Los Dispositivos Móviles

Existen muchos tipos de dispositivos móviles. Hasta hace poco, en las empresas se utilizaban los **ordenadores portátiles**, pero actualmente, casi la totalidad de los empleados hacen uso de ***smartphones***, ya sea para uso personal o corporativo, y también existe una tendencia creciente en el uso de las **tablet**.

Los riesgos más habituales de los dispositivos móviles son la pérdida, el robo y la rotura, destrucción o avería. Sin embargo, aunque en muchos casos esta tecnología tiene un coste elevado, el mayor problema que se deriva de estos incidentes no es la pérdida económica directa, sino la **pérdida o robo de información**.

Para evitar estos riesgos debemos implantar diversas medidas de seguridad que se describen a continuación.

1. Cifrado

Habitualmente, los dispositivos móviles se utilizan fuera de las dependencias de nuestra organización.

Por este motivo, debemos cifrar la información almacenada en estos soportes. Así conseguiremos reducir el impacto que podría ocasionar la pérdida o robo de un dispositivo móvil. Por ejemplo, la pérdida de un ordenador portátil o el robo de un smartphone corporativo.

Existen múltiples herramientas para el cifrado de información, y la mayor parte de fabricantes de herramientas de seguridad tienen aplicaciones para ello. Además, muchas aplicaciones de compresión y ofimáticas disponen de funcionalidades específicas para el cifrado, que pueden resultar útiles para el intercambio de información entre dos partes y suficientes en la mayoría de los casos.

2. BYOD

El BYOD, llamado así por sus siglas en inglés *Bring Your Own Device*, es una tendencia que se basa en que los empleados hacen uso de sus dispositivos personales en el entorno de trabajo.

Esto permite al empleado hacer uso de un dispositivo que está adaptado a sus necesidades y por tanto deriva en una mayor productividad, y a la empresa le supone un ahorro de costes y una mayor productividad de la persona.

Por ejemplo, cada vez es más habitual que los empleados puedan acceder a su correo o agenda corporativa desde su *smartphone* personal, o incluso gestionar información corporativa desde portátiles personales.

Sin embargo, este tipo de prácticas BYOD tienen importantes implicaciones desde el punto de vista de la seguridad de la información, dado que aunque el dispositivo que utilicemos esté personalizado según nuestras preferencias, esto no necesariamente significa que tenga las necesarias medidas de seguridad. Por tanto, debemos poner en marcha e instalar diferentes medidas de seguridad en los dispositivos personales, que permitan sacar el máximo partido al BYOD de una forma siempre segura.

Por lo tanto, siempre que deseemos hacer uso de un dispositivo personal para almacenar o acceder a información corporativa, debemos considerar todos los requisitos de seguridad que aplicaríamos a cualquier equipo corporativo para esa tarea: utilización de cifrado, contraseñas robustas, acceso por clave, uso de herramientas de conexión remota a nuestras oficinas (VPN), etc.

En algunos casos puede ser necesario incluso implantar medidas de seguridad adicionales, dado que en muchas ocasiones estos dispositivos son gestionados por otras personas (pareja, hijos) o se utilizan a menudo fuera de las instalaciones de la empresa (por ejemplo, un móvil personal).

3. Conexiones a redes WiFi públicas

Es frecuente hacer uso de las redes WiFi públicas cuando nos encontramos en lugares públicos, como aeropuertos, cafeterías, tiendas, restaurantes o bibliotecas. Por lo general, lo hacemos para evitar el coste de la conexión 3G o por velocidad, si no tenemos suficiente cobertura de datos.

Sin embargo, las redes WiFi públicas presentan diferentes riesgos, siendo el principal no saber quién controla la WiFi. Esto no significa que el dueño de un local tenga malas intenciones, sino que un usuario malintencionado puede atacar la red y hacerse con su control si ésta no tiene las medidas de seguridad adecuadas, sin que el propietario del local (y proveedor de la conexión) lo sepa.

Si eso sucede, es posible que nuestros datos sean interceptados por algún ciberdelincuente, capturando toda la información que transmitimos. Por ejemplo, sería posible que éste obtuviera el usuario y contraseña que usamos para acceder a la red de nuestra empresa o incluso las claves para gestionar nuestras cuentas bancarias online.

No es recomendable hacer uso de este tipo de redes si vamos a manejar información sensible o confidencial, acceder a nuestras cuentas bancarias, acceder a la red de nuestra empresa o similares. Debemos utilizarlas únicamente en un contexto lúdico (leer noticias, ver contenido multimedia, etc.), sin olvidar no obstante que en los smartphones, muchas aplicaciones como las redes sociales o el correo electrónico realizan tareas de sincronización sin que el usuario sea consciente de ello.

Por tanto, si necesitamos conectividad fuera de nuestras oficinas, debemos buscar alternativas de conexión, como por ejemplo los «pinchos USB» de los operadores de telefonía cuando hagamos uso de portátiles, las conexiones 3G cuando usemos *smartphones* y *tablets* o herramientas de conexión segura a nuestra empresa.

4. Configuraciones de seguridad vs por defecto

Por norma general, las configuraciones de seguridad por defecto de los dispositivos móviles no tienen activadas todas las medidas de seguridad que ofrece el sistema, ya que éstas pueden introducir demasiada complejidad para algunos usuarios básicos.

Sin embargo, cuando se trata de dispositivos que vamos a utilizar en el entorno corporativo, ya sea BYOD o dispositivos de la empresa, es imperativo que apliquemos a cualquier tipo de dispositivo las necesarias medidas de seguridad.

Entre las principales medidas que podemos destacar están las siguientes:

Entre las funcionalidades extras de seguridad que podemos usar, cabe señalar las siguientes:

- Cifrado de los soportes de almacenamiento.
- Contraseña de acceso al sistema.
- Funcionalidad que permita restablecer la configuración por defecto del dispositivo vía remota (también llamado *wipe* remoto).
- Copias de seguridad periódicas.

Adicionalmente, aquellos dispositivos que disponen de un modo administrador pueden llevar configuradas contraseñas de acceso genéricas, como *admin* o 1234. Esta información es pública y es explotada por delincuentes

Por tanto es necesario que antes de utilizar el equipo para el acceso al entorno corporativo, le apliquemos las principales medidas de seguridad, de modo que ante una pérdida del dispositivo o robo, el impacto sea mínimo.

5. Geoposicionamiento

Llamamos geoposicionamiento a la capacidad de algunos dispositivos de ubicarse geográficamente. Esta funcionalidad es utilizada por ejemplo por los GPS para guiar al usuario en su trayecto.

Sin embargo, la información de geoposicionamiento también es utilizada por otros servicios y aplicaciones. Por ejemplo, en diversas redes sociales existe la posibilidad de que autoricemos a la red a posicionarnos, y las aplicaciones para capturar y editar imágenes también guardan información sobre la ubicación en la que se ha la foto.

El principal riesgo asociado a estos datos de localización es que estamos recabando, almacenando y quizás, difundiendo, más información de la necesaria. Esto ocurre en la mayor parte de los casos de forma involuntaria.

Dado que la mayor parte de los dispositivos móviles permiten habilitar y deshabilitar las funciones de geoposicionamiento, según las preferencias y necesidades del usuario, se recomienda deshabilitar esta funcionalidad siempre que no sea estrictamente necesario.