



Universidad Nacional Mayor de San Marcos

Universidad del Perú. Decana de América

Facultad de Ingeniería de Sistemas e Informática

Escuela Profesional de Ingeniería de Sistemas

**Implementación de dispositivos criptográficos para
asegurar la disponibilidad de canales que usan tarjetas
de débito en una entidad financiera**

TRABAJO DE SUFICIENCIA PROFESIONAL

Para optar el Título Profesional de Ingeniera de Sistemas

AUTOR

Fiorella Alessandra BENADUCCI ZAVALA

ASESOR

Víctor Hugo BUSTAMANTE OLIVERA

Lima, Perú

2022



Reconocimiento - No Comercial - Compartir Igual - Sin restricciones adicionales

<https://creativecommons.org/licenses/by-nc-sa/4.0/>

Usted puede distribuir, remezclar, retocar, y crear a partir del documento original de modo no comercial, siempre y cuando se dé crédito al autor del documento y se licencien las nuevas creaciones bajo las mismas condiciones. No se permite aplicar términos legales o medidas tecnológicas que restrinjan legalmente a otros a hacer cualquier cosa que permita esta licencia.

Referencia bibliográfica

Benaducci, F. (2022). *Implementación de dispositivos criptográficos para asegurar la disponibilidad de canales que usan tarjetas de débito en una entidad financiera*. [Trabajo de suficiencia profesional de pregrado, Universidad Nacional Mayor de San Marcos, Facultad de Ingeniería de Sistemas e Informática, Escuela Profesional de Ingeniería de Sistemas]. Repositorio institucional Cybertesis UNMSM.

Metadatos complementarios

Datos de autor	
Nombres y apellidos	IORELLA ALESSANDRA BENADUCCI ZAVALA
Tipo de documento de identidad	DNI
Número de documento de identidad	70901291
URL de ORCID	https://orcid.org/0000-0002-9045-9995
Datos de asesor	
Nombres y apellidos	Víctor HugoBustamante Olivera
Tipo de documento de identidad	DNI
Número de documento de identidad	25655590
URL de ORCID	https://orcid.org/0000-0001-8805-9629
Datos del jurado	
Presidente del jurado	
Nombres y apellidos	Jorge Raúl Díaz Muñante
Tipo de documento	DNI
Número de documento de identidad	07216161
Miembro del jurado 1	
Nombres y apellidos	Mario AgustínHuapaya Chumpitaz
Tipo de documento	DNI
Número de documento de identidad	15386891
Datos de investigación	
Línea de investigación	No aplica
Grupo de investigación	No aplica
Agencia de financiamiento	Sin financiamiento
Ubicación geográfica de la investigación	País: Perú Departamento: Lima Provincia: Lima Distrito: Cercado de Lima

	Jr. Carlos Amezaga No. 375 Universidad Nacional Mayor de San Marcos Latitud: -12.0564232 Longitud: -77.0843327
Año o rango de años en que se realizó la investigación	2022
URL de disciplinas OCDE	2.02.04 -- Ingeniería de sistemas y comunicaciones https://purl.org/pe-repo/ocde/ford#2.02.04



UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA
Escuela Profesional de Ingeniería de Sistemas

Acta Virtual de Sustentación
del Trabajo de Suficiencia Profesional

Siendo las 20:00 horas del día 16 de agosto del año 2022, se reunieron virtualmente los docentes designados como Miembros de Jurado del Trabajo de Suficiencia Profesional, presidido por el Mg. Díaz Muñante Jorge Raúl (Presidente), Mg. Huapaya Chumpitaz Mario Agustín (Miembro) y el Lic. Bustamante Olivera Víctor Hugo (Miembro Asesor), usando la plataforma Meet (<https://meet.google.com/gdy-fkfy-adv>), para la sustentación virtual del Trabajo de Suficiencia Profesional intitulado: **“IMPLEMENTACIÓN DE DISPOSITIVOS CRIPTOGRÁFICOS PARA ASEGURAR LA DISPONIBILIDAD DE CANALES QUE USAN TARJETAS DE DÉBITO EN UNA ENTIDAD FINANCIERA”**, por la Bachiller **Benaducci Zavala Fiorella Alessandra**; para obtener el Título Profesional de Ingeniera de Sistemas.

Acto seguido de la exposición del Trabajo de Suficiencia Profesional, el Presidente invitó a la Bachiller a dar las respuestas a las preguntas establecidas por los miembros del Jurado.

La Bachiller en el curso de sus intervenciones demostró pleno dominio del tema, al responder con acierto y fluidez a las observaciones y preguntas formuladas por los señores miembros del Jurado.

Finalmente habiéndose efectuado la calificación correspondiente por los miembros del Jurado, la Bachiller obtuvo la nota de **17(DIECISIETE)**.

A continuación el Presidente de Jurados el Mg. Díaz Muñante Jorge Raúl, declara a la Bachiller **Ingeniera de Sistemas**.

Siendo las 20:58 horas, se levantó la sesión.

Presidente

Mg. Díaz Muñante Jorge Raúl

Miembro

Mg. Huapaya Chumpitaz Mario Agustín

Miembro Asesor

Lic. Bustamante Olivera Víctor Hugo



UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
Universidad del Perú, DECANA DE AMÉRICA
FACULTAD DE INGENIERIA DE SISTEMAS E INFORMATICA
Escuela Profesional de Ingeniería de Sistemas

INFORME DE EVALUACIÓN DE ORIGINALIDAD

1. Facultad de Ingeniería de Sistemas e Informática
 2. Escuela Profesional de Ingeniería de Sistemas
 3. Autoridad académica que emite el informe de originalidad
Directora(e) de la EPIS
 4. Apellidos y Nombres de la autoridad académica
Dra. Luzmila E. Pró Concepción
 5. Operador del programa informático de similitudes
Dra. Luzmila E. Pró Concepción
 6. Documento evaluado
Título de pregrado: "Implementación de dispositivos criptográficos para asegurar la disponibilidad de canales que usan tarjetas de débito en una entidad financiera"
 7. Autor del documento
Bach. Benaducci Zavala, Fiorella Alessandra
 8. Fecha de recepción del documento **17/09/2022**
 9. Fecha de aplicación del programa informático de similitudes **17/09/2022**
 10. Software utilizado
 - Turnitin
 11. Configuración del programa detector de similitudes
 - Excluye textos entrecomillados
 - Excluye bibliografía
 - Excluye cadenas menores a 40 palabras
 12. Porcentaje de similitudes según programa detector de similitudes **6 (seis)%**
 13. Fuentes originales de las similitudes encontradas
Se adjunta en el anexo 1
 14. Observaciones
-
15. Calificación de originalidad
 - Documento cumple criterios de originalidad, sin observaciones ☒
 - Documento cumple criterios de originalidad, con observaciones ☐
 - Documento no cumple criterios de originalidad ☐
 16. Fecha de informe **18/09/2022**



Firmado digitalmente por PRO
CONCEPCION Luzmila Elisa FAU
20148092282 soft
Motivo: Soy el autor del documento
Fecha: 14.11.2022 12:59:13 -05:00

Firma de evaluador
Dra. Luzmila E. Pró Concepción
Directora (e) de la EPIS



UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
Universidad del Perú, DECANA DE AMÉRICA
FACULTAD DE INGENIERIA DE SISTEMAS E INFORMATICA
Escuela Profesional de Ingeniería de Sistemas

ANEXO 1

Fuentes originales de las similitudes encontradas

- 1. hdl.handle.net: 4%**
- 2. repositorioacademico.upc.edu.pe: 1%**
- 3. vibdoc.com: <1%**
- 4. repositorio.ug.edu.ec: <1%**
- 5. repositorio.puce.edu.ec: <1%**



UNMSM

Firmado digitalmente por PRO
CONCEPCION Luzmila Elisa FAU
20148092282 soft
Motivo: Soy el autor del documento
Fecha: 14.11.2022 12:58:51 -05:00

Firma de evaluador
Dra. Luzmila E. Pró Concepción
Directora (e) de la EPIS

DEDICATORIA

A mis padres y a mi hermana, quienes han confiado en mí en cada paso que he dado a lo largo de mi vida profesional y académica, siendo ellos mi principal soporte.

AGRADECIMIENTOS

Agradezco a quienes me acompañaron durante la elaboración del presente informe, especialmente a mi familia y amigos, ya que fueron un apoyo fundamental en cada momento más allá de lo académico.

También a mis colegas y compañeros, ya que al compartir experiencias, conocimientos y aptitudes a lo largo de mi vida laboral y académica influyeron para que sea la profesional en la que me he convertido.

Y por último, agradezco a mis jefes por compartir su experiencia, por la confianza depositada en mí y el apoyo constante ante los diversos retos a los cuales me enfrento.

UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA
ESCUELA PROFESIONAL DE INGENIERÍA DE INGENIERÍA DE SISTEMAS
Implementación de dispositivos criptográficos para asegurar la disponibilidad de canales que usan tarjetas de débito en una entidad financiera

Autora: Benaducci Zavala, Fiorella Alessandra
Asesor: Bustamante Olivera, Víctor Hugo
Título: Trabajo de Suficiencia Profesional para optar por el Título Profesional de Ingeniera de Sistemas
Fecha: Agosto del 2022

RESUMEN

El presente informe de suficiencia profesional describe la implementación de dispositivos criptográficos para el aseguramiento de la disponibilidad de canales que usan tarjetas de débito de una entidad financiera. La versión que se encontraba en funcionamiento presentaría el cese de soporte de parte del fabricante en los siguientes meses; ante ello, se planteó el cambio a una nueva versión y también de la arquitectura para permitir la alta disponibilidad.

El marco metodológico que se utilizó para llevar a cabo el proyecto es el estándar de Gestión de Proyectos del PMI, basado en la guía PMBOK, que permitió manejar aspectos relacionados a su implementación tales como recursos, costos, proveedores involucrados, cronograma, hitos de cumplimiento y otras características.

Tras la implementación del proyecto, se mejoró la escalabilidad del uso de canales alternativos y se establecieron equipos con mejores prestaciones técnicas que permiten el cumplimiento de nuevos estándares de seguridad además de asegurar la continuidad operativa para las actualizaciones de versiones de software.

Palabras claves: HSM, balanceador de carga, alta disponibilidad, seguridad, PMBOK.

MAJOR NATIONAL UNIVERSITY OF SAN MARCOS
FACULTY OF SYSTEMS AND INFORMATICS ENGINEERING
PROFESSIONAL SCHOOL OF SYSTEMS ENGINEERING

**Implementation of cryptographic devices to ensure the availability of channels
using debit cards in a financial institution**

Author: Benaducci Zavala, Fiorella Alessandra
Advisor: Bustamante Olivera, Víctor Hugo
Title: Professional Sufficiency Work to opt for the Professional Title of Systems Engineer
Date: August 2022

ABSTRACT

This professional sufficiency report describes the implementation of cryptographic devices to ensure the availability of channels that use debit cards of a financial institution. The version that was in operation would be discontinued by the manufacturer in the following months; therefore, a change to a new version was proposed, as well as a change in the architecture to allow high availability.

The methodological framework used to carry out the project is the PMI Project Management standard, based on the PMBOK Guide, which allowed managing aspects related to its implementation such as resources, costs, suppliers involved, schedule, compliance milestones and other characteristics.

After the implementation of the project, the scalability of the use of alternative channels was improved and equipment with better technical performance was established, allowing compliance with new security standards and ensuring operational continuity for software version upgrades

Key words: HSM, load balancer, high-availability, security, PMBOK

TABLA DE CONTENIDO

DEDICATORIA.....	iii
AGRADECIMIENTOS	iv
RESUMEN	v
ABSTRACT	vi
TABLA DE FIGURAS	ix
TABLA DE TABLAS	x
INTRODUCCIÓN	1
CAPÍTULO I: TRAYECTORIA PROFESIONAL.....	3
1.1 Presentación profesional.....	3
1.2 Formación académica.....	3
1.3 Experiencia profesional.....	4
CAPÍTULO II-CONTEXTO EN EL QUE SE DESARROLLA LA EXPERIENCIA	8
2.1 Empresa – Actividad que realiza.....	8
2.2 Visión	8
2.3 Misión.....	8
2.4 Organización de la empresa	8
2.5 Área, cargo y funciones desempeñadas	9
2.6 Experiencia profesional realizada en la Organización.....	10
CAPÍTULO III - ACTIVIDADES DESARROLLADAS	12
3.1 Situación Problemática	12
3.1.1 Definición del problema.....	12
3.2 Solución	12
3.2.1 Objetivos.....	12
3.2.2 Alcance	13
3.2.3 Etapas y metodología	13

3.2.4 Fundamentos utilizados	15
3.2.5 Implementación de las áreas, procesos, sistemas y buenas prácticas.....	31
3.3 Evaluación	56
3.3.1 Evaluación económica / Evaluación Costo-Beneficio.....	56
3.3.2 Interpretación del VAN y del TIR.....	58
CAPÍTULO IV. REFLEXIÓN CRÍTICA DE LA EXPERIENCIA	60
CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES	61
5.1 Conclusiones.....	61
5.2 Recomendaciones.....	63
5.3 Fuentes de información.....	64
5.4 Glosario.....	66

TABLA DE FIGURAS

<i>Figura 1:</i> Organigrama de la entidad financiera	9
<i>Figura 2:</i> Áreas de Riesgos.....	9
<i>Figura 3:</i> Tipos de HSM	17
<i>Figura 4:</i> Ciclo de vida de llave criptográfica	19
<i>Figura 5:</i> Esquemas de Organización del Mercado de Tarjetas de Pago de Cuatro partes	23
<i>Figura 6:</i> Grupos de procesos de la Dirección de Proyectos.....	25
<i>Figura 7:</i> Grupos de procesos de PMBOK	26
<i>Figura 8:</i> Balanceador de carga	27
<i>Figura 9:</i> Cronograma macro	33
<i>Figura 10:</i> Ficha del proyecto	34
<i>Figura 11:</i> Diagrama de arquitectura AS-IS referencial.....	37
<i>Figura 12:</i> Diagrama de arquitectura TO-BE referencial	37
<i>Figura 13:</i> Cronograma macro actualizado	38
<i>Figura 14:</i> Diagrama de arquitectura Desarrollo.....	41
<i>Figura 15:</i> Imagen referencial de la plataforma F5.....	42
<i>Figura 16:</i> Cronograma por hitos para el Pase a Producción.....	46
<i>Figura 17:</i> Ficha referencial del plan de pase a Producción.....	48
<i>Figura 18:</i> Cronograma de evaluación de riesgos.....	52
<i>Figura 19:</i> Plantilla de avance de proyecto	53
<i>Figura 20:</i> Ficha de control de cambios	54
<i>Figura 21:</i> Ficha de cierre de proyecto.....	55
<i>Figura 22:</i> Comparación del rendimiento por segundo (Nivel mínimo).....	57
<i>Figura 23:</i> Comparación del rendimiento por segundo (Nivel máximo)	57
<i>Figura 24:</i> Transacciones con posibilidad a generar reclamos.....	59
<i>Figura 25:</i> Pagos a equipo de Atención de Reclamos.....	59
<i>Figura 26:</i> VAN y TIR	59

TABLA DE TABLAS

<i>Tabla 1:</i> Formación académica profesional.....	3
<i>Tabla 2:</i> Idiomas.....	3
<i>Tabla 3:</i> Cursos	3
<i>Tabla 4:</i> Especialista de Seguridad de la Información.....	4
<i>Tabla 5:</i> Analista Senior de Seguridad de la Información.....	5
<i>Tabla 6:</i> Analista de Seguridad de la Información	6
<i>Tabla 7:</i> Analista de Seguridad de la Información - Freelance	6
<i>Tabla 8:</i> Practicante de Seguridad Informática.....	7
<i>Tabla 9:</i> Área, cargo y funciones desempeñadas	9
<i>Tabla 10:</i> Definiciones.....	15
<i>Tabla 11:</i> Cuadro comparativo de tipos de HSM.....	17
<i>Tabla 12:</i> Uso del HSM	21
<i>Tabla 13:</i> Fases y entregables	31
<i>Tabla 14:</i> Categorías del presupuesto estimado del proyecto.....	32
<i>Tabla 15:</i> Requerimientos del proyecto.....	33
<i>Tabla 16:</i> Distribución de equipos	35
<i>Tabla 17:</i> Roles participantes del proyecto	35
<i>Tabla 18:</i> Cronograma detallado por hitos	38
<i>Tabla 19:</i> Presupuesto detallado.....	39
<i>Tabla 20:</i> Riesgos identificados durante la definición del alcance y planes de acción.....	40
<i>Tabla 21:</i> Aplicaciones integradas al HSM.....	41
<i>Tabla 22:</i> Configuración de virtual server en F5 de Desarrollo.....	43
<i>Tabla 23:</i> Configuración de política virtual server en F5 de Desarrollo	43
<i>Tabla 24:</i> Cronograma de actividades Desarrollo	44
<i>Tabla 25:</i> Configuración de virtual server en F5 de Calidad.....	44
<i>Tabla 26:</i> Configuración de política virtual server en F5 de Calidad	44
<i>Tabla 27:</i> Cronograma de actividades de Certificación	45
<i>Tabla 28:</i> Cronograma de pase a producción	45
<i>Tabla 29:</i> Configuración de virtual server en F5 de Producción	46
<i>Tabla 30:</i> Configuración de política virtual server en F5 de Producción.....	47
<i>Tabla 31:</i> Ficha de pase a producción (Contingencia)	50
<i>Tabla 32:</i> Matriz de riesgos	52
<i>Tabla 33:</i> Estructura de costos del proyecto	56

INTRODUCCIÓN

En el presente trabajo de suficiencia profesional, se describe la renovación de dispositivos criptográficos que ha realizado una entidad financiera para soportar el futuro crecimiento transaccional a través de sus canales, asegurar su disponibilidad y que a su vez permita la implementación de estándares de seguridad para sus tarjetas de débito.

El módulo de seguridad de hardware (HSM) es un procesador criptográfico diseñado de manera específica para la protección del ciclo de vida de las claves criptográficas que permite administrarlas, procesarlas y almacenarlas de modo seguro dentro de un dispositivo reforzado que es resistente a manipulaciones. Estos son utilizados para brindar servicios de cifrado, descifrado, firmas digitales y autenticación que en las industrias de pago, ofrecen además, un conjunto de funciones de seguridad que incluyen la validación y protección de PIN, procesamiento de transacciones, protección de datos confidenciales, entre otras características.

Al ser una entidad financiera y contar con constantes proyectos de implementación de tecnología para el crecimiento del negocio, es necesario que los canales de atención que ofrece como servicios cuenten con disponibilidad para ofrecer productos de calidad a sus clientes. A su vez, implementar uno de los proyectos que permite el cumplimiento del estándar de seguridad EMV Full, que es utilizado para realizar pagos seguros ya que la tarjeta tiene un chip integrado que funciona como un procesador y transmisor en miniatura que incluye datos digitales dinámicos en cada transacción y ayuda a reducir el fraude con tarjetas de débito.

Para el cumplimiento de lo anteriormente descrito, la empresa decidió realizar un proyecto de renovación de dispositivos criptográficos a su nueva versión implementando una arquitectura de alta disponibilidad que tiene relación con todos sus canales de atención con tarjetas de débito, utilizando el marco metodológico de PMI, basado en la guía de PMBOK.

El trabajo se encuentra organizado de la siguiente manera:

- Capítulo I, se desarrolla la trayectoria profesional de la autora y se evidencia la experiencia profesional lograda.
- Capítulo II, se desarrolla el contexto en el cual se aplica el presente trabajo, así como la información genérica de la entidad en la cual ha sido desarrollada.

- Capítulo III, se detalla la metodología y etapas aplicadas en el trabajo realizado, así como la implementación del mismo.
- Capítulo IV, se comenta la reflexión crítica de la autora basada en su experiencia.
- Capítulo V, se indican las conclusiones y recomendaciones en base a lo desarrollado en el presente trabajo.

CAPÍTULO I: TRAYECTORIA PROFESIONAL

1.1 Presentación profesional

La autora del presente informe de suficiencia profesional posee el grado de Bachiller en Ingeniería de Sistemas de la Universidad Nacional Mayor de San Marcos. Posee 5 años de experiencia en banca participando desde el frente de seguridad en distintos proyectos de infraestructura, tanto on premise como cloud, proyectos de gestión, proyectos normativos, identificación y gestión de riesgos, entre otras actividades. Adicionalmente, se encuentra de manera constante en capacitaciones de instituciones reconocidas para su actualización.

A continuación se detalla la experiencia académica y profesional:

1.2 Formación académica

Tabla 1: Formación académica profesional

Universidad Nacional Mayor de San Marcos	
Grado académico	Bachiller
Periodo	2013 - 2017
Formación recibida	Escuela Académica Profesional de Ingeniería de Sistemas – Facultad de Ingeniería de Sistemas e Informática

Nota. Fuente: Elaboración propia

Tabla 2: Idiomas

Asociación cultural peruano británica	
Curso	Inglés
Nivel	Intermedio

Nota. Fuente: Elaboración propia

Tabla 3: Cursos

CISM	
Institución	New Horizons
Formación	Curso concluido

Entrenamiento en criptografía y seguridad del PIN

Institución GMS

Formación Curso concluido

MS – 500 Microsoft 365 Security Administrator

Institución New Horizons

Formación Curso concluido

Interpretación e Implementación de las PCI DSS V3.2.1

Institución Strategos Consulting Services

Formación Curso concluido

Information Security Foundation – Based on ISO/IEC 27001

Institución EXIN

Formación Curso concluido / Certificación obtenida

Curso de Backup

Institución Academia ESET

Formación Curso concluido

Seguridad para PYMES

Institución Academia ESET

Formación Curso concluido

Nota. Fuente: Elaboración propia

1.3 Experiencia profesional

Tabla 4: Especialista de Seguridad de la Información

Especialista de Seguridad de la Información

Empresa Entidad financiera

Periodo Agosto 2021 - Actualidad

Funciones	- Participación en el cumplimiento del estándar PCI DSS. Cumplimiento de requisitos 5 y 12, adicional a proyectos relacionados. - Líder técnico en el proyecto de Gestión de Activos de información - Participación en el proyecto de implementación de EMV Full. - Participación en proyectos de Seguridad de la Información (on premise y cloud). - Participación en el seguimiento de planes de acción para la implementación del Reglamento para la gestión de seguridad de la información y ciberseguridad (Resolución SBS N° 504 - 2021) - Identificación y gestión de riesgos de seguridad de la información de la empresa, a través del diseño y desarrollo de planes de acción necesarios para la eliminación o mitigación de estos en los procesos, servicios y/o proyectos. - Ejecución de actividades de monitoreo, seguimiento de observaciones y cálculo de indicadores. - Gestión documentaria: elaboración, actualización y publicación de procedimientos y normativa interna
------------------	--

Nota. Fuente: Elaboración propia

Tabla 5: Analista Senior de Seguridad de la Información

Analista Senior de Seguridad de la Información	
Empresa	Entidad financiera
Periodo	Marzo 2020 - Julio 2021
Funciones	- Participación en el cumplimiento del estándar PCI DSS. Cumplimiento de requisitos 5 y 12 - Líder técnico en el proyecto de Gestión de Activos de información - Participación en proyectos de Seguridad de la Información (on premise y cloud). - Identificación y gestión de riesgos de seguridad de la información de la empresa, a través del diseño y desarrollo de planes de acción necesarios para la eliminación o mitigación de estos en los procesos, servicios y/o proyectos.

	- Ejecución de actividades de monitoreo, seguimiento de observaciones y cálculo de indicadores. - Gestión documentaria: elaboración, actualización y publicación de procedimientos y normativa interna
--	---

Nota. Fuente: Elaboración propia

Tabla 6: Analista de Seguridad de la Información

Analista de Seguridad de la Información	
Empresa	Entidad financiera
Periodo	Julio 2019 - Febrero 2020
Funciones	- Participación en el cumplimiento del estándar PCI DSS. - Participación en el proyecto de Gestión de Activos de información. - Participación en proyectos de Seguridad de la Información (on premise). - Identificación y gestión de riesgos de seguridad de la información de la empresa, a través del diseño y desarrollo de planes de acción necesarios para la eliminación o mitigación de estos en los procesos, servicios y/o proyectos. - Atención de requerimientos de Seguridad de la Información (evaluación, asignación y/o atención de requerimientos de accesos a aplicaciones, servicios, etc) - Ejecución de actividades de monitoreo, seguimiento de observaciones y cálculo de indicadores. - Gestión documentaria: elaboración, actualización y publicación de procedimientos y normativa interna - Relevamiento de información con áreas usuarias para la gestión de accesos (actualización de matrices de acceso/roles/perfiles).

Nota. Fuente: Elaboración propia

Tabla 7: Analista de Seguridad de la Información - Freelance

Analista de Seguridad de la Información - Freelance	
Empresa	Entidad financiera
Periodo	Octubre 2018 - Junio 2019

Funciones	- Atención de requerimientos de Seguridad de la Información (evaluación, asignación y/o atención de requerimientos de accesos a aplicaciones, servicios, etc) - Relevamiento de información con áreas usuarias para la gestión de accesos (actualización de matrices de acceso/roles/perfiles). - Gestión documentaria: elaboración, actualización y publicación de procedimientos y normativa interna. - Ejecución de actividades de monitoreo, seguimiento de observaciones y cálculo de indicadores.
------------------	--

Nota. Fuente: Elaboración propia

Tabla 8: Practicante de Seguridad Informática

Practicante de Seguridad Informática	
Empresa	Entidad financiera
Periodo	Noviembre 2017 – Octubre 2018
Funciones	- Gestión de la seguridad lógica basada en roles funcionales, gestión de accesos e identidades de los usuarios de Red de Agencias y Sede Administrativa, mediante la herramienta IBM Security Identity Manager. - Gestión del cumplimiento de las políticas de Seguridad de la Información e implementación de controles. - Administración del Correo de la Sección Seguridad Informática para el control, atención y seguimiento de requerimientos. - Apoyo en la elaboración de reportes de auditorías.

Nota. Fuente: Elaboración propia

CAPÍTULO II - CONTEXTO EN EL QUE SE DESARROLLA LA EXPERIENCIA

2.1 Empresa – Actividad que realiza

La entidad financiera en cuestión es un banco líder en su sector, que tiene como objeto realizar operaciones que son propias de una banca múltiple brindando acceso a sus clientes al sistema financiero formal y acompañándolos en sus iniciativas a lo largo del tiempo y sus necesidades.

La empresa se dedica a captar ahorros y otorgar préstamos y cada agencia a nivel nacional tiene la misma estructura en sus actividades, con dos áreas definidas como negocio y operaciones.

Sus servicios están compuestos por ofrecer productos tales como sistema de préstamos, sistemas de ahorros, seguros, atención a sus clientes a través de sus canales alternativos como la banca por teléfono, agentes, cajeros electrónicos o ATM, aplicaciones y la banca por internet que permite realizar operaciones como pago de préstamos y servicios, consulta de movimientos y saldos, transferencias y apertura de cuentas a plazo.

2.2 Visión

La visión de la empresa es ser reconocida como un socio para sus clientes y colaboradores por el servicio que brindan, siendo un referente en la región.

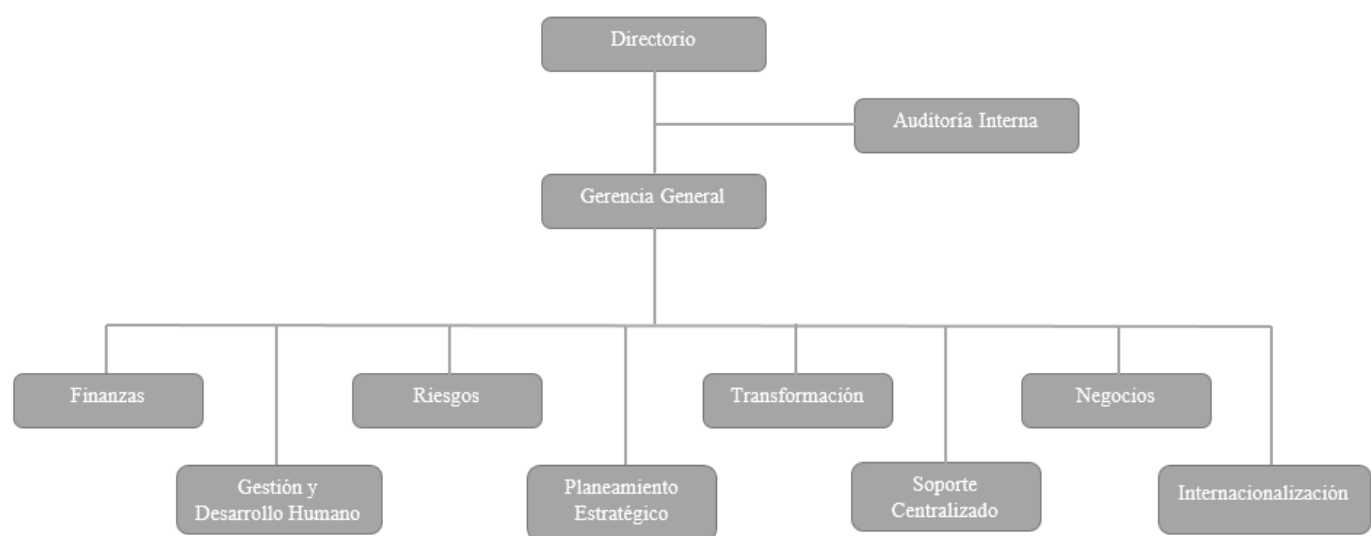
2.3 Misión

La misión de la empresa trata acerca del compromiso por la inclusión financiera y el progreso de sus clientes a favor del crecimiento del país.

2.4 Organización de la empresa

La entidad financiera cuenta con el organigrama de la siguiente manera:

Figura 1: Organigrama de la entidad financiera



Nota. Organigrama de la entidad donde se muestran las divisiones que contiene. Fuente: Empresa, 2021

A continuación se agrega el desglose del área de Riesgos:

Figura 2: Áreas de Riesgos



Nota. La división de Riesgos contiene a las diferentes gerencias y subgerencias. Fuente: Elaboración propia

2.5 Área, cargo y funciones desempeñadas

Tabla 9: Área, cargo y funciones desempeñadas

Área	Cargo	Funciones desempeñadas
Seguridad de la Información	Especialista de Seguridad de la Información	- Líder técnico del proyecto de renovación de dispositivos criptográficos

-
- Participación en el cumplimiento del estándar PCI DSS dentro de la entidad financiera
 - Participación en el proceso de identificación y gestión de riesgos de seguridad de la información de la empresa, a través del diseño y desarrollo de planes de acción necesarios para la eliminación o mitigación de estos en los procesos, servicios y/o proyectos.
 - Participación en el seguimiento de planes de acción para la implementación del Nuevo Reglamento para la gestión de seguridad de la información y ciberseguridad (Resolución SBS N° 504 - 2021) dentro de la organización.
-

Nota. Fuente: Elaboración propia

2.6 Experiencia profesional realizada en la Organización

Dentro del equipo se tienen las siguientes experiencias:

- Participación del proyecto de segregación de funciones de una aplicación con módulos de finanzas, logística, administración, entre otros. De manera paralela la atención de requerimientos de seguridad para la evaluación y atención de requerimientos de accesos a aplicaciones o servicios.
- Ejecución de monitoreos de segunda línea que prueban los controles de seguridad establecidos en la empresa, el seguimiento de las observaciones y el cálculo de KPIs.
- Participación del proyecto de gestión de activos de información, desde el acompañamiento en la actualización de la metodología hasta su puesta en marcha con recurrencia anual.
- Participación de las evaluaciones de riesgos de seguridad realizadas proyectos a demanda y a proveedores. Posteriormente también se incluyeron evaluación a

proyectos relacionados a nuevos productos y cambios importantes cuya interacción incluye el reporte a niveles más altos de la organización.

- Participación desde el frente de seguridad en los proyectos de infraestructura para sistemas on premise y cloud. En este último caso, se participó en la implementación de un ERP con tecnología SaaS y PaaS.
- Parte del equipo encargado del cumplimiento del estándar PCI DSS en la empresa con la participación de las diferentes área involucradas en los requisitos 5 – protección contra malware y actualización de software antivirus regularmente – y el requisito 12 – mantener una política que aborde la seguridad de la información para todo el personal. Adicionalmente de la participación en la gestión de las auditorías externas que se realizan para validar el avance de los requisitos.

CAPÍTULO III - ACTIVIDADES DESARROLLADAS

3.1 Situación Problemática

Dado que los equipos HSM con los que contaba anteriormente la entidad financiera se estaban quedando obsoletos, la empresa se quedaría con una versión desactualizada del firmware en los equipos que soportan el proceso criptográfico, de manera que ante algún incidente de seguridad o rendimiento del dispositivo, no se tendría el soporte por parte de la marca para una posible solución.

Adicionalmente, estos dispositivos se encontraban dentro de la lista de equipos del banco que deben ser renovados por obsolescencia tecnológica, por lo que se establece un tiempo máximo estimado para su renovación de modo que no impacte negativamente en los indicadores de cumplimiento establecidos.

3.1.1 Definición del problema

Los equipos que soportaban la tecnología criptográfica en el banco eran de una versión que se quedaría sin soporte por parte de la marca fabricante a fines del 2022 y que tienen un límite en cuanto a capacidad de procesamiento, es por ello que bajo este escenario, dichos dispositivos criptográficos no soportarían el futuro crecimiento transaccional del banco y tampoco las nuevas implementaciones requeridas para cumplimiento de estándares de seguridad.

Dada esta problemática, se buscó la implementación de la nueva versión de los HSM. Esta implementación impactó en las aplicaciones del banco traducándose en nuevos desarrollos o modificaciones en las configuraciones de la infraestructura, así como un cambio en la arquitectura propuesta para que se brinde la alta disponibilidad del servicio.

3.2 Solución

3.2.1 Objetivos

3.2.1.1 Objetivo general:

Implementar dispositivos criptográficos hacia su nueva versión que cuenta con las prestaciones técnicas necesarias para asegurar el futuro crecimiento transaccional de la entidad financiera, adecuando las aplicaciones integradas y actualizando la arquitectura,

que permitirá brindar la disponibilidad de sus canales de atención al cliente con tarjetas de débito y la implementación de estándares de seguridad requeridos por la industria.

3.2.1.2 Objetivos específicos:

Los objetivos específicos planteados para el proyecto fueron los siguientes:

- Reemplazar los dispositivos criptográficos por la versión más reciente.
- Actualizar la arquitectura permitiendo que los equipos se encuentren en alta disponibilidad y contemplando un balanceador de carga.
- Adecuaciones y configuraciones a nivel de aplicaciones e infraestructura.
- Definir un modelo de gobierno con las responsabilidades de cada área involucrada en el funcionamiento de los equipos y sus componentes en los ambientes en los que se encuentren (Desarrollo, Calidad, Producción o Contingencia).

3.2.2 Alcance

La implementación de la nueva versión de los equipos generó la adecuación de las aplicaciones que hacen uso de estos. Dichos cambios estuvieron relacionados con el cambio de IP, puertos, parámetros de seguridad, entre otros. Cabe resaltar que no se realizaron cambios funcionales en el proyecto, ni a nivel de tramas o parámetros en los canales ya que estos fueron a nivel de configuración; sin embargo, se contempló realizar pruebas en Desarrollo y Calidad para asegurar el correcto funcionamiento y poder realizar el pase a Producción.

El proyecto no contempló la migración de uno de sus canales ya que este se encontraba en proceso de migración mediante otro proyecto, por lo tanto, no fue considerado de cara a la revisión de impacto y a la necesidad de pruebas y certificación.

3.2.3 Etapas y metodología

La gestión del proyecto está basada en la especificación de áreas del conocimiento, promovida por el Project Management Institute, Inc. (PMI), tomando como referencia principal las prácticas plasmadas en la Guía del PMBOK.

a) Inicio del proyecto: Durante esta fase se generó la ficha del proyecto donde se definieron los siguientes puntos:

- Situación actual de la empresa
- Objetivos por cumplir con la implementación
- Presupuesto estimado

- Cronograma macro

Este documento fue utilizado para la presentación del proyecto en diferentes foros para su aprobación.

- b) Planificación del proyecto: Una vez que el proyecto fue aprobado, se adquirieron los equipos HSM y la ficha del proyecto fue presentada en el comité de gestión de la demanda para comunicar su alcance y solicitar el apoyo y participación de las áreas involucradas.

De manera paralela, se realizaron las siguientes actividades:

- Definición detallada del alcance: Durante esta actividad se realizaron reuniones de coordinación con las diferentes áreas del banco para conocer los detalles de las integraciones a realizar. Adicionalmente, se hizo partícipe a los proveedores de las aplicaciones que necesitaron adecuaciones, por el frente de infraestructura, a los proveedores del F5 (dispositivo utilizado para migrar el tráfico hacia uno más servidores) y a los proveedores de los HSM. De esta manera se obtuvo el diagrama de arquitectura actualizado.
 - Desarrollo de cronograma detallado: Durante la planificación se generó el cronograma detallado con las actividades por hitos y fechas específicas.
 - Determinar el presupuesto: Durante esta actividad se definió el presupuesto para la adquisición de las herramientas tecnológicas. La contratación de recursos fue acordada durante la definición del alcance, al igual que el presupuesto para las adecuaciones.
 - Plan de recursos humanos: Tras participar en el comité de gestión de la demanda se identificaron a los participantes de las áreas involucradas. Adicionalmente a los recursos que serían contratados con una estimación temporal.
 - Plan de gestión de riesgos: Donde se identificaron los riesgos de la gestión del proyecto y se definieron planes de acción para la contención.
- c) Ejecución del proyecto: En esta fase se llevó a cabo la implementación del proyecto en base a la información que fue desarrollada en las etapas anteriores:
 - Contratación de recursos
 - Actividades en el ambiente de Desarrollo
 - Actividades en el ambiente de Calidad
 - Pase a producción y ratificaciones
 - Definición del modelo de gobierno

- d) Monitoreo y control del proyecto: De manera semanal el proyecto fue presentado en el comité de seguimiento. En él se presentaron los avances establecidos según cronograma y, en caso las actividades pactadas no se realizaban, los riesgos o problemas y los planes de acción para su remediación.
- e) Cierre del proyecto: Se comunicó a las áreas relacionadas al funcionamiento de los equipos el correcto despliegue de estos en el ambiente de Producción posterior a las ratificaciones realizadas. De manera paralela, se realizó una capacitación a los usuarios encargados de su mantenimiento y dar soporte.

3.2.4 Fundamentos utilizados

3.2.4.1 Dispositivos criptográficos:

Los dispositivos criptográficos son dispositivos hardware que llevan un chip criptográfico para realizar operaciones en su misma lógica. Estos dispositivos pueden ser los siguientes:

3.2.4.1.1 Hardware Security Module (HSM)

Tabla 10: Definiciones

García (2020) indica que este dispositivo permite la seguridad de ciertas transacciones con los siguientes beneficios: Las claves se producen en el equipo como un generador de números aleatorios, su objetivo es que las llaves estén protegidas dentro de un entorno hardware seguro y ofrecen alta disponibilidad	Aguilar (2016) señala que es un dispositivo criptográfico basado en hardware que genera, almacena y protege claves criptográficas. Adicionalmente, aporta aceleración de hardware para operaciones criptográficas (tps)
---	---

Nota. Conceptos y definiciones. Fuente: Elaboración propia

Actualmente este dispositivo es usado por muchas instituciones que buscan salvaguardar y gestionar sus claves criptográficas ya que es un criptoprocador que se encarga de generar, procesar y almacenar claves de forma segura. Los HSM son sistemas de hardware dedicados que están diseñados específicamente para gestionar todo el ciclo

de vida de la clave criptográfica que se produce en él y manejar los procesos de cifrado y descifrado.

Seguridad en los dispositivos

Estos equipos garantizan un nivel de seguridad reglamentario, es decir, cumplen con estrictos controles de seguridad exigidos en la industria tales como los siguientes:

- FIPS 140-2 (Federal Information Processing Standards).- Es un estándar dirigido a la validación de la efectividad del hardware criptográfico que es reconocido a nivel mundial tanto en el sector público como en el privado y define cuatro niveles de seguridad del más bajo (Nivel 1) al más restrictivo (Nivel 4).
- PCI HSM.- Es un conjunto de estándares de cumplimiento de seguridad física y lógica para equipos HSM utilizados en la industria de pagos que define los controles de seguridad necesarios durante el proceso de fabricación, envío, uso y desmantelamiento de los dispositivos empleados en transacciones financieras.

Estos aseguran que las claves de cifrado no se puedan extraer fuera del dispositivo y aseguran que el almacenamiento y la transmisión de datos se encuentre protegido. Un HSM está reforzado contra la manipulación o los daños (control tamper resistant – es decir, el equipo elimina su información ante signos de manipulación) y puede estar situado en una zona físicamente segura de un centro de datos para evitar el contacto no autorizado.

Adicionalmente a lo anterior, la seguridad del software del HSM se consigue mediante una combinación de varias características de seguridad, entre las que se incluyen las siguientes:

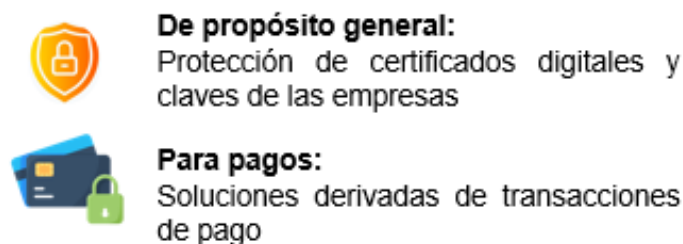
- Dos cerraduras en el panel frontal con llaves físicas independientes
- Tarjetas inteligentes personalizadas emitidas para los agentes de seguridad y de autorización o custodios.
- El dispositivo cambie de estado a un modo Seguro que requiere la presencia de dos agentes de seguridad con llaves físicas diferentes para las cerraduras del panel frontal.
- El dispositivo cambie de estado a un modo Autorizado que requiere la presencia de dos Oficiales de Autorización con tarjetas inteligentes.
- Parámetros de seguridad configurables y registros de auditoría
- Sensores para detectar anomalías de movimiento, tensión y temperatura

Dichos dispositivos pueden realizar múltiples operaciones criptográficas por segundo y permiten que la administración de claves se realice a través del control dual utilizando tarjetas inteligentes, contraseñas o dispositivos USB. Con esto, permiten establecer una separación de funciones o responsabilidades con custodios, administradores y operadores.

Tipos de HSM

- HSM de propósito general: Incluyen algoritmos de encriptación estándar (simétricos, asimétricos y funciones hash) y son utilizados normalmente en entornos de PKI, canales HTTPS, protección de datos sensibles genéricos, protección de certificados digitales y claves delicadas de la organización, entre otros.
- HSM transaccional y para pagos: Son equipos específicos para proporcionar altos niveles de protección de las claves criptográficas y las transacciones de pago que utilizan PIN (generación, validación y traslado del PIN Block en cajeros automáticos y POS), generación de datos para chips EMV (validación de ARQC y generación de ARPC), procesamiento de transacciones de pago con tarjetas de crédito y débito, generación y validación de CVV, entre otros.

Figura 3: Tipos de HSM



Nota. Fuente: Redtrust (2022)

Tabla 11: Cuadro comparativo de tipos de HSM

Ítems	HSM de propósito general	HSM de pago
Industrias	Gobierno y Sector Público, Ciberseguridad, Servicios	Instituciones Bancarias y Financieras

Formatos o tipos de HSM usuales	Dispositivos de hardware físicos dedicados o acceso basado en la nube	Dispositivos de hardware físico dedicado
Estándares de cumplimiento	FIPS 140-2 (nivel 3 o superior), Common Criteria (ISO/IEC 15408) y EN 419 221-5	PCI HSM, FIPS 140-2 (nivel 3 o superior) y requisitos de seguridad específicos para proveedores de la industria de tarjetas de pago

Nota. Comparación en tres criterios entre HSM de propósito general y HSM de pago.

Fuente: Elaboración propia

Un HSM es un entorno informático de confianza por los siguientes motivos:

- Está construido sobre un hardware especializado, probado y certificado en laboratorios especiales.
- Tiene un sistema operativo centrado en la seguridad.
- Limita el acceso a través de una interfaz de red que está estrictamente controlada por normas / reglas internas.
- Tiene protección de acceso físico
- Cuenta con una interfaz de usuario y una interfaz programable
- Oculta y protege activamente el material criptográfico.

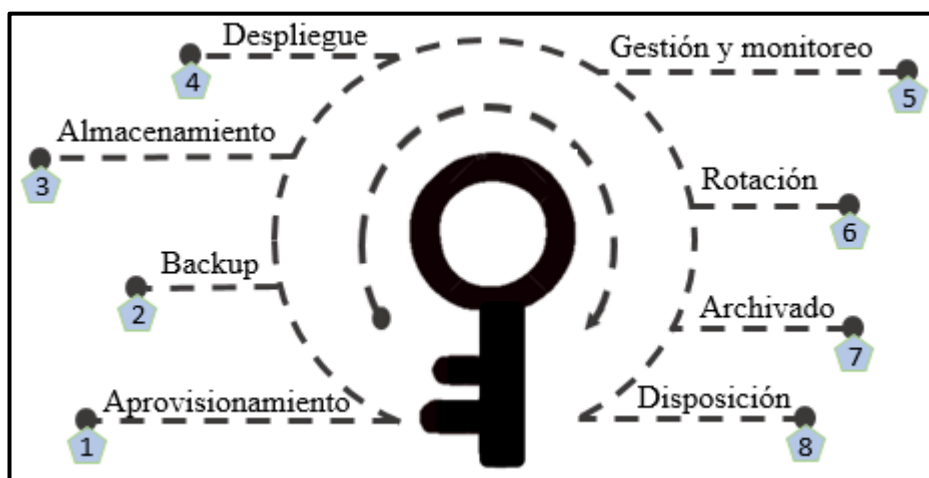
Ciclo de vida de una clave criptográfica

- *Aprovisionamiento*: en esta etapa, las claves son creadas por un HSM o una entidad tercera que realiza esta actividad y para ello se utiliza un generador de números aleatorios.
- *Copia de seguridad y almacenamiento*: se debe realizar una copia de las claves y deben ser almacenadas de forma segura para evitar que la clave se vea comprometida o vulnerada. Las claves privadas deben estar encriptadas antes de ser almacenadas.
- *Despliegue*: implica instalar la clave en un dispositivo criptográfico.
- *Gestión*: las claves se controlan y supervisan bajo los estándares de la industria y las políticas internas de la organización. El sistema de administración de claves

de cifrado maneja la rotación de estas con el objetivo de implementar nuevas a medida que caducan las existentes.

- *Archivado*: las claves que fueron dadas de baja son almacenadas fuera de línea a largo plazo; de esta manera, se podría acceder a los datos existentes que se cifraron con estas cuando sea necesario.
- *Disposición*: las claves deben destruirse de forma segura bajo ciertas políticas de seguridad y de forma permanente cuando se determine que ya no serán necesarias.

Figura 4: Ciclo de vida de llave criptográfica



Nota. Fuente: Elaboración propia

Tipos de llaves utilizados por equipos HSM:

Se cuenta con una estructura de llaves criptográficas que se muestra a continuación:

- **Local Master Key (LMK) – Llave maestra local:**

Esta llave criptográfica se almacena de forma encriptada en el HSM y se utiliza para cifrar todas las claves protegidas ya que a partir de ella se deben generar las llaves que se contemplan por cada canal de atención. Si se borran las LMKs, el HSM ya no puede descifrar ningún dato protegido y esencialmente queda inoperativo.

Para generar esta llave se necesitan tres componentes que se encuentran bajo la protección de tres custodios, de esta manera se cumple el principio de conocimiento dividido.

Como medida adicional en la seguridad de las actividades relacionadas a la LMK en los HSM, se tiene un segundo factor de validación que consiste en que la generación de componentes de LMK, su modificación, restauración o eliminación está sujeto al uso de dos llaves físicas propias de los dispositivos, las cuales deben ser ingresadas y accionadas para desbloquear el uso de este.

- **Zone Master Key (ZMK):**

Ayala, Peñaherrera y Urrea (2015) indican que consiste en una clave de cifrado que se distribuye entre dos o más sitios con una red compartida. Utilizada cuando se requiere el intercambio de llaves con entidades externas. La clave ZMK se cifra bajo un par de la LMK.

- **Zone Pin Key (ZPK):**

Ayala, Peñaherrera y Urrea (2015) señalan que consiste en una clave de cifrado de datos utilizada para cifrar bloques de PIN en la transmisión de información entre partes de una red (con otras entidades). Una ZPK debe cifrarse bajo una ZMK para la transmisión.

- **Terminal Master Key (TMK):**

Ayala, Peñaherrera y Urrea (2015) indican que consiste en una llave de encriptación y es utilizada para distribuir claves de cifrado de datos dentro de la red local (no compartida) a cajeros automáticos o POS. Una TMK está encriptada bajo un par LMK para el almacenamiento local.

- **Terminal PIN Key (TPK):**

Ayala, Peñaherrera y Urrea (2015) señalan que consiste en una clave de cifrado de datos utilizada para cifrar el bloque de PIN en tránsito dentro de una red local, entre un terminal y el adquirente de datos de terminal. Una TPK está encriptada bajo un par LMK para el almacenamiento local.

Funcionamiento:

Los HSM presentan comandos de consola y de host que se configuran según la necesidad de la empresa. Los comandos de host son utilizados para el funcionamiento de las aplicaciones.

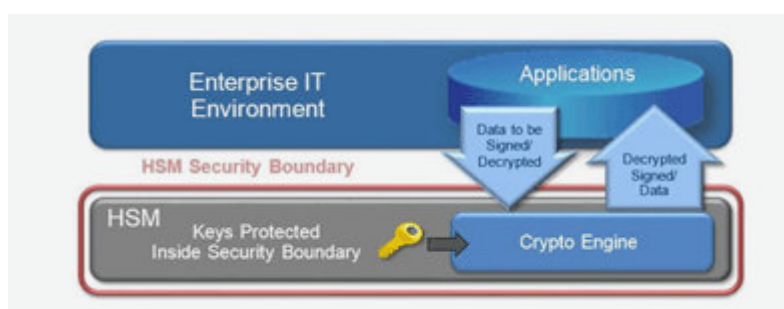
Los dispositivos alojados en los centros de datos de entidades bancarias pueden realizar las siguientes funciones:

- Verificar los números PIN cada vez que un cliente retira dinero de un cajero automático (ATM): Al ingresar el código PIN se genera un bloque de información

encriptado automáticamente. Este se dirige hacia el HSM de la empresa recibiendo una solicitud, en ella se descifra el bloque y envía la respuesta al ATM (si el PIN es válido o no). De esta forma, la información no se transmite en texto claro; es decir, en caso de ser interceptada por algún atacante, esta no será útil ya que la clave reside en el dispositivo y sin ella es imposible obtener el PIN del cliente.

- Validar las transacciones en los terminales de punto de venta (POS) de los comercios cuando los consumidores compran productos.

Tabla 12: Uso del HSM



Nota. Fuente: Entrust (2019)

Casos de uso comunes en el ecosistema de pagos:

- Generación, gestión y validación de PIN
- Traducción de bloqueo de PIN durante el cambio de red de transacciones de cajeros automáticos y puntos de venta
- Validación de tarjeta, usuario y criptograma durante el procesamiento de transacciones de pago
- Emisión de credenciales de pago para tarjetas de pago y aplicaciones móviles
- Gestión de claves de cifrado punto a punto y descifrado seguro de datos
- Compartir claves de forma segura con terceros para facilitar comunicaciones seguras

3.2.4.1.2 Token criptográfico

“Es un dispositivo criptográfico es un lector de chip criptográficos e incorpora el chip criptográfico, todo en un único dispositivo con conexión USB 2.0 tipo A. Estos tokens deben estar certificados con: FIPS 140-2 y/o CC EAL 4+.” (Aguilar, 2016).

3.2.4.1.3 Smart card (tarjeta inteligente)

“Es un dispositivo de las dimensiones de una tarjeta bancaria que contiene un procesador criptográfico seguro y cuenta con circuitos integrados que permiten la ejecución de cierta lógica programada” (RENIEC, 2022).

3.2.4.2 Transacciones con tarjeta de débito

Definiciones

Según Rodríguez (2019), una transacción financiera es una operación u acuerdo realizado entre un comprador y un vendedor en la que se intercambian activos a cambio de un pago impactando en la finanza de ambos roles. Los compradores y vendedores son entidades o actores que por lo regular intercambian productos de valor, como bienes y/o servicios.

De manera paralela, en el mismo documento, Rodríguez (2019) señala que una tarjeta de débito es una tarjeta bancaria que almacena el nombre del titular de la tarjeta y la información del número de cuenta, utilizada para ejecutar operaciones financieras activas (incremento de saldo), pasivas (disminución de saldo) o neutrales (sin incremento o disminución del saldo disponible en la cuenta). En este tipo de tarjeta, el dinero utilizado se debita de la cuenta bancaria del titular.

Una transacción realizada con tarjeta de débito es realizada en el sistema de tarjetas de pago para efectuar alguna actividad relacionada a la adquisición de bienes y servicios; para ello, se pueden utilizar diferentes tipos de canales como plataformas por internet, puntos de venta o POS, cajeros automáticos o ATM, entre otros.

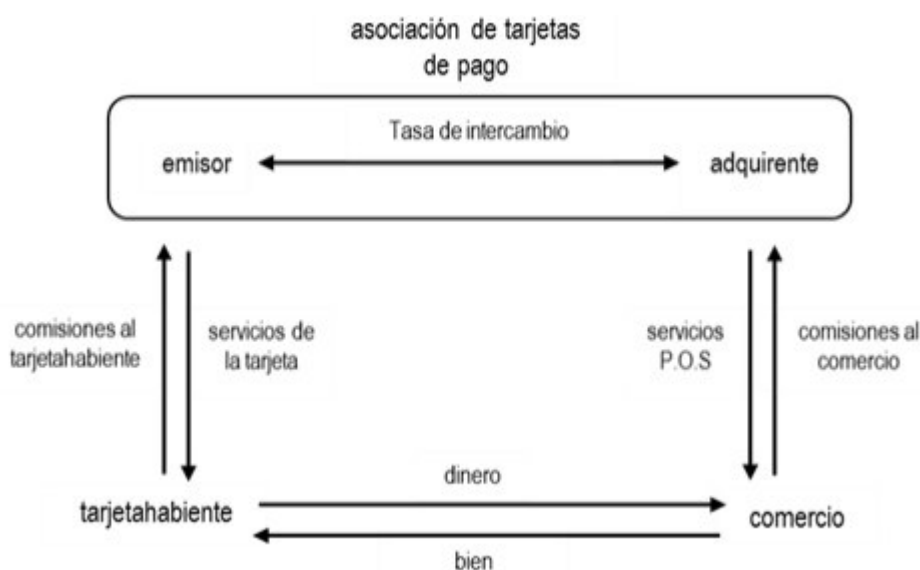
Sistemas de tarjetas de pago

En los sistemas de tarjeta de pago pueden interactuar los siguientes roles:

- a) Titular de la tarjeta o tarjetahabiente: También llamado consumidores, son quienes utilizan los medios de pago para la compra de bienes y servicios.
- b) Comercio: Son quienes aceptan los medios de pagos para vender sus bienes o prestar sus servicios.

- c) Emisor: Son entidades que emiten medios de pago para que sean usados por sus clientes (titular de la tarjeta). Las tarjetas de pago emitidas por el Emisor pueden ser tarjetas de débito o crédito. El banco emisor es el responsable de la fabricación de la tarjeta de pago y su gestión criptográfica asociada.
- d) Adquiriente: Son encargados de afiliar a los comercios para que acepten medios de pagos electrónicos en sus transacciones, es decir, proporciona al Comercio las herramientas necesarias (hardware y software) para aceptar tarjetas de pago

Figura 5: Esquemas de Organización del Mercado de Tarjetas de Pago de Cuatro partes



Nota. Fuente: Indecopi (2018)

Durante todo este proceso se utiliza la criptografía en todos los roles, pero considerando que la entidad financiera de la que se está realizando el trabajo de suficiencia profesional es Emisor, vamos a centrarnos en su criptografía relacionada ya que necesita HSM cuando emite tarjetas, posee claves y administra la criptografía involucrada con las tarjetas. También necesita HSM para autorizar el flujo criptográfico.

Una transacción realizada con una tarjeta de débito usualmente tiene como origen un dispositivo de compra ya sea un terminal POS, un ATM o un PINPAD a través de una red hacia la empresa emisora para conseguir su autorización en relación a la cuenta del tarjetahabiente. Dicha transacción comprende información del titular de la tarjeta y de la transacción financiera (ya sea compra, pago o venta) junto con otra información que puede generarse o agregarse de manera dinámica por los sistemas que intervienen en

el proceso. La empresa emisora autoriza o rechaza la transacción y genera un mensaje de respuesta que es retornado a la terminal en un tiempo corto (medido en segundos). Para transmitir y procesar esta información sensible se utilizan los dispositivos HSM.

Las transacciones con tarjeta de débito se relacionan de la siguiente manera con los HSM:

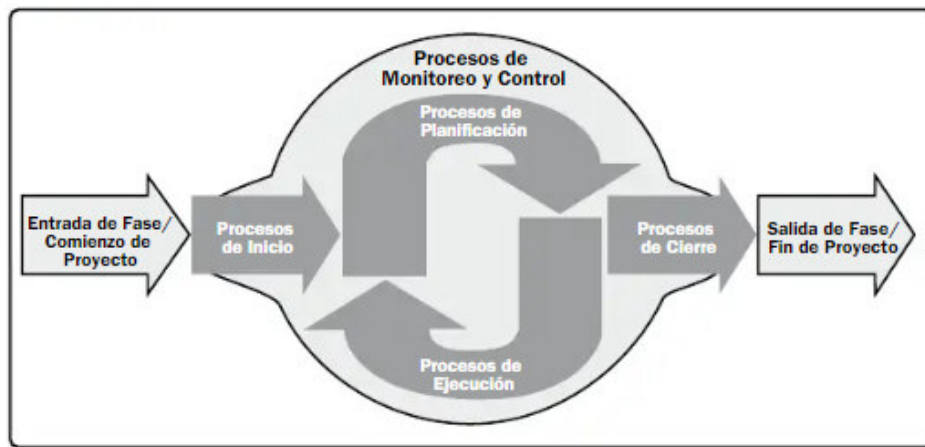
- Verifican que el PIN ingresado por el cliente coincida con el PIN de referencia conocido por el emisor de la tarjeta
- Cifran un bloque de PIN para enviarlo a otro host de autorización
- Realizan una gestión segura de claves de la empresa
- Verifican las transacciones con tarjeta de crédito o débito comprobando los códigos de seguridad de la tarjeta o realizando componentes de procesamiento ARPC y ARQC basado en EMV
- Generan datos para una tarjeta de banda magnética (PVV, CVV)
- Generan un conjunto de claves de tarjeta

3.2.4.3 Gestión de proyectos según el PMBOK®

Project Management Institute (2017) indica que La Guía de los Fundamentos para la Dirección de Proyectos (Guía del PMBOK) provee orientación y conceptos relacionados con la gestión de proyectos. También describe el ciclo de vida de la gestión de proyectos y sus procesos asociados, así como el ciclo de vida del proyecto.

Dentro de la implementación del proyecto en mención se adoptaron los cinco grupos de procesos de la guía del PMBOK de acuerdo a las necesidades del negocio ya que son buenas prácticas:

Figura 6: Grupos de procesos de la Dirección de Proyectos



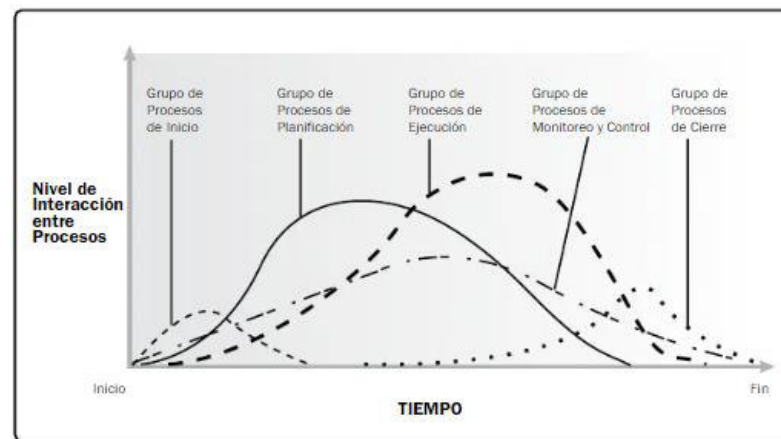
Nota. Fuente: PMBOK – Sexta edición (2017)

- Inicio: Compuesto por procesos que buscan definir un nuevo proyecto obteniendo la autorización para iniciarlo. Se define el alcance inicial, se comprometen los recursos financieros iniciales y se identifican los interesados internos y externos que van a participar.
- Planificación: Compuesto por procesos utilizados para establecer el alcance detallado, objetivos, tiempo, costos, adquisiciones, recursos, comunicación con los interesados y además, definen una línea de cómo se va a llevar a cabo el proyecto.
- Ejecución: Compuesto por procesos que buscan desarrollar el trabajo definido en el plan del proyecto buscando el cumplimiento de la estrategia de este y acciones definidas en la fase anterior.
- Monitoreo y control: Compuesto por procesos que buscan medir el desempeño del proyecto monitoreando sus actividades en comparación con el plan inicial, controlando los cambios y recomendando acciones correctivas o preventivas ante problemas o riesgos. Dentro de este, se conoce la salud del proyecto.
- Cierre: Compuesto por procesos efectuados para finalizar las actividades del plan de proyecto y verificar que los procesos definidos según cronograma se hayan completado. Establece la formalización del cierre del proyecto.

Según Project Management Institute (2017), la naturaleza iterativa de la dirección de proyectos significa que se pueden reutilizar procesos de cualquier grupo a lo largo del ciclo de vida del proyecto.

Ante lo comentado anteriormente, en el siguiente gráfico se puede observar cómo los Grupos de Procesos pueden relacionarse durante un mismo proyecto:

Figura 7: Grupos de procesos de PMBOK

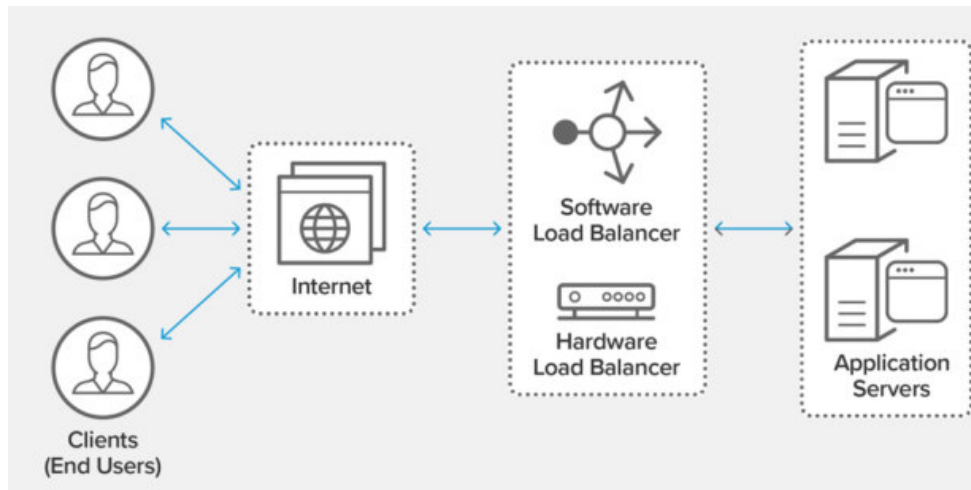


Nota. Fuente: PMBOK – Sexta edición (2017)

3.2.4.4 Balanceador de carga – F5

Un balanceador de carga es un dispositivo que se encarga de distribuir el tráfico de la red o de aplicaciones hacia uno o más servidores y son utilizados para incrementar la capacidad de usuarios concurrentes y la confiabilidad de las aplicaciones. Bastidas (2021) indica que los balanceadores de carga maximizan el rendimiento de los servidores y minimizan de manera efectiva el tiempo de respuesta de estos.

Figura 8: Balanceador de carga



Nota. Funcionamiento de un balanceador de carga. Fuente: NGINX (2022)

Los beneficios de implementar un balanceador de carga según Sit Mexico (2016) citado en Bastidas (2021) son los siguientes:

- Escalabilidad al distribuir solicitudes desde un usuario a varios servidores involucrados en la solución dando un beneficio a la capacidad total del proceso.
- Calidad del servicio debido al tiempo de respuesta a través de la disponibilidad del servicio.
- Disponibilidad al identificar si algún servidor ha dejado de funcionar correctamente evitando que se le envíen peticiones.
- Mantenimiento proactivo ya que se puede intervenir una máquina para repararla o actualizarla sin perjudicar el servicio total que brindan los servidores involucrados.

Características:

Vera (2018) señala que el balanceador de carga cuenta con dos características principales:

- Evita la saturación de un servidor: Evita que la recurrencia de acceso al servidor en un momento determinado afecte el desempeño de la aplicación.

- Gestiona de una manera eficiente los recursos: Permite optimizar y gestionar los recursos para que los aplicativos que se tienen implementados funcionen de la mejor forma posible

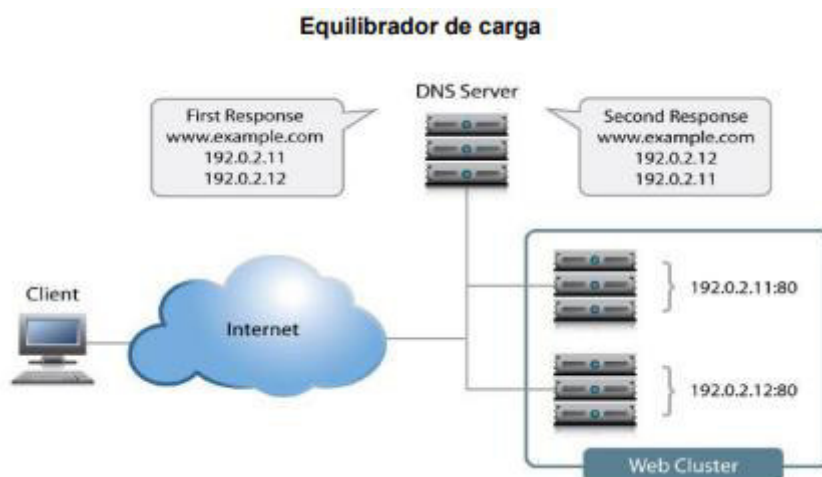
3.2.4.5 Trabajos relacionados a la presente investigación

“Análisis, diseño e implementación de balanceador de carga segmentando la red del sistema de balanzas de pequeñas y medianas empresas del sector industrial ciudad de Guayaquil” (Bastidas Delgado, 2021)

El proyecto de tesis del autor tiene como finalidad la implementación de un balanceador de carga que permita la distribución de forma equilibrada de peticiones realizadas por los usuarios hacia los servidores de la solución, ello con el fin de disminuir el tiempo que toma en realizarse dicha actividad y facilita la disponibilidad de la información.

Para la implementación propuesta en el trabajo, el autor evaluó características del balanceador, realizó comparativas entre un balanceador basado en hardware y otro en software, beneficios de su implementación y algoritmos comunes de equilibrio de carga para que de acuerdo con ello, pueda poner en marcha la solución.

Figura 9: Equilibrador de carga



Nota. Funcionamiento del equilibrio de carga. Fuente: Bastidas Delgado (2021)

“Planeación de un proyecto de implementación para una solución de balanceo de carga BIG-IP F5 en la universidad latinoamericana de Bogotá basado en el modelo PMI” (Perdomo Salazar, Abril Avella & Castro Avendaño, 2020)

Los autores del trabajo de investigación describen el proceso de implementar una solución de balanceo de carga utilizando el modelo PMI. En él se especifican las siguientes actividades como parte del ciclo de vida del proyecto:

- Plan de proyecto
- Diseño e planeación
- Entrega de elementos
- Gestión de los costos
- Plan para la gestión de recursos
- Plan de compras
- Gestión de riesgos
- Gestión de la calidad
- Ejecución de actividades de
- Estabilización de la solución

Figura 10: Grupo de procesos de dirección de proyectos



Nota. Fases realizadas durante la implementación del proyecto. Fuente: Perdomo Salazar, Abril Avella & Castro Avendaño (2020)

“Implementación del método de administración de llaves DUKPT en el simulador ASSET para transacciones financieras en dispositivos punto de venta” (Alba Martinez, 2017)

El autor del trabajo de investigación describe los puntos relacionados a la seguridad que debe existir en el proceso de transacciones en línea con tarjetas de débito y crédito que son realizadas en puntos de venta y operan como switches transaccionales, además de tecnologías de simulación para la implementación de administración de llaves criptográficas.

“Implementación de un modelo simplificado de firma digital basado en la tecnología PKI y la invocación por protocolos. Caso de estudio: Municipalidad de Miraflores” (Aguilar Alcarráz, 2016)

El autor del trabajo de investigación describe los dispositivos criptográficos para la elección del desarrollo de este. En él, se hace mención a tres de ellos donde se mencionan sus características, beneficios y certificaciones internacionales que deben cumplir:

- Tarjetas inteligentes
- Token criptográfico
- Hardware Security Module

“Diseño e implementación de un clúster usando JBoss EAP para aumentar la disponibilidad de los servidores de aplicaciones en una entidad del Estado” (Vera Zegarra, 2018)

El autor del trabajo de investigación detalla la implementación de un clúster para obtener la alta disponibilidad, un balanceo de carga, también el alto rendimiento y escalabilidad necesaria que logre cumplir con las expectativas de sus objetivos, al ser un conjunto de servidores con características en común conectados a través de la red interna.

En dicho trabajo se especifican tipos de balanceo de carga, ya sea en hardware o software y sus características principales.

3.2.5 Implementación de las áreas, procesos, sistemas y buenas prácticas

Las fases desarrolladas durante el proyecto y sus actividades se encuentran descritas en la siguiente tabla:

Tabla 13: Fases y entregables

Fase	Actividades y entregables
Inicio	- Ficha de proyecto - Aprobación de inicio de proyecto
Planificación	- Adquisición de herramientas tecnológicas - Estimación de participantes en el proyecto - Definición detallada del alcance - Diagramas de arquitectura física y lógica - Cronograma detallado - Definición de presupuesto - Plan de gestión de riesgos del proyecto
Ejecución	- Desarrollo - Documento de especificaciones funcionales - Documento de especificaciones técnicas - Plan de pruebas unitarias - Certificación - Plan de pruebas de certificación - Producción - Plan de pase a producción - Ratificaciones - Contingencia - Plan de pase a contingencia - Ratificaciones - Documento de Modelo de gobierno - Evaluación de riesgos
Monitoreo y control	- Ficha de presentación semanal ante comité - Ficha de control de cambios
Cierre	- Ficha de cierre de proyecto

Nota. Fuente: Elaboración propia

3.2.5.1 Detalle de actividades

Se presentan a mayor detalle las actividades realizadas en cada etapa de implementación de la iniciativa.

Etapas 1: Inicio

En esta etapa se completó el formato de la Ficha del Proyecto. Este es el documento inicial para la presentación de los proyectos en los diversos foros de la empresa que contiene principalmente los puntos que se detallan a continuación:

- *Identificación de la situación actual y descripción del proyecto.* Se identificó la situación de la empresa para dicho momento que consistía en la necesidad de implementar una solución que permita soportar el incremento de transacciones mediante una arquitectura de alta disponibilidad donde, para lograr ello, se buscó la renovación de equipos criptográficos hacia su nueva versión para que brinden una mejor prestación a la disponibilidad, continuidad y rendimiento del negocio.
- *Objetivos a cubrir con la implementación.* Se identificaron los objetivos que se cumplirían con la implementación del proyecto:
 - Actualizar la arquitectura permitiendo que los equipos se encuentren en alta disponibilidad
 - Reemplazar los dispositivos criptográficos por la versión más reciente
 - Soportar el futuro incremento de transacciones
 - Definir las responsabilidades de cada área involucrada en el funcionamiento de los equipos y sus componentes
- *Presupuesto estimado.* Se identificaron las categorías para las que se requeriría presupuesto. Estas fueron las siguientes:

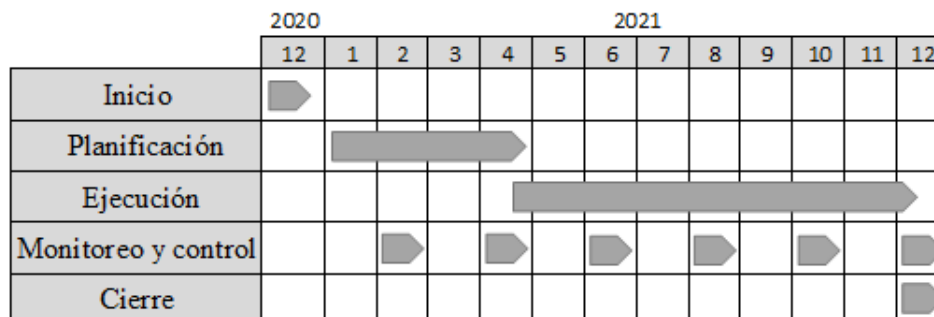
Tabla 14: Categorías del presupuesto estimado del proyecto

Tipo	Descripción
Equipamiento tecnológico	El presupuesto necesario para la adquisición de las herramientas tecnológicas quedó establecido durante esta fase.
Contratación de recursos	El presupuesto estimado para la contratación de recursos fue identificado.

Nota. Fuente: Elaboración propia

- *Cronograma macro.* Para la presentación del proyecto se identificó un cronograma a alto nivel con las actividades a realizarse durante el despliegue.

Figura 11: Cronograma macro



Nota. Fuente: Elaboración propia

- *Requerimientos del proyecto.* Los requerimientos presentados para esta etapa del proyecto fueron los siguientes:

Tabla 15: Requerimientos del proyecto

Ítem	Descripción
1	Actualización de los diagramas de arquitectura físico y lógico
2	Preparación del documento de requerimientos funcionales y técnicos
3	Adecuación de las aplicaciones involucradas en la solución
4	Plan de pruebas de calidad ante el desarrollo
5	Capacitación de usuarios de áreas involucradas
6	Definición del documento de modelo de gobierno

Nota. Fuente: Elaboración propia

La información anteriormente detallada se encuentra en el formato que se muestra a continuación:

Figura 12: Ficha del proyecto

FICHA DE PROYECTO	
Solicitud <u>nov-20</u>	
Proyecto:	Renovación de equipos criptográficos
Portafolio:	
Área solicitante:	Seguridad de la Información
División:	Riesgos
Información del proyecto	
Situación actual:	Los dispositivos criptográficos utilizados en los procesos del banco, no permitirían técnicamente el futuro incremento de transacciones
Descripción:	Cambio de la arquitectura actual y renovación de los equipos criptográficos por otros que brinden una mejor prestación a la disponibilidad, continuidad y rendimiento que busca el negocio.
Objetivos:	- Actualizar la arquitectura permitiendo que los equipos se encuentren en alta disponibilidad - Reemplazar los dispositivos criptográficos por la versión más reciente - Adecuación de aplicaciones para soportar el futuro incremento de transacciones
Presupuesto (M):	5/
Recursos	
Marcar con una X según corresponda:	
Dependencia con otros proyectos:	Sí ☐ No ☒
Precedente de otros proyectos:	Sí ☒ No ☐
Áreas involucradas	Requerimientos del proyecto
Seguridad de la Información	1 Actualización de los diagramas de arquitectura físico y lógico
Arquitectura	2 Preparación del documento de requerimientos funcionales y técnicos
Desarrollo	3 Adecuación de las aplicaciones involucradas en la solución
Calidad	4 Plan de pruebas de calidad ante el desarrollo
Producción	5 Capacitación de usuarios de áreas involucradas
	6 Definición del documento de modelo de gobierno

Nota. Fuente: Elaboración propia

Etapa 2: Planificación

El proyecto fue aprobado en los foros de la empresa, tras esto, se establecieron las actividades y procesos a seguir.

- Se inició el proceso de adquisición de los 4 equipos HSM para que sean ingresados en los centros de datos respectivos. Dentro del contrato con el proveedor se establecieron los siguientes factores para asegurar el cumplimiento del servicio:
 - Características del servicio brindado
 - Características de las herramientas adquiridas
 - Costo detallado
 - SLA
 - Flujo de atención de incidentes
- Una vez adjudicado el proveedor, los equipos fueron recibidos e ingresados con la siguiente distribución:

Tabla 16: Distribución de equipos

Data Center	Cantidad de equipos
Principal	2
Alternativo	2

Nota. Fuente: Elaboración propia

- El proyecto fue presentado en el comité de gestión de la demanda para comunicar su alcance y solicitar la participación de las áreas involucradas. De esta manera, quedaron definidos los participantes clave por cada área y se identificó la necesidad de la contratación de dos recursos adicionales para la fase de implementación. Esta actividad también es conocida como el Plan de Recursos Humanos y quedó definido de la siguiente manera:

Tabla 17: Roles participantes del proyecto

Ítem	Descripción
Equipo de proyecto	- Jefe de Proyecto: Gestión en el proyecto para el cumplimiento de objetivos considerando el manejo de presupuesto, rendición de avance a foros de comité, generación de actas de reuniones, etc.
	- Líder técnico: Integrador de las áreas involucradas en la implementación, liderazgo de los cambios a nivel de infraestructura y aseguramiento del pase a producción.
	- Analista de Aplicaciones: Configuración de las herramientas de aplicaciones y servidores.

Equipo de Desarrollo	El equipo de Desarrollo conformado por un especialista y un supervisor, se encargó de la adecuación de las aplicaciones en coordinación con los proveedores de estas y el apoyo del equipo del proyecto para la gestión con las áreas involucradas.
Equipo de Calidad	El equipo de Calidad conformado por un analista y un supervisor, se encargó de la ejecución del plan de certificación definido.
Proveedor de la herramienta	Con el apoyo del líder técnico y el jefe de proyecto, se consolidaron reuniones de coordinación entre el proveedor y los involucrados para especificaciones técnicas necesarias. Adicionalmente se coordinaron las capacitaciones correspondientes.

Nota. Fuente: Elaboración propia

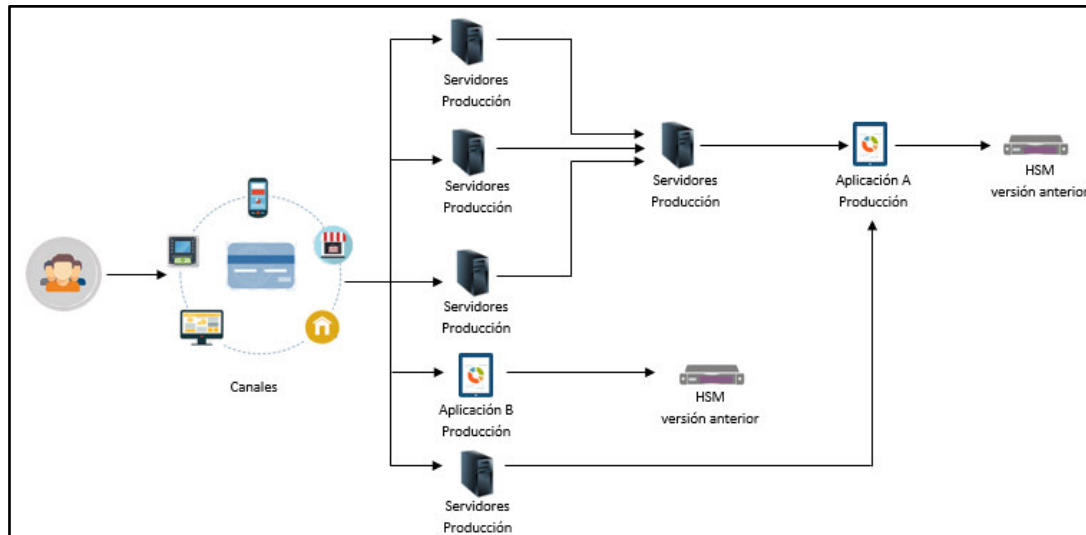
De manera paralela se realizaron las siguientes actividades:

- *Definición detallada del alcance:* Para llevar a cabo esta actividad se pactaron diferentes tipos de reuniones de coordinación:
 - Se involucró a los equipos del banco participando Desarrollo, Arquitectura, Calidad y Producción.
 - Reuniones con los proveedores de las aplicaciones más los equipos del banco, en ellas participaron los equipos de Desarrollo, Arquitectura, Servidores y proveedores relacionados.
 - De manera paralela, se reunieron las áreas de Seguridad de la Información, Seguridad Tecnológica y Arquitectura de Seguridad para validar los controles de seguridad que sean requeridos en el proyecto.
 - Se involucró a los proveedores de los HSM junto con los proveedores de aplicaciones, el equipo de Desarrollo y Arquitectura del banco.
 - Finalmente, se tuvo una reunión que involucró a todos los participantes anteriores para ultimar detalles técnicos de la arquitectura que se estaba proponiendo.

Las reuniones sostenidas duraron 3 meses ya que se realizaron evaluaciones técnicas de las herramientas adquiridas y las adecuaciones que se aspiraban aplicar, obteniendo como resultado de esta actividad los diagramas de arquitectura (AS-IS y TO-BE) físico y lógico.

Se muestra a continuación uno de los entregables de la primera fase que es el diagrama de Arquitectura AS-IS referencial:

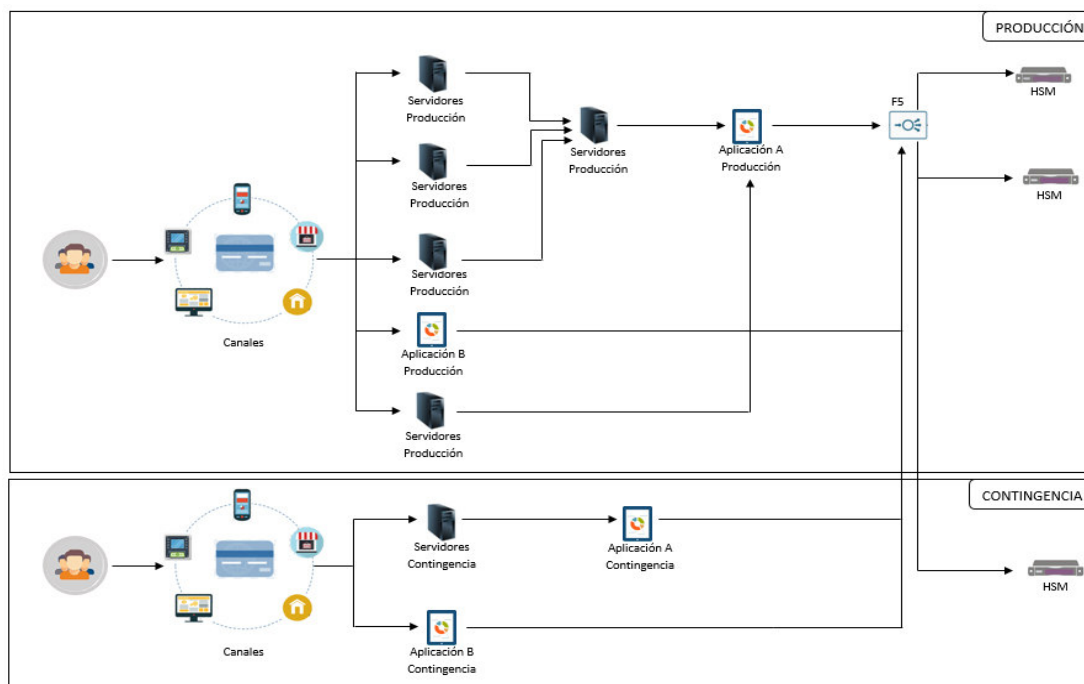
Figura 13: Diagrama de arquitectura AS-IS referencial



Nota. Arquitectura referencial de la versión anterior. Fuente: Elaboración propia

De la misma forma, se muestra el otro entregable que es el diagrama de arquitectura TO-BE referencial:

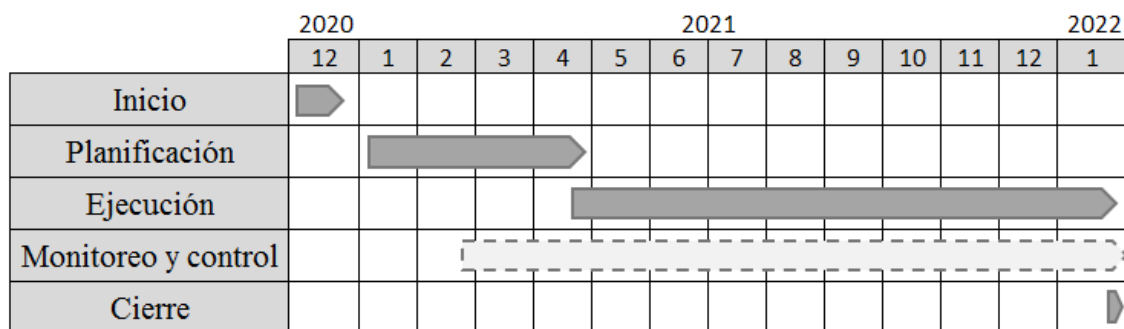
Figura 14: Diagrama de arquitectura TO-BE referencial



Nota. Arquitectura referencial con la nueva versión de equipos. Fuente: Elaboración propia

- *Desarrollo de cronograma detallado:* Una vez obtenido el alcance con mayor detalle y los diagramas de arquitectura actualizados, el equipo de Desarrollo brindó una modificación del cronograma inicial contemplando las actividades por hitos y fechas específicas considerando que la fase de ejecución contempla las actividades en los ambientes de Desarrollo, Calidad, Producción y Contingencia

Figura 15: Cronograma macro actualizado



Nota. Fuente: Elaboración propia

El proyecto ingresó en el portafolio respectivo donde se monitoreó semanalmente su avance, problemas o riesgos presentados para realizar alguna actividad comprometida y planes de acción para subsanarlos, de manera que no impacte negativamente en el cronograma.

Tabla 18: Cronograma detallado por hitos

Actividad	Fecha fin estimada	Responsable
Definición de ficha de proyecto	04/12/2020	Líder técnico
Rackeo de equipos en los centros de datos	21/12/2020	Líder técnico
Entrega de diagramas de Arquitectura	09/04/2021	Arquitecto de infraestructura
Cronograma de definición y ejecución del proyecto	30/04/2021	Jefe de proyecto
Entrega de documentación funcional y técnica	18/06/2021	Supervisor de Desarrollo
Desarrollo - Preparación de configuraciones de infraestructura	16/07/2021	Líder técnico

Desarrollo - Adecuación de aplicaciones	30/09/2021	Supervisor de Desarrollo
Pase a Calidad	11/10/2021	Supervisor de Calidad
Calidad - Finalización de pruebas	30/11/2021	Supervisor de Calidad
Evaluación de riesgos interna	30/11/2021	Seguridad de la Información
Producción - Preparación de configuraciones de infraestructura	13/12/2021	Líder técnico
Solicitud de pase a producción en Comité de Cambios	31/12/2021	Supervisor de Desarrollo y Líder técnico
Pase a producción y Contingencia	24/01/2022	Supervisor de Desarrollo y Líder técnico
Documentación de modelo de gobierno	27/01/2022	Líder técnico
Capacitación de personal involucrado	28/01/2022	Jefe de proyecto
Acta de cierre de proyecto	31/01/2022	Jefe de proyecto

Nota. Fuente: Elaboración propia

- *Determinar el presupuesto:* Posterior a la definición del alcance donde se identificaron los componentes involucrados en la arquitectura y las aplicaciones que requerirían una adecuación, se determinaron las líneas contables para los costos asociados.
 - El presupuesto relacionado a los equipos HSM fue ejecutado en el 2020 con la compra realizada.
 - Para el 2021 se identificaron los costos de las adecuaciones y la gestión de recursos por contratar para el apoyo en el proyecto.

Tabla 19: Presupuesto detallado

Tipo	Subtipo	Año	Monto (S/)
Equipamiento tecnológico	Compra herramientas tecnológicas	2020	774,900.00
	Adecuación de aplicaciones - Desarrollo	2021	24,500.00

Contratación de recursos	Contratación por 7 meses (2 recursos)	2021	115,000.00
---------------------------------	--	------	------------

Nota. Fuente: Elaboración propia

- *Plan de gestión de riesgos:* Durante la fase de planificación se identificaron riesgos que podrían ocurrir durante el despliegue del proyecto:

Tabla 20: Riesgos identificados durante la definición del alcance y planes de acción

Riesgos	Plan de acción
No cumplir con la fecha máxima de pase a producción implicaba una postergación en los cronogramas de proyectos que dependían de este	Seguimiento semanal al proyecto para evitar desvíos en el cronograma
Personal poco calificado, ya que las cajas HSM son herramientas con un manejo muy técnico y que necesita el soporte de personal especializado	Emplear el soporte brindado por el proveedor durante las fases de implementación del proyecto
Poco conocimiento en la integración de los componentes de la arquitectura, ya que se conocían los equipos por separado pero al juntarlos en una misma solución, se tuvieron problemas en cuanto a su conocimiento	Reuniones de coordinación con el equipo del proyecto, Arquitectura de Infraestructura, Desarrollo, proveedores de las aplicaciones integradas, proveedor de las cajas HSM y Seguridad de la Información

Nota. Fuente: Elaboración propia

Considerar que al ingresar al monitoreo semanal, los riesgos presentados durante la ejecución fueron actualizándose al igual que los planes de acción aplicados para contrarrestarlos.

Etapas 3: Ejecución

En esta etapa se realizaron actividades de implementación en 6 grupos:

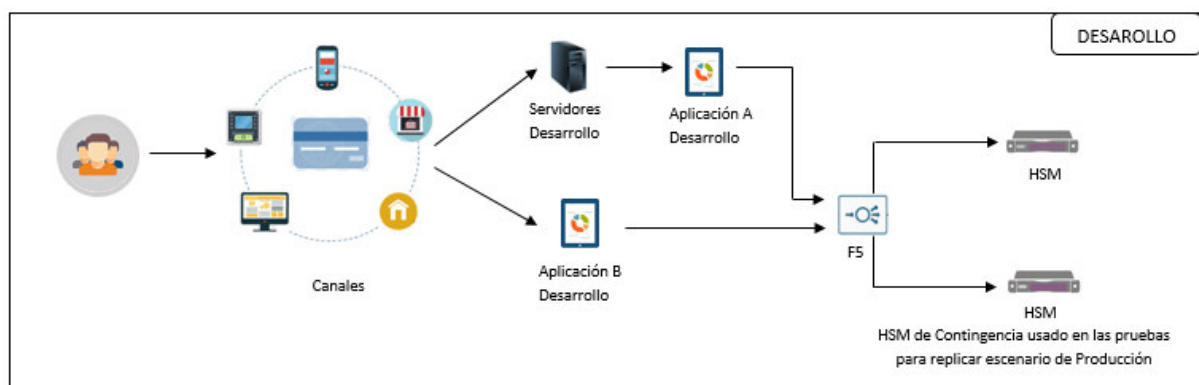
1. Contratación de recursos

Una vez iniciada la etapa de ejecución del proyecto, se activaron los planes de contratación de recursos para las áreas de Producción y Calidad que serían parte del despliegue.

2. Actividades de Desarrollo

Las actividades lideradas por el área de Desarrollo iniciaron con la preparación del Documento de especificaciones funcionales y el Documento de especificaciones técnicas. Considerar que para homogenizar escenarios de prueba, se estableció que el equipo destinado a Contingencia pase a ser del ambiente de Desarrollo y Calidad hasta culminar el ciclo de pruebas establecido. Posterior a ello, retornaría al ambiente de Contingencia para continuar con la arquitectura establecida.

Figura 16: Diagrama de arquitectura Desarrollo



Nota. Arquitectura referencial del ambiente para pruebas. Fuente: Elaboración propia

Tabla 21: Aplicaciones integradas al HSM

Aplicación A	Aplicación B
Permite atender requerimientos de validación de PIN y de Chip de tarjetas de débito, así como requerimientos de cifrado/descifrado de tramas	Utilizada para procesar las operaciones de los clientes que al integrarse con el HSM realiza la traducción de llaves de seguridad

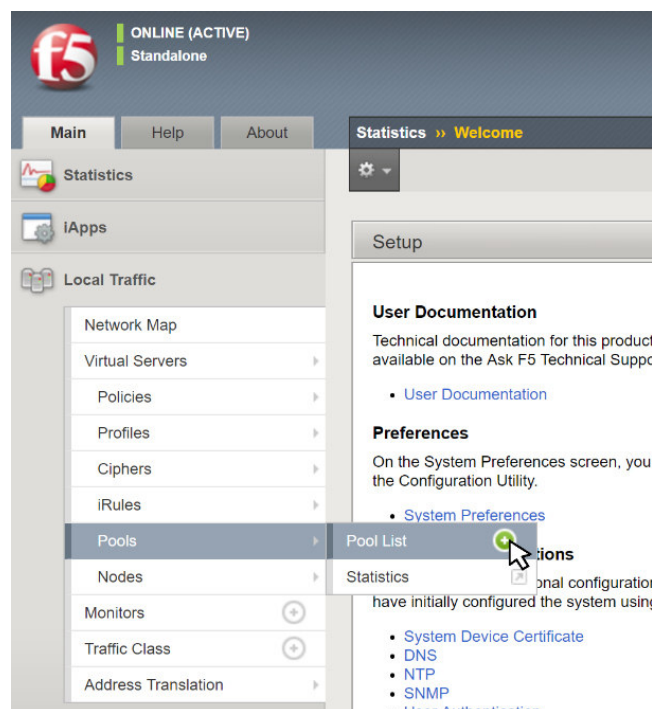
Nota. Se detallan las funcionalidades de las aplicaciones integradas al HSM.

Fuente: Elaboración propia

Una vez culminada la preparación de los documentos, se realizaron las siguientes actividades de forma paralela:

- Configuración de infraestructura: Las tareas definidas para este punto estuvieron a cargo del líder técnico con el apoyo y soporte de las áreas de Arquitectura, Redes, Servidores y Desarrollo.
- Identificación del segmento de red e IPs donde se encontrarían los componentes (HSM y F5)
- Configuración de parámetros del HSM identificando los comandos host que debían estar activos para integrarse con las aplicaciones y puedan brindar funcionamiento adecuado, además de configurar la LMK y las IPs correspondientes.
- Configuración del virtual server del F5 donde se identificaron los pools para las reglas de la siguiente manera:

Figura 17: Imagen referencial de la plataforma F5



Nota. Fuente: F5 (2019)

Tabla 22: Configuración de virtual server en F5 de Desarrollo

Virtual Server ↓ IP del F5	Pool 1 Desarrollo	Prioridad 1	IP HSM 1
		<i>Prioridad 2</i>	<i>IP HSM 2</i>
	Pool 2 Desarrollo	Prioridad 1	IP HSM 2
		<i>Prioridad 2</i>	<i>IP HSM 1</i>

Nota. Fuente: Elaboración propia

Tabla 23: Configuración de política virtual server en F5 de Desarrollo

Políticas Virtual Server	IP Desarrollo Aplicación A	<i>forward traffic</i>	<i>to pool</i>	Pool 1 Desarrollo
	IP Desarrollo Aplicación B	<i>forward traffic</i>	<i>to pool</i>	Pool 2 Desarrollo

Nota. Fuente: Elaboración propia

De esta manera los equipos se encuentran en alta disponibilidad para las dos aplicaciones transaccionales que maneja la empresa.

- Configuración de reglas de firewall para que las aplicaciones puedan comunicarse con el F5 y el F5 con el HSM
- Adecuación de aplicaciones
 - Aplicación A: Dicha aplicación requirió que la adecuación sea de parámetros de sus componentes, así como referenciar la nueva IP del F5 junto con el puerto identificado.
 - Aplicación B: Dicha aplicación requirió que la adecuación sea a tablas y parámetros de sus componentes para aceptar valores que la nueva versión de HSM solicitaba para el funcionamiento, además de referenciar la nueva IP del F5 junto con el puerto identificado.

Una vez que la infraestructura fue configurada con éxito y las adecuaciones fueron culminadas, se inició el plan de pruebas unitarias relacionado a las pruebas en canales para validación de PIN/CHIP, pruebas de intercambio de llaves y pruebas de transferencias inmediatas. A su vez, se realizaron pruebas de permutación en el F5 simulando una caída y saturación.

Tabla 24: Cronograma de actividades Desarrollo

Ítem	Actividad	Días
1	Adecuación desarrollo Aplicación A	21
2	Adecuación desarrollo Aplicación B	14
3	Instalación de componentes	3
4	Pruebas unitarias de aplicaciones	35
5	Pruebas unitarias de permutación de HSM en F5	5
6	Documentación	7

Nota. Fuente: Elaboración propia

Las pruebas culminaron de manera satisfactoria, de manera que se pudo realizar el pase a Calidad en el tiempo determinado.

3. Actividades de Certificación

El pase a Calidad fue en Octubre, para ello se tuvo como actividad predecesora la configuración de la infraestructura para dicho ambiente:

Tabla 25: Configuración de virtual server en F5 de Calidad

Virtual Server ↓ IP del F5	Pool 1 Calidad	Prioridad 1	IP HSM 1
		<i>Prioridad 2</i>	<i>IP HSM 2</i>
	Pool 2 Calidad	Prioridad 1	IP HSM 2
		<i>Prioridad 2</i>	<i>IP HSM 1</i>

Nota. Fuente: Elaboración propia

Tabla 26: Configuración de política virtual server en F5 de Calidad

Políticas Virtual Server	IP Calidad Aplicación A	<i>forward traffic</i>	<i>to pool</i>	Pool 1 Calidad
	IP Calidad Aplicación B	<i>forward traffic</i>	<i>to pool</i>	Pool 2 Calidad

Nota. Fuente: Elaboración propia

Por el lado del equipo de Calidad, se ejecutaron los escenarios de pruebas de certificación definidos para validar que los canales funcionen de manera adecuada ante las modificaciones realizadas.

Tabla 27: Cronograma de actividades de Certificación

Ítem	Actividad	Días
1	Inducción	5
2	Preparación e instalación de ambiente de prueba	4
3	Preparación de data	5
4	Ejecución de pruebas – Ciclo 1	15
5	Corrección de defectos (Desarrollo)	3
6	Preparación e instalación de ambiente de prueba	4
7	Ejecución de pruebas – Ciclo 2	10
8	Pruebas UAT	3
9	Ratificación	2

Nota. Fuente: Elaboración propia

Las pruebas se realizaron de manera satisfactoria, de esta manera se pudo continuar con las actividades del cronograma para el pase a producción.

4. Pase a producción y ratificaciones

Pase a producción:

El pase a producción pudo dividirse en dos tiempos: Pase a Producción y Pase a Contingencia.

Tabla 28: Cronograma de pase a producción

Tipo de pase	Fecha
Pase a Producción	02/01/2022 – 03/01/2022
Pase a Contingencia	22/01/2022 – 24/01/2022

Nota. Fechas propuestas para el pase a Producción. Fuente: Elaboración propia

Figura 18: Cronograma por hitos para el Pase a Producción



Nota. Hitos identificados para el pase a Producción. Fuente: Elaboración propia

- Configuración de parámetros del HSM según los comandos host identificados y probados en Desarrollo y Calidad, además de configurar las IPs correspondientes y la LMK. Esta actividad se realizó con la participación de los custodios de componentes de la LMK a través del proceso de ceremonia de llaves.
- Configuración del virtual server del F5 donde se identificaron los pools para las reglas de la siguiente manera:

Tabla 29: Configuración de virtual server en F5 de Producción

Virtual Server ↓ IP del F5	Pool 1 Producción	Prioridad 1	IP HSM 1
		Prioridad 2	IP HSM 2
		Prioridad 3	IP HSM 3
	Pool 2 Producción	Prioridad 1	IP HSM 2
		Prioridad 2	IP HSM 1
		Prioridad 3	IP HSM 3

Nota. Fuente: Elaboración propia

Tabla 30: Configuración de política virtual server en F5 de Producción

Políticas Virtual Server	- IP Producción Aplicación A	<i>forward traffic to pool</i>	Pool 1
	- IP Contingencia Aplicación A		Producción
	- IP Producción Aplicación B	<i>forward traffic to pool</i>	Pool 2
	- IP Contingencia Aplicación B		Producción

Nota. Fuente: Elaboración propia

- Configuración de reglas de firewall para que las aplicaciones puedan comunicarse con el F5 y el F5, con el HSM
- Preparación de documentación y componentes de reversa identificados en caso el pase a producción no resulte de manera exitosa.
- Preparación del Plan de pase a producción con las actividades y responsables por áreas. Considerar que la estrategia que se tomó en coordinación con todas las áreas involucradas fue enviar la operativa a contingencia de la versión anterior mientras se realizaba el pase en los componentes de producción.

Figura 19: Ficha referencial del plan de pase a Producción

PLAN PASE A PRODUCCIÓN						
			Ticket de aprobación _____			
Proyecto: Fecha de pase: 02/01/2022 - 03/01/2022						
Actividades						
Pasar la operativa a canales de Contingencia						
Paso	Responsable	Actividad	Ticket asociado	Fecha	Hora Ejecución	Observación
1	Aplicaciones/Operadores	Activar Aplicación A y B de Contingencia		02/01/2022	00:00 - 01:30	
2	Monitoreo	Monitoreo de URLs de canales cotingencia			01:30 - 01:45	
3	QA	Ratificación canales			01:45 - 04:00	Se ratificaron todos los canales involucrados
Configuración de servidores de aplicación, F5 y reinicios programados						
Paso	Responsable	Actividad	Ticket asociado	Fecha	Hora Ejecución	Observación
4	Aplicaciones	Validación de conexión		02/01/2022		Se ejecutó antes del pase ya que solo era validación
5	Aplicaciones	Configuración HSM con Aplicación A			02:00 - 03:00	
6	Aplicaciones/Prv F5 (Soporte)	Validación de F5 y carga de llaves			03:00 - 04:00	Con el apoyo de Seguridad por la custodia de llaves
7	Operadores	Ejecución script en BD Aplicación B		03/01/2022	00:00 - 00:20	
8	Aplicaciones	Configuración HSM con Aplicación B			00:20 - 00:40	
9		Actividades adicionales			00:40 - 01:00	
Retornar operativa de canales a Producción						
Paso	Responsable	Actividad	Ticket asociado	Fecha	Hora Ejecución	Observación
10	Aplicaciones/Operadores	Retornar a Aplicación A y B de Producción		03/01/2022	01:00 - 02:30	
Pruebas de ratificación de canales						
Paso	Responsable	Actividad	Ticket asociado	Fecha	Hora Ejecución	Observación
11	QA	Ratificación de canales		03/01/2022	02:30 - 03:30	
12	QA / Monitoreo	Ratificación por monitoreo de operaciones			03:30 - 04:00	
13	Canales	Ratificación de recepciones			06:00 - 06:30	
14	QA / Canales	Ratificación de envíos			08:30 - 09:00	
15	QA / Canales	Pinpad Agencia: Ratificación de validación de PIN, Chip y cambio de PIN			09:00 - 10:00	
Soporte y monitoreo						
Paso	Responsable	Actividad	Ticket asociado	Fecha	Hora Ejecución	Observación
16	Canales	Soporte y monitoreo		03/01/2022	09:00 - 18:00	Soporte y monitoreo del servicio en Producción con los nuevos equipos HSM

Nota. Se muestran las actividades realizadas para el pase a producción. Fuente: Elaboración propia

- El plan de pase a producción se presentó en el Comité de Cambios para que sea aprobado y pueda realizarse. Este comité está conformado por las áreas de Producción, Riesgo Operativo, Seguridad de la Información y Seguridad Tecnológica. Su aprobación fue el 31/12/2021 para que el pase sea ejecutado desde las 00:00 horas del 02/01/2022
- Las actividades de actualización de componentes fueron realizadas de acuerdo al cronograma de pase en conjunto con las pruebas de ratificación.
- La ratificación de los canales culminó el día programado de manera satisfactoria donde se realizaron pruebas como las siguientes:
 - Validación de PIN utilizando pinpad

- Validación de CHIP utilizando pinpad
- Cambio de PIN utilizando pinpad
- Registro de usuario en banca por internet
- Transferencias al mismo banco utilizando banca por internet
- Transferencias interbancaria utilizando banca por internet
- Pago de servicios utilizando banca por internet
- Depósito con tarjeta en agente
- Retiro de efectivo en agente
- Retiro de efectivo en ATM
- Pago de servicios de manera física utilizando POS
- El servicio se mantuvo estable en Producción de manera que el pase fue catalogado como exitoso.

Pase a Contingencia: Para cumplir con esta actividad, se realizó de manera paralela la configuración de infraestructura en el equipo de Contingencia (HSM y Firewall):

- Configuración de parámetros del HSM según los comandos host identificados y probados en Desarrollo y Calidad, además de configurar las IPs correspondientes y la LMK. Esta actividad se realizó con la participación de los custodios de componentes de la LMK a través del proceso de ceremonia de llaves.
- La configuración del F5 de Producción fue replicado para Contingencia de manera automática.
- Configuración de reglas de firewall para que el F5 pueda tener conexión con el HSM
- Preparación de documentación y componentes de reversa identificados en caso el pase a contingencia no resulte de manera exitosa.
- Preparación del Plan de pase a contingencia con las actividades y responsables por áreas. Considerar que la estrategia que se tomó en coordinación con todas las áreas involucradas fue pasar la operativa a Contingencia durante el pase y que el servicio se quede en dicho ambiente por un día para retornarlo a Producción.

Tabla 31: Ficha de pase a producción (Contingencia)

PLAN PASE A CONTINGENCIA						
			Ticket de aprobación _____			
Proyecto:						
Fecha de pase:			22/01/2022 - 24/01/2022			
Actividades						
Configuración de servidores de aplicación, F5 y reinicios programados						
Paso	Responsable	Actividad	Ticket asociado	Fecha	Hora Ejecución	Observación
1	Aplicaciones	Validación de conexión		22/01/2022		Se ejecutó antes del pase ya que solo era validación
2	Aplicaciones	Configuración HSM con Aplicación A			22:00 - 23:00	
3	Aplicaciones	Inactivar HSMs de Producción para redireccionar a HSM de Contingencia			23:00 - 23:20	
4	Aplicaciones/Prv F5 (Soporte)	Validación de F5 y carga de llaves			23:20 - 23:40	Con el apoyo de Seguridad por la custodia de llaves
5	Aplicaciones	Configuración HSM con Aplicación B			23:40 - 00:00	
Pasar operativa de canales de Producción a Contingencia						
Paso	Responsable	Actividad	Ticket asociado	Fecha	Hora Ejecución	Observación
6	Monitoreo	Monitoreo de URLs de canales cotingencia		23/01/2022	00:15 - 00:30	
7	Aplicaciones/Operadores	Activar canales de contingencia			00:30 - 01:30	
Pruebas de ratificación de canales						
Paso	Responsable	Actividad	Ticket asociado	Fecha	Hora Ejecución	Observación
8	QA	Ratificación de canales		23/01/2022	01:30 - 02:30	
9	QA / Monitoreo	Ratificación por monitoreo de operaciones			02:30 - 03:00	
10	Canales	Ratificación de recepciones		24/01/2022	06:00 - 06:30	
11	QA / Canales	Ratificación de envíos			08:30 - 09:00	
12	QA / Canales	Pinpad Agencia: Ratificación de validación de PIN, Chip y cambio de PIN			09:00 - 10:00	
Soporte y monitoreo						
Paso	Responsable	Actividad	Ticket asociado	Fecha	Hora Ejecución	Observación
13	Canales	Soporte y monitoreo		24/01/2022	09:00 - 18:00	Soporte y monitoreo del servicio en Contingencia con los nuevos equipos HSM

Nota. Se muestran las actividades realizadas para el pase a contingencia. Fuente: Elaboración propia

- El plan de pase a contingencia se presentó en el Comité de Cambios para que sea aprobado y pueda realizarse. Su aprobación fue el 21/01/2022 para que el pase sea ejecutado desde las 00:00 horas del 22/01/2022.
- Las actividades de actualización de componentes fueron realizadas de acuerdo al cronograma de pase en conjunto con las pruebas de ratificación
- La ratificación de canales culminó en la fecha programada de manera exitosa realizándose pruebas similares a las realizadas para el pase a Producción anteriormente descritas.
- El servicio se mantuvo estable en Contingencia de manera que el pase fue catalogado como exitoso y el retorno a Producción se realizó el 25/01/2022 según lo establecido. Considerar que posterior al retorno a Producción, se realizó de manera adicional la ratificación para asegurar el buen funcionamiento del servicio en Producción.

5. Definición del modelo de gobierno: El modelo de gobierno es utilizado como una herramienta de gestión que permite la integración de las áreas para asegurar que la tecnología se pueda mantener a lo largo del tiempo. En este documento se plasman las responsabilidades por cada área del banco que va a operar o dar soporte a la nueva versión de los equipos HSM.

Para la generación del documento se realizaron las siguientes actividades:

- Preparación del documento inicial del modelo de gobierno
- Reuniones de coordinación con los líderes de las áreas involucradas para plasmar los servicios brindados o sus responsabilidades mediante el consenso
- Conformidad por parte de los líderes ante lo coordinado
- Socialización del documento del modelo de gobierno
- Marcha blanca de los equipos para tomar control sobre el modelo de gobierno establecido
- Inicio de operaciones del modelo de gobierno

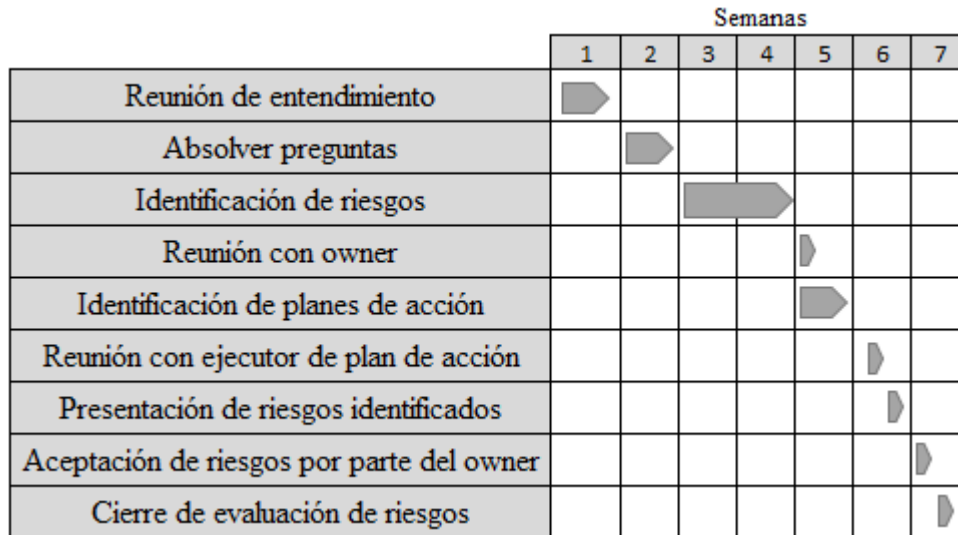
Dentro del documento se incorporaron los siguientes temas:

- Objetivo del documento
- Alcance
- Diagrama de Arquitectura TO-BE
- Temario y ruta de la capacitación realizada
- Documentación interna actualizada con la implementación del proyecto
- Responsabilidades por áreas: Producción, Desarrollo, Calidad, Seguridad de la Información, Seguridad Tecnológica, Arquitectura.
- Servicios brindados por el proveedor como soporte de la herramienta adquirida
- Matriz de escalamiento ante incidentes

6. Evaluación de riesgos: Por la magnitud del proyecto y los cambios que generaría en los componentes dentro de la arquitectura, las áreas de Riesgos junto con el owner de la iniciativa, identificaron la necesidad de realizar una evaluación de riesgos a demanda para el proyecto. Esta actividad fue realizada durante la fase de ejecución para identificar posibles mejoras antes del pase a producción.

La actividad fue realizada de acuerdo con el siguiente cronograma:

Figura 20: Cronograma de evaluación de riesgos



Nota. Se muestran los hitos presentados durante la evaluación de riesgos. Fuente: Elaboración propia

La duración de la evaluación de riesgos fue de siete semanas y tuvo como resultado la identificación de dos riesgos nuevos por la implementación del proyecto:

Tabla 32: Matriz de riesgos

Riesgo	Plan de Acción	Responsable
Indisponibilidad del servicio por falla en la permutación del F5	Ejecutar la permutación hacia el ambiente de Contingencia desde el ambiente de Producción y viceversa	Producción
Falla en la activación del ambiente de Contingencia por falta de procedimientos actualizados	Actualización de manuales relacionados a la adecuación y la nueva versión de los HSM	Desarrollo

Nota. Fuente: Elaboración propia

Los planes de acción establecidos y aprobados por sus áreas ejecutoras fueron llevados a cabo en las fechas acordadas. Culminados, se enviaron los resultados o entregables y se adjuntaron las evidencias.

Etapa 4: Monitoreo y control del proyecto

La implementación del proyecto fue monitoreada semanalmente en el comité del portafolio respectivo donde participan los líderes técnicos y jefes de proyectos de las iniciativas, adicionalmente, los líderes de las áreas de Desarrollo, Calidad, Producción, Continuidad del Negocio, Seguridad de la Información, Seguridad Tecnológica y Arquitectura. En él se presentaron las actividades más relevantes de la semana, porcentaje de avance, riesgos y problemas que podrían haber surgido para las actividades de la semana y los planes de acción relacionados para su mitigación.

Figura 21: Plantilla de avance de proyecto

 Hitos comprometidos	 Tiempo	 Riesgos y problemas	 Plan de acción
<u>Actividades realizadas:</u> <u>Actividades pendientes:</u>		R ☐ P ☐ <u>Descripción</u>	<u>PA:</u> <u>Responsable:</u>

Nota. Fuente: Elaboración propia

Durante la implementación del proyecto se presentaron controles de cambio en relación al cronograma que fueron presentados ante el foro del comité para ser aprobados según motivo o justificación. La ficha presentada para la solicitud fue la siguiente:

Figura 22: Ficha de control de cambios

FICHA DE CONTROL DE CAMBIOS	
	Acta # _____
Fecha de solicitud: _____	
Proyecto: _____	
Portafolio: _____	
Motivo del control de cambios:	
Presupuesto	☐ _____
Dependencia	☐ _____
Recursos	☐ _____
Actividades	☐ _____
Estado del proyecto:	
Planificación	☐ _____
Diseño	☐ _____
Ejecución	☐ _____
Cierre	☐ _____
Observaciones: _____	

_____ RESULTADO	

Nota. Fuente: Elaboración propia

Etapas 5: Cierre del proyecto

Las actividades de cierre de proyecto fueron las siguientes:

- Posterior al pase a producción y contingencia, junto con sus respectivas ratificaciones, se comunicó vía correo a las áreas de Sistemas y de Negocios el despliegue satisfactorio del proyecto. De esta manera se dejó constancia que la implementación fue realizada durante el tiempo establecido y el resultado del mismo.
- El equipo del proyecto gestionó con el proveedor de los equipos HSM una capacitación para las áreas del banco que se encuentran involucradas en la

- operatividad y el soporte de dichos equipos. Esta actividad se realizó en 2 sesiones.
- Preparación de la ficha de cierre de proyecto para presentarla ante el comité del portafolio y el gerente divisional de riesgos

Figura 23: Ficha de cierre de proyecto

FICHA DE CIERRE DE PROYECTO																			
I. Información general																			
Proyecto: _____ Líder técnico del proyecto _____ Fecha: _____																			
II. Entregables del proyecto																			
III. Pendientes																			
IV. Aprobación del documento																			
<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <thead> <tr> <th style="width: 25%;">Cargo</th> <th style="width: 25%;">Responsable</th> <th style="width: 25%;">Fecha</th> <th style="width: 25%;">Firmas</th> </tr> </thead> <tbody> <tr> <td style="height: 20px;"></td> <td></td> <td></td> <td></td> </tr> <tr> <td style="height: 20px;"></td> <td></td> <td></td> <td></td> </tr> <tr> <td style="height: 20px;"></td> <td></td> <td></td> <td></td> </tr> </tbody> </table>				Cargo	Responsable	Fecha	Firmas												
Cargo	Responsable	Fecha	Firmas																

Nota. Fuente: Elaboración propia

3.3 Evaluación

3.3.1 Evaluación económica / Evaluación Costo-Beneficio

a) *Evaluación económica.* El proyecto contempla costos de tecnología y de personal contratados específicamente para la implementación del mismo.

A continuación, la siguiente tabla detalla la estructura de costos del proyecto:

Tabla 33: Estructura de costos del proyecto

Tipo	Subtipo	Año	Costo mensual	Costo total (S/)
Equipamiento tecnológico	Compra herramientas tecnológicas	2020	-	774,900.00
	Adecuación de aplicaciones - Desarrollo	2021	24,500.00	24,500.00
Contratación de recursos	Contratación por 7 meses (2 recursos)	2021	15,000.00	105,000.00
	Equipos y licencias	2021	-	10,000.00
			TOTAL	914,400.00

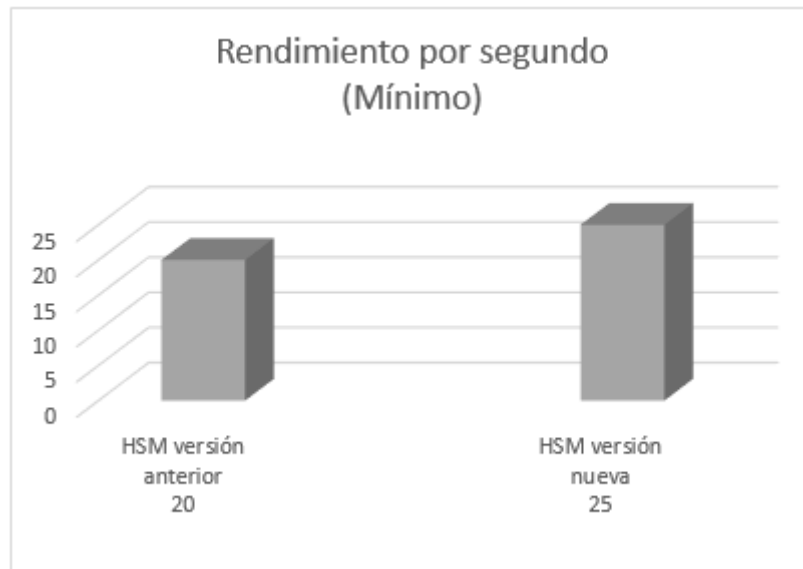
Nota. Fuente: Elaboración propia

b) *Evaluación Costo – Beneficio.* La implementación del proyecto generó beneficios técnicos y funcionales al implementarse, los cuales serán listados a continuación:

1. Aumento en el rendimiento de los equipos HSM

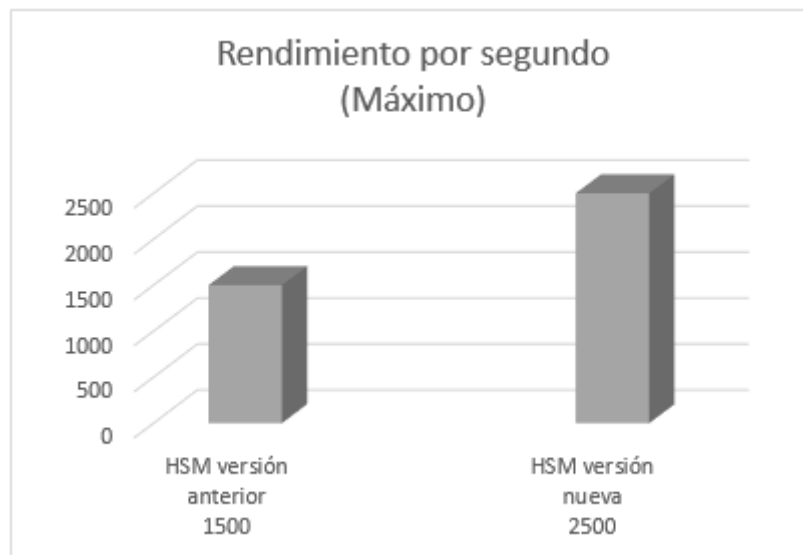
El rendimiento se mide en la nueva versión de los dispositivos en CPS (llamadas por segundo) en lugar de TPS (transacciones por segundo), como es llamado en la versión anterior; sin embargo, miden la misma característica. Esta característica permite que los nuevos equipos tengan un mayor rendimiento ante la cantidad de transacciones que puedan realizarse por segundo de manera simultánea.

Figura 24: Comparación del rendimiento por segundo (Nivel mínimo)



Nota. El gráfico representa el rendimiento por segundo (nivel mínimo) para ambas versiones de equipos HSM. Fuente: Elaboración propia

Figura 25: Comparación del rendimiento por segundo (Nivel máximo)



Nota. El gráfico representa el rendimiento por segundo (nivel máximo) para ambas versiones de equipos HSM. Fuente: Elaboración propia

2. Implementación de características técnicas para el soporte de tarjetas de pago

La nueva versión de los HSM permite técnicamente la implementación de mejoras en el proceso criptográfico que maneja la empresa. Adicionalmente, permite las siguientes características:

- Funciones de verificación de PIN y tarjetas para las principales marcas de pago
- Autorización de transacciones de pago por móvil y gestión de claves
- Carga remota de claves para dispositivos de cajeros y puntos de venta
- Generación e impresión de PIN

3. Mejora en el servicio brindado por el diseño de arquitectura utilizado

Permite que la empresa esté preparada para una operación de régimen 24x7 y cuente con capacidad de respuesta ante el crecimiento de transacciones en un escenario de misión crítica.

4. Equipos con soporte vigente por parte del proveedor

Al renovar los equipos por una nueva versión, obtuvimos las siguientes características de los dispositivos y servicios por partes del proveedor:

- Firmware con nuevas actualizaciones funcionales y de seguridad
- Herramientas con prestaciones técnicas actualizadas
- Mantenimiento preventivo
- Mantenimiento correctivo
- Soporte ante incidentes

3.3.2 Interpretación del VAN y del TIR

Costo del proyecto: El proyecto tuvo una inversión inicial de 914,400.00. El detalle de este se puede observar en la Tabla 33.

Ahorro mensual en atención a Reclamos: Se considerará que el 2% de la diferencia entre las transacciones por minuto de ambas versiones podría generar reclamos por transacciones no procesadas, enviadas, entre otras y que estas tienen que ser atendidas por un equipo de personas dedicadas a realizar esta actividad:

Figura 26: Transacciones con posibilidad a generar reclamos

Tipo de HSM	Tx por minuto		Tx por día	Tx por mes
HSM nueva versión	1500	Diferencia Tx	300	432000
HSM versión anterior	1200	% reclamos	2%	8640
				259200

Nota. Se considera la cantidad de transacciones (TX) que podría generar reclamos en caso los dispositivos no cuenten con capacidad técnica adecuada. Fuente: Elaboración propia

Figura 27: Pagos a equipo de Atención de Reclamos

Soporte a reclamos		Sueldo unitario	Sueldo por equipo
Analistas Call Center	8	4000	32000
Analistas de reclamos	5	5000	25000
Analistas de TI	2	6000	12000
TOTAL MENSUAL			69000

Nota. Monto estimado de salario mensual para equipo de Atención de Reclamos. Fuente: Elaboración propia

Ante los montos indicados anteriormente se aplican las fórmulas de VAN y TIR resultando lo siguiente:

Figura 28: VAN y TIR

Descripción	Año 0	Año 1	Año 2
Beneficios		828000	828000
Inversión	914400		
Flujo de caja	-914400	828000	828000

Tasa	20%
VAN	S/.350,600.00
TIR	51%

Nota. Fuente: Elaboración propia

El VAN resultante del proyecto es positivo considerando 2 años, de ello podemos desprender que el proyecto es rentable. Por otra parte el TIR, que es el beneficio que resulta del proyecto incluyendo la pérdida del valor del dinero en el tiempo, muestra para este proyecto que la tasa de descuento establecida es superada.

CAPÍTULO IV. REFLEXIÓN CRÍTICA DE LA EXPERIENCIA

La experiencia obtenida por la participación en el proyecto permitió la implementación de tecnología e infraestructura que ayudará a mejorar el proceso criptográfico de la entidad financiera utilizando las nuevas capacidades técnicas de los dispositivos criptográficos.

Fue importante la participación de los proveedores de las herramientas y aplicaciones en las reuniones con el equipo del proyecto durante la etapa de planificación para identificar el adecuado funcionamiento de estas en la integración planteada, ya que al ser nueva tecnología, la implementación de las capacidades técnicas que ofrecían los equipos no se encontraba definida totalmente.

La coordinación oportuna con las áreas involucradas en los procesos a actualizar fue necesaria para que se identifique el alcance de manera adecuada y se valide el impacto que generaría.

Para las actividades de pase a producción, dentro de la etapa de ejecución, se tuvo la participación y compromiso por parte de todas las áreas involucradas pese a la extensión y criticidad de la actividad. El compromiso por parte de todos los actores fue clave para asegurar un correcto pase a producción y contingencia dentro del tiempo establecido.

Fue de vital importancia incluir al proyecto en un portafolio para su gestión, de esta manera se trató de forma integral la iniciativa controlando el presupuesto, los recursos y el avance del cronograma en el tiempo adecuado para identificar los riesgos y problemas presentados, con ello, fueron escalados en el momento necesario sin que esto genere retrasos en la fecha máxima de implementación. También dentro del caso de reprogramación de actividades del cronograma, para poder generar la presentación de los controles de cambio en los foros correspondientes.

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

- La metodología de gestión de proyectos empleada, permitió el reemplazo de los equipos HSM por su nueva versión que tiene el firmware actualizado y la capacidad técnica de implementación de estándares de seguridad solicitados por la industria de tarjetas de pago, utilizando fases para su implementación y asegurando la fecha comprometida. (Ver punto 3.2.5.1) De acuerdo con ello, la empresa podrá utilizar y asegurar las funcionalidades mostradas para los dispositivos en las secciones anteriores. (Ver punto 3.2.4.1.1).
- La arquitectura fue actualizada con las mejoras propuestas que permiten que 2 equipos HSM en Producción se encuentren configurados de manera paralela controlados mediante un balanceador de carga o F5 para asegurar la alta disponibilidad aprovechando las funcionalidades propias de este. En esta configuración también se incluyó un nodo adicional que es del ambiente de Contingencia para asegurar la disponibilidad en el caso de que los equipos de producción presenten alguna interrupción y la operativa continúe en dicho ambiente. Los escenarios anteriormente mencionados tuvieron pruebas de Continuidad de Negocio para el aseguramiento de la disponibilidad del servicio. Estas actualizaciones se encuentran descritas en la figura relacionada a la arquitectura TO-BE del proyecto. (Ver punto 3.2.5.1).

Para asegurar que la configuración funcione de manera adecuada, se realizaron pruebas durante la implementación del proyecto.

- Se logró la adecuación de aplicaciones junto con las áreas de Desarrollo y los proveedores relacionados a estas para la integración con los equipos. A nivel de infraestructura, se incluyeron nuevas segmentaciones dedicadas y reglas de habilitación de puertos. Estas se encuentran especificadas en las actividades de Desarrollo y Certificación descritas dentro de la fase de Ejecución. (Ver punto 3.2.5.1)

Para asegurar que el despliegue en Producción cumpla con los requerimientos definidos, fue esencial la definición de una lista de actividades mostradas en las actividades de Pase a Producción y Contingencia dentro de la fase de Ejecución

(Ver punto 3.2.5.1), para dar soporte durante el pase y posterior a este. De esta forma se identificarían y alertarían anomalías en el funcionamiento del servicio.

- En conjunto con las áreas involucradas, se logró la definición de un modelo de gobierno con las responsabilidades competentes para el soporte y operación de los dispositivos y sus componentes en los ambientes en los que se encuentran. Los puntos considerados en el documento de Modelo de gobierno se encuentran dentro de la Fase de Ejecución: Definición del modelo de gobierno. (Ver punto 3.2.5.1). Para lograr identificar a las áreas responsables y la función que cumplen con los equipos que ya se encuentran en Producción, fue importante involucrarlos desde la etapa inicial de planificación.

5.2 Recomendaciones

Para la implementación de este tipo de proyectos se recomienda lo siguiente:

- Generar documentación con las nuevas configuraciones desplegadas en las herramientas tecnológicas considerando todos los ambientes en los que se realizarán actividades.
- Plan de pruebas para cada casuística que se presenta en la ejecución del servicio que va a ser impactado, de esta manera se asegura que no se realicen supuestos ni se presenten problemas en Producción.
- Identificar el proceso de renovación de la tecnología adquirida por la empresa y los procesos involucrados a esta, para coordinar y socializar a los interesados en el menor tiempo posible utilizando los canales formales establecidos por la organización.
- Realizar una evaluación de riesgos integral al proyecto para identificar escenarios de riesgos que podrían presentarse, medir su criticidad de acuerdo con la metodología que cuenta la empresa e identificar planes de acción para su mitigación, en caso requiera.
- Identificar una matriz de escalamiento para incidencias presentadas donde se establezca el tipo de alerta, el tiempo máximo de atención, el área responsable y las acciones a seguir para la mitigación.
- Capacitar al personal involucrado con las herramientas tecnológicas adquiridas para asegurar la implementación de todas las funcionalidades que puedan brindar y, de esta manera, se mejore el servicio buscado

5.3 Fuentes de información

- Aguilar, G. (2016). Implementación de un modelo simplificado de firma digital basado en la tecnología PKI y la invocación por protocolos. Caso de estudio: Municipalidad de Miraflores (tesis de pregrado). Universidad Nacional Mayor de San Marcos, Lima, Perú.
- Alba, M. (2017). Implementación del método de administración de llaves DUKPT en el simulador ASSET para transacciones financieras en dispositivos punto de venta (trabajo de grado). Universidad Autónoma del Estado de México, Valle de Chalco Solidaridad, México
- Ayala, L., Peñaherrera, A. y Urrea, C. (2015). Dirección del Proyecto: Implementación de la Solución Crecimiento Crediticio en Diners Club (tesis de posgrado). Universidad Peruana de Ciencias Aplicadas, Lima, Perú.
- Boireau, O. (2018). Securing the blockchain against hackers. Obtenido de Network Security
- Bastidas, J. (2021). Análisis, diseño e implementación de balanceador de carga segmentando la red del sistema de balanzas de pequeñas y medianas empresas del sector industrial ciudad de Guayaquil (tesis de pregrado). Universidad de Guayaquil, Guayaquil, Ecuador.
- F5, Inc. (2018). *White Papers*. Obtenido de Página oficial de F5: https://www.f5.com/es_es
- García, R. (2020). Análisis de Smart contracts en Ethereum e Identidad Soberana (trabajo fin de Máster). Universidad Politécnica de Madrid, Madrid, España.
- Indecopi. (2018). *Sistema de tarjetas de pago*. Obtenido de Página institucional de Indecopi: <https://www.indecopi.gob.pe/>
- PCI Security Standards Council. (2018). *Glosario de términos de seguridad de pagos y de la información*. Obtenido de Official PCI Security Standards Council Site: <https://es.pcisecuritystandards.org/>

- PCI Security Standards Council. (2018). *Requisitos de seguridad y procedimientos de prueba de PIN v3.0*. Obtenido de Official PCI Security Standards Council Site: <https://es.pcisecuritystandards.org/>
- Perdomo, C., Abril, W. y Castro, L. (2020). Planeación de un proyecto de implementación para una solución de balanceo de carga BIG-IP F5 en la universidad latinoamericana de Bogotá basado en el modelo PMI (trabajo de grado). Universidad Santo Tomás, Bogotá, Colombia.
- Project Management Institute, Inc;. (2017). *La guía de los fundamentos para la dirección de proyectos (Guía del PMBOK) / Project Management Institute*. Estados Unidos: Project Management Institute, Inc.
- Rodríguez, D. (2019). Los servicios financieros digitales del Banco de la Nación (tesis de posgrado). Universidad Nacional Federico Villarreal, Lima, Perú.
- Redtrust (2022). Tecnología HSM en la gestión de claves y certificados digitales. Obtenido de Redtrust a Keyfactor company.
- Vera, R. (2018). Diseño e implementación de un clúster usando JBoss EAP para aumentar la disponibilidad de los servidores de aplicaciones en una entidad del Estado (trabajo de suficiencia profesional). Universidad Nacional Mayor de San Marcos, Lima, Perú.

5.4 Glosario

HSM: El módulo de seguridad de hardware proporciona un conjunto de servicios criptográficos con seguridad. Dentro de este está incluido la generación de claves, traducción de PIN, creación de criptogramas, entre otros. (PCI Security Standards Council, 2018)

Criptografía: Es el método para asegurar que los datos sean ininteligibles a las personas o herramientas tecnológicas y puedan ser legibles utilizando un método conocido solo por el emisor y receptor.

Emisor de la tarjeta: Institución o empresa que emite tarjetas de pago para el titular o cliente.

EMV: Es un estándar utilizado para realizar pagos seguros interoperables a nivel internacional. En él, el elemento clave es la inclusión de los datos digitales dinámicos en cada transacción, de manera que reduzcan el riesgo de fraude y por lo tanto resulten seguras. Cuando un cliente utiliza un dispositivo con estas características, la autenticación dinámica permite identificar en ese mismo instante si es un pago auténtico y si fue aprobado por ese cliente.

Cifrado: Se utiliza la criptografía para convertir la información matemáticamente en un formato ilegible excepto para aquellos titulares de una clave específica.

PIN: El número de identificación personal es el código que autentica al titular de la tarjeta en un proceso de autorización.

Chip: Se utiliza para procesar transacciones de acuerdo al estándar EMV

Chip y PIN: Proceso de verificación por parte del consumidor al introducir su PIN en un terminal de pago habilitado con chip tipo EMV al comprar bienes o servicios.

Terminal de pago: Es un dispositivo de hardware utilizado para aceptar pagos con tarjeta del cliente. También es conocido como POS (terminal de punto de venta).

ARQC: Llamado Criptograma de requerimiento de transacción, es generado por la tarjeta en base a los datos de la transacción, una vez generado este criptograma, este dato se incluye en la trama que es enviada al emisor para su autorización.

ARPC: Llamado Criptograma de respuesta de transacción, es generado como respuesta por el emisor en base a la verificación de ARQC. El ARPC se envía de regreso a través de la red de pago al terminal de punto de venta para autorizar la transacción.