Uso de certificados UC en dispositivos móviles

El uso de dispositivos móviles para almacenar certificados digitales de identidad de cargos y empleados públicos de la Universidad ofrece comodidad, pero también **presenta importantes riesgos de seguridad**. Es crucial identificar estos riesgos y establecer medidas que protejan tanto a los usuarios como a la institución.

Los siguientes serían los riesgos más importantes que pueden comprometer el certificado:

- Pérdida o robo del dispositivo.
- Falta de control sobre aplicaciones instaladas.
- Mayor exposición a ataques de phishing e ingeniería social: Las limitaciones de tamaño de pantalla y usabilidad pueden dificultar la detección de intentos de phishing.
- Uso no restringido del certificado: Una vez importado, el certificado puede ser utilizado sin restricciones, aumentando el riesgo de uso indebido.

Actualmente la Universidad no hace ninguna gestión sobre el parque de móviles corporativos, más allá de la entrega y control de los aspectos propios de las comunicaciones de voz y datos.

Por tanto, los dispositivos móviles corporativos son equivalentes a un dispositivo personal, en el que **toda la responsabilidad sobre su configuración y uso recae en el propio usuario, que asume el importante riesgo personal que supone cargar su certificado en un dispositivo móvil.**

Por ello, de ser necesario usar certificados de cargos o de empleado público desde un dispositivo móvil, se proponen las siguientes **medidas de seguridad**:

- Los dispositivos deberán estar soportados por el fabricante, con actualizaciones de seguridad mensuales.
- El usuario será responsable de revisar mensualmente las actualizaciones del sistema y semanalmente las actualizaciones de aplicaciones.
- Activar el bloqueo automático tras apagarse la pantalla.
- Usar un pin de 6 dígitos o una contraseña alfanumérica, y para facilitar el uso, activar las opciones de biometría (huella/FaceID). El desbloqueo con cámara en Android no es muy seguro.
- Limitar las notificaciones que se muestran con la pantalla bloqueada, de forma que no se muestre su contenido hasta desbloquear.
- No instalar aplicaciones fuera de las tiendas oficiales de Google o Apple. No activar características especiales como la depuración usb.
- Si se instalan aplicaciones, verificar puntuación y número de descargas. Cuidado con los clones de aplicaciones conocidas y los enlaces patrocinados.
- Evitar conectarse a redes WiFi públicas no seguras. Usar una VPN de ser necesario, aunque el uso de la VPN UC sólo protege el tráfico contra los servidores de la universidad.
- Evitar si es posible los puntos de carga públicos, usar siempre nuestro cargador.

Proceso de importación de certificados

El proceso de importación y uso de certificados en dispositivos móviles Android o iOS es similar, es necesario transferir la copia de seguridad del certificado al dispositivo (por correo electrónico o un servicio de nube que tengamos configurado) e importarlo.

En el caso de Android, los certificados se gestionan desde Ajustes → Seguridad → Certificados de usuario. La ubicación exacta de este menú varía entre cada modelo de teléfono.

En ese menú veremos los certificados importados y los podremos eliminar.

En el caso de iOS, al importar un certificado, tenemos que confirmar con nuestra contraseña su carga. Para ello, tras importarlo, tenemos que ir a Configuración > General > VPN y gestión de dispositivos, y en el apartado Perfiles confirmar la importación.

En ambos sistemas operativos, no hay forma de pedir una contraseña antes de usar los certificados importados, por lo que tenemos que asegurar que los teléfonos tienen activada una opción de desbloqueo seguro, con una contraseña compleja y desbloqueo con biometría para facilitar su uso (huella o touchid/faceid).

Este requisito es imprescindible.