**Área Responsable**:

División de Tecnología de la Información

Subgerencia Integración TI - Negocio

Gestión de la Demanda

**Fecha de creación:** 18/10/2022

**Fecha de actualización**:

18/10/2022

**Objetivo:**

Proporcionar información detallada de los requerimientos funcionales y no funcionales del sistema, describiendo sus características, comportamiento y reglas de negocio, los cuales han sido revisados y validados por todos los interesados.

Este documento se crea en base a los requisitos de alto nivel identificados en la Iniciativa de Negocio solicitada a Tecnología de la Información.

**Alcance:**

Aplica a iniciativas y proyectos que requieren desarrollo de software.

Este documento es propiedad del Banco Interamericano de Finanzas, con carácter reservado para uso exclusivo dentro del Banco, no pudiéndose usar o proporcionar a terceros, constituyendo falta grave el uso no autorizado o la entrega a terceros de esta información, además de la responsabilidad penal subyacente.

DOCUMENTO DE ESPECIFICACIÓN FUNCIONAL

**TI-EA2023-12608 - R10 Compliance por EH: Desarrollos Complementarios Vulnerabilidades Cyberlego-APP-BxI EMPRESAS**

**Versión V.1.0**



# ACEPTACIÓN

A través del presente dejo constancia de haber revisado, leído y aprobado el contenido de la información mostrada en este documento, asimismo asumo la responsabilidad, normativas y regulaciones inherentes al área que represento.

|  |  |  |
| --- | --- | --- |
| NOMBRE | ÁREA | ROL |
| Jaime Madrid | Líder Canales PJ | Usuario solicitante |
| Juan Gala | Aplicaciones de Canales PJ | Líder Integrador |

Todo control de cambio funcional que se vea reflejado en este documento debe ser aprobado por el líder de esta iniciativa.

# HISTORIAL DE VERSIONES

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| VERSIÓN | FECHA VERSIÓN | ELABORADO POR | REVISADO POR | DESCRIPCIÓN |
| 1.0 | 16/10/2023 | Magdalena Cortez |  | Creación del documento |

# GLOSARIO DE TERMINOS

|  |  |
| --- | --- |
| TÉRMINO | DEFINICIÓN |
| EH | El ethical hacking es la práctica de realizar evaluaciones de seguridad utilizando las mismas técnicas que emplean los hackers; pero con la aprobación y autorización de la organización a la que se está hackeando, con el objetivo de utilizar las tácticas, técnicas y estrategias de los ciberdelincuentes para localizar posibles puntos débiles y reforzar la protección de una organización frente a las brechas de seguridad y de datos. |
| TLS | Protocolo **TLS Transport Layer Security** utilizado para crear una conexión cifrada entre el navegador de un usuario y un servidor web. |
| BPIE | Banca por Internet BanBif Empresas |
| APPE | Aplicación móvil BanBif Empresas |

[ACEPTACIÓN 2](#_Toc151568973)

[HISTORIAL DE VERSIONES 3](#_Toc151568974)

[GLOSARIO DE TERMINOS 3](#_Toc151568975)

[1. Objetivos y Beneficios 5](#_Toc151568976)

[1.1 Objetivos 5](#_Toc151568977)

[1.2 Beneficio 5](#_Toc151568978)

[2. Introducción 5](#_Toc151568979)

[2.1 Resumen Ejecutivo 5](#_Toc151568980)

[2.1 Pedido Regulatorio 5](#_Toc151568981)

[2.2 Supuestos 6](#_Toc151568982)

[2.3 Fuera de Alcance 6](#_Toc151568983)

[2.4 Restricciones 6](#_Toc151568984)

[3. Impacto 6](#_Toc151568985)

[3.1 Productos y/o Servicios 6](#_Toc151568986)

[3.2 Canales 6](#_Toc151568987)

[3.3 Áreas de Negocio 6](#_Toc151568988)

[3.4 Aplicaciones 6](#_Toc151568989)

[3.5 Procesos 7](#_Toc151568990)

[4. Proceso AS IS 7](#_Toc151568991)

[5. Proceso TO BE 8](#_Toc151568992)

[6. Especificación de Requerimientos Funcionales 8](#_Toc151568993)

[7. impacto en aplicaciones importantes 8](#_Toc151568994)

[7.1 Impacto en la Posición del Cliente - IBS 8](#_Toc151568995)

[7.2 Impacto en Gestión Bancaria 8](#_Toc151568996)

[7.3 Impacto en Monitor 8](#_Toc151568997)

[7.4 Impacto en la Contabilidad 8](#_Toc151568998)

[7.5 Impacto en el Módulo IBS Préstamos / Cronogramas 8](#_Toc151568999)

[7.6 Impacto en Reportes Regulatorios 9](#_Toc151569000)

[7.7 Impacto en otros reportes existentes 9](#_Toc151569001)

[7.8 Impacto en el Sistema de Emisión de Comprobantes de Pago Electrónicos 9](#_Toc151569002)

[7.1 Impacto en RPAs 9](#_Toc151569003)

[8. Especificación de Requerimientos No Funcionales 9](#_Toc151569004)

[8.1 CL - Realizar adecuaciones a nivel de balanceador F5 para que acepte el protocolo TLS 1.2 en el BPIE y APPE. 9](#_Toc151569005)

[8.1.1 Para la BPIE: 9](#_Toc151569006)

[8.1.2 Para la APPE: 11](#_Toc151569007)

[9. Otros Impactos No Funcionales 11](#_Toc151569008)

[9.1 Impacto en Sistemas Externos 11](#_Toc151569009)

[9.2 Disponibilidad 11](#_Toc151569010)

[9.3 Volumetría y Proyección 11](#_Toc151569011)

[9.4 Impacto en el cierre 12](#_Toc151569012)

[9.5 Log de Auditoría 12](#_Toc151569013)

[9.6 Gestión de Accesos y Perfiles 12](#_Toc151569014)

[10. Análisis de Datos 12](#_Toc151569015)

[11. Control de Versiones Plantilla DEF 12](#_Toc151569016)

1. Objetivos y Beneficios

## Objetivos

* Atención de Compliance asignadas a Plataforma CyberLego para lo cual se requiere migrar el TLS 1.0 a TLS 1.2 de las aplicaciones BPIE y APPE

## Beneficio

* Protección ante ataques informáticos

1. Introducción

## Resumen Ejecutivo

Actualmente se han identificado 6 vulnerabilidades en la Plataforma CyberLego

|  |  |
| --- | --- |
| Compliance - 812 | Plataforma FX - 1- Acceso a API sin Autorización desde Internet |
| Compliance - 813 | Plataforma FX - 2- JWT - Ataque de Confusión |
| Compliance - 814 | Plataforma FX - 3- Generación de JWT sin necesidad de una sesión activa |
| Compliance - 817 | Plataforma FX - 5- Control inadecuado de solicitudes |
| Compliance - 819 | Plataforma FX - 7- Inadecuado manejo de parámetros |
| Compliance - 836 | Upgrade CyberLego - Adecuaciones Manejo de parámetros |

Esta iniciativa iba ser atendida por el equipo de Cyberlego; pero con la nueva distribución del organigrama de Operaciones y Tecnología, cada canal atenderá la solución de forma independiente.

El presente documento atenderá la solución para la vulnerabilidad **836** según la iniciativa **TI-EA2023-12608 - R10 Compliance por EH: Desarrollos Complementarios Vulnerabilidades Cyberlego-APP-BPI EMPRESAS**

## Pedido Regulatorio

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **¿Iniciativa regulatoria?** | Si | X | No |  |  | **Tipo de observación:** | | R.S. / Oficio SBS |  |  |
|  |  |  |  |  |  |  |  | Observación SBS |  |  |
| **Fecha límite implementación:** | 31-12-2023 | | | |  |  |  | SUNAT |  |  |
|  |  |  |  |  |  |  |  | BCR |  |  |
| **Contingencia en caso de no llegar a la fecha perentoria:** | | | | | |  |  | Auditoría interna |  |  |
|  | | | | | | |  | Auditoría externa |  |  |
|  | Regulación ASA |  |  |
| Otro: |  |  |  |

## Supuestos

* Disponibilidad de los ambientes previos (DES / UAT) de las aplicaciones que participan en esta iniciativa.
* Disponibilidad de los usuarios para las pruebas de certificación.
* Recursos externos disponibles para la implementación de esta iniciativa (proveedores), en caso se requiera.
* El requerimiento es netamente técnico y no hay impacto en funcionalidades de productos o servicios ofrecidos al cliente.
* El Equipo de Ingeniería TI quien diseña la solución.

## Fuera de Alcance

Está fuera de alcance cualquier cambio de funcionalidad o de contenido no especificado en este documento.

## Restricciones

Cualquier cambio de funcionalidad que sea factible de atender deberá ser gestionado mediante un control de cambio, siempre y cuando, la presente iniciativa se encuentre en planificación. De haberse iniciado el desarrollo, el cambio de funcionalidad deberá solicitarse como una nueva iniciativa.

1. Impacto

## Productos y/o Servicios

* Aplicaciones - EH Cyberlego BPIE y APPE

## Canales

* BPIE y APPE

## Áreas de Negocio

* Riesgo Operacional
* Canal Digital Empresas
* Integración
* TI

## Aplicaciones

* Aplicaciones - EH Cyberlego BPIE y APPE

## Procesos

* Actualización de protocolo – Arquitectura Banca Empresas

1. Proceso AS IS

Actualmente se ha identificado vulnerabilidad asociada a Cyberlego, debido a que las **aplicaciones** **BPIE y la APPE** presentan obsolescencia.

Según el análisis realizado a la BPIE por el equipo de Canales Digitales Empresas, Cyberlego si puede comunicarse con el protocolo TLS 1.2 por tener una plataforma actualizada; las Apis de la capa de aplicación se comunican con la Capa de Integración, mediante balanceadores (F5), los cuales hacen una traducción del TLS de 1.0 a la versión 1.2 para llegar finalmente a la capa de Base de Datos.

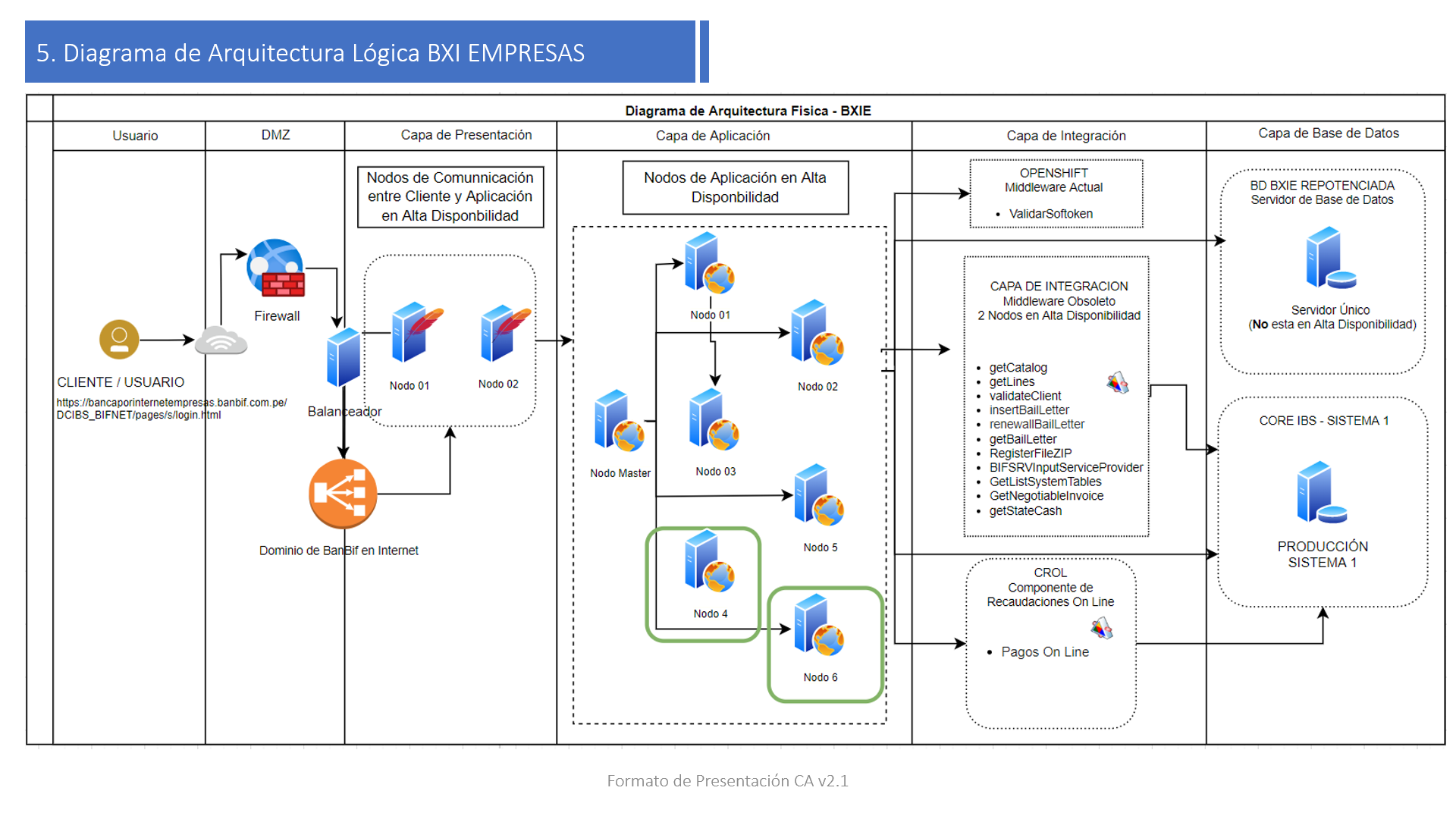


Ilustración 1 - As IS - Arquitectura BPIE

Para la APPE desde la Capa de Presentación se tienen los dispositivos, se sube al store a las aplicaciones que están en un lenguaje móvil y se comunica con Openshit (Capa de Integración con TLS versión 1.0.) y se realiza la traducción al TLS de 1.2 para llegar finalmente a la capa de Base de Datos.

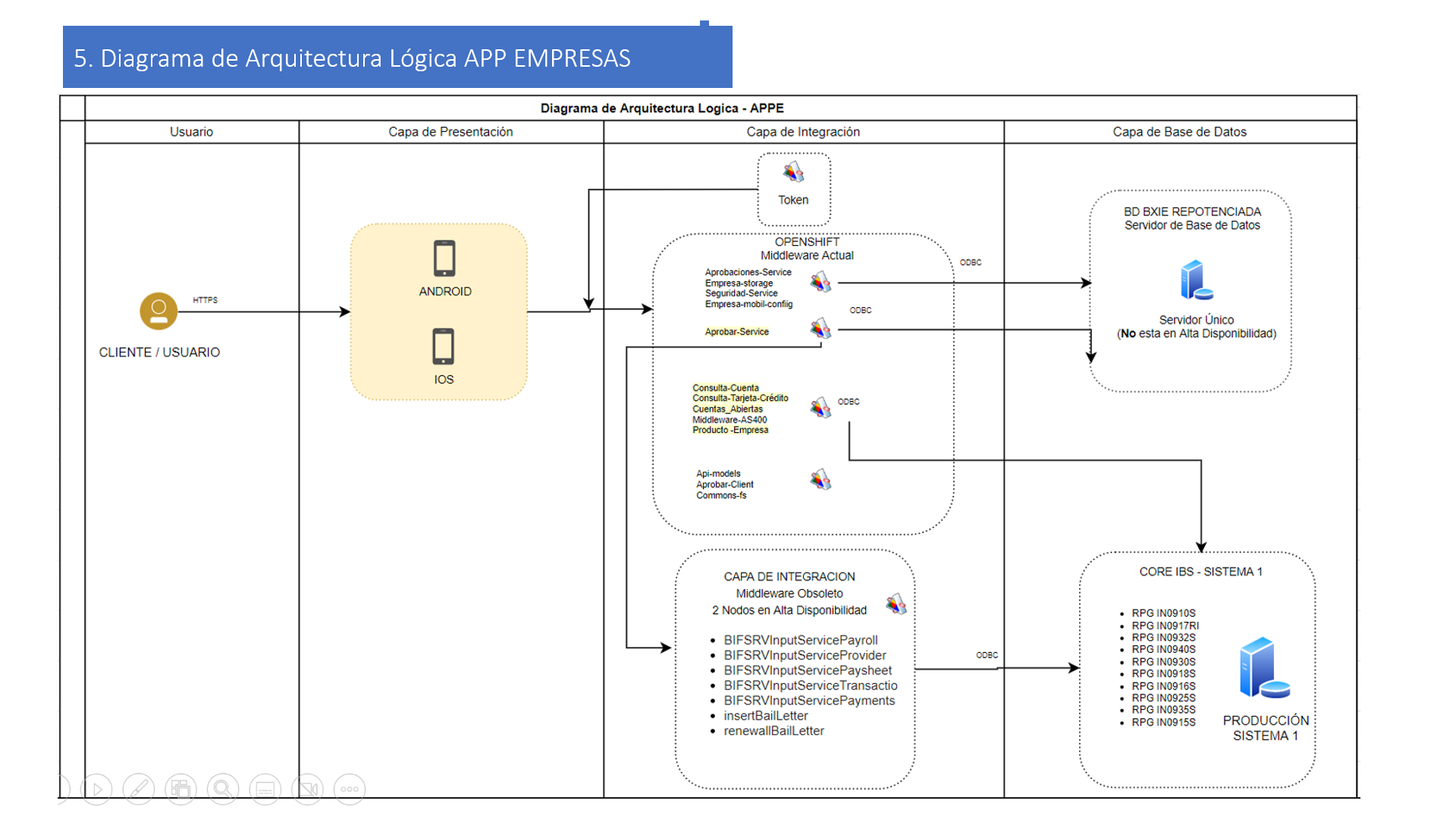


Ilustración 2 - AS IS Arquitectura APPE

1. Proceso TO BE

Se requiere hacer adecuaciones a nivel de baleanceador F5 de tal manera que solo acepte el protocolo con la versión de TLS 1.2. y ya no se debe salir por TLS 1.0. Por tal se requiere hacer pruebas de regresión en ambiente UAT y en ambiente de Post Producción.

1. Especificación de Requerimientos Funcionales

No aplica. A nivel funcional no hay impacto.

1. impacto en aplicaciones importantes

## Impacto en la Posición del Cliente - IBS

*No hay impacto en esta sección.*

## Impacto en Gestión Bancaria

*No hay impacto en esta sección.*

## Impacto en Monitor

*No hay impacto en esta sección.*

## Impacto en la Contabilidad

*No hay impacto en esta sección.*

## Impacto en el Módulo IBS Préstamos / Cronogramas

*No hay impacto en esta sección.*

## Impacto en Reportes Regulatorios

*No hay impacto en esta sección.*

## Impacto en otros reportes existentes

*No hay impacto en esta sección.*

## Impacto en el Sistema de Emisión de Comprobantes de Pago Electrónicos

*No hay impacto en esta sección.*

## Impacto en RPAs

*No hay impacto en esta sección.*

1. Especificación de Requerimientos No Funcionales

**Lista de Requerimientos No Funcionales**

|  |  |  |  |
| --- | --- | --- | --- |
| Cod. Req. | Proceso | Nombre Requerimiento Funcional y/o Historia de Usuario | Aplicación / Módulo |
| REQ001 | CL | Realizar adecuaciones a nivel de balanceador F5 para que acepte el protocolo TLS 1.2 para la BPIE y APPE. | BPIE /APPE |

## CL - Realizar adecuaciones a nivel de balanceador F5 para que acepte el protocolo TLS 1.2 para la BPIE y APPE.

Se requiere realizar adecuaciones a nivel de balanceador F5 de tal manera que solo acepte el protocolo con la versión de TLS 1.2 y ya no se debe salir por TLS 1.0. Por tal se necesita hacer pruebas de regresión en ambiente UAT y en ambiente de Post Producción de las funcionalidades relacionadas a las siguientes Apis:

## Para la BPIE:

Para la Api https://api-desembolsopj.apps.dombif.peru se requiere probar la opción:

***Crédito en Línea*,** donde se debe validar el funcionamiento de las opciones: ***Consulta de Líneas y Registro de Desembolso.***

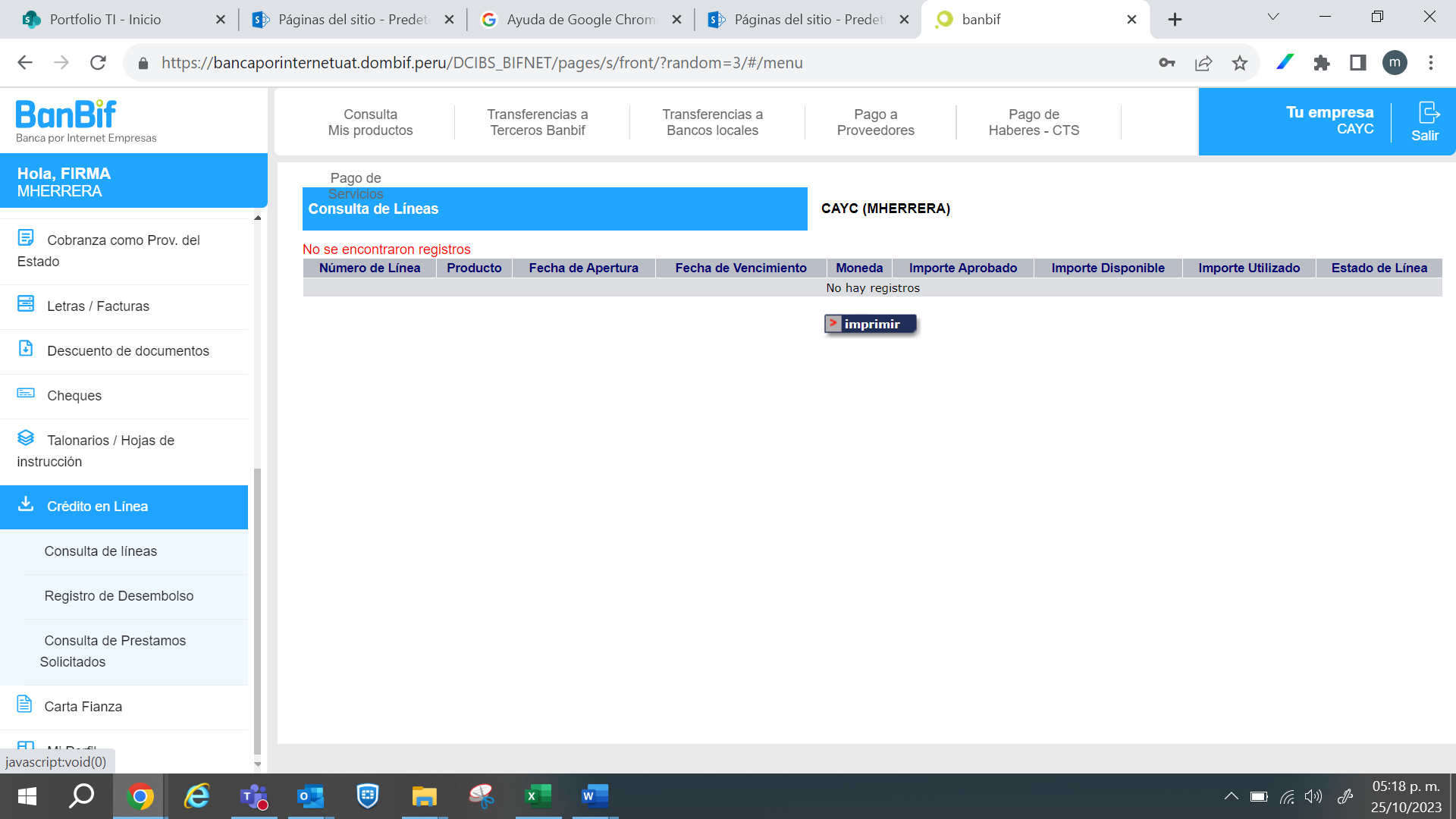


Ilustración 3 – Funcionalidad relacionada al Api Desembolsos BPIE

Para el Api https://api-desembolsopj.apps.dombif.peru se requiere probar la opción:

***Pagos Varios – Leasing – Agregar***, considerar realizarlo con el usuario operador.

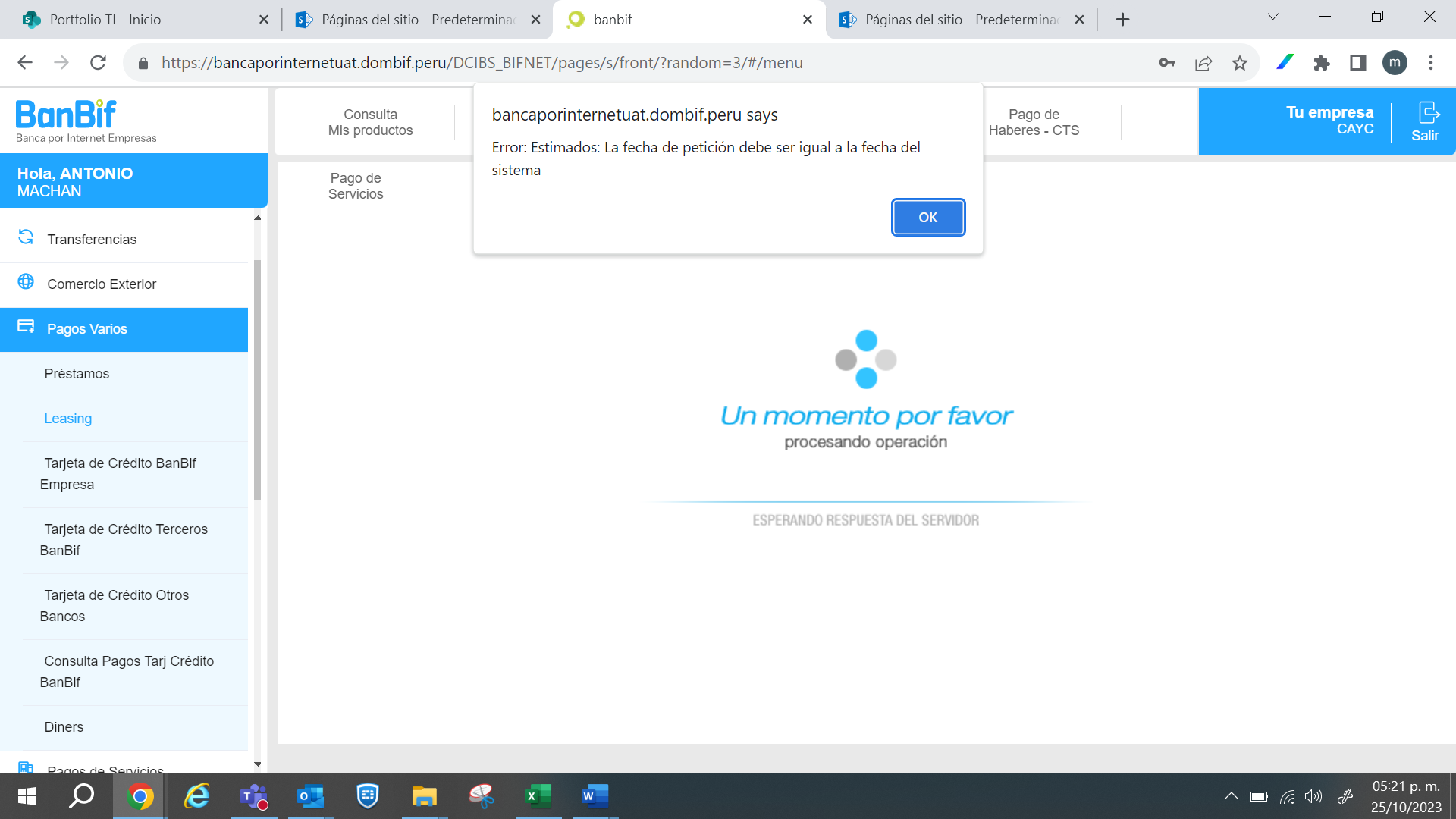


Ilustración 4 - Funcionalidad relacionada al Api Leasing BPIE

Para el Api https://api-softtoken.apps.dombif.peru se requiere probar la funcionalidad del ***Token Digital***, el cual se solicita al aprobar operaciones desde la BPIE. Hay que considerar que el cliente previamente debe estar afiliado al token digital y debe consultar el token desde la APPE.

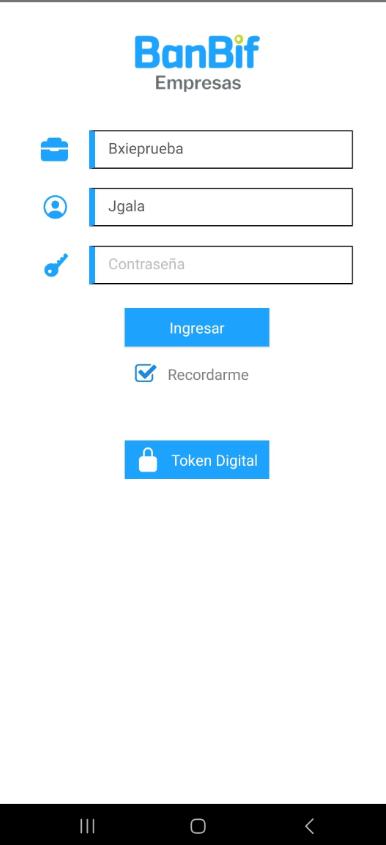
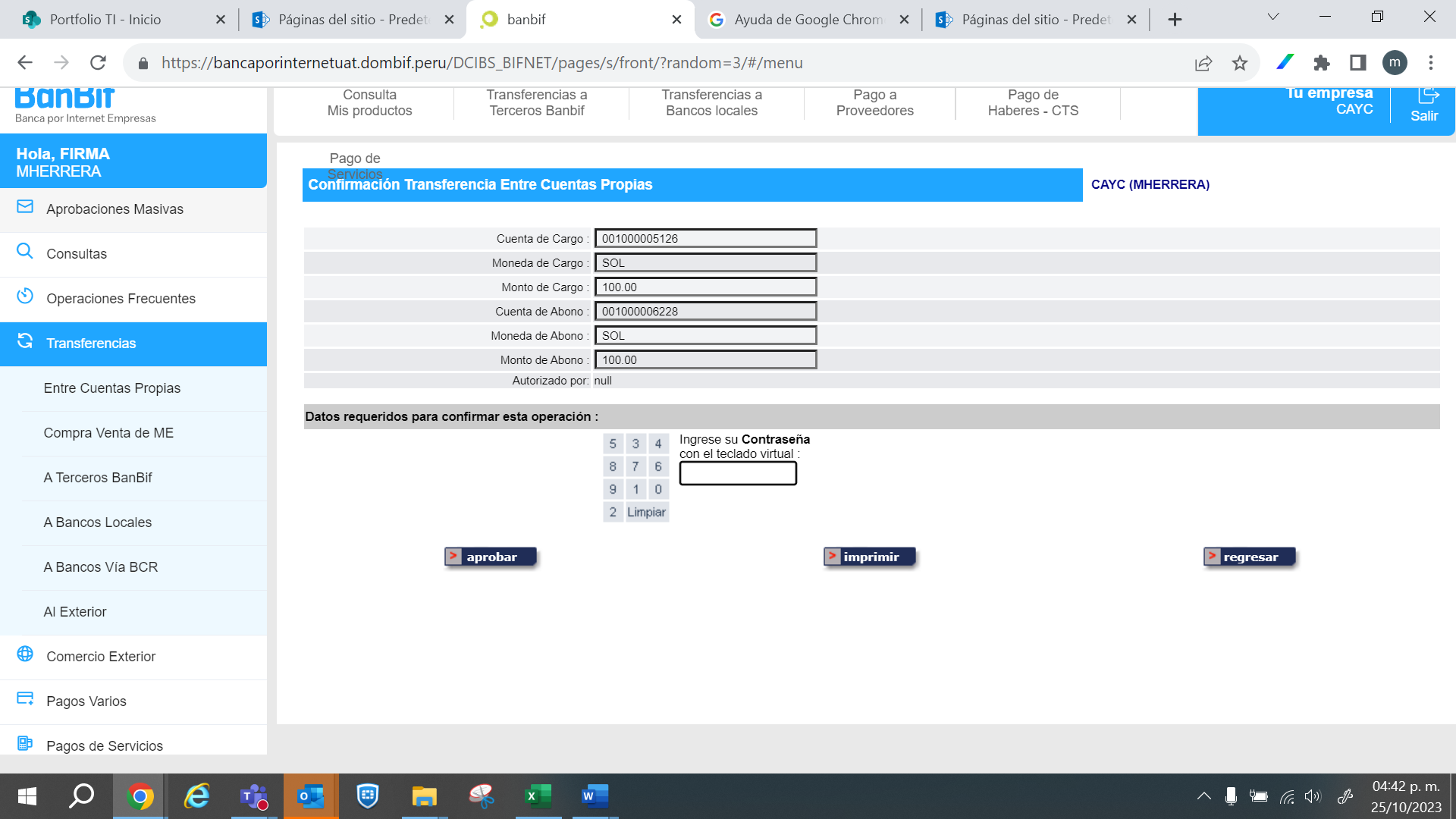
 

Ilustración 5 - Consulta del Token Digital desde al APPE



Ingreso de los 6 dígitos que se muestran en la APP

Ilustración 6 – Funcionalidad relacionada al api del Soft Token desde la BPIE

## Para la APPE:

Para el Api https://api-banca-movil-empresas.apps.banbifapimarket.com.pe se requiere probar el inicio de sesión exitoso desde al APPE.

Interfaz de usuario gráfica, Texto, Aplicación, Sitio web

Descripción generada automáticamenteInterfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Ilustración 7 - Validación del api de inicio de sesión en APPE

1. Otros Impactos No Funcionales

## Impacto en Sistemas Externos

*No hay impacto en esta sección.*

## Disponibilidad

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **24x7 (L-D)** |  |  | **5x8 (L-V)** |  |  | **6x8 (L-S)** |  |  | **Otro:** |  |  |  |

*No hay impacto en esta sección.*

## Volumetría y Proyección

|  |  |  |
| --- | --- | --- |
|  | *Estimación en la implementación:* | *Proyección a 3 años (estimación a alto nivel)* |
| *Cantidad de usuarios que van a usar la aplicación:*  *(Puede expresarse por día, mes)* |  |  |
| *Cantidad de transacciones que va realizar la aplicación:*  *(Puede expresarse en día, mes, y debe ser sobre las transacciones de la nueva capacidad funcional, mas no lo existente)* |  |  |
| *Horas pico:*  *(Rango de horas con más alta transacción)* |  |  |
| *Fecha de alta transacción:*  *(últimos días del mes, quincenas, demanda por campañas)* |  |  |

*No hay impacto en esta sección.*

## Impacto en el cierre

Impacto en el proceso de cierre:

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **diario** |  |  | **mensual** |  |  | **anual** |  |  | Otro: |  |  |  |

*No hay impacto en esta sección.*

## Log de Auditoría

*No hay impacto en esta sección.*

## Gestión de Accesos y Perfiles

*No hay impacto en esta sección.*

1. Análisis de Datos

*No hay impacto en esta sección, debido a que no hay transformación de datos*

|  |  |  |  |
| --- | --- | --- | --- |
| **Proceso:** | | | |
| **Datos de Entrada** | | | |
| **Campo** | **Valor** | **Validaciones** | **Transformación** |
|  |  |  |  |
| **Datos de Salida** | | | |
| **Campo** | **Valor** | **Validaciones** | **Transformación** |
|  |  |  |  |

1. Control de Versiones Plantilla DEF

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| VERSIÓN | FECHA VERSIÓN | ELABORADO POR | REVISADO POR | DESCRIPCIÓN |
| 1.0 | 02/10/2020 | Carolina Taipe | George Romain | Creación del documento. |
| 2.0 | 02/05/2022 | Carolina Taipe | George Romain | Se agrega impacto en RPA e impacto en el sistema de emisión de comprobantes de pago electrónicos (sección 8). |
| 3.0 | 18/10/2022 | Carolina Taipe |  | Se agrega el listado y especificación de requerimientos no funcionales (sección 9).  Se renombra título de la sección 10: Otros impactos no funcionales. |