EVALUACIÓN DE CONTROLES GENERALES DE TI Y SU IMPACTO EN LOS ESTADOS FINANCIEROS

Roberto Avilés Blesa
Máster en Ingeniería Informática
Business Intelligence

David Amorós / Jorge Velilla
María Isabel Guitart

12/06/2017

Licencias alternativas (elegir alguna de las siguientes y sustituir la de la página anterior)

A) Creative Commons:

Esta obra está sujeta a una licencia de Reconocimiento-NoComercial-SinObraDerivada 3.0 España de Creative Commons

Esta obra está sujeta a una licencia de Reconocimiento-NoComercial-CompartirIgual 3.0 España de Creative Commons

Esta obra está sujeta a una licencia de Reconocimiento-NoComercial 3.0 España de Creative Commons

Esta obra está sujeta a una licencia de Reconocimiento-SinObraDerivada 3.0 España de Creative Commons

Esta obra está sujeta a una licencia de Reconocimiento-CompartirIgual 3.0 España de Creative Commons

Esta obra está sujeta a una licencia de Reconocimiento 3.0 España de Creative Commons

B) GNU Free Documentation License (GNU FDL)

C) Copyright

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Evaluación de Controles Generales de TI y su Impacto en los Estados Financieros*
Nombre del autor:	*Roberto Avilés Blesa*
Nombre del consultor/a:	*David Amorós Alcaraz* *Jorge Velilla Velasco (externo)*
Nombre del PRA:	*María Isabel Guitart Hormigo*
Fecha de entrega (mm/aaaa):	06/2017
Titulación::	*Master en Ingeniería Informática*
Área del Trabajo Final:	*Business Intelligence*
Idioma del trabajo:	*Español*
Palabras clave	*Auditoría* *COBIT* *QlikSense*

Resumen del Trabajo (máximo 250 palabras): *Con la finalidad, contexto de aplicación, metodología, resultados i conclusiones del trabajo.*

Los Sistemas de Tecnologías de Información, cada vez con mayor frecuencia, intervienen significativamente en los flujos de datos de los diferentes procesos de negocio en las empresas; introduciendo, transformando, procesando y almacenando información crítica que componen sus estados financieros.
Debido a los controles automáticos que nos ofrecen estos Sistemas y a la dependencia del negocio en ellos para un preciso y completo procesamiento de la información, y con el objeto de garantizar que las entidades reflejan una imagen fiel de sus estados financieros, es necesario validar una serie de aspectos relacionados con el entorno de control de sus Sistemas.

A través de las buenas prácticas en el ámbito de la gestión de Servicio de TI (ITIL), normativas internacionales (ISO20000) y marcos de control (COBIT); se han identificado los riegos inherentes en los Sistemas de TI con impacto en los estados financieros y se ha definido un marco de objetivos de control a cubrir para mitigarlos. A través de un caso de estudio sobre una startup fictici, se han identificado los controles en los Sistemas de TI, que les permiten cubrir los objetivos de control definidos, y se ha auditado su diseño, implementación y efectividad operativa.

Con los resultados obtenidos de esta Auditoría, se ha diseñado un Cuadro de Mando basado en Qlik Sense, cuyo público objetivo es la Dirección TI de la entidad, y que representa los elementos clave evaluados, permitiendo actuar sobre las deficiencias de control observadas.

Abstract (in English, 250 words or less):

More and more frequently, the Information Technology Systems, significantly contribute in entities business processes data flows; introducing, transforming, processing and storing critical information that constitute its financial statements.

For a precise and complete processing of the information, the entities have an high dependency on automated controls offered by these Systems; and in order to guarantee that the entities reflect a faithful image of their financial statements, it is necessary to validate a series of aspects related to the control environment of their Systems.

Through good practices in the field of IT Service Management (ITIL), international standards (ISO20000) and control frameworks (COBIT); identified the risks inherent in IT systems with impact on the financial statements and defined control objectives framework to be covered to mitigate them.Through a fictitious case study, identified the controls in their IT systems, which allow entity to cover the defined control objectives, and subsequently, audited their design, implementation and operational effectiveness.

With the results obtained from this Audit, designed a Scorecard based on Qlik Sense, whose target audience was the IT Management of the entity, and which represents the key elements evaluated, allowing them to act on the observed control deficiencies.

Índice

Lista de figuras

1. Introducción

1.1 Contexto y justificación del Trabajo

Actualmente, un elevado porcentaje de entidades utilizan los Sistemas de Tecnologías de Información (TI en adelante) como pilares clave para obtener, procesar y transformar la información dentro de sus procesos de negocio, incluyendo su información financiera. Debido a esta dependencia en las TI, y para que la Entidad refleje y proporcione una imagen fiel de sus estados financieros, es necesario definir y evaluar el entorno de control de sus Sistemas. La problemática actual, a nivel nacional en España, radica en que gran parte de las entidades carecen de un departamento de Auditoría Interna de TI responsable de definir e implementar un marco de control de TI que pueda asegurar la robustez de la información soportada.

El proyecto a desarrollar, está orientado a cubrir estas necesidades: se definirá, a través de las mejores prácticas observadas en la industria, un marco de objetivos de control que cubra los riesgos de TI inherentes a los Sistemas que intervienen en el flujo de información financiera. Se evaluará, como caso de estudio ficticio, el marco de control de una startup en base a los objetivos definidos y por último, se presentarán los resultados de esta auditoría a través de un Cuadro de Mando (Cuadro de Mando o CM en adelante).

Este Cuadro de Mando representará la relación de objetivos de control esperados junto con el resultado de la auditoría, además del desempeño de los diferentes procesos de TI evaluados. Permitirá al público objetivo, la Dirección de IT de la empresa auditada, de una forma ágil y sencilla, interpretar estos resultados para que sean capaces de tomar una serie de decisiones estratégicas para corregir las desviaciones y deficiencias encontradas.

1.2 Objetivos del Trabajo

Una vez presentado el escenario, con el objeto y el alcance del proyecto, los objetivos a lograr una vez finalizado el proyecto e implantado el CM, son:

- Definir un **marco de objetivos de control** aplicable a cualquier Sistema de TI, que cubra los riesgos inherentes a estos sistemas, basado en las buenas prácticas, en el contexto de la información sobre estados financieros.

- **Identificar, evaluar y documentar las deficiencias** de control del caso de estudio.

- **Representar** de forma clara y concisa a los interesados, a través de un CM, el **resultado de la auditoría**, que les permita:
    - Tomar de decisiones sobre las **deficiencias** encontradas en base al **impacto** potencial.
    - Evaluar el **desempeño** de los **procesos de TI** evaluados.
    - Para ello, el CM que deberá cumplir con las siguientes premisas:
        - **Usabilidad**: Debe ser fácil de usar, con ayudas e interfaces intuitivas.
        - **Accesibilidad**: Capacidad multidispositivo y multisistema para acceder desde cualquier ubicación conectada a Internet.
        - **Seguridad**: Restricción de acceso para limitar entrada a usuarios clave autorizados.
        - **Costes**: Relación calidad/precio óptima.
        - **Escalabilidad**: Solución escalable y fácilmente adaptable a las cambiantes necesidades del negocio.
        - **Manejo de Datos**: Capacidad para trabajar e integrar diferentes fuentes de datos.
        - **Rendimiento**: El sistema debe soportar el manejo de un número elevado de datos durante su funcionamiento.

1.3 Enfoque y método seguido

En primer lugar, para alcanzar el primer objetivo de definir un marco de objetivos de control para los Sistemas de TI, se ha optado utilizar y adaptar un modelo ya existente en el mercado basado en COBIT. Se ha elegido esta estrategia ya que COBIT es un marco aceptado internacionalmente como una buena práctica para el control de la información sobre las TI y los riesgos que conllevan.

Para conseguir identificar, evaluar y representar las deficiencias de control del caso de estudio a través de una Auditoría, se ha optado por una estrategia similar, utilizar las mejores prácticas del mercado basadas en ITIL e ISO 20000, al igual que metodología de Auditoría desarrollada por ISACA, como organización reconocida a nivel mundial para la evaluación de los Sistemas de TI.

Por último, para representar los resultados a los interesados, se ha desarrollado un nuevo CM, en base a los indicadores definidos en el transcurso del proyecto y utilizando tecnología existente basada en Qlik Sense. En base al análisis realizado de esta herramienta con otras opciones del mercado, se ha considerado la más apropiada para realizar el proyecto. Para más detalle, consultar el capítulo 4, apartado 4.3.

1.4 Planificación del Trabajo

Roberto Avilés, como Responsable del Proyecto de Auditoría TI, deberá mantener una estrecha relación colaborativa con el Director del Proyecto, Jorge Velilla, interesado clave del proyecto que proporcionará apoyo financiero, los recursos y el asesoramiento necesario para poder llevarlo a cabo.

Además, deberán establecerse sólidos procesos de comunicación con la entidad auditada, *FastLoans S.A*., concretamente con su Director de TI, otro de los interesados clave, para transmitir de forma precisa y correcta el objetivo de la auditoría a realizar; además de posibilitar un entendimiento de los de sus sistemas de información y su posterior revisión.

Al establecer estos canales de comunicación e involucración, se podrán definir claramente los elementos clave a plasmar en el Cuadro de Mando Integral en unas fases tempranas del proyecto.

La estructuración del trabajo que se presenta en este apartado comprende los trabajos que deben desarrollarse dentro del proyecto acorde al alcance definido, y comprende los siguientes conjuntos de tareas a alto nivel:

- Identificar los riesgos y objetivos de control asociados a los Sistemas de TI.
- Auditar el entorno de Control de TI de “FastLoans S.A.”.
- Publicar un Cuadro de Mando que represente los resultados obtenidos.

Adjunto se puede observar el detalle de las tareas a través de un diagrama de Gantt, indicando los hitos comentados anteriormente y fechas de realización:

	Task Name	Durat	Start	Finish	Predecessor
1	**Proyecto “Evaluación de Controles Generales de TI y su impacto en los estados financieros”**	**77 days**	**Thu 23/02/17**	**Mon 12/06/17**	
2	**Plan de Proyecto**	**7 days**	**Thu 23/02/17**	**Mon 06/03/17**	
3	Definición del Objeto, Alcance y Objetivos	2 days	Thu 23/02/17	Fri 24/02/17	
4	Identificación de los intervinientes y stakeholders	2 days	Sat 25/02/17	Mon 27/02/17	3
5	Planificación de las tareas y entregables	4 days	Tue 28/02/17	Fri 03/03/17	4
6	Plan de Proyecto	0 days	Mon 06/03/17	Mon 06/03/17	5
7	**Identificar los riesgos y objetivos de control asociados a los Sistemas de TI**	**5 days**	**Tue 07/03/17**	**Tue 14/03/17**	
8	Análisis marcos gobierno y buenas prácticas (COBIT, ITIL, ISOs)	3 days	Tue 07/03/17	Thu 09/03/17	5
9	Identificación áreas relevantes de control y objetivos asociados	2 days	Fri 10/03/17	Mon 13/03/17	8
10	Objetivos de Control definidos	0 days	Tue 14/03/17	Tue 14/03/17	9
11	**Auditar el entorno de Control de TI de “FastLoans S.A.”**	**19 days**	**Tue 14/03/17**	**Mon 10/04/17**	
12	Realizar un Entendimiento de TI en la entidad	2 days	Tue 14/03/17	Wed 15/03/17	9
13	Identificar los controles asociados al entorno de TI y relacionarlos con los objetivos de control	3 days	Thu 16/03/17	Mon 20/03/17	12
14	Evaluar el Diseño, Implementación y Efectividad operativa de esos controles	8 days	Tue 21/03/17	Thu 30/03/17	13
15	Identificar deficiencias, debilidad, mejoras a los controles evaluados	4 days	Fri 31/03/17	Wed 05/04/17	14
16	Evaluar el impacto de las deficiencias encontradas sobre la información que afecta a estados financieros	2 days	Thu 06/04/17	Fri 07/04/17	15
17	Resultados Evaluación del Diseño, Implementación y Efectividad de los Controles	0 days	Mon 10/04/17	Mon 10/04/17	16
18	**Publicar un Cuadro de Mando que represente los resultados de la Auditoría**	**60 days**	**Mon 06/03/17**	**Fri 26/05/17**	
19	Evaluar los requerimientos de los stakeholders	2 days	Mon 06/03/17	Tue 07/03/17	5
20	Definir los elementos necesarios del entorno en QlikSense (seguridad, escalabilidad, costes, usabilidad)	2 days	Wed 08/03/17	Thu 09/03/17	19
21	Diseñar los indicadores clave a incorporar que cubrirán los requerimientos	3 days	Mon 10/04/17	Wed 12/04/17	17;20
22	Evaluar diferentes soluciones BI en el mercado	2 days	Thu 13/04/17	Fri 14/04/17	19;20;21
23	Diseñar los modelos gráficos de representación de esos indicadores	5 days	Mon 17/04/17	Fri 21/04/17	22
24	Tratar los datos obtenidos de la Auditoría para su posterior carga	5 days	Mon 24/04/17	Fri 28/04/17	23
25	Implementar la solución en la Herramienta	20 days	Mon 01/05/17	Fri 26/05/17	24
26	Prototipo Funcional en la Herramienta	0 days	Mon 15/05/17	Mon 15/05/17	
27	Versión Final en la Herramienta	0 days	Fri 26/05/17	Fri 26/05/17	
28	Realización de la Entrega Final (Producto, Memoria, Presentación	15 days	Mon 22/05/17	Fri 09/06/17	
29	Entregable Final (Producto, Memoria, Presentación)	0 days	Mon 12/06/17	Mon 12/06/17	28

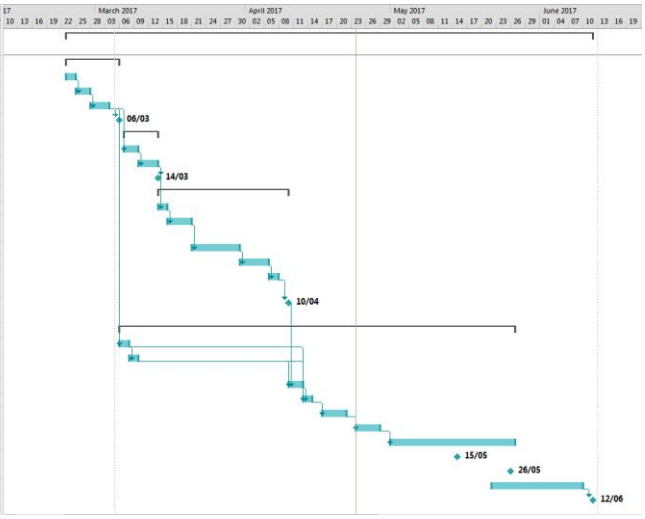

Figura 1. Diagrama Gantt tareas a realizar

Para obtener el detalle completo de las tareas del proyecto, consultar el ***capítulo Anexos, apartado 8.1***.

1.5 Breve sumario de productos obtenidos

La realización de las tareas contenidas en el punto anterior, darán lugar a los siguientes entregables/productos clave:

Fecha	Descripción hito
23/02/2017	Inicio del Proyecto
06/03/2017	Plan de Proyecto (PAC1)
14/03/2017	Objetivos de Control definidos (PAC2)
10/04/2017	Resultados de la Evaluación del Diseño, Implementación y Efectividad Operativa de los controles de FastLoans S.A. (PAC2)
08/05/2017	ETL y Modelado (PAC3)
15/05/2017	Prototipo Funcional del Cuadro de Mando
26/05/2017	Puesta en producción del Cuadro de Mando
12/06/2017	Entregable Final del Proyecto: Producto, Memoria y Presentación

1.6 Breve descripción de los otros capítulos de la memoria

Capítulo 1. Introducción
Definición del escenario, motivación y objetivos del proyecto. Se presenta el enfoque, el registro de interesados y la planificación con el detalle de tareas a realizar durante el ciclo de vida del proyecto.

Capítulo 2. Diseño y Definición de los Objetivos de Control
Análisis de buenas prácticas y definición del marco de objetivos de control que cubren los riesgos inherentes a los Sistemas de SI, en el ámbito de la información financiera.
Apartado inicial y clave del proyecto que permitirá establecer un entorno de control ideal que será utilizado como base en el resto de fases del proyecto.

Capítulo 3. Auditoría Entorno Control Caso Estudio.
Entendimiento y posterior auditoría de “FastLoans S.A.”, permitiendo evaluar el Diseño, Implementación y Efectividad operativa de su marco de control e identificar deficiencias y su impacto en la información sobre estados financieros.
Apartado donde se extraerán y generarán todos los datos, a partir de la auditoría, que se representarán en la siguiente fase del proyecto.

Capítulo 4. Diseño e Implementación de un Cuadro de Mando
Análisis de los requerimientos funcionales de los key stakeholders y de las restricciones y limitaciones del proyecto y diseño de los indicadores asociado.
Evaluación de las diferentes soluciones de Business Intelligence (BI en adelante) en el mercado en base a las necesidades recogidas.
Extracción, Transformación y Carga (ETL en adelante) de la información obtenida durante la auditoría.
Diseño e implementación del modelo de tablas en la herramienta de BI.

Desarrollo de los modelos gráficos y tratamiento de datos en un prototipo funcional y posterior formación a los usuarios.
Puesta en marcha del Cuadro de Mando.
Este último apartado, recoge todos los datos generados en capítulos anteriores para generar información útil a los stakeholders en forma de Cuadro de Mando.

Capítulo 5. Conclusión
Este capítulo recoge las lecciones aprendidas, la consecución o no de los objetivos planteados y las asunciones realizadas.

Capítulo 6. Glosario
Apartado que recoge la terminología técnica utilizada durante el ciclo de vida del proyecto.

Capítulo 7. Bibliografía
Se refleja toda la bibliografía empleada para la realización del proyecto: publicaciones, manuales, proveedores utilizados y websites consultados.

Capítulo 8. Anexos
En este último punto, se incluyen todos los documentos generados durante la ejecución del proyecto, necesarios en cada una de las fases donde se referencian.

2. Diseño y Definición de los Objetivos de Control

2.1 Contexto de Riesgos/Objetivos de Control

Los Sistemas de TI diseñados, implementados y explotados por diferentes entidades a lo largo del mundo, están sujetos a una serie de riesgos inherentes que deben ser gestionados convenientemente para mitigar o suprimir su impacto, de manera que no afecte a la información que tratan estos Sistemas y en última instancia, al propio negocio en sí mismo, cumpliendo los siguientes principios sobre la información:

- **Efectividad**: Información relevante y pertinente, proporcionada en forma oportuna, correcta, consistente y utilizable.
- **Eficiencia**: Se debe proveer información mediante un empleo óptimo de los recursos.
- **Confidencialidad**: Protección de la información sensible contra divulgación no autorizada.
- **Integridad**: Referido a la exactitud y completitud de la información, así como su validez acorde a las expectativas de la entidad.
- **Disponibilidad**: Accesibilidad a la información cuando sea necesario y almacenamiento de los recursos y sus capacidades.
- **Cumplimiento**: con las leyes, regulaciones y compromisos contractuales de la entidad.
- **Confiabilidad**: Información apropiada para la toma de decisiones por parte de la entidad.

Bajo este contexto, el primer objetivo de este proyecto será diseñar y definir un marco de objetivos de control, que ayude a entidades de todos los tamaños e ámbitos (comerciales, sin ánimo de lucro, sector público…) a generar una consciencia del riesgo de TI al que están sujetas y a partir de esta idea, poder desarrollar un proceso integrado y dinámico de control interno, que desarrolle un marco general con los objetivos a cubrir para mitigar estos riesgos.

Para las entidades, contar con un ambiente de control interno, ofrece una serie de ventajas tanto internas, como a clientes e inversores:

- Mayor compromiso por la integridad y los valores éticos.
- Mayor confianza en la supervisión efectuada.
- Mayor capacidad para identificar, analizar y responder a los riesgos y cambios del entorno, tanto de IT como de negocio.
- Mayor entendimiento sobre los controles en los sistemas, para determinar aquellos redundantes o ineficientes.

En este proyecto, no se van a detallar los objetivos, funciones, componentes ni las actividades detalladas del proceso de control interno, debido sobre todo a una serie de restricciones de tiempo, presupuesto y a que no es un objetivo principal del propio proyecto. En vez de ello, se

asumirá la existencia de ese ente, que colaborará durante la definición del marco de objetivos de control.

2.2 Estándares y Buenas Prácticas

Tal y como se adelantó en el apartado 1.3, para definir un marco de objetivos de control de TI, se utilizará como base COBIT (Control Objectives for Information Systems and related Technology) en su versión 5 frente a otros marcos debido a que es el resultado de una investigación con expertos a nivel mundial, desarrollado por ISACA (Information Systems Audit and Control Association) y ampliamente aceptado por el mercado.

Este modelo, a través de ISACA, se encarga de vincular las TI con prácticas de control, y de investigar, desarrollar, publicar y promover estas prácticas de manera que se utilicen de forma cotidiana por parte de las entidades en diferentes niveles (gerencia, auditoría, responsables de TI y usuarios finales).

Figura 2. Principios de COBIT 5
Fuente: COBIT® 5, Figura 2. © ISACA® Todos los derechos reservados

COBIT intenta englobar la totalidad de los recursos TI de las entidades:

- **Datos**: todos los objetos de información (interna y externa, estructurada o no, gráficas…)
- **Aplicaciones**: entendido como los sistemas de información, que integran procedimientos manuales y automáticos.
- **Tecnología**: hardware y software, sistemas operativos, sistemas de administración de bases de datos, de redes, telecomunicaciones…
- **Instalaciones** (físicas): incluye los recursos necesarios para alojar y dar soporte a los sistemas de información.
- **Recursos humanos**: habilidad, conciencia y productividad del personal para planear, adquirir, prestar servicios, dar soporte y monitorizar los sistemas de TI.

La estructura del modelo de objetivos de control propuesto por COBIT 5 se divide en 2 grandes dominios:

- **Gobierno**: Área donde se evalúan las necesidades de negocio para alinear las metas de TI con las de la Entidad. Establecen la dirección del área de TI a través de la priorización y la toma de decisiones, midiendo el rendimiento y cumplimiento de las políticas y procedimientos definidos.
- **Gestión**: Área encargada de planificar, construir, ejecutar y controlar las actividades definidas desde Gobierno para alcanzar las metas de la Entidad.

Estos dominios agrupan un total de 37 procesos, y estos últimos están formados por una serie de actividades unidas con el objetivo de lograr un determinado output, un resultado medible. En la siguiente imagen podemos observar la representación del marco propuesto:

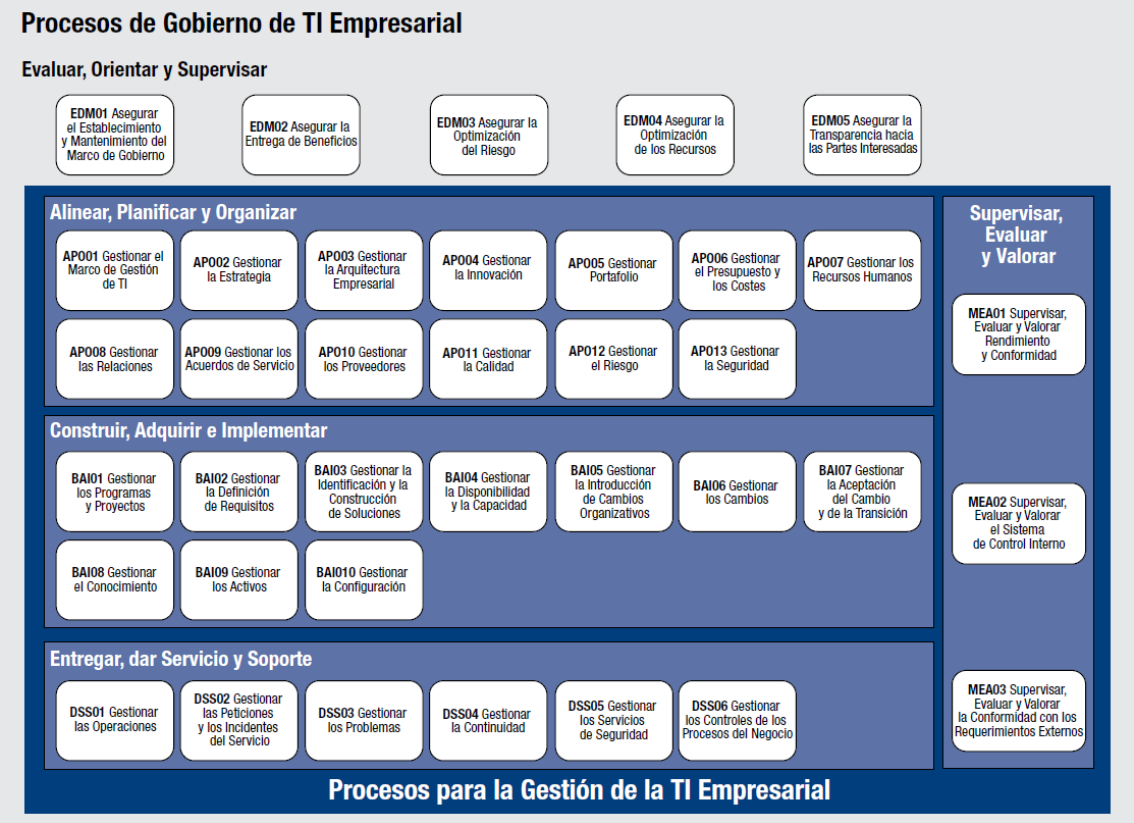

Figura 3. Procesos de COBIT 5
Fuente: COBIT® 5, Figura 16. © ISACA® Todos los derechos reservados

Una de las razones por las que COBIT está ampliamente extendido en el mercado es porque no trabaja de forma aislada para construir y actualizar su marco de control, sino que se nutre de numerosos estándares y normativas internacionales.

La siguiente imagen muestra la relativa coincidencia entre COBIT 5 y esas otras fuentes de conocimiento:

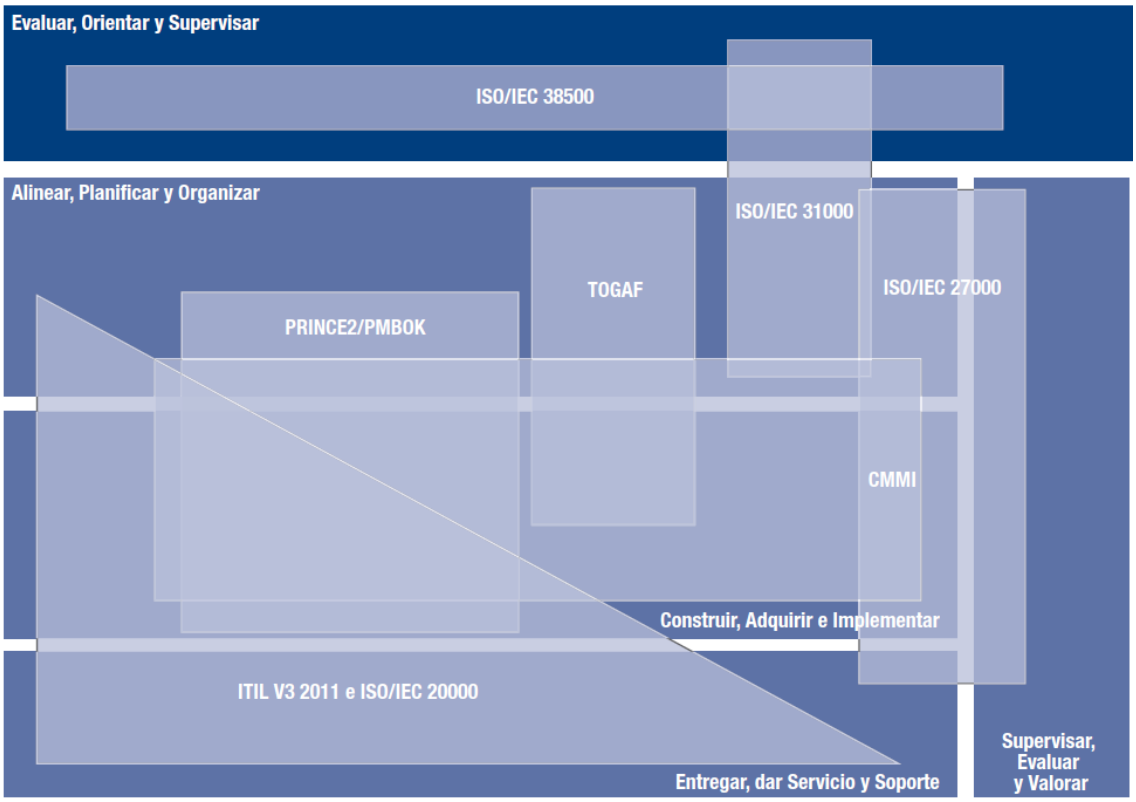

Figura 4. COBIT 5 vs estándares y buenas prácticas
Fuente: COBIT® 5, Figura 25. © ISACA® Todos los derechos reservados

2.3 Diseño adaptado del Marco de Riesgos/Objetivos de Control

El marco presentado sirve para conocer el escenario completo, la máxima expresión de control TI. Esta situación, rara vez es la más adecuada para todas las entidades, donde cada una de ellas debe organizar y plantear sus procesos de forma personalizada, en base a sus factores intrínsecos diferenciadores, como son sus dimensiones, tipo de negocio, personal especialista, proveedores…

En el contexto del proyecto actual, se ha adaptado y adecuado el marco presentado a la realidad del objeto del proyecto, donde se priorizan los procesos que pueden afectar directa e indirectamente a la información que afecta a los estados financieros de una Entidad, es decir, aquellos incorporados en el dominio de la Gestión, más alineados a ITIL e ISO 20000, en detrimento de los procesos de Gobierno y del ámbito de la Supervisión y evaluación, dando como resultado la siguiente tabla de Objetivos de Control de TI, dividida en las diferentes Áreas que engloban los procesos para la gestión de las TI:

Área	Componente / Riesgo	Objetivo de Control
Alinear, Planificar y Organizar	**Marco de Gestión de TI** Aclarar y mantener el gobierno de la misión y la visión corporativa de TI. Implementar y mantener mecanismos y autoridades para la gestión de la información y el uso de TI en la entidad para apoyar los objetivos de gobierno en consonancia con las políticas establecidas. *Riesgos asociados:* *Segregación de funciones incompatible/inexistente que comprometan las actividades de determinado personal clave, afectando a la información sobre estados financieros.* *Políticas/procedimientos inexistentes o inmaduros que provoquen que los usuarios no actúen acorde a sus responsabilidades.*	**APO01.01 Definir la estructura organizativa** Establecer una estructura organizativa interna y extensa que refleje las necesidades del negocio y las prioridades de TI. Implementar las estructuras de gestión requeridas (p. ej., comités) para permitir que la toma de decisiones se lleve a cabo de la forma más eficaz y eficiente posible.
		APO01.02 Establecer roles y responsabilidades Establecer, acordar y comunicar roles y responsabilidades del personal de TI, así como de otras partes interesadas con responsabilidades en las TI corporativas, que reflejen claramente las necesidades generales del negocio y los objetivos de TI, así como la autoridad, las responsabilidades y la rendición de cuentas del personal relevante.
		APO.01.03 Mantener el cumplimiento con las políticas y procedimientos Poner en marcha procedimientos para mantener el cumplimiento y medición del funcionamiento de las políticas; hacer cumplir las consecuencias del no cumplimiento o del desempeño inadecuado. Seguir las tendencias y el rendimiento del personal.
	Gestionar los Recursos Humanos Proporcionar un enfoque estructurado para garantizar una óptima estructuración, ubicación, capacidades de decisión y habilidades de los recursos humanos. Esto incluye la comunicación de las funciones y responsabilidades definidas, la formación y planes de desarrollo personal y las expectativas de desempeño, con el apoyo de gente competente y motivada. *Riesgos asociados:* *Personal no concienciado en el ámbito de seguridad que por desconocimiento/negligencia provoquen incidentes que afecten a la información contenida en los sistemas.* *Personal obsoleto o con permisos inadecuados que pongan en compromiso la integridad de la información.*	**APO02.01 Mantener las habilidades y competencias del personal** Definir y gestionar las habilidades y competencias necesarias del personal. Verificar regularmente que el personal tenga las competencias necesarias para cumplir con sus funciones sobre la base de su educación, formación y/o experiencia y verificar que estas competencias se mantienen, con programas de capacitación y certificación en su caso. Proporcionar a los empleados aprendizaje permanente y oportunidades para mantener sus conocimientos, habilidades y competencias al nivel requerido para conseguir las metas empresariales.
		APO02.02 Gestionar el personal contratado Asegurar que el personal contratado y los proveedores externos que apoyan a la empresa con capacidades de TI son añadidos, modificados o eliminados de los Sistemas en tiempo y forma.
	Gestionar la Seguridad Definir, operar y supervisar un sistema para la gestión de la seguridad de la información. *Riesgos asociados:* *Incidentes de la seguridad de la información no gestionados correctamente y que afecten a la información sobre estados financieros en la Entidad.*	**APO03.01 Establecer y mantener un SGSI** Establecer y mantener un Sistema de Gestión de Seguridad de la Información (SGSI) que proporcione un enfoque estándar, formal y continuo a la gestión de seguridad para la información, tecnología y procesos de negocio que esté alineados con los requerimientos de negocio y la gestión de seguridad en la empresa.

Construir, Adquirir e Implementar	**Gestionar los Programas y Proyectos** Gestionar todos los programas y proyectos del portafolio de inversiones de forma coordinada y en línea con la estrategia corporativa. Iniciar, planificar, controlar y ejecutar programas y proyectos y cerrarlos con una revisión post-implementación. *Riesgos asociados:* *Desarrollos, proyectos no gestionados adecuadamente, provocando que funcionalidades no autorizadas o comprometidas se trasladen al entorno productivo, afectando a la información financiera contenida en los sistemas.*	**BAI.01.01 Enfoque de programas y proyectos** Mantener un enfoque estándar y definido alineado al entorno de la entidad que cubra todo el ciclo de vida del producto.
		BAI.01.02 Planificar y aprobar programas y proyectos Identificar soluciones y realizar un estudio de viabilidad antes de la adquisición/desarrollo, aprobadas por un nivel apropiado de negocio y de IT.
		BAI.01.03 Gestionar el riesgo de los programas y proyectos Minimizar los riesgos específicos asociados con los programas y proyectos mediante un proceso pruebas (de desarrollo, infraestructura, funcionales por usuarios) y seguimiento de las mismas, para determinar si las funcionalidades están alineadas con los objetivos del programa/proyecto.
		BAI.01.04 Cerrar el programa y proyecto Llevar a cabo una revisión post-implantación para confirmar salidas y resultados, identificar lecciones aprendidas y desarrollar un plan de acción ante incidentes detectados.
	Gestionar los Cambios Gestionar todos los cambios de una forma controlada, incluyendo cambios estándar y de de emergencia en relación con los procesos de IT, aplicaciones e infraestructura. Incluye normas y procedimientos de cambio, análisis de impacto, priorización y autorización, cambios de emergencia, seguimiento, reporte, cierre y documentación. *Riesgos asociados:* *Cambios normales o de emergencia no gestionados adecuadamente, provocando que funcionalidades no autorizadas o comprometidas se trasladen al entorno productivo, afectando a la información financiera contenida en los sistemas.*	**BAI.02.01 Evaluar, priorizar y autorizar peticiones de cambio** Evaluar las peticiones de cambio para determinar su impacto en los procesos de negocio y los servicios TI. Asegurar que los cambios son registrados, priorizados, categorizados, analizados, autorizados, planificados y programados.
		BAI.02.02 Gestionar cambios de emergencia Gestionar los cambios de emergencia para minimizar su impacto y futuras incidencias, asegurando que está controlado y se realiza de forma segura. Verificar que son evaluados y autorizados una vez hecho el cambio.
		BAI.02.03 Gestionar la transición de los cambios Definir y establecer un entorno seguro de pruebas que refleje las características, capacidades, medidas de seguridad y cargas del entorno productivo, del que estará segregado. Los desarrolladores, también deberán tener restringido el acceso al entorno productivo.
		BAI.02.04 Pasar a Producción El paso a producción deberá estar controlado hasta obtener la aceptación del negocio e IT cuando sea necesairo.
Entregar, dar Servicio y Soporte	**Gestionar las Operaciones** Coordinar y ejecutar las actividades y los procedimientos operativos requeridos para entregar servicios de TI tanto internos como externalizados, incluyendo la ejecución de procedimientos operativos estándar predefinidos y las actividades de monitorización requeridas. *Riesgos asociados:* *Elementos hardware y software que podrían interrumpir el servicio normal debido a su obsolescencia, caducidad de licencias, capacidades inadecuadas o protección medioambiental insuficiente; afectando negativamente a la disponibilidad e integridad de la información que contienen. Ante la pérdida de alguno de estos elementos, el riesgo de no poder recuperar la información financiera contenida en ellos.*	**DSS.01.01 Monitorización de la Infraestructura** Establecer y mantener un modelo lógico de la infraestructura, activos y servicios y la forma de registrar los elementos de configuración (CIs del inglés, configuration items) y las relaciones entre estos activos, incluyendo jobs de sistema e interfaces.
		DSS.01.02 Gestionar el Entorno e Instalaciones Mantener las medidas para la protección contra factores ambientales. Instalar equipamiento y dispositivos especializados para supervisar y controlar el entorno; de manera que esté en línea con las leyes y regulaciones, requerimientos técnicos y de negocio y directrices de salud y seguridad en el trabajo.
		DSS.01.02 Asegurar los activos de información Asegurar que los activos de información sean salvaguardados y recuperables a través de los métodos aprobados, incluyendo la información en formato electrónico, en formato físico e información en tránsito.

	Gestionar Servicios de Seguridad Proteger la información de la empresa para mantener aceptable el nivel de riesgo de seguridad de la información de acuerdo con la política de seguridad. Establecer y mantener los roles de seguridad y privilegios de acceso de la información y realizar la supervisión de la seguridad. *Riesgos asociados:* *Accesos físicos y lógicos con medidas de seguridad inadecuadas o ineficientes, que permitan acceder/manipular a personal no autorizado a información sensible relacionada con los estados financieros.*	**DSS.02.01 Gestionar la identidad del usuario y el acceso lógico** Asegurar que todos los usuarios tengan derechos de acceso a la información de acuerdo con los requerimientos de las unidades de negocio a las que pertenecen, y coordinar con ellos las aprobaciones necesarias.
		DSS.02.02 Gestionar el acceso físico a los activos de TI Definir e implementar procedimientos para conceder,limitar y revocar acceso a locales, edificios y áreas deacuerdo con las necesidades del negocio, incluyendo emergencias y cualquier tipo de personal (interno, externo, temporal, visitante)
		DSS.02.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización Gestionar los roles de negocio, responsabilidades, niveles de autoridad y segregación de tareas necesarias para apoyar los objetivos del proceso de negocio. Realizar revisiones periódicas de los permisos y acciones de los usuarios, incluyendo los usuarios administradores.
	Gestionar las Peticiones e Incidentes de Servicio Proveer una respuesta oportuna y efectiva a las peticiones de usuario y la resolución de todo tipo de incidentes. Recuperar el servicio normal; registrar y completar las peticiones de usuario; y registrar, investigar, diagnosticar, escalar y resolver incidentes. *Riesgos asociados:* *Incidentes no detectados/no resueltos en tiempo y forma que interrumpan la prestación normal del Servicio, llegando a afectar a la información contenida en los sistemas.*	**DSS.03.01 Registrar, clasificar y priorizar peticiones e incidentes** Identificar, registrar y clasificar peticiones de servicio e incidentes, y asignar una prioridad según la criticidad del negocio y los acuerdos de nivel de servicio (SLAs).
		DSS.03.02 Investigar, diagnosticar y resolver incidentes Identificar y registrar síntomas de incidentes, determinar posibles causas y asignar recursos a su resolución. Solicitar y probar las soluciones identificadas y ejecutar acciones de recuperación para restaurar el servicio TI relacionado.
	Gestionar la Continuidad Establecer y mantener un plan para permitir al negocio y a TI responder a incidentes e interrupciones de servicio para la operación continua de los procesos críticos para el negocio y los servicios TI requeridos y mantener la disponibilidad de la información a un nivel aceptable para la empresa *Riesgos asociados:* *Identificación incorrecta/inexistente de los elementos críticos para el negocio, impidiendo o perjudicando, ante una situación de desastre su recuperación y la propia continuidad de la actividad del negocio.*	**DSS.04.01 Definir la política de continuidad del negocio, objetivos y alcance** Definir la política y alcance de continuidad de negocio alineada con los objetivos de negocio. Evaluar las opciones de gestión de la continuidad y escoger una estrategia viable y efectiva en coste, que pueda asegurar la continuidad y recuperación de la empresa frente a un desastre u otro incidente mayor o disrupción.
		DSS.04.02 Ejercitar, probar y revisar el plan de continuidad Probar el plan de continuidad periódicamente y compararlo con resultados predeterminados, para payudar a verificar que el plan funcionará tal y como se espera.

Figura 5. Marco de Riesgos/Objetivos de Control

3. Auditoría Entorno Control FastLoans S.A.

3.1 Entendimiento TI

Objetivo:

En el marco de la auditoría financiera realizada sobre FastLoans S.A. (en adelante FastLoans o la Entidad) para el ejercicio fiscal 2016, se ha llevado a cabo una revisión del entorno de control y riesgos asociados al uso de las tecnologías de la información, con el fin de realizar un entendimiento del nivel de control de los sistemas de información de la entidad para apoyar la auditoría financiera.

Descripción de la Entidad:

FastLoans S.A. es una startup que ofrece productos financieros a sus clientes a través de Internet; fundada en Barcelona en 2013, con sede en la propia ciudad y con oficinas en Madrid y Londrés, formada por más de 60 trabajadores de diversas nacionalidades (Francia, Suecia, España, Holanda, Austria, Rusia, Bulgaria,…) y más de 300M € en préstamos hasta el momento.

El servicio que ofrecen se basa en el concepto de micropréstamo online, que permiten a sus Clientes obtener dinero rápido, desde los 100 a los 500 €, con una documentación mínima obtenida directamente a través de un formulario online en Internet, sin necesidad de interactuar con una oficina física, y con una respuesta prácticamente inmediata. Este servicio presenta grandes ventajas basadas en la rapidez y sencillez de la tramitación, con respecto a las entidades financieras tradicionales.

Alcance:

El proyecto está dirigido a obtener un entendimiento de los elementos clave de las actividades de TI y cómo la entidad responde a los riesgos surgidos de la utilización de TI, incluyendo una breve descripción de las siguientes áreas de los sistemas de información:

- Alinear, Planificar y Organizar.
- Construir, Adquirir e Implementar
- Entregar, dar Soporte y Servicio.

Debido a que el proceso de Auditoria sobre estados financieros se ha apoyado en los procesos de IT y sus controles de aplicación, el alcance contemplado incluye la revisión del diseño, implementación y la efectividad operativa de los controles generales de IT inherentes a las áreas anteriormente citadas.

La revisión de los controles generales de IT se realizará sobre el sistema SAP, ya que da soporte al proceso de Contabilidad en la Entidad,

aplicación donde se introduce, transforma, procesa y almacena toda la información crítica que componen sus estados financieros.

Interesados Clave:

Se han mantenido una serie de reuniones con el personal clave para obtener el entendimiento y posterior evaluación del entorno de control IT en la Entidad:

Nombre	Puesto en la organización
Jorge Velilla	Director Proyecto Auditoría
Roberto Avilés	Responsable Proyecto Auditoría
Joan Ortega	FastLoans – Director TI
Álvaro Martínez	FastLoans – Responsable Proyectos TI
Paula Vidal	FastLoans – Responsable Seguridad TI
Ramón Cerezo	FastLoans – Responsable Infraestructuras TI

3.2 Mapa de Sistemas TI

Una vez realizada la reunión inicial con el Director de IT, se ha generado el mapa de Sistemas de TI utilizados en la Entidad. En el siguiente gráfico, se han detallado los diferentes procesos de negocio relevantes para la Auditoría, y qué Sistemas de TI intervienen en ellos, identificando las interfaces y relaciones entre ellos:

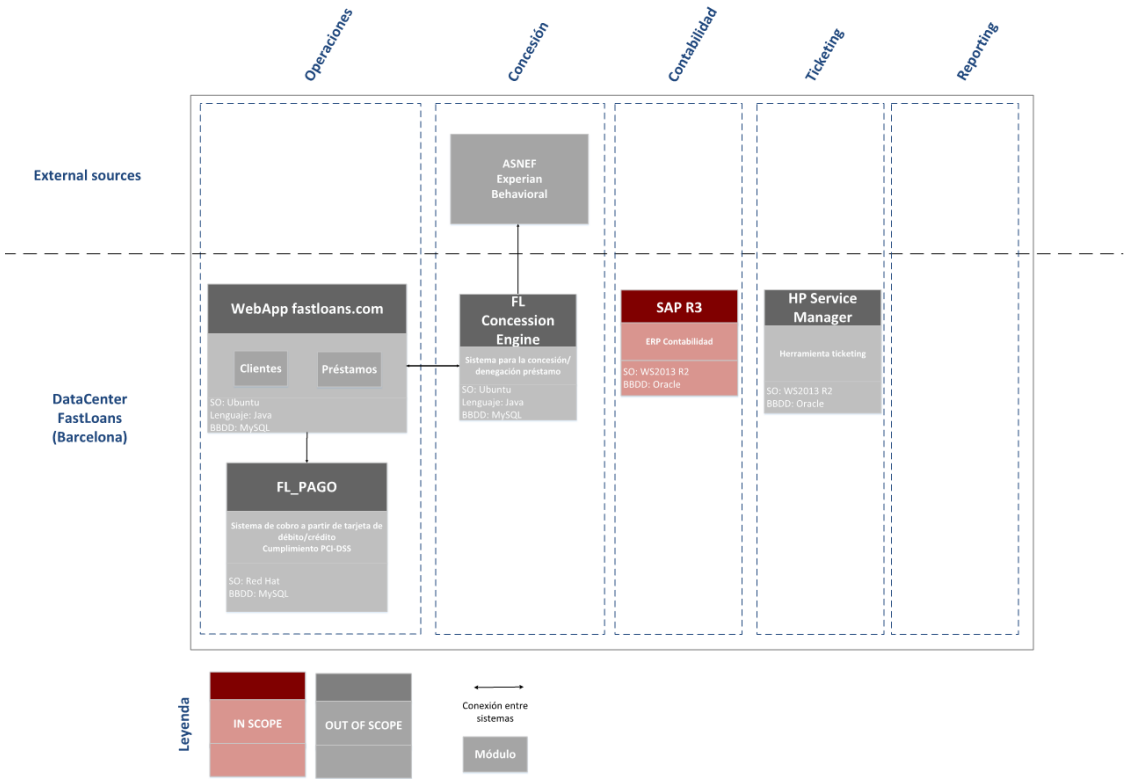

Figura 6. Mapa Sistemas TI FastLoans

En este mapa de sistemas se puede observar la operativa del negocio, desde el momento en que un Cliente accede a la web “fastloans.com” solicitando un micro préstamo, donde posteriormente el software de concesión evalúa la viabilidad de la operación, utilizando diferentes fuentes externas y por último, cómo este tipo de operaciones se reflejan en contabilidad, a través de SAP, que registra todos los apuntes contables sobre estas ventas, además de las diferentes compras de la entidad y otro tipo de actividades que afectan a los estados financieros de FastLoans.
Adicionalmente, se ha detectado que utilizan HP Service Manager como herramienta de ticketing, como soporte a los procesos de TI implantados en la entidad.

3.3 Identificación de Controles

Una vez completado este entendimiento inicial del entorno de TI, que ha permitido determinar el alcance del trabajo de Auditoría TI, se han mantenido reuniones con el resto del personal clave del Departamento de TI en la Entidad, para identificar su marco de controles, obteniendo la siguiente relación de riesgos-objetivos-controles:

Área	Componente / Riesgo	Objetivo de Control	¿Se ha encontrado un control relacionado con el Objetivo de Control?	Controles FastLoans
Alinear, Planificar y Organizar	**Marco de Gestión de TI**	**APO.01.01 Definir la estructura organizativa**	Sí	APO.01.01.01 Estructura orgánica FastLoans
		APO.01.02 Establecer roles y responsabilidades	Sí	APO.01.02.01 Segregación de Responsabilidades entre los Usuarios de TI y Negocio
		APO.01.03 Mantener el cumplimiento con las políticas y procedimientos	Sí	APO.01.03.01 Publicación de las políticas en la Intranet
				APO.01.03.02 Seguimiento de las políticas
	Gestionar los Recursos Humanos	**APO.02.01 Mantener las habilidades y competencias del personal**	No	No se ha detectado ningún control que cubra el riesgo sobre el personal no concienciado sobre las diferentes políticas implantadas en la Entidad.
		APO.02.02 Gestionar el personal contratado	Sí	APO.02.02.01 Altas, Bajas y Modificaciones de Usuario
		APO.02.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización	Sí	DSS.02.03.01 Identificación de usuarios
				DSS.02.03.02 Monitorización de accesos de usuarios
				DSS.02.03.03 Revisión permisos de usuario
	Gestionar la Seguridad	**APO.03.01 Establecer y mantener un SGSI**	Sí	APO.03.01.01 Política de Seguridad
				APO.03.01.02 Actualización de la política de seguridad
Construir, Adquirir e Implementar	**Gestionar los Programas y Proyectos**	**BAI.01.01 Enfoque de programas y proyectos**	Sí	BAI.01.01.01 Gestión de Proyectos
		BAI.01.02 Planificar y aprobar programas y proyectos	Sí	BAI.01.02.01 Análisis de viabilidad y aprobación
		BAI.01.03 Gestionar el riesgo de los programas y proyectos	Sí	BAI.01.03.01 Proceso de pruebas e implantación de Proyectos
		BAI.01.04 Cerrar el programa y proyecto	Sí	BAI.01.03.01 Revisión Post-implementación
	Gestionar los Cambios	**BAI.02.01 Evaluar, priorizar y autorizar peticiones de cambio**	Sí	BAI.02.01.01 Gestión de Cambios

		BAI.02.02 Gestionar cambios de emergencia	Sí	BAI.02.02.01 Gestión de Cambios de Emergencia
		BAI.02.03 Gestionar la transición de los cambios	Sí	BAI.02.03.01 Segregación de funciones en el paso a producción BAI.02.03.02 Separación de entornos
		BAI.02.04 Pasar a Producción	Sí	BAI02.04.01 Proceso de pruebas e implantación de los Cambios
Entregar, dar Servicio y Soporte	**Gestionar las Operaciones**	**DSS.01.01 Monitorización de la Infraestructura**	Sí	DSS.01.01.01 Monitorización de la infraestructura de IT
				DSS.01.01.02 Detección efectiva de problemas en los Batchs Jobs
		DSS.01.02 Gestionar el Entorno e Instalaciones	Sí	DSS.01.02.01 Medidas de Seguridad Física y Medioambiental en el CPD
		DSS.01.03 Asegurar los activos de información	Sí	DSS.01.03.01 Gestión de backups
				DSS.01.03.02 Pruebas de restauración
	Gestionar Servicios de Seguridad	**DSS.02.01 Gestionar la identidad del usuario y el acceso lógico**	Sí	DSS.02.01.01 Parametrización de contraseñas
		DSS.02.02 Gestionar el acceso físico a los activos de TI	Sí	DSS.02.02.01 Gestión y Control de Accesos al CPD
	Gestionar las Peticiones e Incidentes de Servicio	**DSS.03.01 Registrar, clasificar y priorizar peticiones e incidentes**	Sí	DSS.03.01.01 Gestión de Incidentes
		DSS.03.02 Investigar, diagnosticar y resolver incidentes	Sí	
	Gestionar la Continuidad	**DSS.04.01 Definir la política de continuidad del negocio, objetivos y alcance**	Sí	DSS.04.01.01 Plan de continuidad de negocio incluyendo DRP
		DSS.04.02 Ejercitar, probar y revisar el plan de continuidad	Sí	DSS.04.02.01 Pruebas de restauración del DRP

Figura 7. Relación de Objetivos de Control vs Controles FastLoans

3.3 Evaluación del Diseño, Implementación y Efectividad Operativa de los Controles de IT

Una vez identificado el marco de control en la entidad, se han mantenido entrevistas detalladas con cada uno de los interlocutores clave, para evaluar el diseño e implementación de estos controles durante el año de auditoría, 2016, y posteriormente se han obtenido evidencias para evaluar la efectividad operativa de los mismos.

Debido a la complejidad de la evaluación, no es posible presentarla directamente en la propia memoria del proyecto. Para entender y estudiar la auditoría realizada, se adjunta el documento completo con el trabajo realizado sobre los controles generales de TI en la entidad, para el sistema en el alcance, SAP. El detalle se puede encontrar en el ***capítulo Anexos, apartado 8.2***.

4. Diseño e Implementación de un Cuadro de Mando

4.1 Identificar los Requerimientos de los Stakeholders y del Entorno

Uno de los objetivos principales del proyecto, es el diseño e implementación de un Cuadro de Mando cuyo público objetivo son los key stakeholders identificados en las fases iniciales del proyecto, capítulo 1 apartado 1.4. Los interesados clave en este proyecto son:

- El Director de Proyecto de Auditoría: principalmente pretende obtener un medio para ofrecer valor añadido a sus Clientes a través de la presentación mediante un CM de los resultados de la Auditoría.
- El Director TI de la entidad auditada: Requiere conocer los resultados de la auditoría, pero además necesita saber en detalle por cada proceso auditado, las debilidades y áreas de mejoras en el mismo.

El CM debe cubrir una serie de requerimientos funcionales y no funcionales diferenciados, orientados a negocio y al entorno de TI.

Para identificar los requerimientos de negocio, se han mantenido una serie de reuniones con los interesados clave, identificando los siguientes requerimientos funcionales:

- Interpretar de manera ágil y eficaz los **resultados** de la **auditoría** realizada tanto de forma global como por área auditada.
- Identificar los posibles **riesgos** a los que la entidad está expuesta.
- Obtener información sobre cada uno de los **procesos de TI** evaluados, de manera que:
    - Permita evaluar el grado de **madurez** del mismo.
    - Permita medir su grado de **desempeño**.
    - Permita identificar **desviaciones** al proceso y **áreas de mejora**.

A nivel de entorno de TI, en base a la experiencia del equipo de proyecto y a las reuniones mantenidas, se han identificado los siguientes requerimientos no funcionales, ya introducidos en las fases iniciales como objetivos dentro del desarrollo del Cuadro de Mando:

- **Usabilidad**: Debe ser fácil de usar, con ayudas e interfaces intuitivas.
- **Accesibilidad**: Capacidad multidispositivo y multisistema para acceder desde cualquier ubicación conectada a Internet.
- **Seguridad**: Restricción de acceso para limitar entrada a usuarios clave autorizados.
- **Costes**: Relación calidad/precio óptima.
- **Escalabilidad**: Solución escalable y fácilmente adaptable a las cambiantes necesidades del negocio.
- **Manejo de Datos**: Capacidad para trabajar e integrar diferentes fuentes de datos.
- **Rendimiento**: El sistema debe soportar el manejo de un número elevado de datos durante su funcionamiento.

4.2 Indicadores Clave de Rendimiento (KPI)

Un indicador clave de rendimiento (KPI en adelante) es una métrica utilizada para cuantificar el desempeño de una serie de factores, actividades o procesos; relevantes para el éxito de una entidad.

Estos KPIs deben ser SMART, es decir:

- **Specific**: El objetivo debe ser lo más concreto posible.
- **Measurable**: Debe poder medirse, de manera que sea cuantificable.
- **Achievable**: Debe ser ambicioso y atractivo para los interesados y así lograr su involucración para su consecución.
- **Relevant**: Debe ser realista y alcanzable en base a las capacidades y recursos disponibles.
- **Timely**: Debe estar acotado en el tiempo, con un tiempo límite para su consecución.

En base a las reuniones mantenidas con los interesados clave del Departamento de TI de la entidad auditada, a los objetivos y requisitos funcionales a alcanzar, los siguientes KPIs formarán y serán representados en el Cuadro de Mando:

- A nivel general:
  - % de cumplimiento de la Auditoría Global con respecto al escenario ideal.
  - % de cumplimiento de la Auditoría por Áreas con respecto al escenario ideal.
  - Número de controles inefectivos con respecto al total y nivel de riesgo asociado.
  - Nivel de madurez de los procesos evaluados, en una escala del 0 al 5 conforme al modelo de madurez recomendado por COBIT.

- Por proceso auditado:
  - Gestión de Usuarios:
    - % de uso de usuarios genéricos y administradores con respecto al total de usuarios.
    - Grado de robustez en la complejidad de contraseñas.
    - % de desviaciones con respecto al total en la gestión de altas/bajas/modificaciones de usuario.
    - Número de accesos a investigar con respecto al total de accesos por parte de los usuarios (por ubicación y tiempo).

  - Gestión de Incidentes:
    - Volumetrías de incidentes y tiempos de resolución por prioridad y tipología (consulta, incidente, incidente generalizado).
    - % desviación de los tiempos de resolución en los incidentes en base a los Acuerdos de Nivel de Servicio (SLA) definidos.
    - % de incidencias no resueltas satisfactoriamente con respecto al total.

- Gestión de Cambios:
  - Volumetrías de cambios y tiempos de resolución por tipología (normales o de emergencia).
  - % de cambios no resueltos satisfactoriamente con respecto al total.
- Gestión de Proyectos:
  - % de desviación de los tiempos de ejecución de los proyectos con respecto al presupuestado.
  - % de proyectos no finalizados satisfactoriamente con respecto al total.

4.3 Evaluación Soluciones Business Intelligence

Las soluciones de Business Intelligence (BI en adelante) permiten diseñar e implementar CMs para la representación de los KPIs relevantes en las entidades. Estos CMs son usados por el público objetivo para acceder a los datos de los negocios y proporcionar reportes, análisis, visualizaciones y alertas; de manera que puedan tomar decisiones en base a la información presentada.

Actualmente el mercado dispone de multitud de herramientas de BI para cubrir estas necesidades, dificultando el poder reconocer qué plataforma es la más adecuada para los potenciales clientes. Por ello, en el ámbito del proyecto y contando con la limitación de recursos disponibles para realizar este estudio, se ha optado por utilizar un proveedor externo especializado en la evaluación de este tipo de herramientas, “Select Hub”.

A través de su amplia base de conocimiento, se ha evaluado un informe de evaluación de las principales herramientas del mercado (338 soluciones), obteniendo los siguientes resultados:

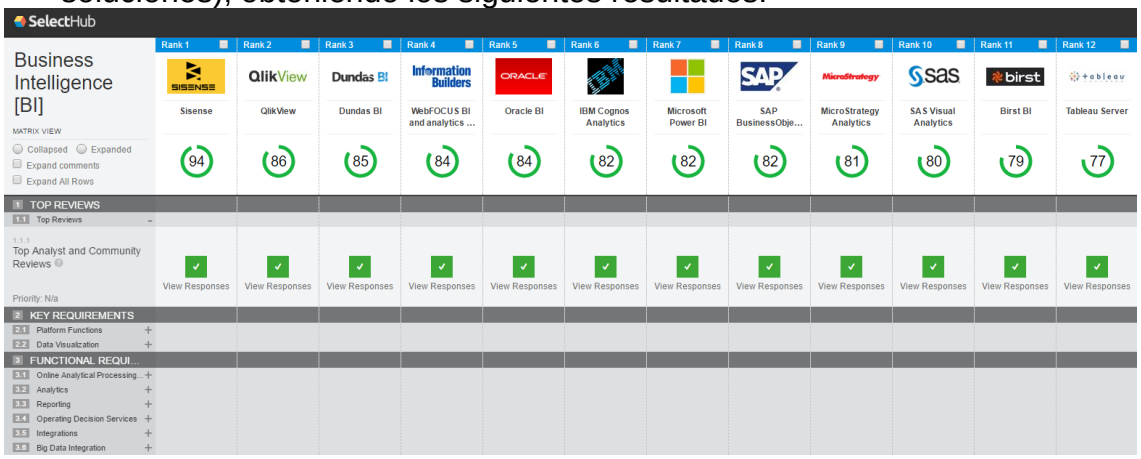

Figura 8. Estudio comparativo Soluciones de BI

Para obtener un mayor detalle, se puede consultar el informe completo proporcionado por el proveedor: https://app.selecthub.com/reports/580037b2deba89470db76486160c8f0e_9c902db7c92f95c582e2436c15d2272f

La herramienta escogida para el proyecto, es QlikView, en su variante Qlik Sense, que se encuentra en la 2ª posición del ranking. Se ha optado por esta opción, en lugar de la primera, debido a una serie de motivos adicionales al análisis cuantitativo realizado:

- El equipo desarrollador disponible tiene amplia experiencia con esta tecnología.
- Los costes iniciales de inversión inicial son inferiores a Sisense, incluyendo una modalidad gratuita.
- La comunidad de colaboradores de QlikView es muy amplia y activa.

4.4 Diseño y Arquitectura de la Solución BI

Una vez seleccionada la herramienta de BI a utilizar, el siguiente paso es definir la arquitectura de la solución, desde la identificación de los datos origen, la definición de los procesos de Extracción, Transformación y Carga en Qlik Sense y por últi mo el modelado en Qlik Sense, siguiendo este esquema:

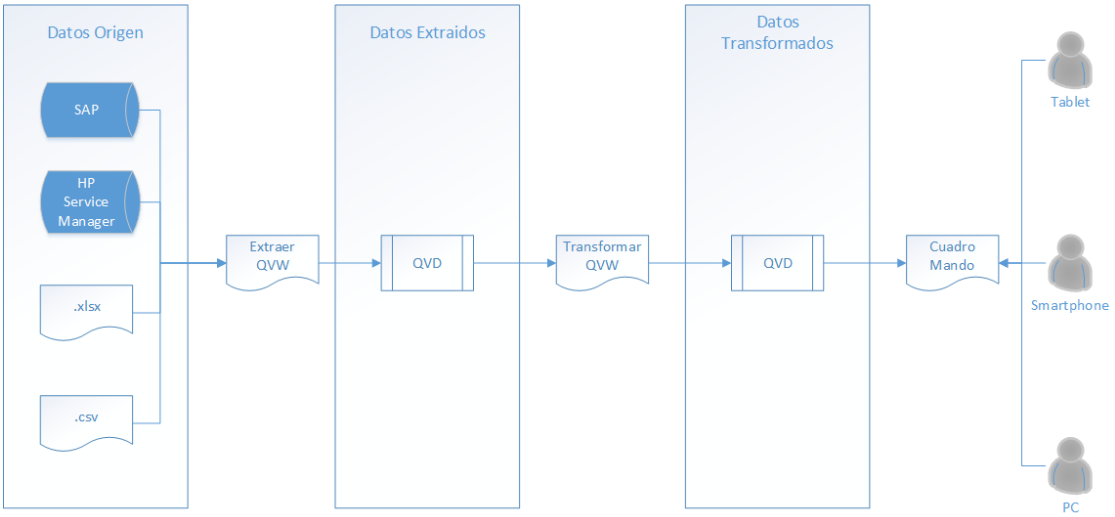

Figura 9. Arquitectura de la Solución BI

4.4.1 Orígenes de datos

Para realizar la Auditoría de los Sistemas de TI de Fastloans S.A., las evidencias proporcionadas por la entidad se extraen de varios de sus sistemas, identificados durante el Entendimiento de TI realizado en un punto anterior, concretamente:

- **SAP ERP**: Sistema de Planificación de Recursos (ERP) utilizado en la entidad para gestionar todos sus procesos clave de negocio; contabilidad, gestión de almacén, coste de producción, recursos humanos, gestión de ventas, gestión de compras; todo ello a través de una serie de los módulos que están conectados en una base de datos central común, basada en **Oracle 11g.** (*)

Las tablas utilizadas son las siguientes:

- V_USR_NAME: Listado completo de usuarios con nombre, apellidos e ID.
- RSUSR002: Listado de usuarios administradores.
- RSPARAM: Parámetros de configuración de SAP, entre los que se encuentra la parametrización de contraseñas.
- SM20: Extracto del log de auditoría con las conexiones por cada usuario, con el detalle de día y hora de conexión.

- **HP Service Manager**: Herramienta de ticketing para la gestión de los procesos clave de TI implantados en la entidad; gestión del Service Desk, gestión de peticiones, gestión de incidencias, gestión de cambios y gestión de proyectos. Este aplicativo también utiliza una base de datos **Oracle 11g.** (*)

  Las tablas utilizadas con las siguientes:

  - PROBSUMMARYM1: Tabla con la totalidad de incidentes y peticiones de altas/bajas/modificaciones de usuario registradas en HP Service Manager.
  - SLORESPONSEM1: Extracto de los cumplimientos e incumplimientos de SLAs por ticket.
  - CM3RM1: Tabla con la totalidad de cambios/proyectos registrados en HP Service Manager.

- **Resultado Auditoría**: La evaluación de los controles Generales de TI sobre SAP se ha realizado en una hoja de cálculo basada en Excel, con formato **.xlsx**.

  Los ficheros utilizados son los siguientes:

  - Auditoria_Controles_Generales_FastLoans_import: Resultado de la auditoría por área de control junto con el nivel de riesgo asociado.-> completar con nivel de riesgo
  - Madurez_Procesos: Evaluación del grado de madurez de los procesos auditados, gestión de usuarios, incidentes, cambios, proyectos y backups/recoveries.

  Para obtener un mayor detalle sobre los datos origen, consultar el ***capítulo 8 de Anexos, apartado 8.3. Orígenes de Datos***, que recoge de manera comprimida, todos los ficheros origen utilizados.

(*) Nota: Debido a una serie de restricciones de tiempo y presupuesto en el proyecto, no ha sido viable montar un laboratorio para recrear las bases de datos de SAP y HPSM. En vez de utilizar conectores ODBC y OLEDB en Qlik Sense, se ha simplificado el modelo para que la extracción de los datos se realice desde ficheros .xlsx.

4.4.2 Procesos ETL en Qlik Sense

Qlik Sense es capaz de construir un modelo de datos con procesos ETL (Extracción, Transformación y Carga) usando el lenguaje de script de la propia Herramienta, permitiendo realizar transformaciones complejas y crear un modelo de datos escalable.

Para la **Extracción** de los sistemas origen nombrados anteriormente es necesario utilizar en el script una serie de sentencias:

- **SELECT**: utilizada para seleccionar directamente de una tabla a partir de una fuente de datos por ODBC o proveedor OLE DB.
- **LOAD**: carga los campos directamente desde un archivo, una tabla previamente cargada en Qlik Sense, desde una web o desde una sentencia SELECT anterior.

Debido a la asunción en el proceso de extracción en el proyecto actual, básicamente se han utilizado sentencias LOAD para importar los datos al CM.

La fase de **Transformación** consiste en manipular y modificar los datos importados mediante funciones de script y de aplicar una serie de reglas para generar una nueva estructura, acorde a los KPIs a representar en el CM objetivo.

Las operaciones más frecuentes realizadas en el proyecto actual han sido:

- A nivel de resultados generales de la auditoría:
  - Agrupación de datos en base a áreas afectadas.
  - Traducción de valores codificados en base a niveles de riesgo.

- A nivel de Gestión de Usuarios:
  - Unir tablas de usuarios con roles (administrador).
  - Renombrar campos.
  - Calcular nuevos campos a partir de origen (genéricos).

- A nivel de Gestión de Incidentes:
  - Unir tabla de incidentes con incumplimientos de SLA.
  - Traducción de valores codificados (Códigos de resolución)
  - Validación de los datos (filtrado por incidencias).
  - Cálculos de fechas (tiempos de resolución).

- A nivel de Gestión de Cambios/Proyectos:
  - Traducción de valores codificados (Códigos de resolución y prioridades)
  - Validación de los datos (filtrado por tipo de cambio/proyecto).
  - Cálculos de fechas (tiempos de resolución y horas de trabajo).

La última fase de **Carga**, se debe planificar, programar y ejecutar el script para cargar el modelo de datos definido en la Herramienta.

El proyecto actual se recargará diariamente; ya que la planificación más restrictiva, parte de los datos extraídos tanto de SAP como de HPSM, que requieren de una actualización diaria para representar el estado de los procesos con una precisión aceptable y adecuada para los objetivos perseguidos. A nivel de los objetivos generales de la auditoría, la información de la propia evaluación su frecuencia es anual, ya que la auditoría externa contratada por la entidad se realiza con esa frecuencia.

Para obtener un mayor detalle sobre los procesos de ETL, consultar el ***capítulo 8 de Anexos, apartado 8.4. Scripting Qlik Sense***, que recoge el scripting realizado en Qlik Sense.

4.5 Construcción de Informes en Qlik Sense

Por último, una vez completadas las transformaciones sobre los datos origen, se ha trabajado en construir la parte gráfica y visual del Cuadro de Mando, de manera que represente los KPIs introducidos anteriormente.

Este CM se encuentra publicado en Internet en el Cloud de Qlik, y es accesible con invitación, sin necesidad de instalar ningún tipo de software adicional, a través de la siguiente URL:

https://eu.qlikcloud.com/view/58d63a1283ab010001266620

Para obtener un mayor detalle sobre el aspecto gráfico del CM, además del resumen del proyecto, se ha preparado una video presentación utilizando *Camtasia Studio*.
Debido al tamaño del archivo de video, se ha adjuntado directamente en el aula en el último entregable del proyecto.

5. Conclusiones

Una vez finalizado el proyecto, es posible analizar su desempeño a través de una serie de apartados que trataremos a continuación:

- **Consecución de objetivos y lecciones aprendidas:**
  El proyecto se ha construido en base a 3 objetivos principales, que se han logrado de manera efectiva:
  - En primer lugar, la creación de un marco de objetivos de control, que ha permitido conocer los riesgos inherentes en los Sistemas de TI y cómo mitigarlos.
  - A continuación, la realización de una Auditoría sobre un caso de estudio ficticio ha permitido obtener un conocimiento de cómo evaluar un marco de controles de TI en un entidad.
  - Por último, la representación de los resultados de la Auditoría y el desempeño de los procesos auditados a través de un Cuadro de Mando ha permitido capacitar al interesado para diseñar una serie de KPIs relevantes para el negocio, además de otorgar el conocimiento para representarlos a través de Qlik Sense.

- **Planificación del proyecto:**
  El calendario del proyecto y los hitos planteados inicialmente han sido cumplidos sin desviaciones observadas durante todo el ciclo de vida del proyecto.
  El único apartado cuyo coste ha sido superior al planificado fue la generación de datos ficticios que poblasen las diferentes fuentes de datos utilizadas. A través de un esfuerzo puntual del equipo de desarrollo, ha sido posible cumplir con los timings en esa fase.

- **Asunciones y simplificaciones:**
  Como se ha indicado en el apartado “4.4.2 Procesos ETL en Qlik Sense”, se han realizado una serie de asunciones y simplificaciones debido al escenario en el que se encontraba el propio proyecto, con una serie de restricciones de tiempo y presupuesto.

  Principalmente ha consistido en simplificar la conexión con las diferentes fuentes de datos, en vez de utilizar las bases de datos propias de HPSM y SAP, se ha extraído el contenido de sus tablas en ficheros de extensión .xlsx.

  Como línea de trabajo futura, sería viable implementar estas conexiones directamente contando con un laboratorio de pruebas y las licencias necesarias para recrear el escenario.

6. Glosario

Business Continuity Plan (BCP): el Plan de Continuidad del Negocio indica cómo una organización debe recuperar y restaurar sus funciones críticas parcialmente o totalmente interrumpidas dentro de un tiempo predeterminado después de una interrupción no deseada o desastre.

Change Advisory Board (CAB)/ Emergency Change Advisory Board (ECAB):
El Comité asesor de Cambios / Cambios de Emergencia está formado por un grupo de personas que asesora al Gerente de Cambio en la evaluación, priorización y programación de Cambios/Cambios de Emergencia. Generalmente está formado por representantes de todas las áreas dentro del Departamento de TI, el negocio y terceros tales como proveedores.

COBIT: Objetivos de Control para Información y Tecnologías Relacionadas. Marco de mejores prácticas, dirigida al control y supervisión de tecnología de la información (TI), publicada y mantenida por ISACA.

Control: Políticas, procedimientos, prácticas y estructuras organizacionales para proporcionar seguridad razonable de que los objetivos organizacionales se alcanzarán y que los eventos no deseados se evitarán o detectarán y corregirán.

Control Interno: conjunto de planes, principios, normas, procedimientos y mecanismos encargados de verificar y evaluar todas la actividades y operaciones desarrolladas en la organización, así como también la forma como se administra la información y los recursos, y si dicha gestión va acorde a las políticas trazadas por la dirección y a su vez, sujeta a las normativas vigentes.

Disaster Recovery Plan (DRP): el Plan de Recuperación ante Desastres es un proceso, normalmente incluido en el BCP, de recuperación que cubre los datos, hardware y software crítico, para que un negocio pueda continuar sus operaciones en caso de la ocurrencia de un desastre.

Configuration Item (CI): un Elemento de Configuración en la gestión de configuración de una entidad corresponde a cualquier tipo de componente que requiera ser controlado por la propia entidad por su valor clave en la misma.

Objetivo de control: Una declaración de que el resultado o propósito deseado se alcanzará al implantar mecanismos de control en una actividad particular de tecnología de información.

Proceso: secuencia de actividades dispuesta con algún tipo de lógica que se enfoca en lograr algún resultado específico.

Stakeholders/interesados: los empleados, los clientes, los proveedores de bienes y servicios son afectados o pueden ser afectados por las actividades de una entidad.

Riesgo: es la vulnerabilidad ante un potencial perjuicio o daño para las unidades, personas, organizaciones o entidades

7. Bibliografía

- **COBIT® 5:**
  ISBN 978-1-60420-282-3
  © 2012 ISACA. Todos los derechos reservados. Para pautas de uso, ver *www.isaca.org/COBITuse*

- **COBIT® 5. Procesos Catalizadores:**
  ISBN 978-1-60420-285-4
  © 2012 ISACA. Todos los derechos reservados. Para pautas de uso, ver *www.isaca.org/COBITuse*

- **SelectHub:**
  Proveedor de Selección de Software.
  https://app.selecthub.com/reports/580037b2deba89470db76486160c8f0e_9c902db7c92f95c582e2436c15d2272f
  Visitada el 29/04/2017

- **Manual de usuario Qlik Sense:**
  https://help.qlik.com
  Visitada durante Mayo/Junio 2017

- **Comunidad QlikView:**
  https://community.qlik.com/
  Visitada durante Mayo/Junio 2017

- **Esquema de Base de Datos HP Service Manager**
  http://helpfiles.intactcloud.com/SM/9.31/SM9.31_OnlineHelp/Content/Resources/PDF/SM_ERDs.pdf
  Visitada durante Mayo/Junio 2017

- **Camtasia Studio:**
  Software para la captura y edición de video
  http://discover.techsmith.com/camtasia-brand-desktop/
  Visitada durante Mayo/Junio 2017

8. Anexos

8.1 Diagrama de Gantt del Proyecto:

8.1.Planificación_Proyecto.mpp

8.2 Auditoría TI sobre los Controles Generales de SAP en FastLoans:

8.2.Auditoria_Controles_Generales_Fast

8.3 Orígenes de Datos:

8.3.Origenes_Datos.zip

8.4 Scripting Qlik Sense:

8.4.Main.txt

8.4.Extractions.txt

8.4.Transformations.txt