UF1. Seguridad en dispositivos móviles y IoT

Índice

Introducción

El aspecto esencial de la gestión de los soportes es asignar recursos adecuados a los usuarios autorizados.

El correcto dimensionamiento requiere que la Gestión de los soportes disponga de información fiable sobre los márgenes de seguridad y disponibilidad. Por este motivo se repasaran los siguientes puntos:

1. Implementación de funcionamiento seguro de dispositivos móviles e IOT
2. Arquitectura de los dispositivos móviles
3. Sistemas operativos móviles: instalación y configuración
4. Aseguramiento de los servicios a los dispositivos móviles
5. Arquitectura de los dispositivos IOT
6. Sistemas operativos de IOT: instalación y configuración
7. Aseguramiento de los servicios de IOT
8. Puesta en servicio y recuperación del funcionamiento de los dispositivos

Implementación de funcionamiento seguro de dispositivos

Con la aparición de teléfonos inteligentes, tabletas y discos en la nube la naturaleza de los soportes ha cambiado muchísimo[1].

Este cambio reclama de sistemas que gestionen los dispositivos móviles (MDM del inglés *Mobile Device Manager*) e IOT.

- En el siguiente vídeo se presenta el funcionamiento que un MDM ofrecería a la entidad y como el gestor revisaría sus capacidades: control-soportes-meraki.
- Los MDM localizan los dispositivos y permiten disponer de un inventario actualizado (el gestor debería incorporar estos datos secundarios como datos personales a proteger)

Otro tipo de soportes que se deben considerar son los adjuntos de los correos y los ficheros que se envíen por la red.

- En el siguiente vídeo se muestra un ejemplo común, dónde un correo de servidor corporativo prohíbe el envío de ficheros adjuntos con ciertas características: control-correo-corporativo.
- El anterior caso nos presenta la necesidad de identificar, si los usuarios autorizados se instalan aplicaciones no autorizadas para poder acceder a la información cuando se encuentren fuera de un centro de tratamiento, como ejemplo observar el vídeo: control-shadow-it.

1 Antes eran unidades de disco tipo CD, DVD, USB, SD.

Sistemas operativos móviles: instalación y configuración

Para practicar en la gestión de soportes se deben verificar medidas de seguridad, que permiten disponer de configuraciones configuraciones para:

- Evitar la instalación de aplicaciones indebidas
- Evitar la compra de aplicaciones sin consentimiento
- Crear usuarios con aplicaciones pre-asignadas
- Deshabilitar la camera fotográfica

También se debe conocer el protocolo de baja de los soportes. Si la respuesta fuera:

- Cuando los usuarios dejan de utilizar su portátil, móvil, *tablet* o *pendrive*; se lo entregan al departamento informático.
- En el departamento informático se reinstala el sistema de fábrica y se pone a disposición del nuevo usuario autorizado que lo necesite. En el caso de los pendrive se formatean.

Aseguramiento de los servicios a los dispositivos móviles

Así mismo, se debería verificar el cifrado realizado en los soportes, para garantizar un control de acceso seguro.

- En el siguiente vídeo se presenta una de las tecnologías de cifrado más usadas en equipos portátiles Windows (en el informe de auditoría se debería valorar si esta medida existe y si garantiza la calidad del tratamiento): control-bitlocker
- El último vídeo presenta como también los teléfonos inteligentes y *tablets* se deberían cifrar (se muestra el ejemplo con un dispositivo Android): control-cifrado-android
- Por último se podrían solicitar alternativas más seguras. En el siguiente video se presentan algunos dispositivos que llevan el cifrado integrado: control-ironkey. Estos permiten evitar que el usuario se despreocupe de realizar una tarea previa de instalar algún software para descifrar.

En la gestión de los soportes, la gestión de la ciberseguridad debe verificar la existencia de las autorizaciones emitidas por la persona habilitada como responsable para permitir la salida de soportes y documentos que contengan datos personales, incluso cuando dicha salida se efectúa mediante incorporación de los datos en un correo electrónico o como adjunto en el mismo.

La Organización debe:

1. Elaborar o disponer de los correspondientes documentos de autorización para habilitar a las personas que corresponda para permitir la salida de soportes y documentos que contengan datos personales, incluso cuando dicha salida se efectúe mediante incorporación de los datos en un correo electrónico o como adjunto en el mismo.
2. Incluir en el documento de seguridad el listado de los usuarios autorizados para poder llevar a cabo la salida de soportes y documentos que contengan datos personales mediante incorporación de los datos en un correo electrónico o como adjunto en el mismo.

Uno de los aspectos más descuidados son la identificación de los ficheros temporales que se generan por parte de las aplicaciones de tratamiento. Se pueden clasificar en dos categorías:

Contenido temporal generado por el tratamiento:

1. Archivos temporales de: *cachés* de actividades, historiales, *cookies*, *dumps* de memoria, archivos abiertos recientemente, etc.
2. Deberían quedar protegidos para estar disponibles por el propio usuario y si fuera necesario el administrador.

3. Existen herramientas que permiten automatizar su eliminación.

Contenido temporal generado por el usuario:

1. Archivos temporales creados para disponer de ellos durante una visita, compartir con un colaborador, etc.
2. Deberían quedar protegidos con unos derechos digitales que permitan incluir fecha de caducidad en el tratamiento y controlar acceso des de fuera de los sistemas de información conocidos por el responsable.
3. Existen tecnologías que permiten aplicar derechos digitales predeterminados a la documentación ofimática (Word, Pdf, etc.)

En el siguiente ejemplo se muestra como un editor de textos crea ficheros temporales para disponer de una copia de seguridad de las versiones anteriores. Se observará si dicho fichero de versión anterior dispone de las mismas medidas de seguridad.

Como ejemplo observar el vídeo: control-temporales

La última reflexión introduce ¿Como cumplir con las medidas de seguridad cuando los ficheros se almacenan en un soporte y por consiguiente salen del sistema de información y las medidas de seguridad que en él se aplican? -.

Para ello se utilizan las medidas de derechos digitales que actualmente soportan los documentos ofimáticos más comunes.

Puesta en servicio y recuperación del funcionamiento de los dispositivos

En numerosas intervenciones aparece la necesidad de recuperar el funcionamiento de los dispositivos.

Como ejemplo se propone el estudio de la copia de seguridad de WhatsApp. Porqué las entidades están incorporando aplicaciones de este estilo como un canal de comunicación de marketing digital, entre su entorno y o su personal[2].

Ejercicios

Cifrado 7zip

Se adjunta el fichero 7zip con el contenido temporal a compartir[3].

2Incluso me lo he encontrado en un hospital. Dónde el personal médico se había creado un grupo para informarse sobre: operaciones, resultados (con fotos de pacientes incluidas).

3He asistido a talleres de colegios de abogados que lo recomendaban para dar seguridad a los adjuntos incluidos en el correo electrónico

- En el siguiente vídeo encontrareis el reto: control-7zip
- Así mismo, se adjunta el archivo temporal a descifrar.

Responded con vuestra opinión sobre el contenido del secreto y si consideráis que el fichero temporal 7zip ofrecería medidas de seguridad suficientes.

Cifrado de soportes y ficheros

Durante las auditorías os indicaran (y deberéis comprobar) la existencia de métodos de cifrado en ficheros (que almacenen imágenes de sistemas, bases de datos, documentación ofimática, etc.) o en unidades y discos.

En esta tarea, utilizaremos la aplicación Veracrypt (de código abierto y licencia libre) para cifrar el documento que se adjunta.

Para disponer de una guía, seguid este vídeo: control-veracrypt