(4)d. Lista de aplicaciones obligatorias: navegador, gestor de email, mensajería instantánea, antimalware, firewall personal, etc.

Para el correcto funcionamiento de dispositivos externos en la universidad, estos deberán de tener un mínimo de software y obligatoriamente conexión a internet que no obstaculice la fluidez tanto de las clases como de la administración.

**(4.1) Ordenadores o similares:**

Será obligatorio tanto para el PDI como para el PAS tener esta serie de aplicaciones, o que permitan sus mismas funciones; ya sea instaladas o en la nube (en este caso deberán asegurar el constante acceso a la red):

* Reproductor multimedia
* Lector y editor de archivos de texto (incluyendo PDFs, al menos lectura)
* Hoja de cálculo
* Gestor de emails
* Mensajería instantánea
* Navegador de internet
* Aplicación de videoconferencia/llamadas
* Antivirus/Antimalware (será suficiente el preinstalado en el S.O)
* Firewall (será suficiente el preinstalado en el S.O)

(4.1.1) Aplicaciones regidas:

Además de las dichas anteriormente que serán comunes para cualquier rol de la universidad, cada rol deberá instalarse aquellas aplicaciones que sean exigidas por su superior, es decir, los estudiantes aquellas dichas por sus profesores, y el personal de la universidad por su jefe.

(4.1.2) Aplicaciones en la nube:

En caso de que el alumno no deseé instalar las aplicaciones en su dispositivo, tendrá la opción de utilizar myApps u Office365 online version, no obstante, si la susodicha aplicación no se encuentra en ninguna de estas dos si se verá obligado a instalársela como bien dice en el apartado 4.1.1.

**(4.2) Dispositivos móviles:**

A no ser que el dispositivo móvil no sea lo suficiente potente como para cargar las respectivas aplicaciones, tanto los PDI como PAS deberán tener instalado en su smartphone:

* Gestor de emails
* Mensajería instantánea

Además de la correspondiente aplicación de teléfono inteligente diseñada para su rol (si es que existe) como puede ser la app “URJC”.

**(4.3) Otros dispositivos:**

Cualquier otro dispositivo que lleve el sujeto como apoyo a la hora de realizar su trabajo no exigirá ningún tipo de software.

(5)e. List of aplicaciones y practices prohibidas (por ejemplo, jailbreak o root)

Antes de entrar en términos concretos aclarar que cualquier aplicación descargada de manera ilegal queda completamente prohibida, ya que cualquier aplicación/tarea que sea exigida en la universidad deberá poder realizarse de manera totalmente legal.

**(5.1) Jailbreak/Root:**

Realizar Jailbreak en un dispositivo iOS o rootear cualquier otro sistema operativo ya sea Windows, Linux o Android puede resultar muy provechoso si se trata de un usuario con un conocimiento avanzado; no obstante, también es una práctica que puede llegar a ser peligrosa y dañina si se hace de manera descuidada.

(5.1.1) PDI:

(5.1.1.1) Estudiantes:

Exceptuando un ambiente controlado y seguro como puede ser una máquina virtual o una práctica supervisada por el profesor, la universidad desaconseja el uso de este recurso y se desvincula de cualquier daño al dispositivo que se pueda producir por ponerlo en marcha. Si llegará a afectar como daño colateral a la cuenta de URJC (y relacionados) del alumno la universidad no se haría cargo y cabe la posibilidad de que no tome acción en ello.

Sin embargo, si el daño ocurre en un ambiente controlado la universidad intentará hacer lo posible para que esto no afecte a su cuenta URJC (y relacionados) o en caso de que el daño ya se haya realizado repararlo en la medida de lo posible.

(5.1.1.2) Personal docente e investigador:

Si un profesor o investigador realiza esta práctica en dispositivos relacionados con la universidad se considera que lo hace bajo su responsabilidad y con total conocimiento. En caso de producirse alguna falla y que esta afecte a la URJC, la universidad podrá a llegar a tomar ciertas represalias sobre el individuo dependiendo de la magnitud; desde leves sanciones hasta el despido y cargas penales.

(5.1.1.3) PAS:

A no ser que el uso de esta práctica sea razonado, totalmente necesario y aprobado por un superior, queda totalmente prohibida en dispositivos relacionados con la universidad. Llevando su uso sin justificación al despido inmediato del sujeto haya llegado o no a producir algún daño que afecte a la URJC; evitando así con esta prematura acción, cualquier objetivo vulnerable que pudiera poner en riesgo a la integridad de la universidad.

**(5.2) Lista de aplicaciones prohibidas:**

Estas restricciones solo son aplicables al PAS, ya que una brecha en sus dispositivos supondría mayor peligro además de que la universidad les proporciona portátiles, por lo tanto, no sería necesario la política BYOD; si aun así desean trabajar con sus propios dispositivos deberán de seguir estas restricciones:

Aplicaciones restringidas (debido a su dudosa seguridad o brechas anteriores):

Angry Birds

Dropbox

Facebook

Whatsapp

Twitter

Skype

Onedrive

Outlook

Netflix

Google Drive

Pokemon Go

Youtube

Cydia

Viber

Soduku

Powerpoint

Line

Pandora

SugarSync

CamScanner

Winzip

CamCard

OPlayer

WeChat

Mobile Ticket

PDF Reader

(6) Lista de app stores permitidas.

Para el PDI este apartado serán meras recomendaciones, no obstante, recomendamos su lectura, puesto que si llegará a ocurrir cualquier daño por no seguirlas quedaría bajo la total responsabilidad del individuo siendo posible que la universidad no tomará cartas en el asunto cuando se viera afectada la cuenta URJC (y relacionados) del sujeto.

Mientras que el PAS deberá cumplir las restricciones del 6.1

**(6.1) Dispositivos Andriod/iOS**

Aunque las markets oficiales de Android (Play Store) y iOS (App Store) no son totalmente seguras, cuentan con un porcentaje de malware menor al 3%, siendo la forma más fiable de descargar aplicaciones. Por tanto, excluyendo a las aplicaciones no permitidas del (5) estaría permitido descargar cualquier aplicación de la Play Store/App Store siendo también las únicas apps stores permitidas.

**(6.2) Ordenadores o similares:**

En estos dispositivos no habrá ninguna restricción mayor a las del apartado (5); sin embargo, desde la universidad recomendamos la descarga de aplicaciones desde app store conocidas y fiables que cierto que, aunque no son 100% seguras nos otorgan cierta confianza como puede ser Microsoft Store o aplicaciones fiables como las de Adobe o las de Google, obviamente desde su página oficial.