación de letras mayúsculas y minúsculas, números y símbolos, y cambiarlas regularmente en los dispositivos personales.
2. Donde sea posible, activar la autenticación multifactor (MFA) para añadir una capa adicional de seguridad al acceder a aplicaciones y servicios tanto personales como institucionales.
3. El personal debe ejercer precaución al acceder a recursos institucionales administrativos, académicos o de investigación protegidos desde redes públicas o inseguras. Estos accesos deben ser hechos prefiriendo siempre conexiones protegidas como VPNs.
4. Asegurar instalar regularmente las actualizaciones de software y sistema operativo.
5. No instalar software de fuentes no confiables. Se sugiere que las aplicaciones y programas sean descargados solo de tiendas oficiales o sitios web de confianza.
6. El dispositivo personal debe tener instalado y actualizado un software antivirus confiable.
7. Se debe evitar almacenar datos institucionales en dispositivos personales. De ser esto necesario, se utilizará herramientas de cifrado de dispositivos de almacenamiento y archivos, según establece la *Guía para el Manejo de los Datos de la Universidad de Puerto Rico* [2].
8. El intercambio de información y la colaboración se realizará a través de aplicaciones y servicios oficiales institucionales que cumplan con las políticas de seguridad y privacidad de la universidad. Es vital verificar con las respectivas Oficinas de Sistemas de Información antes de usar servicios de terceros no oficialmente aprobados para compartir información privada o restricta.
9. Puede que el acceso a ciertos recursos institucionales desde dispositivos personales requiera de alguna aplicación y/o autorización adicional (ej. cliente de VPN). Es recomendable consultar con las respectivas Oficinas de Sistemas de Información para obtener orientación específica.

En el marco de esta normativa de "*Bring Your Own Device*" (BYOD) adoptada por la Universidad de Puerto Rico, es importante destacar que, aunque es permitido el uso de dispositivos personales para fines educativos, administrativos y/o investigativos, la responsabilidad de mantener y configurar estos dispositivos recae completamente en el usuario. El personal técnico de la institución no está obligado a proporcionar apoyo en cuanto a configuraciones, instalaciones de software, actualizaciones, o cualquier otro tipo de asistencia técnica relacionada con dispositivos personales. Esto incluye, pero no se limita a, la instalación de aplicaciones específicas, la gestión de problemas de seguridad como virus o malware, y la configuración de redes.

Los usuarios deben comprender que, al utilizar sus dispositivos personales con propósitos institucionales, asumen la total responsabilidad de asegurar que estos cumplan con todas las normativas y políticas establecidas por la Universidad de Puerto Rico.

La Universidad, a través del personal técnico se reserva expresamente el derecho de restringir o prohibir el uso de cualquier dispositivo personal que se identifique como no conforme con las políticas y normativas establecidas. Además, la Universidad se reserva el derecho de desconectar o aislar cualquier dispositivo personal del acceso a la red y recursos institucionales si se considera que representa una amenaza para la seguridad de la información y los sistemas de la Universidad.

[2] https://www.upr.edu/itdocs/wp-content/uploads/sites/126/2024/03/Clasificacion-de-los-Datos-Guia.pdf

Adicionalmente, es importante subrayar que la Universidad de Puerto Rico no asume responsabilidad alguna por daños que puedan ocurrir en los equipos personales de los usuarios ni por la pérdida o compromiso de información personal almacenada en dichos dispositivos como resultado de su uso en el entorno universitario. El uso de dispositivos personales bajo la política de "*Bring Your Own Device*" (BYOD) se realiza bajo el entendimiento de que la protección y el mantenimiento del equipo son responsabilidad exclusiva del usuario.

Si un equipo utilizado bajo el concepto de BYOD es robado, perdido o comprometido, es responsabilidad del usuario reportar a la Oficina de Sistemas de Información de su Unidad inmediatamente. Esta determinará los pasos a seguir para minimizar los riesgos asociados a este tipo de incidente.

Al aceptar utilizar sus dispositivos personales dentro del marco de la normativa de BYOD, los usuarios reconocen y aceptan estas condiciones, comprometiéndose a colaborar en todo momento con las iniciativas de seguridad y cumplimiento de la Universidad. Se espera que todos los usuarios comprendan y respeten estas disposiciones, actuando siempre con responsabilidad y diligencia en el uso de sus dispositivos personales dentro del contexto universitario. La cooperación y el compromiso de cada miembro de la comunidad universitaria son fundamentales para mantener un entorno digital seguro y eficiente.