Práctica 1: Análisis de riesgos mediante la meto- dología MAGERIT y planes de seguridad.

Juan Francisco García Delgado y Juan José Montoya Segura

8 de Noviembre de 2018

1 Introducción

Hemos decidido analizar el funcionamiento de una empresa moderna, basada en una comunicación servidor-cliente de manera sencilla para el usuario a través de una app móvil. En este caso, UBER.
UBER es una plataforma de alquiler de vehículos con conductor, opera en más de 80 países alrededor del mundo, por tanto, consideramos que tiene una infraestructura en su sistema informático digna de ser estudiada. En cualquier caso, no disponemos de *datos oficiales* facilitados por la compañía, así que esta es nuestra libre aproximación a lo que una organización de tal calibre puede requerir para mantener su correcto funcionamiento ininterrumpido.

Figure 1: Logo de UBER

2 Activos para considerar

En las siguientes categorías:

2.1 Activos esenciales

[BD] Base de datos: Base de datos principal, es un recurso básico en nuestra organización, en esta se leen y escriben datos de los *usuarios*, *vehículos* y *servicio*.
[T] Servicio de transporte: Es el servicio que se presta al usuario final, el transporte de punto a punto. El objetivo de nuestra organización es básicamente este.
[AC] Atención al cliente: Servicio que se presta al *usuario final*, establecido para resolver sus dudas y posibles problemas con el transporte o su facturación.

2.2 Equipamiento: Aplicaciones

[APPC] APP Conductor: Es una pieza de *software* que corre en los terminales móviles de nuestros conductores, nos permite localizarles en todo momento, dar órdenes y recibir información del vehículo.
[APPCL] APP Cliente: Es la parte del *software* que ejecuta el cliente final en su terminal móvil, dándole acceso al servicio de la manera más sencilla y fiable posible.
[SSV] Software servidor: Es el *software* que corre en nuestro servidor principal, se encarga de recibir los datos de las aplicaciones de conductor y cliente y utilizar la *base de datos* para trasladar dicha información.

2.3 Equipamiento: Equipos

[FW] Firewall: Es un equipo informático físico que se encarga de proteger nuestra red de posibles ataques en caso de un uso malicioso.
[SBD] Servidor de bases de datos: Es el equipo informático en el cual se almacena la base de datos.
[SV] Servidor principal: Máquina física que corre el *software servidor* al cual se conectan *clientes* y *conductores*.
[SV2] Servidor secundario: Máquina física que haría el relevo en caso de algún fallo de disponibilidad o integridad en nuestro *servidor principal*.
[C] Coche: Es el conjunto mecánico de la herramienta principal de transporte, se busca la máxima fiabilidad y seguridad de cara al usuario y los empleados.
[GPS] GPS Coche: Sensor capaz de recaudar datos de ruta, velocidad y otros parámetros para ser contabilizados de cara al servicio de transporte y atención al cliente.
[BAK] Sistemas de replicación: Servicio de *copias de seguridad* que se encarga de la integridad de los datos tanto de la base de datos como del servidor principal y secundario.

2.4 Equipamiento: Comunicaciones

[INT] Conexión a internet: Conexión a internet de banda ancha con capacidad suficiente para dar servicio a todos nuestros *usuarios* y *conductores* al mismo tiempo. Se busca la mayor fiabilidad.

2.5 Servicios subcontratados

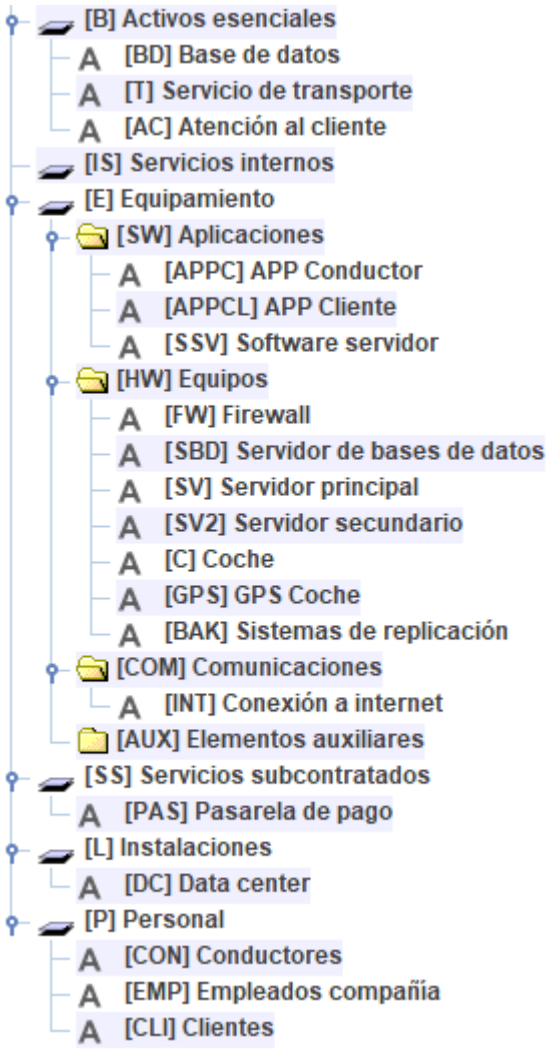
[PAS] Pasarela de pago: Plataforma que nos permite autorizar y cobrar el pago a nuestros clientes. Está proporcionada por un banco como entidad externa, la cual nos da ciertas garantías de funcionamiento y privacidad.

2.6 Instalaciones

[DC] Data center: Es el espacio reservado en un edificio debidamente climatizado, conectado, securizado y mantenido para alojar todos nuestros equipos informáticos.

2.7 Personal

[CON] Conductores: Los conductores son empleados que se encargan de utilizar el *coche*, *GPS del coche* y la parte de *app conductor*. Dan el servicio de transporte y tienen contacto directo con el cliente.
[EMP] Empleados compañía: Los empleados internos son los que se encargan de mantener, implementar y actualizar tanto el sistema informático como los vehículos. También hay una sección dirigida a la atención al cliente.
[CLI] Clientes: Son los usuarios finales de la plataforma, buscan el servicio de transporte a buen precio, con fiabilidad y seguridad.


[B] Activos esenciales
[BD] Base de datos
[T] Servicio de transporte
[AC] Atención al cliente
[IS] Servicios internos
[E] Equipamiento
[SW] Aplicaciones
[APPC] APP Conductor
[APPCL] APP Cliente
[SSV] Software servidor
[HW] Equipos
[FW] Firewall
[SBD] Servidor de bases de datos
[SV] Servidor principal
[SV2] Servidor secundario
[C] Coche
[GPS] GPS Coche
[BAK] Sistemas de replicación
[COM] Comunicaciones
[INT] Conexión a internet
[AUX] Elementos auxiliares
[SS] Servicios subcontratados
[PAS] Pasarela de pago
[L] Instalaciones
[DC] Data center
[P] Personal
[CON] Conductores
[EMP] Empleados compañía
[CLI] Clientes

3 Valoración de los activos

Tenemos distintas dimensiones de valoración para clasificar nuestros activos, estas son los atributos que hacen valioso nuestro activo. Se hacen los análisis de riesgo respecto a esto para valorar las consecuencias de que se materialicen las amenazas.

Las distintas dimensiones son: [**D**] **Disponibilidad**, [**I**] **Integridad de los datos** y [**C**] **Confidencialidad de la información**.

En el caso de la disponibilidad, vemos el valor que tendría si no estuviera disponible. Esta afecta a todo tipo de activos, desde los servicios, pasando por los equipos hasta al software escrito para el correcto funcionamiento de la organización. A menudo requiere un tratamiento por escalones, ya que el **coste de esta es más exponencial que lineal.**

La integridad de los datos de la organización también juega un papel importante ya que no sabemos qué consecuencias podría tener si estos fueran modificados sin ningún control ni registro. Es fácil no solo caer en un fallo del servicio proporcionado, sino también incurrir en ciertos problemas legales debido a comunicar cierta información crítica de manera errónea o no al cliente objetivo. Estas alteraciones **pueden ser causadas de forma voluntaria o ininteccionada.**

Hablando de la confidencialidad, se puede dar el caso de tener causar graves daños a nuestra organización por errores simples, ya sean de acceso a los datos o de comunicación, por ello, es importante conocer qué comunicamos al público y qué guardamos en distintos niveles, de manera que, por ejemplo, un cliente no pueda conocer los datos de otro o ciertos empleados no puedan acceder a otro nivel de información más sensible. En el caso de una filtración, **se puede llegar a litigios serios que cesarían nuestra organización.**