

Práctica 1: Análisis de riesgos mediante la metodología 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 Sistema de la información de nuestra organización

Nuestra organización dispone de tres servidores en su datacenter, estos servidores son responsables de contactar tanto con la aplicación del cliente como con la del conductor. Estos servidores están conectados a internet a través de un firewall, que nos garantiza mayor seguridad en las comunicaciones.

En nuestro servidor principal corre el software de servidor, que conecta al de base de datos para obtener los datos de nuestros clientes y viajes. Existe un segundo servidor que se pondría en funcionamiento en caso de fallo del primero. Todos estos datos son replicados por el servidor de backup.

Se da al cliente, además del servicio de transporte, uno de atención al mismo, proporcionado por los empleados internos. El servicio de transporte implica que los conductores y los clientes utilicen el coche que manda los datos GPS a la compañía.

Para el pago, se usa la pasarela externa para no recoger los datos de pago del cliente.

3 Identificación de los Principales Activos

En las siguientes categorías:

3.1 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.

3.2 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.

3.3 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.

3.4 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.

3.5 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.

3.6 Instalaciones

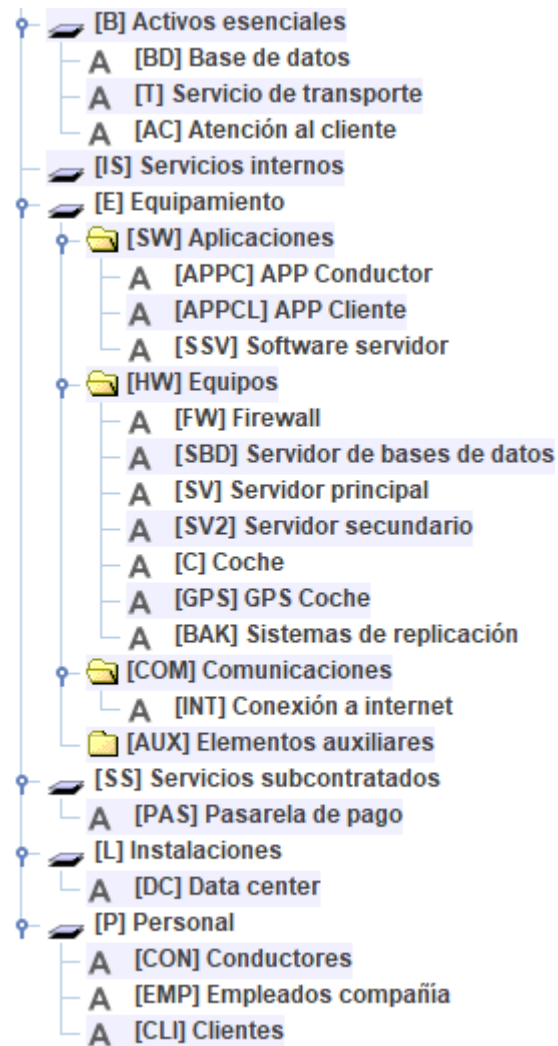
[DC] **Data center:** Es el espacio reservado en un edificio debidamente climatizado, conectado, securizado y mantenido para alojar todos nuestros equipos informáticos.

3.7 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.

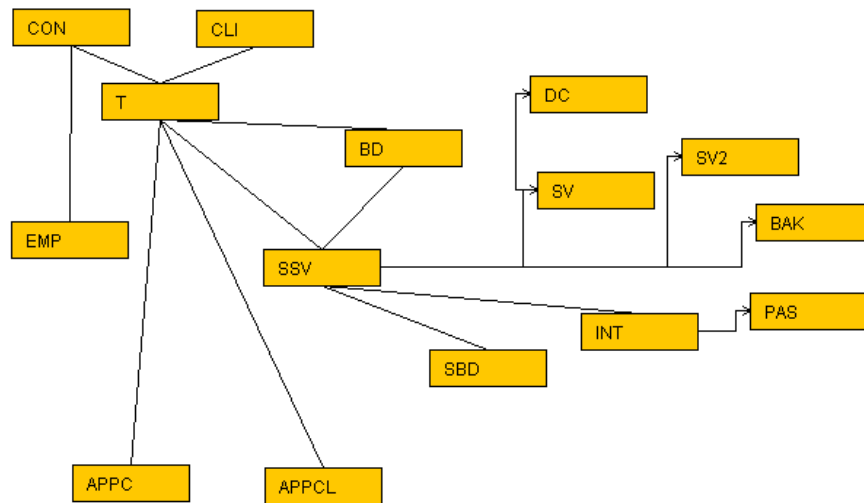
[CLI] **Clientes:** Son los usuarios finales de la plataforma, buscan el servicio de transporte a buen precio, con fiabilidad y seguridad.



4 Análisis de la dependencia de entre activos

Consideramos ciertos niveles de dependencia entre los distintos activos, de manera que ciertas partes de la organización no funcionen sin su nivel inferior.

4.1 Grafo de dependencias



5 Valoración de los activos en sus distintas dimensiones

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 inintencionada**.

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**.

5 VALORACIÓN DE LOS ACTIVOS EN SUS DISTINTAS DIMENSIONES

Las valoraciones quedan de la siguiente manera en **PILAR**:

activo	[D]	[I]	[C]
ACTIVOS			
🔑 📁 [B] Activos esenciales			
A [BD] Base de datos	2,1M	2,1M	2,1M
A [T] Servicio de transporte	2,1M	1M	1M
A [AC] Atención al cliente	215K	2,1M	2,1M
🔑 📁 [IS] Servicios internos			
🔑 📁 [E] Equipamiento			
🔑 📁 [SW] Aplicaciones			
A [APPC] APP Conductor	1M	1M	2,1M
A [APPCL] APP Cliente	2,1M	2,1M	2,1M
A [SSV] Software servidor	2,1M	2,1M	2,1M
🔑 📁 [HW] Equipos			
A [FW] Firewall	215K	215K	1M
A [SBD] Servidor de bases de datos	2,1M	2,1M	2,1M
A [SV] Servidor principal	2,1M	2,1M	2,1M
A [SV2] Servidor secundario	2,1M	2,1M	2,1M
A [C] Coche	2,1M	2,1M	2,1M
A [GPS] GPS Coche	2,1M	215K	1M
A [BAK] Sistemas de replicación	2,1M	2,1M	1M
🔑 📁 [COM] Comunicaciones			
A [INT] Conexión a internet	1M	2,1M	1M
📁 [AUX] Elementos auxiliares			
🔑 📁 [SS] Servicios subcontratados			
A [PAS] Pasarela de pago	215K	2,1M	2,1M
🔑 📁 [L] Instalaciones			
A [DC] Data center	2,1M	2,1M	2,1M
🔑 📁 [P] Personal			
A [CON] Conductores	1M	2,1M	1M
A [EMP] Empleados compañía	1M	2,1M	1M
A [CLI] Clientes	2,1M	2,1M	2,1M

6 Identificación y valoración de las amenazas

Tras introducir todos los datos de valoración en el software **PILAR**, disponemos del siguiente informe de amenazas, el cual será mostrado a continuación:

[BD] Base de datos

amenaza	frecuencia	[D]	[I]	[C]
[E.15] Alteración de la información	1	-	50%	-
[E.18] Destrucción de la información	1	1%	-	-
[E.19] Fugas de información	1	-	-	10%
[A.5] Suplantación de la identidad	10	-	10%	50%
[A.6] Abuso de privilegios de acceso	10	1%	10%	50%
[A.11] Acceso no autorizado	100	-	10%	50%

[T] Servicio de transporte

[AC] Atención al cliente

[APPC] APP Conductor

amenaza	frecuencia	[D]	[I]	[C]
[I.5] Avería de origen físico o lógico	1	50%	-	-
[E.8] Difusión de software dañino	1	10%	10%	10%
[E.20] Vulnerabilidades de los programas (software)	1	1%	20%	20%
[E.21] Errores de mantenimiento / actualización de programas (software)	10	1%	1%	-
[A.8] Difusión de software dañino	1	100%	100%	100%
[A.22] Manipulación de programas	1	50%	100%	100%

[APPCL] APP Cliente

amenaza	frecuencia	[D]	[I]	[C]
[I.5] Avería de origen físico o lógico	1	50%	-	-
[E.8] Difusión de software dañino	1	10%	10%	10%
[E.20] Vulnerabilidades de los programas (software)	1	1%	20%	20%
[E.21] Errores de mantenimiento / actualización de programas (software)	10	1%	1%	-
[A.8] Difusión de software dañino	1	100%	100%	100%
[A.22] Manipulación de programas	1	50%	100%	100%

[SSV] Software servidor

amenaza	frecuencia	[D]	[I]	[C]
[I.5] Avería de origen físico o lógico	1	50%	-	-
[E.8] Difusión de software dañino	1	10%	10%	10%
[E.20] Vulnerabilidades de los programas (software)	1	1%	20%	20%
[E.21] Errores de mantenimiento / actualización de programas (software)	10	1%	1%	-
[A.8] Difusión de software dañino	1	100%	100%	100%
[A.22] Manipulación de programas	1	50%	100%	100%

[FW] Firewall

amenaza	frecuencia	[D]	[I]	[C]
[N.1] Fuego	0,1	100%	-	-
[N.2] Daños por agua	0,1	50%	-	-
[N.*] Desastres naturales	0,1	100%	-	-
[I.1] Fuego	0,5	100%	-	-
[I.2] Daños por agua	0,5	50%	-	-
[I.*] Desastres industriales	0,5	100%	-	-
[I.3] Contaminación medioambiental	0,1	50%	-	-
[I.4] Contaminación electromagnética	1	10%	-	-
[I.5] Avería de origen físico o lógico	1	50%	-	-
[I.6] Corte del suministro eléctrico	1	100%	-	-
[I.7] Condiciones inadecuadas de temperatura o humedad	1	100%	-	-
[I.8] Fallo de servicios de comunicaciones	1	50%	-	-
[I.11] Emanaciones electromagnéticas	1	-	-	1%
[E.2] Errores del administrador del sistema / de la seguridad	1	20%	20%	20%
[E.9] Errores de [re-]encaminamiento	1	-	-	10%
[E.10] Errores de secuencia	1	-	10%	-
[E.15] Alteración de la información	1	-	1%	-
[E.19] Fugas de información	1	-	-	10%
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	10%	-	-
[E.24] Caída del sistema por agotamiento de recursos	10	50%	-	-
[E.25] Pérdida de equipos	1	100%	-	50%
[A.5] Suplantación de la identidad	1	-	10%	50%
[A.7] Uso no previsto	1	10%	10%	10%
[A.9] [Re-]encaminamiento de mensajes	1	-	-	10%
[A.10] Alteración de secuencia	1	-	10%	-
[A.11] Acceso no autorizado	1	10%	10%	50%
[A.12] Análisis de tráfico	1	-	-	2%
[A.14] Interceptación de información (escucha)	1	-	-	10%
[A.15] Modificación de la información	1	-	10%	-
[A.18] Destrucción de la información	1	50%	-	-
[A.23] Manipulación del hardware	0,5	50%	-	50%
[A.24] Denegación de servicio	10	100%	-	-
[A.25] Robo de equipos	0,5	100%	-	50%
[A.26] Ataque destructivo	1	100%	-	-

[SBD] Servidor de bases de datos

amenaza	frecuencia	[D]	[I]	[C]
[N.1] Fuego	0,1	100%	-	-
[N.2] Daños por agua	0,1	50%	-	-
[N.*] Desastres naturales	0,1	100%	-	-
[I.1] Fuego	0,5	100%	-	-
[I.2] Daños por agua	0,5	50%	-	-
[I.*] Desastres industriales	0,5	100%	-	-
[I.3] Contaminación medioambiental	1	50%	-	-
[I.4] Contaminación electromagnética	1	10%	-	-
[I.5] Avería de origen físico o lógico	1	50%	-	-
[I.6] Corte del suministro eléctrico	1	100%	-	-
[I.7] Condiciones inadecuadas de temperatura o humedad	1	100%	-	-
[I.10] Degradación de los soportes de almacenamiento de la información	1	100%	-	-
[I.11] Emanaciones electromagnéticas	1	-	-	1%
[E.1] Errores de los usuarios	1	1%	5%	10%
[E.8] Difusión de software dañino	1	10%	10%	10%
[E.15] Alteración de la información	1	-	1%	-
[E.18] Destrucción de la información	1	100%	-	-
[E.19] Fugas de información	1	-	-	10%
[E.20] Vulnerabilidades de los programas (software)	1	1%	20%	20%
[E.21] Errores de mantenimiento / actualización de programas (software)	10	1%	1%	-
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	10%	-	-
[E.24] Caída del sistema por agotamiento de recursos	10	50%	-	-
[E.25] Pérdida de equipos	1	100%	-	50%
[A.5] Suplantación de la identidad	10	-	10%	50%
[A.6] Abuso de privilegios de acceso	10	1%	10%	50%
[A.7] Uso no previsto	1	1%	-	1%
[A.8] Difusión de software dañino	1	100%	100%	100%
[A.11] Acceso no autorizado	100	10%	10%	50%
[A.15] Modificación de la información	5	-	100%	-
[A.18] Destrucción de la información	1	100%	-	-
[A.22] Manipulación de programas	1	50%	100%	100%
[A.23] Manipulación del hardware	0,5	50%	-	50%
[A.24] Denegación de servicio	2	100%	-	-
[A.25] Robo de equipos	1	100%	-	100%
[A.26] Ataque destructivo	1	100%	-	-

[SV] Servidor principal

amenaza	frecuencia	[D]	[I]	[C]
[N.1] Fuego	0,1	100%	-	-
[N.2] Daños por agua	0,1	50%	-	-
[N.*] Desastres naturales	0,1	100%	-	-
[I.1] Fuego	0,5	100%	-	-
[I.2] Daños por agua	0,5	50%	-	-
[I.*] Desastres industriales	0,5	100%	-	-
[I.3] Contaminación medioambiental	0,1	50%	-	-
[I.4] Contaminación electromagnética	1	10%	-	-
[I.5] Avería de origen físico o lógico	1	50%	-	-
[I.6] Corte del suministro eléctrico	1	100%	-	-
[I.7] Condiciones inadecuadas de temperatura o humedad	1	100%	-	-
[I.11] Emanaciones electromagnéticas	1	-	-	1%
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	10%	-	-
[E.24] Caída del sistema por agotamiento de recursos	10	50%	-	-
[E.25] Pérdida de equipos	1	100%	-	50%
[A.11] Acceso no autorizado	1	10%	10%	50%
[A.23] Manipulación del hardware	0,5	50%	-	50%
[A.24] Denegación de servicio	2	100%	-	-
[A.25] Robo de equipos	0,5	100%	-	50%
[A.26] Ataque destructivo	1	100%	-	-

[SV2] Servidor secundario

amenaza	frecuencia	[D]	[I]	[C]
[N.1] Fuego	0,1	100%	-	-
[N.2] Daños por agua	0,1	50%	-	-
[N.*] Desastres naturales	0,1	100%	-	-
[I.1] Fuego	0,5	100%	-	-
[I.2] Daños por agua	0,5	50%	-	-
[I.*] Desastres industriales	0,5	100%	-	-
[I.3] Contaminación medioambiental	0,1	50%	-	-
[I.4] Contaminación electromagnética	1	10%	-	-
[I.5] Avería de origen físico o lógico	1	50%	-	-
[I.6] Corte del suministro eléctrico	1	100%	-	-
[I.7] Condiciones inadecuadas de temperatura o humedad	1	100%	-	-
[I.11] Emanaciones electromagnéticas	1	-	-	1%
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	10%	-	-
[E.24] Caída del sistema por agotamiento de recursos	10	50%	-	-
[E.25] Pérdida de equipos	1	100%	-	50%
[A.11] Acceso no autorizado	1	10%	10%	50%
[A.23] Manipulación del hardware	0,5	50%	-	50%
[A.24] Denegación de servicio	2	100%	-	-
[A.25] Robo de equipos	0,5	100%	-	50%
[A.26] Ataque destructivo	1	100%	-	-

[C] Coche

amenaza	frecuencia	[D]	[I]	[C]
[N.1] Fuego	0,1	100%	-	-
[N.2] Daños por agua	0,1	50%	-	-
[N.*] Desastres naturales	0,1	100%	-	-
[I.1] Fuego	0,5	100%	-	-
[I.2] Daños por agua	0,5	50%	-	-
[I.*] Desastres industriales	0,5	100%	-	-
[I.3] Contaminación medioambiental	0,1	50%	-	-
[I.4] Contaminación electromagnética	1	10%	-	-
[I.5] Avería de origen físico o lógico	1	50%	-	-
[I.6] Corte del suministro eléctrico	1	100%	-	-
[I.7] Condiciones inadecuadas de temperatura o humedad	1	100%	-	-
[I.11] Emanaciones electromagnéticas	1	-	-	1%
[E.8] Difusión de software dañino	1	10%	10%	10%
[E.20] Vulnerabilidades de los programas (software)	1	1%	20%	20%
[E.21] Errores de mantenimiento / actualización de programas (software)	10	1%	1%	-
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	10%	-	-
[E.24] Caída del sistema por agotamiento de recursos	10	50%	-	-
[E.25] Pérdida de equipos	1	100%	-	50%
[A.8] Difusión de software dañino	1	100%	100%	100%
[A.11] Acceso no autorizado	1	10%	10%	50%
[A.22] Manipulación de programas	1	50%	100%	100%
[A.23] Manipulación del hardware	0,5	50%	-	50%
[A.24] Denegación de servicio	2	100%	-	-
[A.25] Robo de equipos	0,5	100%	-	50%
[A.26] Ataque destructivo	1	100%	-	-

[GPS] GPS Coche

amenaza	frecuencia	[D]	[I]	[C]
[N.1] Fuego	0,1	100%	-	-
[N.2] Daños por agua	0,1	50%	-	-
[N.*] Desastres naturales	0,1	100%	-	-
[I.1] Fuego	0,5	100%	-	-
[I.2] Daños por agua	0,5	50%	-	-
[I.*] Desastres industriales	0,5	100%	-	-
[I.3] Contaminación medioambiental	0,1	50%	-	-
[I.4] Contaminación electromagnética	1	10%	-	-
[I.5] Avería de origen físico o lógico	1	50%	-	-
[I.6] Corte del suministro eléctrico	1	100%	-	-
[I.7] Condiciones inadecuadas de temperatura o humedad	1	100%	-	-
[I.11] Emanaciones electromagnéticas	1	-	-	1%
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	10%	-	-
[E.24] Caída del sistema por agotamiento de recursos	10	50%	-	-
[E.25] Pérdida de equipos	1	100%	-	50%
[A.11] Acceso no autorizado	1	10%	10%	50%
[A.23] Manipulación del hardware	0,5	50%	-	50%
[A.24] Denegación de servicio	2	100%	-	-
[A.25] Robo de equipos	0,5	100%	-	50%
[A.26] Ataque destructivo	1	100%	-	-

[BAK] Sistemas de replicación

amenaza	frecuencia	[D]	[I]	[C]
[N.1] Fuego	0,1	100%	-	-
[N.2] Daños por agua	0,1	50%	-	-
[N.*] Desastres naturales	0,1	100%	-	-
[I.1] Fuego	0,5	100%	-	-
[I.2] Daños por agua	0,5	50%	-	-
[I.*] Desastres industriales	0,5	100%	-	-
[I.3] Contaminación medioambiental	0,1	50%	-	-
[I.4] Contaminación electromagnética	1	10%	-	-
[I.5] Avería de origen físico o lógico	1	50%	-	-
[I.6] Corte del suministro eléctrico	1	100%	-	-
[I.7] Condiciones inadecuadas de temperatura o humedad	1	100%	-	-
[I.11] Emanaciones electromagnéticas	1	-	-	1%
[E.8] Difusión de software dañino	1	10%	10%	10%
[E.15] Alteración de la información	1	-	1%	-
[E.18] Destrucción de la información	1	1%	-	-
[E.19] Fugas de información	1	-	-	10%
[E.20] Vulnerabilidades de los programas (software)	1	1%	20%	20%
[E.21] Errores de mantenimiento / actualización de programas (software)	10	1%	1%	-
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	10%	-	-
[E.24] Caída del sistema por agotamiento de recursos	10	50%	-	-
[E.25] Pérdida de equipos	1	100%	-	50%
[A.5] Suplantación de la identidad	10	-	10%	50%
[A.6] Abuso de privilegios de acceso	10	1%	10%	50%
[A.8] Difusión de software dañino	1	100%	100%	100%
[A.11] Acceso no autorizado	100	10%	10%	50%
[A.22] Manipulación de programas	1	50%	100%	100%
[A.23] Manipulación del hardware	0,5	50%	-	50%
[A.24] Denegación de servicio	2	100%	-	-
[A.25] Robo de equipos	0,5	100%	-	50%
[A.26] Ataque destructivo	1	100%	-	-

[INT] Conexión a internet

amenaza	frecuencia	[D]	[I]	[C]
[I.8] Fallo de servicios de comunicaciones	1	50%	-	-
[E.2] Errores del administrador del sistema / de la seguridad	1	20%	20%	20%
[E.9] Errores de [re-]encaminamiento	1	-	-	10%
[E.10] Errores de secuencia	1	-	10%	-
[E.15] Alteración de la información	1	-	1%	-
[E.19] Fugas de información	1	-	-	10%
[E.24] Caída del sistema por agotamiento de recursos	1	50%	-	-
[A.5] Suplantación de la identidad	1	-	10%	50%
[A.7] Uso no previsto	1	10%	10%	10%
[A.9] [Re-]encaminamiento de mensajes	1	-	-	10%
[A.10] Alteración de secuencia	1	-	10%	-
[A.11] Acceso no autorizado	1	-	10%	50%
[A.12] Análisis de tráfico	1	-	-	2%
[A.14] Interceptación de información (escucha)	1	-	-	10%
[A.15] Modificación de la información	1	-	10%	-
[A.18] Destrucción de la información	1	50%	-	-
[A.24] Denegación de servicio	10	50%	-	-

[PAS] Pasarela de pago

amenaza	frecuencia	[D]	[I]	[C]
[I.5] Avería de origen físico o lógico	1	50%	-	-
[E.8] Difusión de software dañino	1	10%	10%	10%
[E.15] Alteración de la información	1	-	50%	-
[E.18] Destrucción de la información	1	1%	-	-
[E.19] Fugas de información	1	-	-	10%
[E.20] Vulnerabilidades de los programas (software)	1	1%	20%	20%
[E.21] Errores de mantenimiento / actualización de programas (software)	10	1%	1%	-
[A.5] Suplantación de la identidad	10	-	10%	50%
[A.6] Abuso de privilegios de acceso	10	1%	10%	50%
[A.8] Difusión de software dañino	1	100%	100%	100%
[A.11] Acceso no autorizado	100	-	10%	50%
[A.22] Manipulación de programas	1	50%	100%	100%

[DC] Data center

amenaza	frecuencia	[D]	[I]	[C]
[N.1] Fuego	1	100%	-	-
[N.2] Daños por agua	1	100%	-	-
[N.*] Desastres naturales	0,5	100%	-	-
[I.1] Fuego	1	100%	-	-
[I.2] Daños por agua	1	100%	-	-
[I.*] Desastres industriales	1	100%	-	-
[I.3] Contaminación medioambiental	1	10%	-	-
[I.4] Contaminación electromagnética	0,1	10%	-	-
[A.6] Abuso de privilegios de acceso	1	10%	-	-
[A.7] Uso no previsto	1	10%	-	-
[A.26] Ataque destructivo	0,1	100%	-	-
[A.27] Ocupación enemiga	1	100%	-	-

[CON] Conductores

amenaza	frecuencia	[D]	[I]	[C]
[E.15] Alteración de la información	1	-	10%	-
[E.18] Destrucción de la información	1	1%	-	-
[E.19] Fugas de información	1	-	-	10%
[A.15] Modificación de la información	1	-	50%	-
[A.18] Destrucción de la información	1	10%	-	-
[A.19] Revelación de información	1	-	-	50%
[A.28] Indisponibilidad del personal	0,5	10%	-	-
[A.29] Extorsión	0,9	10%	10%	50%
[A.30] Ingeniería social (picaresca)	0,5	10%	10%	50%

[EMP] Empleados compañía

amenaza	frecuencia	[D]	[I]	[C]
[E.15] Alteración de la información	1	-	10%	-
[E.18] Destrucción de la información	1	1%	-	-
[E.19] Fugas de información	1	-	-	10%
[A.15] Modificación de la información	1	-	50%	-
[A.18] Destrucción de la información	1	10%	-	-
[A.19] Revelación de información	1	-	-	50%
[A.28] Indisponibilidad del personal	0,5	10%	-	-
[A.29] Extorsión	0,9	10%	10%	50%
[A.30] Ingeniería social (picaresca)	0,5	10%	10%	50%

[CLI] Clientes

























amenaza	frecuencia	[D]	[I]	[C]
[E.15] Alteración de la información	1	-	10%	-
[E.18] Destrucción de la información	1	1%	-	-
[E.19] Fugas de información	1	-	-	10%
[A.15] Modificación de la información	1	-	50%	-
[A.18] Destrucción de la información	1	10%	-	-
[A.19] Revelación de información	1	-	-	50%
[A.28] Indisponibilidad del personal	0,5	10%	-	-
[A.29] Extorsión	0,9	10%	10%	50%
[A.30] Ingeniería social (picaresca)	0,5	10%	10%	50%

7 Identificación y valoración de las salvaguardas

Tras introducir todos los datos de valoración en el software **PILAR**, disponemos del siguiente informe de salvaguardas, el cual viene adjunto como "Evaluación de salvaguardas".

8 Estimación del Impacto Residual tras la aplicación de las salvaguardas.

Con todos los datos que disponemos, PILAR genera el siguiente informe de impactos tras las salvaguardas:

as...	tdp	salvaguarda	... f...	... recom...	... t...	PILAR
		SALVAGUARDAS				
G	EL	 [IA] Identificación y autenticación		9		L2-L5
T	EL	 [AC] Control de acceso lógico		7		L2-L4
G	PR	 [D] Protección de la Información		7		L2-L4
G	EL	 [K] Protección de claves criptográficas				n.a.
G	PR	 [S] Protección de los Servicios				n.a.
G	PR	 [SW] Protección de las Aplicaciones Informáticas (SW)		8		L2-L5
G	PR	 [HW] Protección de los Equipos Informáticos (HW)		8		L2-L5
G	PR	 [COM] Protección de las Comunicaciones		9		L2-L5
G	PR	 [IP] Sistema de protección de frontera lógica				n.a.
G	PR	 [MP] Protección de los Soportes de Información		7		L2-L4
G	PR	 [AUX] Elementos Auxiliares		7		L2-L4
F	EL	 [HW_0049] Protección física del equipamiento		6		L3-L4
F	PR	 [L] Protección de las Instalaciones		7		L2-L4
F	EL	 [PPS] Protección del perímetro físico				n.a.
P	PR	 [PS] Gestión del Personal		7		L2-L4
G	PR	 [PDS] Servicios potencialmente peligrosos				n.a.
G	CR	 [IR] Gestión de incidentes		7		L2-L4
T	PR	 [tools] Herramientas de seguridad		9		L3-L5
G	CR	 [V] Gestión de vulnerabilidades		6		L2-L4
T	MN	 [A] Registro y auditoría				n.a.
G	RC	 [BC] Continuidad del negocio		5		L2-L3
G	AD	 [G] Organización		6		L2-L4
G	AD	 [E] Relaciones Externas		7		L2-L4
G	AD	 [NEW] Adquisición / desarrollo		6		L2-L4

9 Planes de seguridad

Utilizando las herramientas que PILAR nos brinda, desarrollamos el plan de seguridad a desarrollar, el cual viene adjunto como "Plan de seguridad".

[27002:2013] Código de prácticas para los controles de seguridad de la inform

proyecto: *[UBER] Practica 1 UBER*

fecha: 08-nov-2018

clasificación: CONFIDENCIAL

1. Datos del proyecto

UBER	Practica 1 UBER
Organización	UBER
Descripción	Servicio de transportes
Autor	Juan Francisco García Delgado, Juan José Montoya Segura
Versión	1.0
biblioteca	[std] Biblioteca INFOSEC (20.8.2017)

Licencia

[edu] ual.es
 Fiabilidad y Gestión de Riesgos
 Grado de Ingeniería Informática
 Universidad de Almería
 [... 1.3.2019]

2. Dominios de seguridad

- [base] Base

3. Fases del proyecto

- [current] situación actual
- [target] situación objetivo
- [PILAR] recomendación

4. Dominio de seguridad: [base] Base

4.1. [5] Políticas de seguridad de la información