Universidad Nacional Federico Villarreal

VRIN | VICERRECTORADO DE INVESTIGACIÓN

FACULTAD DE INGENIERÍA INDUSTRIAL Y DE SISTEMAS

ARQUITECTURA DE ENRUTAMIENTO FRONT DOOR, UTILIZANDO MICROSOFT AZURE, PARA MEJORAR EL ACCESO WEB AL SERVICIO DIGITAL DE UNA ENTIDAD FINANCIERA

Línea de investigación:
Sistemas de información y optimización

Tesis para optar el Título Profesional de Ingeniero de Sistemas

Autor

Cárdenas Quispe, Aléxis Pedro Lino

Asesor

Gamboa Cruzado, Javier Arturo

ORCID: 0000-0002-0461-4152

Jurado

Ángeles Lazo, Ana María

Meza Armas, Orlando Eleodoro

Ogosi Auqui, José Antonio

Lima - Perú

2026

ARQUITECTURA DE ENRUTAMIENTO FRONT DOOR, UTILIZANDO MICROSOFT AZURE, PARA MEJORAR EL ACCESO WEB AL SERVICIO DIGITAL DE UNA ENTIDAD FINANCIERA

INFORME DE ORIGINALIDAD

26%	25%	4%	16%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	developer.mozilla.org Fuente de Internet	3%
2	core.ac.uk Fuente de Internet	2%
3	hdl.handle.net Fuente de Internet	2%
4	runebook.dev Fuente de Internet	2%
5	Submitted to Universidad Cesar Vallejo Trabajo del estudiante	1%
6	repositorio.autonoma.edu.pe Fuente de Internet	1%
7	repositorioacademico.upc.edu.pe Fuente de Internet	1%
8	repositorio.ucv.edu.pe Fuente de Internet	1%
9	Submitted to Universidad Nacional Federico Villarreal Trabajo del estudiante	1%
10	tecsify.com Fuente de Internet	<1%
11	www.coursehero.com Fuente de Internet	<1%

Universidad Nacional
Federico Villarreal

VRIN | VICERRECTORADO DE INVESTIGACIÓN

FACULTAD DE INGENIERÍA INDUSTRIAL Y DE SISTEMAS

ARQUITECTURA DE ENRUTAMIENTO FRONT DOOR, UTILIZANDO MICROSOFT AZURE, PARA MEJORAR EL ACCESO WEB AL SERVICIO DIGITAL DE UNA ENTIDAD FINANCIERA

Línea de Investigación:

Sistemas de Información y Optimización

Tesis para optar por el Título Profesional de Ingeniero de Sistemas

Autor

Cárdenas Quispe, Aléxis Pedro Lino

Asesor

Gamboa Cruzado, Javier Arturo

ORCID: 0000-0002-0461-4152

Jurado

Ángeles Lazo, Ana María

Meza Armas, Orlando Eleodoro

Ogosi Auqui, José Antonio

Lima - Perú

2026

DEDICATORIA

A Dios,

A Mi Madre,

Patricia,

A mi Padre, Antonio,

A mi Hermana, Aléxia,

A mis Abuelos.

AGRADECIMIENTOS

Mi alma agradece la grandeza del Señor.

A Dios Padre Nuestro Rey del Universo,

A la Virgen Nuestra Madre Santa,

A mis Padres, mis Abuelos, mi Familia, unidos en Cristo.

A mi Universidad, a mi Centro de Labores.

ÍNDICE

Resumen ..... **xiv**

Abstract ..... **xv**

I. INTRODUCCIÓN **1**

1.1 Descripción y formulación del problema 1
1.1.1 Problema General *6*
1.1.2 Problemas Específicos *6*

1.2 Antecedentes 7
1.2.1 Antecedentes Nacionales *7*
1.2.2 Antecedentes Internacionales *9*

1.3 Objetivos 13
1.3.1 Objetivo General *13*
1.3.2 Objetivos Específicos *13*

1.4 Justificación 13
1.4.1 Conveniencia *14*
1.4.2 Relevancia social *14*
1.4.3 Implicaciones prácticas *14*
1.4.4 Utilidad metodológica *14*
1.4.5 Valor teórico *15*

1.5 Hipótesis 16
1.5.1 Hipótesis General *16*
1.5.2 Hipótesis Específicas *16*

II. MARCO TEÓRICO **17**

2.1 Bases teóricas sobre el tema de investigación 17
2.1.1 Arquitectura de Enrutamiento en Azure Front Door *17*
2.1.2 Acceso vía web al servicio digital *18*
2.1.3 Microsoft Azure *19*
2.1.4 Características de componentes en Microsoft Azure *20*
2.1.5 Azure Portal *22*
2.1.6 Cliente, servidor, solicitud, respuesta, tiempo de respuesta *23*
2.1.7 Internet, web, navegador web, página web, sitio web, DNS, CNAME *24*
2.1.8 Dominio, número de dominios redirigidos, FQDN, estructura jerárquica de un dominio *24*
2.1.9 ICANN, IANA, DNS Root Zone, TLD, gTLD, ccTLD, SLD, ccSLD *27*
2.1.10 Punto Pe, NIC.PE *27*
2.1.11 Número de dominios expuestos hacia el navegador web del cliente *28*
2.1.12 HTTP, HTTPS, TLS *28*
2.1.13 Certificado digital, PFX, DigiCert *29*
2.1.14 Número de dominios con redirección de HTTP a HTTPS *30*
2.1.15 Número soluciones de seguridad WAF, Bots *30*
2.1.16 HTTP Status Response Codes *31*

2.1.17 URI, URL, URN *39*
2.1.18 Microsoft Edge DevTools *41*
2.1.19 Mozilla Firefox Private Browsing *41*
2.1.20 Digicert SSL Certificate Checker *42*
2.1.21 Azure Log Analytics, KQL *42*

III. MÉTODO **44**

3.1 Tipo de investigación 44

3.2 Ámbito temporal y espacial 46

3.3 Variables 46
3.3.1 Conceptualización *46*
3.3.2 Operacionalización *47*

3.4 Población y muestra 49

3.5 Instrumentos 50
3.5.1 Investigación de Campo *50*
3.5.2 Investigación Experimental *51*
3.5.3 Investigación Documental *52*
3.5.4 Confiabilidad, validez y objetividad de instrumentos *52*

3.6 Procedimientos 54

3.7 Análisis de datos 54

3.8 Consideraciones éticas 55

IV. RESULTADOS **57**

4.1 Diagnóstico de componentes y configuraciones 57

4.2 Plan de trabajo 57

4.3 Validación previa a producción 57

4.4 Creación de componentes y configuraciones en la implementación de la solución 58
4.4.1 Creación de front-ends *61*
4.4.2 Creación de grupo de back-end *82*
4.4.3 Creación de reglas de enrutamiento *86*

4.5 Monitoreo y comprobación del acceso al servicio 96

4.6 Presentación de resultados 97

4.7 Contrastación de las hipótesis 101
4.7.1 Contrastación de la H_1 ..... *101*
4.7.2 Contrastación de la H_2 ..... *106*
4.7.3 Contrastación de la H_3 ..... *110*
4.7.4 Contrastación de la H_4 ..... *114*
4.7.5 Contrastación de la H_5 ..... *118*

4.8 Análisis Estadístico Descriptivo 122
4.8.1 Incrementar el número de dominios redirigidos *122*

4.8.2 Disminuir el número de dominios expuestos hacia el navegador web del cliente 126
4.8.3 Incrementar el número de dominios con redirección de HTTP a HTTPS 128
4.8.4 Habilitar una solución de seguridad WAF 132
4.9 Nuevo proceso de acceso web al servicio digital 136
V. DISCUSIÓN DE RESULTADOS 137
VI. CONCLUSIONES 140
VII. RECOMENDACIONES 142
VIII. REFERENCIAS 144
IX. ANEXOS.....150
Anexo A. Matriz de consistencia 150
Anexo B. Matriz de operacionalización de la variable dependiente 152
Anexo C. Plan de trabajo.....153
Anexo D. Validación previa a producción 156
Anexo E. Registros completos de grupo control y grupo experimental.....157
Anexo F. Consulta KQL en Azure Logs Analytics para la extracción y análisis de eventos WAF 159
Anexo G. Nuevo proceso de acceso web al servicio digital Cambix de la Entidad Financiera Banco de Comercio 160

ÍNDICE DE TABLAS

Tabla 1 Indicadores y Datos de Preprueba....4

Tabla 2 AS IS / TO BE 5

Tabla 3 Simbología y terminología por componente en los servicios de Microsoft Azure....20

Tabla 4 Clasificación de códigos de estado de respuesta HTTP....32

Tabla 5 Conceptualización de variable independiente....46

Tabla 6 Conceptualización de variable dependiente....47

Tabla 7 Operacionalización de variable independiente 48

Tabla 8 Operacionalización de variable dependiente 48

Tabla 9 Detalles de la Población y Muestra de la Investigación 49

Tabla 10 Técnicas e instrumentos de investigación de campo 50

Tabla 11 Técnicas e instrumentos de investigación experimental....51

Tabla 12 Técnicas e instrumentos de investigación documental 52

Tabla 13 Detalle de instrumentos y técnicas para la medición de indicadores....53

Tabla 14 Resultados de Posprueba del Gc y Posprueba del Ge para I_1, I_2, I_3, I_4 e I_5....98

Tabla 15 Promedio de los indicadores de la Posprueba del Gc y Ge....99

Tabla 16 Registros de posprueba en el grupo experimental recolectados con Log Analytics 100

Tabla 17 Valores de las mediciones para H_1....101

Tabla 18 Resumen del resultado del cálculo del valor del Estadístico de Prueba 105

Tabla 19 Valores de las mediciones para H_2....106

Tabla 20 Valores de las mediciones para H_3....110

Tabla 21 Valores de las mediciones para H_4....114

Tabla 22 Valores de las mediciones para H_5....118

Tabla 23 Resultados para número de dominios redirigidos....122

Tabla 24 Resultados para número de dominios expuestos 126

Tabla 25 Resultados para número de dominios con redirección HTTPS 128

Tabla 26 Resultados para número de soluciones de seguridad WAF 132

ÍNDICE DE FIGURAS

Figura 1 Proceso de Acceso web al servicio digital Cambix de la Entidad Financiera Banco de Comercio 4

Figura 2 Flujo de navegación AS IS de los clientes para acceder vía web al servicio digital de Cambix 5

Figura 3 Estructura jerárquica de un dominio 26

Figura 4 Relación entre una URI, URL y URN mediante un Diagrama de Venn 40

Figura 5 Comparación entre las partes de una URL frente a una URI 40

Figura 6 Comparación entre las partes de una URL frente a una URN y una URI 41

Figura 7 Vista de Azure Log Analytics y KQL desde Azure Portal 43

Figura 8 Diagrama de diseño de preprueba-posprueba con grupo de control 45

Figura 9 Etapas del análisis de resultados 55

Figura 10 Recurso cambix-prod del servicio de Cambix 57

Figura 11 Vista de la consola de administración de recursos de Azure Portal 58

Figura 12 Vista de acceso al servicio de Azure Front Door 59

Figura 13 Información general de la instancia fdappsbc en Azure Front Door 59

Figura 14 Vista inicial del Diseñador de Front Door 60

Figura 15 Creación de front-end para el dominio cambix.com.pe 61

Figura 16 Registro DNS en nic.pe para el dominio cambix.com.pe 62

Figura 17 Creación de front-end para el dominio www.cambix.com.pe 63

Figura 18 Registro DNS en nic.pe para el dominio www.cambix.com.pe 63

Figura 19 Creación de front-end para el dominio cambix.pe 64

Figura 20 Registro DNS en nic.pe para el dominio cambix.pe 64

Figura 21 Creación de front-end para el dominio www.cambix.pe 65

Figura 22 Registro DNS en nic.pe para el dominio www.cambix.pe 65

Figura 23 Configuración HTTPS en front-end del dominio cambix.com.pe 66

Figura 24 Configuración de certificado digital en front-end del dominio cambix.com.pe 67

Figura 25 Configuración de WAF en front-end del dominio cambix.com.pe.....68

Figura 26 Configuración HTTPS en front-end del dominio www.cambix.com.pe.....69

Figura 27 Configuración de certificado digital en front-end del dominio www.cambix.com.pe 70

Figura 28 Configuración de WAF en front-end del dominio www.cambix.com.pe 71

Figura 29 Configuración HTTPS en front-end del dominio cambix.pe 72

Figura 30 Configuración de certificado digital en front-end del dominio cambix.pe 73

Figura 31 Configuración de WAF en front-end del dominio cambix.pe.....74

Figura 32 Configuración HTTPS en front-end del dominio www.cambix.pe.....75

Figura 33 Configuración de certificado digital en front-end del dominio www.cambix.pe...76

Figura 34 Configuración de WAF en front-end del dominio www.cambix.pe 77

Figura 35 Directiva waf001 para la habilitación de solución de seguridad WAF 78

Figura 36 Asociaciones de directiva waf001 78

Figura 37 Reglas administradas de directiva waf001 79

Figura 38 Reglas personalizadas de directiva waf001 79

Figura 39 Almacén de claves kv-bancom-prod para la gestión de certificados digitales.....80

Figura 40 Front-ends completos 81

Figura 41 Vista parcial del Diseñador de Front Door con front-ends completos 81

Figura 42 Creación del grupo de back-end bkpoolcambix 82

Figura 43 Agregar back-end cambix-prod.....83

Figura 44 Completar creación del grupo de back-end bkpoolcambix con back-end cambix-prod 84

Figura 45 Grupo de back-end completo 85

Figura 46 Vista parcial del Diseñador de Front Door con grupo de back-end completo 85

Figura 47 Creación de regla Rule-cambix 86

Figura 48 Configuración de protocolo aceptado regla Rule-cambix 86

Figura 49 Configuración de front-ends en regla Rule-cambix 87

Figura 50 Configuración de back-end en regla Rule-cambix 87

Figura 51 Creación de regla http-to-https 88

Figura 52 Configuración de protocolo aceptado regla http-to-https 88

Figura 53 Configuración de front-ends en regla http-to-https 89

Figura 54 Configuración de back-end en regla Rule-cambix 89

Figura 55 Creación de regla redirect04-cambix 90

Figura 56 Configuración de protocolo aceptado regla redirect04-cambix 91

Figura 57 Configuración de front-ends en regla redirect04-cambix 91

Figura 58 Configuración de back-end en regla redirect04-cambix 92

Figura 59 Reglas de enrutamiento completas 93

Figura 60 Vista final del Diseñador de Front Door 93

Figura 61 Nuevo flujo de navegación de los clientes para acceder vía web al servicio digital de Cambix 94

Figura 62 Flujo de reglas de enrutamiento para el acceso al servicio de Cambix 94

Figura 63 Arquitectura de Enrutamiento Front Door para el servicio de Cambix 95

Figura 64 Validación de acceso al servicio mediante un navegador web 96

Figura 65 Prueba de normalidad indicador I_1 99

Figura 66 Gráfica de Distribución para H_1 102

Figura 67 Fórmula Welch-Satterthwaite para calcular los grados de libertad (degrees of freedom) 102

Figura 68 Cálculo del valor del Estadístico de Prueba mediante la Prueba t de Student en Minitab 103

Figura 69 Resultado de la Prueba t de Student para medias de las 2 muestras en Minitab .. 104

Figura 70 Gráfica de Distribución para H_2 107

Figura 71 Cálculo del valor mediante la Prueba U de Mann-Whitney en Minitab para H_2 . 108

Figura 72 Resultado de la Prueba U de Mann-Whitney en Minitab para H_2 109

Figura 73 Gráfica de Distribución para H_3 111

Figura 74 Cálculo del valor mediante la Prueba U de Mann-Whitney en Minitab para H_3 . 112

Figura 75 Resultado de la Prueba U de Mann-Whitney en Minitab para H_3 113

Figura 76 Gráfica de Distribución para H_4 115

Figura 77 Cálculo del valor mediante la Prueba U de Mann-Whitney en Minitab para H_4 . 116

Figura 78 Resultado de la Prueba U de Mann-Whitney en Minitab para H_4 117

Figura 79 Gráfica de Distribución para H_5 119

Figura 80 Cálculo del valor mediante la Prueba U de Mann-Whitney en Minitab para H_5 . 120

Figura 81 Resultado de la Prueba U de Mann-Whitney en Minitab para H_5 121

Figura 82 Resultados del Grupo de Control en número de dominios redirigidos 123

Figura 83 Resultados del Grupo Experimental en número de dominios redirigidos 123

Figura 84 Revisión de códigos de estado de respuesta HTTP con Microsoft Edge DevTools - 1 124

Figura 85 Revisión de códigos de estado de respuesta HTTP con Microsoft Edge DevTools - 2 124

Figura 86 Revisión de códigos de estado de respuesta HTTP con Microsoft Edge DevTools - 3 125

Figura 87 Revisión de códigos de estado de respuesta HTTP con Microsoft Edge DevTools - 4 125

Figura 88 Resultados del Grupo de Control en número de dominios expuestos 127

Figura 89 Resultados del Grupo Experimental en número de dominios expuestos 127

Figura 90 Revisión de dominios expuestos en navegación web con Mozilla Firefox Private Browsing 128

Figura 91 Resultados del Grupo de Control en número de dominios con redirección HTTPS 129

Figura 92 Resultados del Grupo Experimental en número de dominios con redirección HTTPS 129

Figura 93 Revisión de certificados digitales con Digicert SSL Certificate Checker 130

Figura 94 Revisión de códigos de estado de respuesta HTTP con Microsoft Edge DevTools 131

Figura 95 Revisión de logs con Azure Log Analytics 132

Figura 96 Resultados del Grupo de Control en número de soluciones de seguridad WAF . 133

Figura 97 Resultados del Grupo Experimental en número de soluciones de seguridad WAF 133

Figura 98 Modo de operación y acción tomada en tráfico malicioso 134

Figura 99 Intentos de ataques dirigidos a rutas específicas de la aplicación 134

Figura 100 Regla de seguridad activada y detalle del tipo de ataque detectado 135

Figura 101 Nuevo proceso de Acceso web al servicio digital Cambix de la Entidad Financiera Banco de Comercio 136

Figura 102 Resultados de Estadística Descriptiva 137

Resumen

El Banco de Comercio emprendió un proceso de transformación digital, evolucionando de un modelo tradicional hacia uno basado en tecnologías y servicios digitales, sin embargo, la infraestructura de comunicaciones responsable de la publicación de sus servicios carece de funcionalidades de enrutamiento y de protección contra amenazas en la web, afectando la accesibilidad, operatividad, identidad corporativa, seguridad y reputación de la organización. Ante esta limitante, se plantea implementar una Arquitectura de Enrutamiento en Microsoft Azure Front Door para mejorar el acceso vía web al servicio digital de la entidad financiera. En línea con el marco de trabajo de Microsoft Azure se realizó un diagnóstico inicial de componentes, la elaboración de un plan de trabajo para implementar la solución, una validación preliminar en un entorno de pruebas, el despliegue en el entorno productivo y una verificación de la solución mediante monitoreo y pruebas de funcionalidad. Los resultados obtenidos demostraron que la implementación de la solución tuvo un impacto significativo en la mejora del acceso vía web al servicio digital de Cambix del Banco de Comercio, centralizando el tráfico de múltiples dominios en un único dominio principal y fortaleciendo la seguridad del servicio mediante la integración de un Firewall de Aplicaciones Web.

Palabras clave: Computación en la nube, Microsoft Azure, Arquitectura de Enrutamiento Front Door, redirección de dominio, Firewall de Aplicaciones Web, seguridad a nivel de aplicación.

Abstract

Banco de Comercio embarked on a digital transformation process, evolving from a traditional model to one based on digital technologies and services. However, the communications infrastructure responsible for publishing its services lacks routing capabilities and protection against web threats, impacting the organization's accessibility, operability, corporate identity, security, and reputation. Given this limitation, the implementation of a Routing Architecture in Microsoft Azure Front Door was proposed to improve web access to the financial institution's digital service. In line with the Microsoft Azure framework, an initial component diagnosis was performed, a work plan was developed to implement the solution, a preliminary validation in a test environment was carried out, deployment in the production environment was completed, and the solution was verified through monitoring and functionality testing. The results obtained demonstrated that the implementation of the solution had a significant impact on improving web access to Banco de Comercio's Cambix digital service, centralizing traffic from multiple domains into a single main domain and strengthening the service's security through the integration of a Web Application Firewall.

Keywords: Cloud computing, Microsoft Azure, Front Door Routing Architecture, domain redirection, Web Application Firewall, application-level security.

I. INTRODUCCIÓN

1.1 Descripción y formulación del problema

Los constantes cambios en el mercado global y la acelerada transformación digital han impulsado a las organizaciones a fortalecer su presencia en entornos digitales y su identidad corporativa frente a sus clientes, mediante plataformas tecnológicas seguras, confiables y de fácil acceso, que les permitan transmitir de manera clara sus objetivos y valores institucionales. Tras la pandemia, la banca mundial deja de ser un negocio tradicional para irse convirtiendo en uno tecnológico, centrado en la digitalización de sus servicios (Goyes, 2020).

A nivel nacional, el sistema financiero peruano también ha experimentado una acelerada transformación digital. Las entidades bancarias del país han apostado por migrar progresivamente sus servicios hacia plataformas digitales con el fin de mejorar la accesibilidad, la seguridad y la eficiencia operativa. Sin embargo, este proceso ha enfrentado desafíos relacionados con la infraestructura tecnológica, especialmente en la gestión de dominios, enrutamiento del tráfico web y protección contra amenazas, aspectos fundamentales para garantizar la continuidad y seguridad de los servicios financieros en línea.

Aquí se presenta a Bancom (Banco de Comercio), una entidad financiera peruana, privada y dedicada a actividades bancarias, que emprendió un proceso de transformación digital con la implementación de nuevos servicios digitales. Uno de estos servicios digitales es Cambix, la plataforma del Banco que ofrece un servicio para el cambio de dólares a soles, y soles a dólares; a través de transferencias inmediatas, disponible para clientes de cualquier entidad financiera del Perú, y con un tipo de cambio competitivo y acorde al mercado. Actualmente, el servicio de Cambix tiene asignado 2 dominios, que son cambix.com.pe y cambix.pe; ambos con el subdominio triple www, como resultado se tienen 4 diferentes vías para el acceso por la web; que son cambix.com.pe, cambix.pe, www.cambix.com.pe y www.cambix.pe. Estos dominios y subdominios se implementaron desde el lanzamiento del

servicio de Cambix en noviembre de 2019, por motivos de estrategia de marketing definida en ese momento, por lo que las 4 URL respectivas son ya conocidas y expuestas a los clientes.

El problema es que la infraestructura de comunicaciones del Banco responsable de publicar el servicio de Cambix carece de funcionalidades de enrutamiento y de un mecanismo de protección contra amenazas comunes en la web; esta carencia tecnológica imposibilita centralizar los accesos al servicio de Cambix a través de un único dominio principal, genera elevados tiempos de respuesta, y dificulta la gestión y seguridad del servicio. Ante esta limitante en la publicación del servicio de Cambix, se plantea aplicar una tecnología moderna en Microsoft Azure para optimizar la infraestructura de comunicaciones del Banco a través de una Arquitectura de Enrutamiento diseñada para la publicación de los servicios en la nube. Si bien las 4 URL finalmente llevan al servicio, el inconveniente es que se pierde la centralización de actividades de analítica de negocio del servicio; esto quiere decir, que se tienen 4 fuentes separadas para un mismo servicio, impidiendo un análisis centralizado y preciso de estadísticas de acceso y seguimiento de eventos de los clientes (Martínez, 2022). Además, dificulta los esfuerzos por focalizar la publicidad de la URL del servicio y da lugar a que exista confusión en los clientes sobre cuál de las 4 URL es la oficial y correcta a la que deberían acceder. Y más aún, el servicio se encuentra expuesto sin la protección de una solución que pueda hacer frente a ataques automatizados de bots maliciosos que pueden afectar la seguridad, el rendimiento y la disponibilidad del servicio, comprometiendo la reputación del Banco.

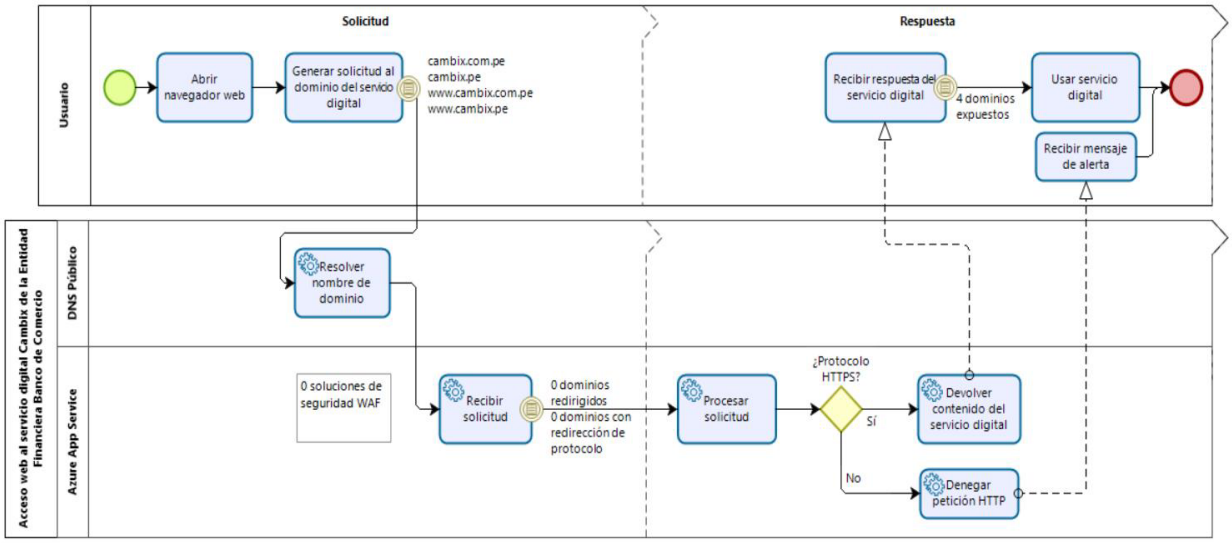
Por este motivo, se plantea redireccionar todo simplemente al dominio centralizado cambix.com.pe, definido como principal, para allí hacer la analítica y para ser el único frontis oficial y seguro expuesto hacia los clientes. De esta manera, siempre se mostrará el dominio principal en la barra de búsqueda del navegador, sin importar cuál de las 4 URL utilice el cliente para acceder; es decir, sea cual sea cualquiera de las 4 URL por las que el cliente acceda, siempre se redirigirá automáticamente a cambix.com.pe. Esto implica que los clientes deben

acceder al servicio web de Cambix a través del dominio principal, y al mismo tiempo es necesario mantener operativos los anteriores dominios como accesos por dominios alternos. De este modo, los clientes que accedan por dichos dominios alternos no se verán afectados, sino que serán redirigidos automáticamente al dominio principal. Esto es importante porque muchos clientes, ya sea de manera intencional o sin intención, podrían seguir accediendo a las anteriores URL, y no deben experimentar interrupciones en su flujo de acceso al servicio. Más bien, se busca disminuir el tiempo de respuesta en cada acceso al servicio (Perera, 2023). En la situación actual, los dominios dirigen directamente al servicio mediante registros DNS en NIC.PE (Punto.pe). Sin embargo, utilizar solo registros DNS para realizar una redirección no es una solución óptima para la entidad, pues se depende de las restricciones y limitaciones impuestas por la empresa registradora de dominios, que pueden generar varios inconvenientes, como mensajes de advertencia en el navegador del usuario, la imposibilidad técnica de realizar una redirección adecuada de HTTP a HTTPS, la imposibilidad de implementar un Firewall de Aplicaciones Web (WAF) para proteger contra bots y amenazas comunes en la web a nivel de aplicación (Cuiña, 2021), y, como se mencionó, la incapacidad de reemplazar el dominio alternativo por el dominio principal en la barra de búsqueda del navegador.

La Figura 1 muestra el flujograma del proceso de acceso web al servicio descrito. La Figura 2 muestra el flujo de navegación actual (AS IS) de los clientes para acceder al servicio digital de Cambix, donde el usuario cliente ingresa la URL con el dominio de Cambix y por medio de registros DNS en NIC.PE se dirige la solicitud directamente hacia un servicio de App Service en Microsoft Azure, que gestiona la solicitud y devuelve al cliente la página web de Cambix, manteniendo la URL ingresada inicialmente. En este proceso no se redirecciona ningún dominio para focalizar el dominio principal, y no se implementa un WAF para la protección del servicio frente a ataques a nivel de aplicación, de acuerdo con lo descrito.

Figura 1

Proceso de Acceso web al servicio digital Cambix de la Entidad Financiera Banco de Comercio



La Tabla 1 detalla los indicadores y los datos de preprueba de los indicadores mencionados, mientras la Tabla 2 muestra una comparativa de la situación actual y la situación propuesta consecuente con la mejora de dichos indicadores.

Tabla 1

Indicadores y Datos de Preprueba

Indicador	Datos de Preprueba
Tiempo de respuesta (Perera, 2023)	13.48 segundos
Número de dominios redirigidos (Martínez, 2022)	0 dominios redirigidos
Número de dominios expuestos hacia el navegador web del cliente (Martínez, 2022)	4 dominios expuestos
Número de dominios con redirección de HTTP a HTTPS (Martínez, 2022)	0 dominios con redirección de protocolo
Número de soluciones de seguridad WAF (Cuiña, 2021)	0 soluciones de seguridad WAF

Nota: Esta tabla muestra los indicadores actuales en el proceso de acceso web al servicio digital de Cambix.

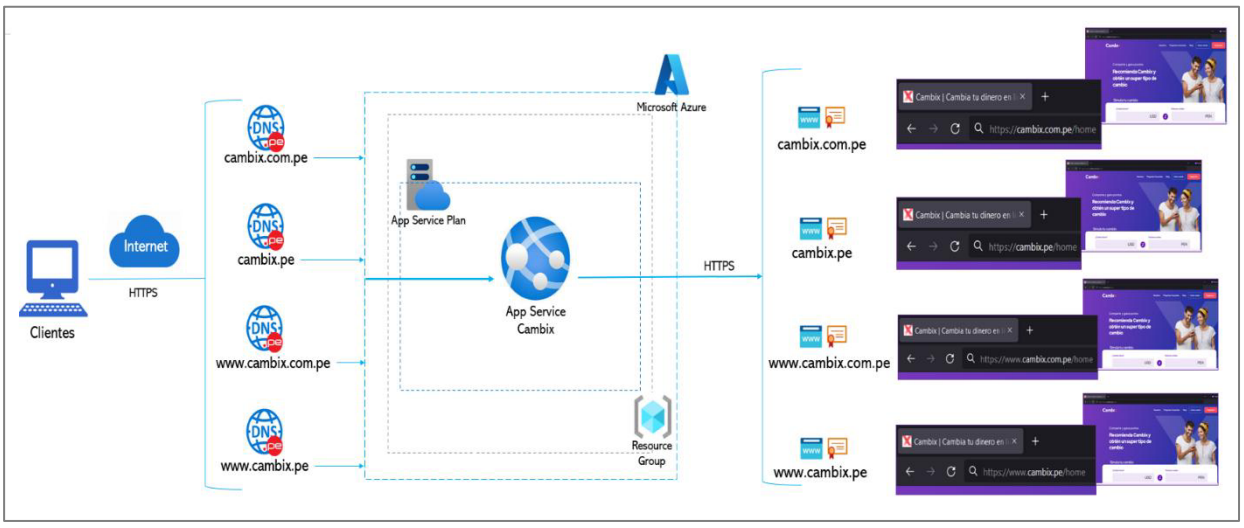
Tabla 2

AS IS / TO BE

Situación Actual (AS IS)	Situación Propuesta (TO BE)
Tiempos altos en la respuesta del servicio.	Tiempos bajos en la respuesta del servicio.
Falta de redirección de dominios.	Redirección de 3 dominios alternos hacia el dominio principal.
Ambigüedad por múltiples dominios expuestos hacia el navegar web del cliente, visibles en la barra de direcciones. Al ser el mismo servicio se debe exponer únicamente uno.	Focalización al exponer únicamente el dominio principal, para ser visible en la barra de direcciones del navegador web del cliente.
Falta de redirección de peticiones a nivel de protocolo HTTP a HTTPS para forzar la navegación segura, solo se tiene una restricción para denegar las peticiones HTTP.	Redirección de peticiones a nivel de protocolo HTTP a HTTPS para los 4 dominios.
Falta de una solución WAF como capa de seguridad a nivel de aplicación.	Habilitación de una solución WAF que será una capa de seguridad a nivel de aplicación.

Figura 2

Flujo de navegación AS IS de los clientes para acceder vía web al servicio digital de Cambix



1.1.1 Problema General

¿De qué manera la implementación de una Arquitectura de Enrutamiento en Azure Front Door, utilizando Microsoft Azure, mejora el acceso vía web al servicio digital de una entidad financiera?

1.1.2 Problemas Específicos

a. ¿En qué medida la implementación de una Arquitectura de Enrutamiento en Azure Front Door, utilizando Microsoft Azure, disminuye el tiempo de respuesta en el acceso vía web al servicio digital de una entidad financiera del Perú?
b. ¿En qué medida la implementación de una Arquitectura de Enrutamiento en Azure Front Door, utilizando Microsoft Azure, incrementa el número de dominios redirigidos para el acceso vía web al servicio digital de una entidad financiera del Perú?
c. ¿En qué medida la implementación de una Arquitectura de Enrutamiento en Azure Front Door, utilizando Microsoft Azure, disminuye el número de dominios expuestos hacia el navegador web del cliente en el acceso vía web al servicio digital de una entidad financiera del Perú?
d. ¿En qué medida la implementación de una Arquitectura de Enrutamiento en Azure Front Door, utilizando Microsoft Azure, incrementa el número de dominios con redirección de HTTP a HTTPS para el acceso vía web al servicio digital de una entidad financiera del Perú?
e. ¿De qué manera la implementación de una Arquitectura de Enrutamiento en Azure Front Door, utilizando Microsoft Azure, incrementa el número de soluciones de seguridad WAF en el acceso vía web al servicio digital de una entidad financiera del Perú?

1.2 Antecedentes

1.2.1 Antecedentes Nacionales

En referencia a los trabajos previos revisados sobre la implementación de soluciones utilizando Microsoft Azure, se tiene a Yacolca y Lopez (2022), quienes, en su investigación titulada "Sistema Web para el proceso de identificación biométrica con reconocimiento facial de clientes para la aseguradora Pacífico Seguros en Lima, 2021", en la Universidad Ricardo Palma, plantearon como objetivo desarrollar una solución tecnológica que contribuya a mejorar la experiencia de usuario de los clientes y reducir la exposición a riesgos de ciberseguridad en la aseguradora Pacífico Seguros; allí se presentó la utilización de una arquitectura orientada a microservicios en la nube, empleando componentes como Kubernetes, Dockers y Azure Front Door en Microsoft Azure. Siendo Pacifico Seguros una empresa de seguros, ofreciendo múltiples productos tales como los: seguros de vida, accidentes, renta vitalicia, familiares, complementario de trabajo de riesgo, etc., brindándose bajo diferentes tipos de coberturas; debe implementar procesos de autenticación y así controlar los accesos a los servicios que brindan a través de canales digitales y con ellos aumentar la confianza de los clientes respecto al uso de estos; así mismo reiterando su compromiso con la SBS (Superintendencia de Banca y Seguros), asegurando sus servicios por canales digitales. Tras implementar como solución una web de identificación biométrica, se concluye que dicha solución permitió reducir la exposición a riesgos de ciberseguridad en la compañía, influyendo también significativamente en la mejora de la experiencia del cliente.

Así mismo, Quispe (2021), realizó un estudio titulado "Diseño de escalamiento inteligente del Customer Relationship Management (CRM) bajo el modelo de nube hibrida entre azure y universidad privada peruana", en la Universidad Peruana de Ciencias Aplicadas; allí indicó el uso de un modelo de nube híbrida como una solución eficaz e inteligente en los

servidores CRM de cualquier Universidad Privada Peruana, usando los modelos de servicios de cómputo en la nube. Se presentó una propuesta de diseño de arquitectura en la nube de Microsoft Azure para la migración de servidores que soportan el Sistema Dynamic CRM 2015; debido a que, con el crecimiento exponencial de la información en los últimos años, este software requiere atención sobre calificada, ya sea en esfuerzo humano, como en adquisiciones de recursos de cómputo. Asimismo, el presente trabajo permitiría evidenciar los cambios necesarios que permitirán adaptarse al nuevo acontecimiento de un ecosistema en la nube. Se decidió un enfoque combinado a través de una nube híbrida On-Premise y Microsoft Azure. De esta forma se han podido utilizar infraestructuras de computación en la nube para construir lo que se puede definir como un servicio PaaS, en el cual se hace posible el intercambio de datos entre las aplicaciones que ahí residen y las aplicaciones alojadas en el centro de datos de la institución. Se concluye que con la investigación se logró cumplir con los objetivos propuestos y la solución planteada representa una aproximación válida para afrontar el problema del escalamiento de los servidores del CRM en la universidad.

Así también, Ruiz (2019), quien en su investigación “Migración de servidores a la nube de Microsoft Azure para mejorar la continuidad de los servicios TI, de la Fiduciaria en el año 2018”, en la Universidad San Ignacio de Loyola, define que, mediante una arquitectura en Microsoft Azure, la empresa La Fiduciaria puede migrar sus servidores físicos para un adecuado plan de contingencia de servicios. Se indica también que los sistemas basados en la nube se han convertido en una herramienta fundamental, ya que los proveedores de dichos servicios han invertido en tecnologías avanzadas para la protección de datos, privacidad, conectividad segura y un mejor control de accesos. Se concluye que tras la implementación de los servidores en la nube se logró reducir el tiempo de reanudación de los servicios de la empresa ante cualquier ataque o desastre que se pueda presentar, logrando así un adecuado plan de continuidad en la empresa.

Según Caldas (2016), en su investigación “Prácticas de gestión en la mejora en la calidad de servicios de Tecnologías de la Información al adoptar Cloud Computing”, en la Universidad Científica del Sur, las organizaciones de tecnología de la información proveen una serie de servicios que deben soportar diversos procesos críticos del negocio para cumplir objetivos y estrategias empresariales; al mismo tiempo la computación en la nube como tecnología emergente facilita una serie de servicios que progresivamente son adoptados por las empresas; y será necesario que el mismo sea gestionado con la calidad debida a fin de que aporte valor al negocio.

Así también, Llauce (2020), en su estudio “Implementación de una arquitectura de computación en la nube (cloud computing) diseñada para escalabilidad automática y alta disponibilidad basado en la plataforma de amazon web services (AWS) en la Universidad de Lambayeque”, en la Universidad Pedro Ruiz Gallo, indica que el actual crecimiento exponencial de Internet como herramienta fundamental para los servicios ofrecidos en línea también conlleva a tener usuarios cada vez más exigentes, es entonces necesario evaluar la infraestructura actual para determinar cierta problemática u oportunidad de mejora, y poder luego definir y elaborar una arquitectura tecnológica a través de tecnologías emergentes como las que ofrece la computación en la nube, que impactan positivamente y aprovechan las mejores herramientas de seguridad disponibles. Es estudio de Llauce concluye que la implementación de la arquitectura cloud computing propuesta para los sistemas y aplicaciones de la Universidad de Lambayeque es viable y aplicable.

1.2.2 Antecedentes Internacionales

Según Loaiza (2021), en su estudio titulado “Cloud Security Posture Management (CSPM) in Azure”, elaborado en la Metropolia University of Applied Sciences, Finlandia, las soluciones basadas en la nube deben alinearse a configuraciones de seguridad correctas basadas

en las mejores prácticas y el centro de recomendaciones de Microsoft, para permitir a las organizaciones proteger sus soluciones, mapear las vulnerabilidades, y garantizar una adecuada gestión de la arquitectura de seguridad de sus servicios en la nube.

También Goyes (2020), en su investigación titulada "Estudio de impacto del modelo cloud computing en la gestión de servicios de información gerencial en la banca privada Caso: Banco Internacional", elaborado en la Universidad Andina Simón Bolívar, Ecuador, sostuvo que, el Cloud Computing es un modelo de prestación de servicios tecnológicos, que permite el acceso a recursos compartidos de cómputo (redes, servidores, aplicaciones, servicios, plataformas, entre otros) bajo demanda y de forma ágil, facilitando al negocio el acceso a servicios según sus necesidades, acelerando el ritmo de la innovación de las organizaciones. La investigación realiza un estudio comparativo del modelo Cloud Computing vs On premise para la gestión de Servicios de Información Gerencial, tomando como caso de estudio al Banco Internacional del Ecuador, a través de un análisis que permitirá al sector financiero contar con un referente para la adopción de este paradigma tecnológico. Como base se realiza la comparación del modelo Cloud Computing vs On Premise, desde las siguientes perspectivas: financiera, tecnológica, normativa, de seguridad y de adopción del modelo. Todas éstas consideradas necesarias para la implementación de servicios en la nube, que garanticen la eficiencia, confidencialidad, disponibilidad e integridad de los datos, factores importantes para contar con la confianza de las áreas de negocio y por tanto del cliente.

Hoy en día, hay una interdependencia creciente entre el uso de la tecnología y el logro de objetivos corporativos; en ese sentido, la habilidad que tienen las empresas para relacionar el uso de la tecnología, sistemas de información, estrategias y lograr sus objetivos, es actualmente cada vez mayor. Las metas que se traza una empresa dependen a menudo de lo que sus sistemas de información sean capaces de realizar (Laudon y Laudon, 2012, p. 44, como se citó en Goyes, 2020); y la Banca en específico, realiza grandes inversiones en tecnología,

como un medio para alcanzar sus objetivos de negocio, buscando además excelencia operacional, desarrollar nuevos productos, modelos de negocio, servicios, tener más cercanía con clientes, proveedores y ser más asertivos en la toma de decisiones.

Según la Superintendencia de Bancos de Ecuador, el 73% de las transacciones que se realizaron en instituciones financieras del país en el 2017 fueron en canales electrónicos. Por otra parte, el Banco Central informa que la tasa de crecimiento del uso de los medios de pago digitales durante los últimos cinco años fue del 16%, pero entre 2016 y 2017 aumentó 30%. (Tapia, 2018, párr. 2-3, como se citó en Goyes, 2020). En la búsqueda de la eficiencia, varios bancos entre 2016 y 2017, redujeron el número de agencias que tenían en el país para fortalecer los servicios en el área digital, lo que representó montos considerables de inversión y costos. Todo esto se trata de una tendencia mundial que tiene que ver con un cambio en las demandas de los consumidores de la nueva generación y una mayor penetración de las tecnologías.

La demanda de servicios financieros en el mercado requiere de constante renovación e innovación tecnológica, como: infraestructura, comunicaciones, software y aplicaciones que conllevan grandes inversiones financieras, que también se reflejan en la administración y mantenimiento de dichos servicios. Es así como el modelo Cloud Computing, se ha convertido en una alternativa para la implementación de servicios tecnológicos. La nube, como se le denomina generalmente, es un espacio de almacenamiento, procesamiento de datos y archivos ubicado fuera de las instalaciones del cliente, conectado a través de Internet, que puede alojar casi cualquier servicio. La investigación de Goyes busca determinar los beneficios y desafíos que ha tenido el Banco Internacional de Ecuador, al adoptar el modelo de Cloud Computing, en la gestión de servicios de TI, específicamente para el Sistema de Información Gerencial. Adicionalmente, este estudio podrá ser tomado como referencia o ser replicado en instituciones, no solo financieras, que deseen adoptar el modelo Cloud Computing para la provisión de servicios de TI.

Sobre la investigación de Goyes, se concluye que el modelo Cloud Computing en la gestión de Servicios de Información Gerencial, es más eficiente en costos y permite además el despliegue de servicios de forma más rápida que el modelo On Premise. Así también, se concluye que en Banco Internacional del Ecuador existe una acertada gestión de riegos y seguridad sobre servicios tecnológicos en la nube; y que los proveedores de nube no están exentos a eventos que comprometan la calidad o up time del servicio, sin embargo, cumplen con los estándares y controles de Banco Internacional para el Sistema de Información Gerencial (Goyes, 2020).

Según Galiveeti et al. (2021), en su artículo científico titulado "Cybersecurity Analysis: Investigating the Data Integrity and Privacy in AWS and Azure Cloud Platforms", el campo de la tecnología de la información sigue siendo dominante en términos de adopción de tecnologías modernas. Además, hay una mayor adopción de tecnologías en diversos ámbitos e industrias, una de esas tecnologías que emerge rápidamente es el avance de la computación en la nube. Un número importante de usuarios y organizaciones buscan plataformas en la nube para aprovechar sus operaciones y productividad. La tecnología continúa ganando más atención en el ámbito empresarial de TI. Las plataformas en la nube ofrecen una mayor flexibilidad para soportar la computación en tiempo real y surgen como un marco más sólido que ofrece ofertas a través de Internet. Amazon Web Services (AWS) y Microsoft Azure son dos plataformas clave en la nube que permiten a los usuarios utilizar la nube como fuente de almacenamiento, acceso y recuperación de datos. En el período moderno de rápido cambio tecnológico global, las soluciones en la nube de AWS y Azure se adoptan ampliamente como plataformas de almacenamiento público para sistemas de información masiva. Ambas plataformas de servidores ofrecen ofertas privadas, públicas, híbridas y comunitarias a distintas organizaciones. Se concluye que, en la computación en la nube, las cuestiones clave son la confidencialidad y la protección de los datos disponibles en las herramientas de la nube, por lo

cual es indispensable diseñar marcos efectivos que puedan identificar el ingreso de información no aprobada y garantizar a los clientes que la solución de computación en la nube es segura.

1.3 Objetivos

1.3.1 Objetivo General

Implementar una Arquitectura de Enrutamiento en Azure Front Door, utilizando Microsoft Azure, para mejorar el acceso vía web al servicio digital de una entidad financiera.

1.3.2 Objetivos Específicos

a. Disminuir el tiempo de respuesta en el acceso vía web al servicio digital de una entidad financiera del Perú.
b. Incrementar el número de dominios redirigidos para el acceso vía web al servicio digital de una entidad financiera del Perú.
c. Disminuir el número de dominios expuestos hacia el navegador web del cliente en el acceso vía web al servicio digital de una entidad financiera del Perú.
d. Incrementar el número de dominios con redirección de HTTP a HTTPS para el acceso vía web al servicio digital de una entidad financiera del Perú.
e. Incrementar el número de soluciones de seguridad WAF en el acceso vía web al servicio digital de una entidad financiera del Perú.

1.4 Justificación

La presente investigación se justifica por lo siguiente:

1.4.1 Conveniencia

El estudio ayudará a centralizar el acceso vía web al servicio digital a través de la implementación de una Arquitectura de Enrutamiento en Azure Front Door, permitiendo redirigir los múltiples dominios expuestos hacia solamente el dominio principal e incluyendo la habilitación de un Web Application Firewall como una capa de seguridad contra Bots a nivel de aplicación; favoreciendo así la marca, los objetivos y la seguridad del servicio digital ofrecido por la entidad financiera.

1.4.2 Relevancia social

Realizar la implementación de una Arquitectura de Enrutamiento en Azure Front Door proporcionará a los clientes del servicio digital de Cambix un acceso directo y transparente a la URL oficial en la web; así como una capa de seguridad contra Bots para reforzar la protección del servicio e información de los clientes; en beneficio de los actuales y futuros clientes del servicio digital de Cambix, así como en beneficio de la entidad financiera.

1.4.3 Implicaciones prácticas

El estudio permitirá la redirección de múltiples dominios a un único dominio centralizado, permitirá exponer y publicitar a los clientes un único dominio principal, permitirá focalizar la publicidad del servicio, permitirá habilitar una solución de seguridad contra Bots y amenazas comunes en la web como capa de seguridad a nivel de aplicación; se va a optimizar la infraestructura de comunicaciones del Banco responsable de la publicación de los servicios en la nube.

1.4.4 Utilidad metodológica

El estudio permitirá realizar la implementación de una Arquitectura de Enrutamiento en Azure Front Door en la plataforma Microsoft Azure, a través de la creación y configuración

de recursos en la nube de acuerdo con las directivas y prácticas recomendadas (estándares) de Microsoft Azure.

1.4.5 Valor teórico

El estudio permitirá comprobar si la implementación de una Arquitectura de Enrutamiento en Azure Front Door generaría o no un impacto positivo en el acceso vía web al servicio digital de una entidad financiera del Perú, a través de la redirección de dominios y la habilitación de un firewall de aplicaciones web de capa 7.

De igual manera, la presente investigación considera las siguientes limitaciones:

a. La investigación se limita al acceso vía web para el servicio digital de Cambix, del Banco de Comercio del Perú; se deben considerar las variaciones pertinentes en el acceso vía web para otros servicios; ya que es posible replicar la Arquitectura de Enrutamiento en Azure Front Door propuesta, pero cada entidad define y adecua el tratamiento de sus dominios web, la definición de sus dominios principales, la estrategia de redirección de sus dominios y la habilitación de soluciones de seguridad.
b. La investigación se limita a la implementación de una Arquitectura de Enrutamiento en Azure Front Door propuesta para el servicio digital de Cambix; no se contempla modificación o actualización alguna a nivel de aplicación, funcionalidad o código fuente de dicho servicio.
c. La investigación se limita a la implementación de la solución a través de Microsoft Azure, debido a que en la actualidad el Banco de Comercio cuenta con un contrato vigente con este proveedor de servicios en la nube y tiene además el servicio digital de Cambix albergado allí. Se deben considerar las variaciones pertinentes para otros proveedores de servicios en la nube, debido a que cada uno establece y personaliza sus servicios de red para el enrutamiento de tráfico web.

1.5 Hipótesis

1.5.1 Hipótesis General

Si se implementa una Arquitectura de Enrutamiento en Azure Front Door, utilizando Microsoft Azure, entonces mejora el acceso vía web al servicio digital de una entidad financiera.

1.5.2 Hipótesis Específicas

a. Si se implementa una Arquitectura de Enrutamiento en Azure Front Door, utilizando Microsoft Azure, entonces disminuye el tiempo de respuesta en el acceso vía web al servicio digital de una entidad financiera del Perú.
b. Si se implementa una Arquitectura de Enrutamiento en Azure Front Door, utilizando Microsoft Azure, entonces incrementa el número de dominios redirigidos para el acceso vía web al servicio digital de una entidad financiera del Perú.
c. Si se implementa una Arquitectura de Enrutamiento en Azure Front Door, utilizando Microsoft Azure, entonces disminuye el número de dominios expuestos hacia el navegador web del cliente en el acceso vía web al servicio digital de una entidad financiera del Perú.
d. Si se implementa una Arquitectura de Enrutamiento en Azure Front Door, utilizando Microsoft Azure, entonces incrementa el número de dominios con redirección de HTTP a HTTPS para el acceso vía web al servicio digital de una entidad financiera del Perú.
e. Si se implementa una Arquitectura de Enrutamiento en Azure Front Door, utilizando Microsoft Azure, entonces incrementa el número de soluciones de seguridad WAF en el acceso vía web al servicio digital de una entidad financiera del Perú.

II. MARCO TEÓRICO

2.1 Bases teóricas sobre el tema de investigación

2.1.1 Arquitectura de Enrutamiento en Azure Front Door

A continuación, para describir la variable independiente, que es Arquitectura de Enrutamiento en Azure Front Door, se presenta el concepto de Microsoft Learn (2023a), que indica que se refiere a la estructura y diseño de los componentes que se utilizan para enrutar el tráfico de red a través de la infraestructura de entrega de contenido global de Azure. El enrutamiento es el proceso de selección de rutas en cualquier red (Amazon Web Services [AWS], s.f.). Una red de entrega de contenido (CDN, Content Delivery Network) es un sistema distribuido de servidores que almacenan en caché contenido cerca de los usuarios finales para reducir la latencia y mejorar el tiempo de respuesta de las aplicaciones, con el fin de garantizar una experiencia de usuario rápida y fluida, independientemente de la ubicación geográfica del cliente.

Azure Front Door es un servicio moderno y seguro de CDN global, que proporciona una solución de enrutamiento de tráfico, balanceo de carga y protección contra amenazas para aplicaciones web. Se compone principalmente de los componentes de front-end, grupos de back-end y reglas de enrutamiento, que se diseñan y configuran para dirigir y gestionar el acceso al contenido de una aplicación o sitio web. Es un servicio moderno y seguro porque combina la tecnología CDN con capacidades de seguridad, en un único servicio integrado, permitiendo así proteger las aplicaciones web frente a ciberataques, así como aceleración en la entrega del contenido. También se puede hacer referencia a Azure Front Door simplemente como Front Door.

El enrutamiento del tráfico de Azure Front Door se basa en reenvíos y redirecciones a nivel de dominios y protocolos, y se lleva a cabo en varias etapas. Primero, el tráfico se enruta

desde el cliente hasta Front Door; aquí Front Door permite tener múltiples dominios personalizados a través de configuraciones en los front-ends y los usuarios hacen solicitudes a Front Door a través de estos dominios. Luego, Front Door utiliza la configuración de reglas de enrutamiento para determinar el back-end hacia donde enviar el tráfico para recuperar el contenido; las reglas de enrutamiento son el núcleo de la arquitectura de Front Door, pues definen cómo y hacia dónde se debe enviar el tráfico. Finalmente, los grupos de back-end contienen la configuración de los servidores back-end (también llamados servidor de origen) en donde se aloja el contenido original del sitio web; después de ser procesado por las reglas de enrutamiento se envía el tráfico al back-end configurado para dar respuesta a la solicitud inicial del cliente. El firewall de aplicaciones web de Front Door y la configuración de almacenamiento en caché se pueden habilitar en el proceso de enrutamiento. Decir Arquitectura de Enrutamiento Front Door es una manera concisa de referirse a la Arquitectura de Enrutamiento en Azure Front Door.

En resumen, la Arquitectura de Enrutamiento en Azure Front Door se refiere a cómo se organizan los componentes para proporcionar un servicio de enrutamiento eficiente, seguro y confiable.

2.1.2 Acceso vía web al servicio digital

De igual manera, para describir la variable dependiente, se considera lo mencionado por Martínez (2022), quien lo refiere como el acceso transparente a contenido multimedia a través de un navegador web, acceso a Internet y el protocolo HTTP. Un servicio digital se proporciona a través de una plataforma en línea, como una aplicación móvil o un sitio web.

El acceso vía web a un servicio digital permite a los usuarios acceder al servicio desde cualquier lugar donde tengan acceso a Internet y un navegador web. Por ejemplo, si se tiene una cuenta bancaria en línea, se puede acceder a ella desde cualquier lugar con acceso a Internet

y un navegador web. De esta manera, se puede realizar transacciones bancarias, verificar el saldo y realizar otras operaciones bancarias sin tener que visitar una sucursal física.

Decir acceso web equivale a decir acceso vía web, pero de una forma más directa y común. Incluir la palabra vía añade un tono más formal y explícito, para resaltar que el acceso se realiza a través de la web.

2.1.3 Microsoft Azure

La computación en la nube, también llamada cloud computing, es un modelo que permite el acceso a recursos informáticos a través de Internet (National Institute of Standards and Technology [NIST], 2022). Una de las plataformas de computación en la nube más reconocidas y aplicadas a nivel mundial es Microsoft Azure, una plataforma administrada por Microsoft, que ofrece una serie de servicios en la nube para diseñar, desarrollar, implementar y administrar aplicaciones y soluciones sostenibles, escalables y seguras en la nube, a través de una red mundial de centros de datos.

También se le conoce como simplemente Azure, y proporciona una gama de capacidades de cómputo, incluyendo los modelos de servicio de software como servicio (SaaS), plataforma como servicio (PaaS) e infraestructura como servicio (IaaS), ofreciendo así servicios de máquinas virtuales, almacenamiento, redes, opciones para servidores físicos, plataformas de desarrollo, bases de datos, etc.; con todas las certificaciones en materia seguridad y protección de datos. Un marco que se puede utilizar con Microsoft Azure es el Well-Architected Framework, que proporciona un conjunto de principios, consideraciones de diseño y mejores prácticas para crear soluciones óptimas en la nube. El marco considera una serie de etapas clave: diagnóstico de componentes y configuraciones existentes, elaboración de un plan de trabajo, validación preliminar en un entorno de pruebas, despliegue en el entorno productivo y verificación de la solución mediante monitoreo y pruebas de funcionalidad; junto

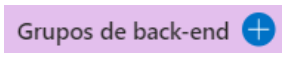
con una serie de recomendaciones organizadas en torno a sus cinco pilares: confiabilidad, seguridad, optimización de costos, excelencia operativa y eficiencia del rendimiento, que ayudan a evaluar y mejorar las cargas de trabajo en Azure (Microsoft Learn, 2023b).

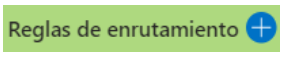
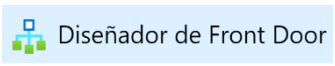
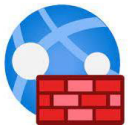
2.1.4 Características de componentes en Microsoft Azure

La Tabla 3 muestra un listado de los diversos componentes asociados a los servicios de Microsoft Azure oportunos para esta investigación, presentando la simbología y terminología para cada componente.

Tabla 3

Simbología y terminología por componente en los servicios de Microsoft Azure

Componente	Simbología	Terminología
Front Door		Servicio moderno y seguro de CDN en la nube, que proporciona una plataforma para el enrutamiento de tráfico y balanceo de carga para aplicaciones web. Se conoce también como Perfil de Front Door y CDN.
Front-end/dominios		El host de front-end especifica el subdominio deseado en el dominio predeterminado de Front Door para enrutar el tráfico desde ese host a través de dicho servicio. Posteriormente también se puede incorporar dominios personalizados.
Grupos de back-end		Un grupo back-end es un conjunto de servidores back-end equivalentes entre los que Front Door equilibra la carga de las solicitudes de cliente.

Componente	Simbología	Terminología
Reglas de enrutamiento		Una regla de enrutamiento o routing roule asigna el host de front-end y un patrón de ruta de acceso de dirección URL coincidente a un grupo back-end específico.
Edge Location		Una Edge Location o Ubicación Perimetral en Front Door, es la zona geográfica desde donde se transfieren los datos hacia los clientes o usuarios finales, es decir, la zona desde donde serán enviados los recursos de un sitio web para que carguen en el navegador web de un usuario.
Diseñador de Front Door		Sección de la plataforma que permite la creación y configuración de front-end/dominios, grupos de back-end y reglas de enrutamiento en Front Door.
Suscripción		Una suscripción de Azure concede acceso a los servicios de Azure. También determina cómo se notifica el uso de los recursos y cómo se facturan los servicios.
Grupo de recursos		Un grupo de recursos es un contenedor que almacena los recursos relacionados con una solución de Azure. El grupo de recursos incluye los recursos que se desean administrar como grupo.
Recurso		Un recurso es un elemento administrable que está disponible a través de Azure.
Firewall de aplicaciones web (WAF)		WAF de Azure, integrado de forma nativa, que ofrece protección a las aplicaciones web frente a vulnerabilidades de seguridad.
Almacén de claves (Key Vault)		Servicio que permite almacenar y administrar de forma segura secretos como contraseñas, claves de API, certificados digitales y otros datos sensibles.

Componente	Simbología	Terminología
App Service		App Service de Azure es un modelo de implementación de servidores web como servicio PaaS. Permite generar, implementar y escalar rápidamente aplicaciones web y móviles que se ejecutan en cualquier plataforma.
App Service Plan (ASP)		Un ASP define las características que obtendrán las aplicaciones (App Services) que se coloquen en dicho plan, como la región, número de instancias (VM), tamaño de la instancia, y plan de tarifa. Cuando se crea un ASP en una determinada región, se crea un conjunto de recursos de proceso para ese ASP en dicha región.

Nota: Esta tabla presenta simbología y terminología por componente en los servicios de Microsoft Azure oportunos para esta investigación; para conocer la totalidad de los servicios ofrecidos por Microsoft Azure, y/o detallar la información, se puede consultar la información oficial de Microsoft Azure en Azure Portal.

2.1.5 Azure Portal

Azure Portal es la consola unificada de Microsoft Azure para la implementación y administración de soluciones en la nube a través de un navegador web. Azure Portal tiene presencia en cada centro de datos de Azure. Esta configuración hace que Azure Portal sea resistente a errores individuales del centro de datos y ayuda a evitar ralentizaciones de red al estar cerca de los usuarios. Azure Portal se actualiza continuamente y no requiere tiempo de inactividad para las actividades de mantenimiento (Microsoft Learn, 2023c).

2.1.6 Cliente, servidor, solicitud, respuesta, tiempo de respuesta

En el acceso web a un servicio digital, un cliente es el dispositivo, aplicación o navegador web utilizado por un usuario para acceder a un recurso o servicio en Internet, enviado solicitudes a un servidor y recibiendo las respuestas necesarias para mostrar contenido y funcionalidades. Un servidor es un sistema que recibe, procesa y responde a las solicitudes enviadas por los clientes, entregando los recursos e información necesaria (MDN Web Docs, 2023b).

Una solicitud, también conocida como petición o request, es el mensaje que un cliente envía a un servidor para pedir un recurso, e incluye datos como el método HTTP y cabeceras. Una respuesta, también conocida como response, es el mensaje que el servidor devuelve al cliente después de procesar la solicitud, y contiene el resultado de esa operación, junto con un código de estado de respuesta HTTP e información relevante para el cliente. Un método HTTP es una instrucción, definida por el protocolo HTTP, que un cliente indica en una solicitud para especificar la operación a realizar sobre un recurso del servidor, como obtener datos, enviarlos, actualizarlos o eliminarlos (MDN Web Docs, 2023b).

El tiempo de respuesta es el intervalo total que transcurre desde que un cliente envía una solicitud al servidor hasta que recibe la respuesta completa, reflejando la rapidez con la que el sistema procesa la petición y entrega la información solicitada. El TTFB (Time To First Byte) es el tiempo que transcurre desde que el navegador envía una petición hasta que recibe el primer byte de la respuesta. PLT (Full Page Load Time) es el tiempo que tarda una página en cargar por completo. En navegadores web, el tiempo del evento Load indica que la respuesta del servicio está completa a nivel de recursos (Perera, 2023).

2.1.7 Internet, web, navegador web, página web, sitio web, DNS, CNAME

Internet es la mayor red de comunicaciones del planeta, compuesta por la interconexión de miles de redes de todo el mundo. La web (Word Wide Web) es una colección global de páginas web disponibles a través de Internet. Un navegador web es un software que permite el acceso a la web. Una página web es un documento en la web, al cual se accede a través de un navegador web, y un sitio web es un conjunto de páginas web referentes a un mismo tema. DNS es el sistema de nombres de dominio (Domain Name System), que permite la gestión y traducción de un nombre de dominio hacía un registro que hace referencia a un servidor en Internet.

Un registro DNS, también llamado archivo de zona, es una instrucción que define la información que referencia al servidor de destino; existen una serie tipos de registros, cada uno con una finalidad específica, como los registros Tipo A que referencian a una dirección IP, o los registros CNAME (nombre canónico) que referencian a otro dominio (Google Support, s.f.-a).

2.1.8 Dominio, número de dominios redirigidos, FQDN, estructura jerárquica de un dominio

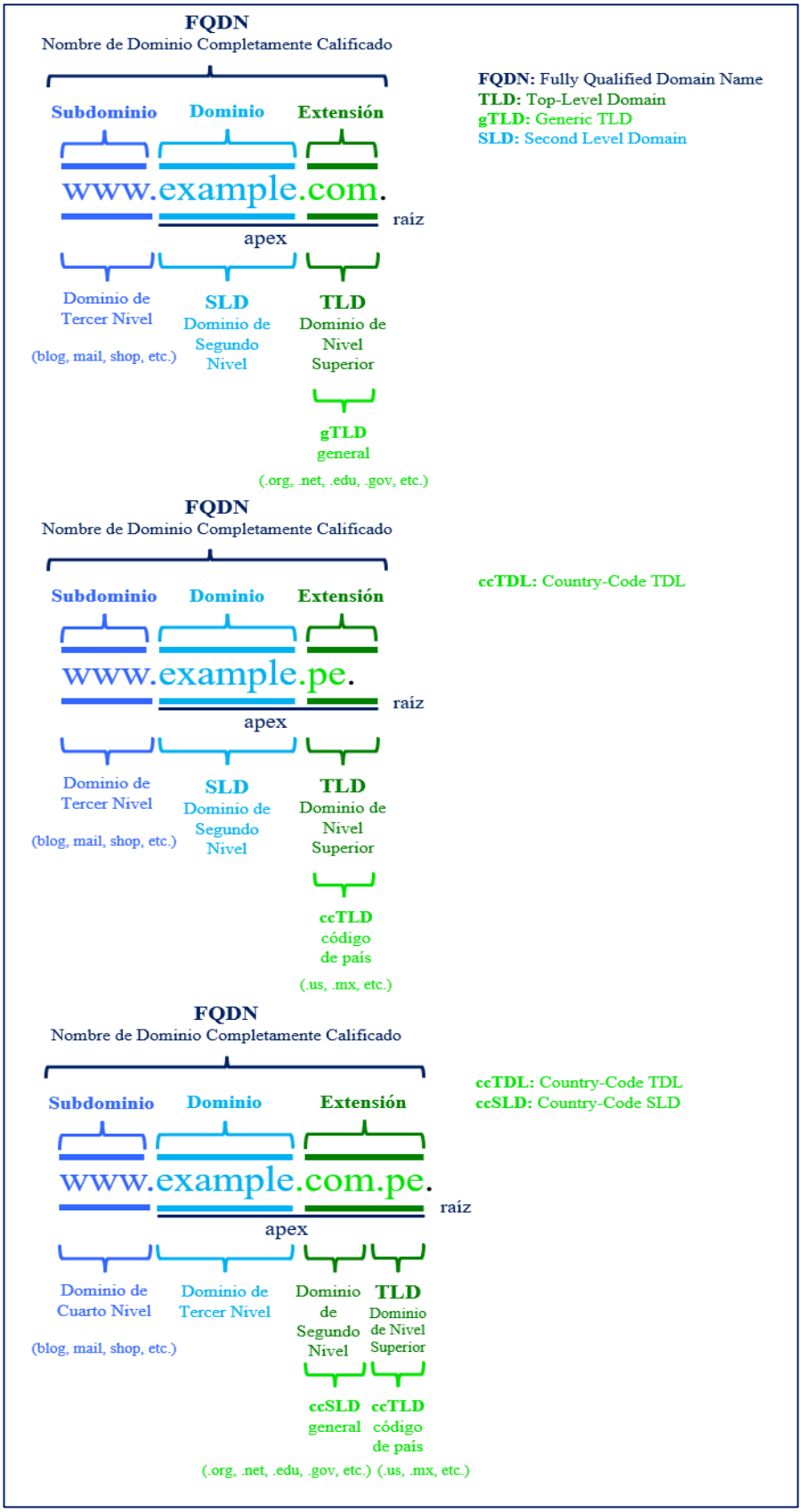
Un dominio es un nombre único que identifica un servidor en Internet y permite al acceso a un sitio web, compuesto normalmente por el nombre de una organización o sitio web y la extensión de dominio. Un dominio redirigido es aquel que, al ser introducido en el navegador, lleva al usuario a otro dominio diferente. Por ejemplo, si se escribe www.google.com.pe, se podría redirigir a www.google.com, que es el dominio principal de Google. Esto puede ser útil para saber la popularidad de un sitio web, el alcance de su audiencia o la eficiencia de su estrategia de marketing. Esto se hace para facilitar el acceso de los usuarios a los sitios web que tienen diferentes versiones o extensiones según el país o el idioma.

Existen diferentes tipos de redirecciones, pero la más común y recomendada es la redirección 301, que indica que el cambio de dominio es permanente y que el contenido se ha trasladado definitivamente a una nueva URL (Localizador de Recursos Uniforme, o por sus siglas en inglés Uniform Resource Locator). Esto ayuda a evitar problemas de duplicidad de contenido y penalizaciones por parte de los motores de búsqueda. Es así que, el número de dominios redirigidos es una medida que indica cuántos dominios diferentes se dirigen a un mismo dominio (Google Support, s.f.-b).

Un dominio se compone de varias partes jerárquicas, que juntas forman una dirección única en Internet. La estructura básica incluye: el subdominio (que clasifica secciones específicas de un sitio web), el dominio (que corresponde al nombre principal registrado) y la extensión de dominio (o dominio de nivel superior, que representa la parte final del dominio y forma parte del estándar de Internet). Aunque el subdominio www es técnicamente un subdominio del dominio base (apex), ambos pueden configurarse, resolverse en el sistema DNS y operar de manera completamente independiente. Por tanto, en términos prácticos y funcionales es válido considerarlos operativamente como dominios distintos. Todas las partes conforman el FQDN (Fully Qualified Domain Name), nombre de dominio completamente calificado que representa el nombre absoluto de un host en la jerarquía DNS y permite identificarlo de forma única en Internet. El FQDN incluye un punto final (.) que señala el dominio raíz (representa el punto de partida o raíz de toda la estructura de dominios en Internet), pero este suele omitirse en las interfaces de usuario debido a razones de usabilidad. En dominios que combinan un código de país y un tema genérico, como “.com.pe”, el nombre de dominio registrado se convierte en el dominio de tercer nivel, por ende, un subdominio de este se convierte en un dominio de cuarto nivel. La Figura 3 detalla la estructura descrita.

Figura 3

Estructura jerárquica de un dominio



2.1.9 ICANN, IANA, DNS Root Zone, TLD, gTLD, ccTLD, SLD, ccSLD

Existen organizaciones globales que de manera estructurada regulan el otorgamiento de dominios en Internet, como la Corporación de Internet para la Asignación de Nombres y Números (ICANN), que coordina la asignación de nombres de dominio y de direcciones IP para garantizar el funcionamiento, seguridad, estabilidad y unificación de Internet (Internet Corporation for Assigned Names and Numbers [ICANN], s.f.).

La Autoridad de Números Asignados en Internet (IANA) es una función dentro de ICANN, encargada de tareas técnicas relacionadas con la gestión de identificadores de Internet, como la administración del espacio global de direcciones IP y la administración de los dominios de nivel superior en la zona raíz DNS. Mientras que ICANN supervisa IANA y establece políticas para asegurar Internet, IANA implementa esas decisiones a nivel técnico (Internet Assigned Numbers Authority [IANA], s.f.). La zona raíz DNS (DNS Root Zone) representa el nivel más alto de la jerarquía del sistema de nombres de dominio. Es un archivo maestro que contiene la lista de todos los dominios de nivel superior TLDs (Top-Level Domains) válidos en Internet. Incluye tanto dominios genéricos gTLDs (Generic Top-Level Domains, como .com, .org, .net, .edu, .gov, etc.) como dominios de código de país ccTLDs (Country-Code Top-Level Domains, como .pe, .us, .mx, etc.). La parte debajo de un TLD se denomina dominio de segundo nivel SLD (Second-Level Domain). En caso un gTLD se establezca debajo de un ccTLD, este pasa a denominarse dominio de segundo nivel con código de país ccSLD (Country-Code Second-Level Domain, como .com.pe, .edu.mx, etc.).

2.1.10 Punto Pe, NIC.PE

Punto Pe, es la empresa registradora de dominios responsable de los dominios con extensión ".pe" referentes al Perú. El ".pe" ha sido administrado por la Red Científica Peruana, institución que ha desempeñado la función de Network Information Center en el Perú

(NIC.PE). A través de su gestión, el ".pe" ha logrado preservar la estabilidad de los dominios peruanos y la operatividad de Internet (Punto Pe, s.f.).

2.1.11 Número de dominios expuestos hacia el navegador web del cliente

Mozilla Developer Network Web Docs (MDN Web Docs, 2023a), refiere al número de dominios expuestos hacia el navegador web del cliente, como una medida de la cantidad de dominios que el navegador reconoce y muestra en la barra de direcciones al acceder a un sitio web. La visibilidad de estos dominios es esencial para la navegación web, ya que permite a los usuarios identificar y acceder a sitios específicos. El número de dominios expuestos al navegador puede afectar el rendimiento y la seguridad de la página web; es necesario tener una estrategia clara que justifique el uso de múltiples dominios, de lo contrario las páginas web pueden ser vulnerables a ataques, fraude por suplantación de dominio, problemas de indexación en los motores búsqueda por contenido duplicado, o incluso pérdida de la propiedad del dominio, lo que puede poner en riesgo la privacidad y la seguridad de los usuarios.

2.1.12 HTTP, HTTPS, TLS

Sobre el protocolo HTTP, se considera la definición de MDN Web Docs (2023b), que señala que el protocolo de transferencia de hipertexto o HTTP, por sus siglas en inglés HyperText Transfer Protocol, es un protocolo de la capa de aplicación para la transmisión de documentos hipermedia en la red. Diseñado para la comunicación entre los navegadores y servidores web, siguiendo el clásico modelo cliente-servidor, en el que un cliente establece una conexión con el servidor, realiza una petición y espera hasta que recibe una respuesta del mismo. Clientes y servidores se comunican intercambiando mensajes individuales. Los mensajes que envía el cliente, normalmente un navegador web, se llaman peticiones, y los mensajes enviados por el servidor se llaman respuestas.

HTTPS (HTTP Secure) es una versión encriptada del protocolo HTTP. Utiliza TLS (Transport Layer Security) para cifrar toda la comunicación entre un cliente y un servidor. Esta conexión segura permite a los clientes intercambiar datos confidenciales de forma segura con un servidor, por ejemplo, para actividades bancarias o compras en línea (MDN Web Docs, 2023c). TLS, anteriormente conocido como SSL (Secure Sockets Layer), es un protocolo criptográfico que permite que la autenticación entre cliente y servidor para garantizar la confidencialidad e integridad de datos en la comunicación. Cuando un servidor y un cliente se comunican mediante TLS, se garantiza que ningún tercero pueda escuchar o alterar ningún mensaje. Todos los navegadores web modernos admiten el protocolo TLS, y requiere que el servidor proporcione un certificado digital válido que confirme su identidad para establecer una conexión segura (MDN Web Docs, 2023d).

2.1.13 Certificado digital, PFX, DigiCert

De acuerdo con DigiCert, Inc. (s.f.-a), un certificado digital es un archivo electrónico que autentica la identidad en línea de una persona o empresa, y permite a los usuarios y destinatarios de la web tener la seguridad de que los datos que introducen van a parar a una fuente de confianza. Un certificado digital se instala en el servidor o plataforma que alberga un sitio web, y permite establecer conexiones seguras desde un navegador web, ya que la trasferencia de datos se realiza mediante el protocolo HTTPS a través de TLS. Un certificado contiene un par de claves, una pública y otra privada, las cuales funcionan juntas para establecer una conexión cifrada. El certificado también contiene la información del sujeto, que es la identidad del propietario del certificado o sitio web. Un sitio web seguro expone un icono de candado en la barra de direcciones del navegador web, al hacer clic allí, se puede ver detalles del certificado instalado. La extensión .crt es la extensión estándar para identificar a un archivo de certificado digital, sin embargo, estos certificados también se pueden presentar en formato PFX en archivos con la extensión .pfx que contienen la información de cifrado del certificado.

Los certificados digitales los emiten las autoridades de certificación (CA, por sus siglas en inglés Certification Authority). DigiCert es una entidad CA con una sólida reputación y uno de los proveedores líderes de certificados digitales a nivel global (CertSuperior, s.f.).

2.1.14 Número de dominios con redirección de HTTP a HTTPS

El número de dominios con redirección de HTTP a HTTPS es una medida que indica cuántos sitios web envían el tráfico de peticiones con el protocolo HTTP hacía la versión con el protocolo HTTPS, forzando así la navegación mediante este protocolo seguro (MDN Web Docs, 2023e). La redirección de HTTP a HTTPS es una técnica que consiste en enviar una respuesta al cliente que le indica que acceda al mismo recurso web, pero usando el protocolo HTTPS en lugar de HTTP. De esta forma, se evita que la información sea interceptada o modificada por terceros malintencionados. El número de dominios con redirección de HTTP a HTTPS se puede estimar usando herramientas de análisis web o consultando bases de datos públicas que recopilan información sobre los dominios registrados. La redirección de HTTP a HTTPS se puede implementar de diferentes formas según el servicio web que se utilice.

2.1.15 Número soluciones de seguridad WAF, Bots

El número de soluciones de seguridad WAF es una medida que expresa la existencia de un firewall de aplicaciones web disponible para proteger las aplicaciones web. Un firewall de aplicaciones web (WAF) es un componente de seguridad que protege las aplicaciones web. Es un sistema que filtra, monitoriza y bloquea el tráfico web malicioso que llega a una aplicación, a través de un conjunto de reglas, análisis de comportamiento y políticas de inteligencia de amenazas diseñadas para monitorear y distinguir entre tráfico de red malicioso y tráfico de red seguro, particularmente para los protocolos web HTTP y HTTPS. Un WAF previene ataques de capa 7, pues opera en la séptima capa del modelo OSI, también conocida como capa de aplicación. En lugar de filtrar según una dirección IP, un WAF puede investigar los paquetes de datos para determinar si incluyen bots maliciosos u otras amenazas.

Un bot es un programa informático que realiza tareas repetitivas en Internet, como rastrear sitios web, enviar spam o realizar compras falsas. Algunos bots pueden ser beneficiosos, como los que indexan el contenido para los motores de búsqueda, pero otros pueden ser maliciosos y dañar la seguridad, el rendimiento y la disponibilidad de las aplicaciones web. Aproximadamente el 20% de todo el tráfico de Internet proviene de bots con intención maliciosa (Microsoft Learn, 2023d).

Los WAF han evolucionado para proteger contra bots maliciosos, abuso de API (interfaz de programación de aplicaciones que permite que diferentes aplicaciones se comuniquen entre sí para intercambiar datos) y elementos incluidos en el Top 10 de OWASP, como protección DDoS y protección contra robo de datos. La protección que ofrece un WAF también se puede obtener como servicio de seguridad en la nube, y en actualidad proveedores de servicios en la nube, o por siglas en inglés Cloud Service Provider (CSP), como Microsoft Azure, posibilitan su incorporación como componente de seguridad en las soluciones implementadas en la nube (Palo Alto Networks, s.f.).

2.1.16 HTTP Status Response Codes

Los códigos de estado de respuesta HTTP (HTTP Response Status Codes, o simplemente HTTP Status Codes), son códigos que indican si se ha completado satisfactoriamente una petición HTTP específica. Las respuestas se agrupan en cinco clases (MDN Web Docs, 2023f).

1. Informational responses (100 – 199)
2. Successful responses (200 – 299)
3. Redirection messages (300 – 399)
4. Client error responses (400 – 499)
5. Server error responses (500 – 599)

La Tabla 4 detalla la clasificación de los códigos de estado de respuesta HTTP.

Tabla 4

Clasificación de códigos de estado de respuesta HTTP

Código	Respuesta	Detalle
Informational responses		
100	Continue	Esta respuesta provisional indica que todo hasta ahora está bien y que el cliente debe continuar con la solicitud o ignorarla si ya está terminada.
101	Switching Protocols	Este código se envía en respuesta a un encabezado de solicitud Upgrade por el cliente e indica que el servidor acepta el cambio de protocolo propuesto por el agente de usuario. Los encabezados HTTP permiten al cliente y servidor enviar información junto a una solicitud o respuesta.
102	Processing	Este código indica que el servidor ha recibido la solicitud y aún se encuentra procesándola, por lo que no hay respuesta disponible.
103	Early Hints	Este código de estado está pensado principalmente para ser usado con el encabezado Link, permitiendo que el agente de usuario empiece a precargar recursos mientras el servidor prepara una respuesta.
Successful responses		
200	OK	La solicitud ha tenido éxito. El significado del éxito varía dependiendo del método HTTP: - **GET**: El recurso solicitado ha sido recuperado y transmitido en el cuerpo del mensaje. - **HEAD**: Los encabezados de representación se incluyen en la respuesta sin el cuerpo del mensaje. Respuesta idéntica a la de una petición GET, pero sin el cuerpo del mensaje. - **PUT** o **POST**: El recurso que describe el resultado de la acción (actualización o creación) se transmite en el cuerpo del mensaje. - **TRACE**: El cuerpo del mensaje contiene el mensaje de solicitud recibido por el servidor (tras efectuar una prueba de bucle al recurso).
201	Created	La solicitud ha tenido éxito y se ha creado un nuevo recurso como resultado de ello. Ésta suele ser la respuesta enviada después de solicitudes POST.

Código	Respuesta	Detalle
Successful responses		
202	Accepted	La solicitud se ha recibido, pero aún no se ha actuado. Está destinado para los casos en que otro proceso o servidor maneja la solicitud, o para el procesamiento por lotes.
203	Non-Authoritative Information	La petición se ha completado con éxito, pero su contenido no se ha obtenido de la fuente originalmente solicitada, sino que se recoge de una copia local o de un tercero. Excepto esta condición, se debe preferir una respuesta de 200 OK en lugar de esta respuesta.
204	No Content	La petición se ha completado con éxito, pero su respuesta no tiene ningún contenido, aunque los encabezados pueden ser útiles.
205	Reset Content	La petición se ha completado con éxito, pero su respuesta no tiene contenidos y además, el agente de usuario tiene que inicializar la página desde la que se realizó la petición, este código es útil por ejemplo para páginas con formularios cuyo contenido debe borrarse después de que el usuario lo envíe.
206	Partial Content	La petición servirá parcialmente el contenido solicitado. Esta característica es utilizada por herramientas de descarga como wget para continuar la transferencia de descargas anteriormente interrumpidas, o para dividir una descarga y procesar las partes simultáneamente.
207	Multi-Status	Transmite información sobre varios recursos en situaciones en las que varios códigos de estado podrían ser apropiados.
208	Already Reported	Usado dentro de elementos de respuesta DAV (Web Distributed Authoring and Versioning es una extensión HTTP que permite actualizar contenido de forma remota desde un cliente), cuando el listado de elementos ya se notificó previamente, por lo que no se van a volver a listar.
226	IM Used	El servidor ha cumplido una petición GET para el recurso y la respuesta es una representación del resultado de una o más manipulaciones de instancia aplicadas a la instancia actual.

Código	Respuesta	Detalle
Redirection messages		
300	Multiple Choices	Esta solicitud tiene más de una posible respuesta, y el usuario debe escoger una de ellas.
301	Moved Permanently	La URL del recurso solicitado ha sido cambiada permanentemente, y la nueva URL se devuelve en la respuesta.
302	Found	Este código de respuesta significa que el recurso de la URI solicitada ha sido cambiado temporalmente. Nuevos cambios en la URI serán agregados en el futuro. Por lo tanto, la misma URI debe ser usada por el cliente en futuras solicitudes.
303	See Other	El servidor envía esta respuesta para indicarle al cliente que obtenga el recurso solicitado en otro URI usando una solicitud GET.
304	Not Modified	Esta es usada para propósitos de caché. Le indica al cliente que la respuesta no ha sido modificada. Entonces, el cliente puede continuar usando la misma versión almacenada en su caché.
307	Temporary Redirect	El servidor envía esta respuesta para indicarle al cliente que obtenga el recurso solicitado en otro URI con el mismo método que se utilizó en la solicitud anterior. Tiene la misma semántica que el código de respuesta HTTP 302 Found, con la excepción de que el agente de usuario no debe cambiar el método HTTP utilizado: si se utilizó un POST en la primera solicitud, se debe utilizar un POST en la segunda solicitud. Un 307 Internal Redirect no es un código oficial, pero puede presentarse en configuraciones de servidores web. Es una redirección iniciada por el navegador web con un propósito muy específico: desviar a los visitantes de la versión HTTP de un sitio web a la versión HTTPS más segura.
308	Permanent Redirect	Significa que el recurso ahora está ubicado permanentemente en otro URI, especificado por el encabezado Location. Tiene la misma semántica que el código de respuesta HTTP 301 Moved Permanently, con la excepción de que el usuario no debe cambiar el método HTTP utilizado.

Código	Respuesta	Detalle
Client error responses		
400	Bad Request	El servidor no pudo interpretar la solicitud debido una sintaxis inválida.
401	Unauthorized	El cliente debe autenticarse para obtener la respuesta solicitada. Aunque el estándar HTTP especifica “no autorizado”, semánticamente esta respuesta significa "no autenticado". Es similar a 403, pero en este caso, la autenticación es posible.
402	Payment Required	Este código de respuesta está reservado para futuros usos. El objetivo inicial de crear este código era usarlo en sistemas de pagos digitales, sin embargo, se usa muy raramente y aún no existe una convención estándar.
403	Forbidden	Prohibido. El cliente no tiene permisos de acceso al contenido; es decir, no está autorizado, por lo que el servidor rechaza otorgar el recurso solicitado. A diferencia de 401 Unauthorized, aquí el servidor sí conoce la identidad del cliente.
404	Not Found	El servidor no pudo encontrar el recurso solicitado. Este código de respuesta es uno de los más conocidos debido a su frecuente ocurrencia en la web. En el navegador esto significa que no se reconoce la URL. En una API, esto también puede significar que el objetivo es válido pero el recurso en sí no existe. Los servidores también pueden enviar esta respuesta en lugar de 403 Forbidden para ocultar la existencia de un recurso a un cliente no autorizado.
405	Method Not Allowed	El servidor conoce el método de solicitud, pero el recurso de destino no lo admite. Por ejemplo, es posible que una API no permita llamar a DELETE para eliminar un recurso. Los métodos GET y HEAD, nunca deben ser deshabilitados y no deberían retornar este código de error.
406	Not Acceptable	Esta respuesta es enviada cuando el servidor, después de aplicar una negociación de contenido, no encuentra ningún contenido que se ajuste a los criterios dados por el usuario.
407	Proxy Authentication Required	Esto es similar al código 401, pero la autenticación debe realizarse mediante un proxy (equipo informático que intercepta conexiones de red originadas desde un cliente hacia un servidor de destino).

Código	Respuesta	Detalle
Client error responses		
408	Request Timeout	Esta respuesta se envía en una conexión inactiva por parte de algunos servidores, incluso sin ninguna solicitud previa por parte del cliente. Significa que el servidor desea cerrar esta conexión no utilizada. También hay que tener en cuenta que algunos servidores simplemente cierran la conexión sin enviar este mensaje.
409	Conflict	Esta respuesta se envía cuando una solicitud entra en conflicto con el estado actual del servidor.
410	Gone	Esta respuesta se envía cuando el contenido solicitado se ha eliminado permanentemente del servidor, sin dirección de reenvío. Se espera que los clientes eliminen sus cachés y enlaces al recurso. La especificación HTTP pretende que este código de estado se utilice para "servicios promocionales por tiempo limitado". Las API no deberían sentirse obligadas a indicar recursos que se han eliminado con este código de estado.
411	Length Required	El servidor rechaza la petición porque el campo de encabezado Content-Length no está definido y el servidor lo requiere.
412	Precondition Failed	El cliente ha indicado condiciones previas en sus encabezados que el servidor no cumple.
413	Payload Too Large	La entidad de solicitud es más larga que los límites definidos por el servidor. El servidor puede cerrar la conexión o devolver un campo de encabezado Retry-After.
414	URI Too Long	La URI solicitada por el cliente es más larga de lo que el servidor está dispuesto a interpretar.
415	Unsupported Media Type	El formato multimedia de los datos solicitados no está soportado por el servidor, por lo que el servidor rechaza la solicitud.
416	Requested Range Not Satisfiable	No se puede cumplir el rango especificado en el campo de encabezado Rango en la solicitud. Es posible que el rango esté fuera del tamaño de los datos del URI de destino.
417	Expectation Failed	Significa que la expectativa indicada por el campo de encabezado Expect solicitada no puede ser cumplida por el servidor.

Código	Respuesta	Detalle
Client error responses		
418	I'm a teapot	Indica que el servidor se rehúsa a preparar café porque es una tetera. Este error es una referencia al Hyper Text Coffee Pot Control Protocol, creado como parte de una broma del April Fools' Day (día de los inocentes) de 1998.
421	Misdirected Request	La solicitud se dirigió a un servidor que no puede producir una respuesta. Esto puede ser enviado por un servidor que no esté configurado para producir respuestas para la combinación de esquema (https) y autoridad (dominio y puerto) que se incluyen en el URI de solicitud.
422	Unprocessable Entity	La petición estaba bien formada (sintaxis) pero no se pudo seguir debido a errores de semántica (coherencia).
423	Locked	El recurso al que se accede está bloqueado.
424	Failed Dependency	La solicitud falló debido a la falla de una solicitud previa.
426	Upgrade Required	El servidor se niega a realizar la solicitud utilizando el protocolo actual, pero podría estar dispuesto a hacerlo después de que el cliente actualice a un protocolo diferente. El servidor envía un encabezado Upgrade en la respuesta para indicar los protocolos requeridos.
428	Precondition Required	El servidor origen requiere que la solicitud sea condicional.
429	Too Many Requests	El usuario ha enviado demasiadas solicitudes en un periodo de tiempo dado.
431	Request Header Fields Too Large	El servidor no está dispuesto a procesar la solicitud porque los campos de encabezado son demasiado largos.
451	Unavailable For Legal Reasons	El usuario solicita un recurso ilegal, como alguna página web censurada por algún gobierno.
Server error responses		
500	Internal Server Error	El servidor ha encontrado una situación que no sabe cómo manejar.

Código	Respuesta	Detalle
Server error responses		
501	Not Implemented	El método solicitado no está soportado por el servidor y no puede ser manejado. Los únicos métodos que los servidores soportan (y por lo tanto no deben devolver este código) son GET y HEAD.
502	Bad Gateway	Esta respuesta de error significa que el servidor, mientras trabajaba como puerta de enlace para obtener la respuesta necesaria para manejar la solicitud, obtuvo una respuesta inválida.
503	Service Unavailable	El servidor no está listo para manejar la solicitud. Las causas comunes son que el servidor está inactivo por mantenimiento o está sobrecargado.
504	Gateway Timeout	Esta respuesta de error es dada cuando el servidor está actuando como una puerta de enlace y no puede obtener una respuesta a tiempo.
505	HTTP Version Not Supported	La versión de HTTP usada en la solicitud no está soportada por el servidor.
506	Variant Also Negotiates	El servidor tiene un error de configuración interno en el que un recurso variante elegido está configurado para participar en la negociación de contenido (proceso mediante el cual el servidor y el cliente acuerdan qué formato de contenido usar para responder a una solicitud, si no pueden acordar un formato se genera un conflicto), por lo que no es un punto final de negociación adecuado.
507	Insufficient Storage	El método no se pudo realizar en el recurso porque el servidor no puede almacenar la representación necesaria para completar con éxito la solicitud.
508	Loop Detected	El servidor detectó un ciclo infinito mientras procesaba la solicitud.
510	Not Extended	Se requieren extensiones compatibles con la solicitud para que el servidor la cumpla.
511	Network Authentication Required	Indica que el cliente necesita autenticarse para obtener acceso a la red.

Nota: Adaptado de *HTTP response status codes* por MDN Web Docs (2023f).

2.1.17 URI, URL, URN

URI es un Identificador de Recursos Uniforme, un estándar para identificar a un recurso publicado en la web. Se compone de una cadena de texto que contiene el nombre de un recurso, o ser más completa y contener el esquema (protocolo, sistema de reglas que definen y permiten la comunicación entre dispositivos para la transmisión de información), autoridad (dominio y puerto), la ruta al recurso (ubicación del recurso en el servidor web), parámetros (lista de pares clave valor) y ancla (para representar una parte dentro del recurso) (MDN Web Docs, 2023g).

URL es un Localizador de Recursos Uniforme, un mecanismo usado por los navegadores para localizar y obtener cualquier recurso publicado en la web. Es una cadena de texto que contiene el esquema (protocolo), el dominio, el puerto (por lo general, se omite si el servidor web utiliza los puertos estándar 80 y 443), y complementariamente la ruta al recurso, parámetros y ancla. Las URL también se denominan dirección web o enlace (MDN Web Docs, 2023h).

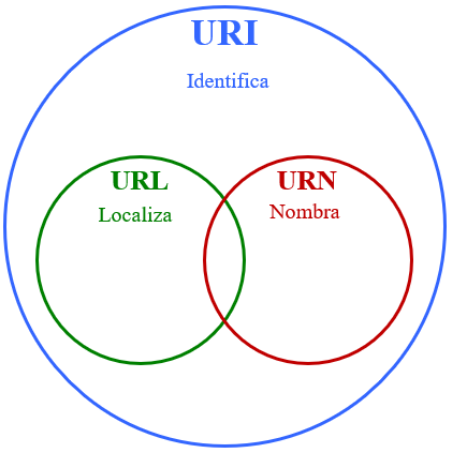
URN es el Nombre de Recurso Uniforme, un estándar para dar un nombre único y persistente a un recurso, sin especificar donde localizarlo en la web. Se compone de una cadena de caracteres que contiene el esquema estándar urn, el nombre del sistema identificador y el nombre específico del recurso; por ejemplo “urn:isbn:0123456789” para identificar un libro por el Sistema Internacional de Numeración de Libros, o “urn:issn:1234-5678” para identificar una revista por el Número Internacional Normalizado de Publicaciones Seriadas (International Standard Serial Number [ISSN], s.f.).

Las URI identifican y las URL localizan; sin embargo, los localizadores también son identificadores, ya que una URL es un subconjunto de una URI; quiere decir que cada URL también es una URI, pero no toda URI es una URL. Así también, una URN es un subconjunto de una URI (Stack Overflow, 2020). La Figura 4 muestra la relación de pertenencia de conjunto entre una URI, URL y URN, mediante un Diagrama de Venn. La Figura 5 muestra un ejemplo

con las partes que componen una URL, en comparación a una URI. La Figura 6 muestra un ejemplo funcional con las partes que componen una URL en comparación a una URN y una URI.

Figura 4

Relación entre una URI, URL y URN mediante un Diagrama de Venn



Nota: Nótese como todas la URL y URN son una URI, pero no todas las URI necesariamente serán una URL, ni todas las URN formarán parte de una URL.

Figura 5

Comparación entre las partes de una URL frente a una URI

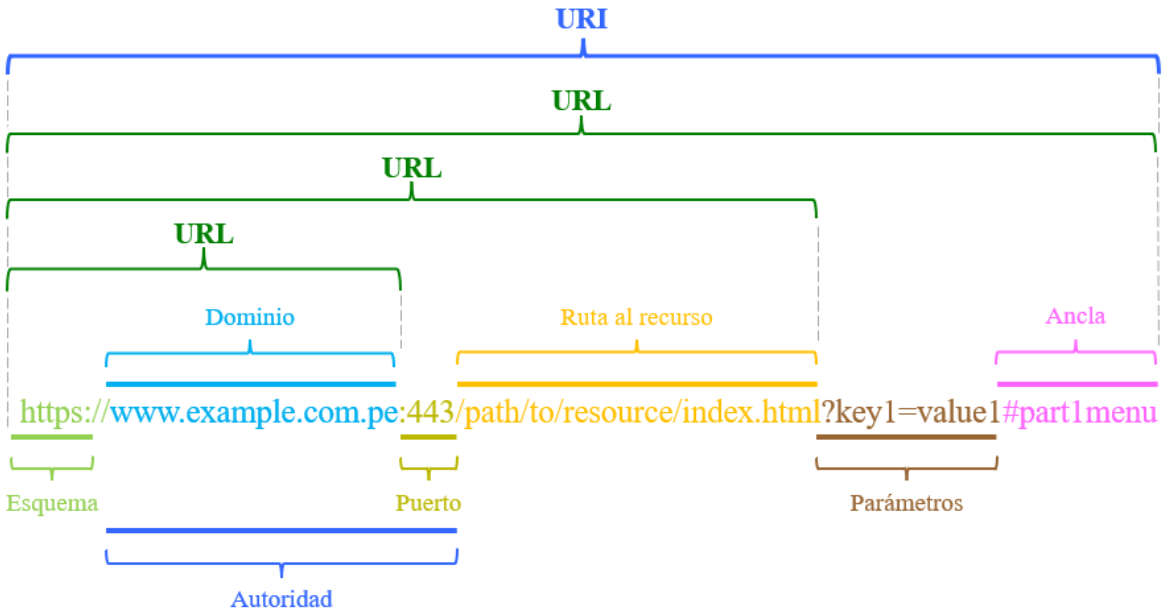
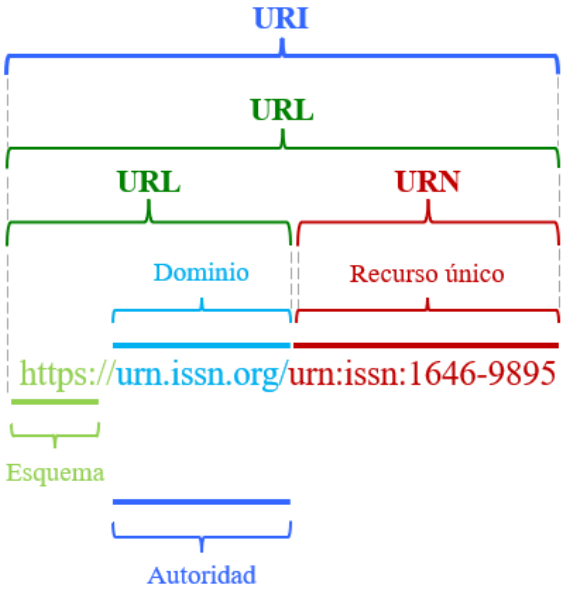


Figura 6

Comparación entre las partes de una URL frente a una URN y una URI



2.1.18 Microsoft Edge DevTools

Microsoft Edge DevTools es una herramienta integrada directamente en el navegador Microsoft Edge que permite inspeccionar, emular y depurar el comportamiento de una página web. DevTools se ejecuta dentro del navegador y proporciona un entorno visual al que se accede presionando la combinación de teclas Ctrl+Shift+I en Windows y Linux, o Comando+Opción+I en macOS; también, presionando la tecla F12; o simplemente haciendo clic derecho en la pantalla y seleccionando la opción Inspeccionar (Microsoft Learn, 2023e).

Microsoft Edge DevTools dispone de un panel de Red (Network) que proporciona un entorno para inspeccionar los parámetros de las solicitudes y respuestas HTTP intercambiadas entre cliente y servidor al acceder a un sitio web (Microsoft Learn, 2023f).

2.1.19 Mozilla Firefox Private Browsing

Mozilla Firefox es un navegador web con amplia compatibilidad y múltiples herramientas de navegación para los usuarios finales, disponible para Windows, macOS y

Linux en máquinas de escritorio; así como Android y iOS en dispositivos móviles. Una importante funcionalidad de Mozilla Firefox es la navegación privada (Private Browsing), que elimina automáticamente la información de navegación, por lo cual no se agrega ninguna página web visitada a la lista del historial de navegación, ni a la lista de la barra de direcciones, no se almacenan cookies (archivos que guardan información con las preferencias de navegación de un sitio web para presentar esta información personalizada en posteriores visitas), ni almacena archivos en caché (memoria que almacena copias de los archivos de un sitio web solicitado, de forma que las siguientes peticiones pueden ser respondidas por el propio caché y no por el servidor web) (Mozilla Support, s.f.-a).

La barra de direcciones de un navegador web muestra la URL con el dominio del sitio web al que se accede. Incluye una función que recuerda las páginas visitadas y aprende de los hábitos de navegación del usuario. De esta forma, los sitios web visitados con mayor frecuencia se muestran en la parte superior de la lista con tan solo escribir un carácter (Mozilla Support, s.f.-b). Con esta herramienta se asegura que todas las pruebas de acceso al sitio web se realicen como si se tratase del primer acceso de un usuario a dicho sitio web, para comprobar el dominio expuesto en el navegador web.

2.1.20 Digicert SSL Certificate Checker

Digicert SSL Certificate Checker es una herramienta de diagnóstico de instalación de certificados digitales. Esta herramienta permite verificar que un certificado digital esté instalado correctamente, así como comprobar la información del propietario y autoridad de certificación (DigiCert, Inc., s.f.-b).

2.1.21 Azure Log Analytics, KQL

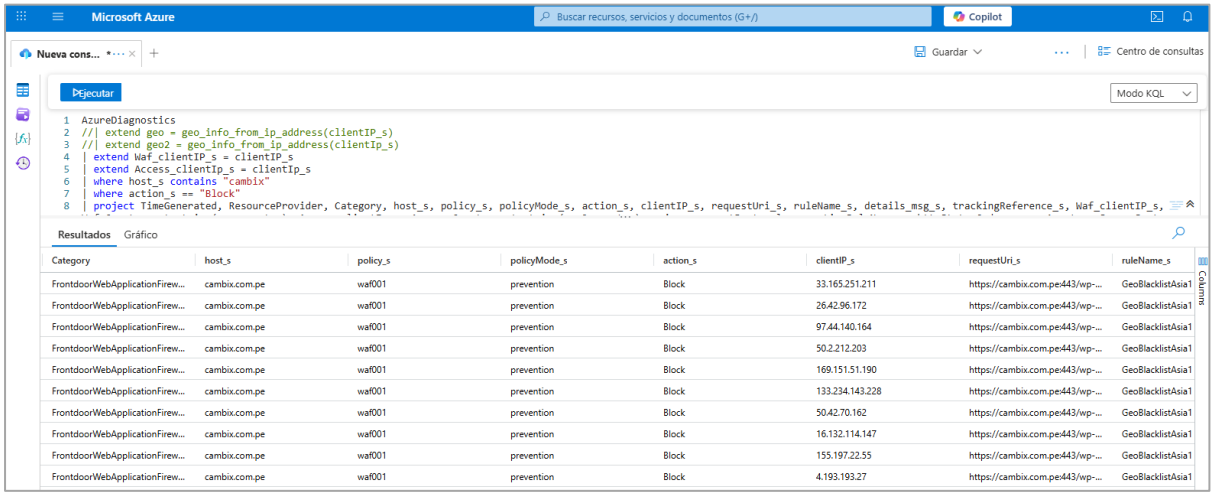
Log Analytics es una herramienta de Azure Portal que se usa para editar y ejecutar consultas de logs (información con los eventos de un sistema) de un recurso en Azure, y

analizar los resultados de forma interactiva (Microsoft Learn, 2023g). Las consultas se escriben mediante el Lenguaje de Consulta Kusto (KQL), un lenguaje diseñado para el análisis de datos en los modelos tabulares de tablas y columnas de Microsoft Azure (Microsoft Learn, 2024).

El WAF de Azure Front Door proporciona informes detallados sobre cada solicitud y amenaza que detecta. El registro se integra con los registros de diagnóstico de Log Analytics. La Figura 7 muestra un ejemplo de la vista del servicio. Azure Front Door proporciona dos tipos de registros: registros de acceso y registros de WAF. Los registros de acceso incluyen todas las solicitudes que pasan por Azure Front Door, mientras que los registros de WAF incluyen cualquier solicitud que coincida con una regla de WAF, las cuales pueden permitir o bloquear una solicitud. Además, los registros de WAF proporcionan información sobre lo que el WAF evalúa, empareja y bloquea, para inspeccionar lo que sucede con cada solicitud (Microsoft Learn, 2023h).

Figura 7

Vista de Azure Log Analytics y KQL desde Azure Portal



III. MÉTODO

3.1 Tipo de investigación

Tipo Aplicada. Este tipo de investigación está interesada en la aplicación de los conocimientos a la solución de un problema práctico inmediato. De este modo, se busca aplicar los conocimientos científicos en la solución de problemas reales y concretos, en este caso, en la mejora del acceso vía web a un servicio digital. El objetivo final es mejorar el acceso vía web a Cambix a través de la implementación de una Arquitectura de Enrutamiento en Microsoft Azure Front Door, con el fin de ofrecer un servicio seguro, operativo, centralizado y de fácil acceso para el cliente. Así también, como lo señala Vara (2015, p. 235), la investigación empresarial generalmente es aplicada, porque busca solucionar un problema concreto, práctico y sus resultados son utilizados inmediatamente en la solución de problemas de la realidad cotidiana de las empresas.

Nivel Descriptivo y Explicativo. Pues según Carrasco (2019), esta investigación responde a las preguntas: ¿Qué cambios y modificaciones se han producido?, ¿qué mejoras se han logrado?, ¿cuál es la eficiencia del nuevo sistema?, etc. En este nivel se aplica un nuevo sistema, modelo, tratamiento programa, método o técnicas para mejorar y corregir la situación problemática, que ha dado origen al estudio de investigación.

La investigación explicativa establece relaciones entre conceptos, explica por qué ocurre un fenómeno y por qué se relacionan dos o más variables. No solo se limita a describir o comparar fenómenos, sino que busca identificar la causa del cambio observado tras la implementación de una solución técnica, permitiendo establecer una relación causa-efecto entre las variables involucradas. La investigación explicativa proporciona un sentido de entendimiento del fenómeno, y, de hecho, implica los propósitos de las investigaciones con los demás alcances (exploración, descripción, correlación); así pues, aunque un estudio sea en

esencia explicativo, contendrá elementos exploratorios, descriptivos y correlacionales (Hernández y Mendoza, 2018, p. 113), es decir, también explora, describe y establece correlaciones que permitan responder cómo es la realidad que es objeto de investigación o de estudio.

Diseño Experimental Puro. La presente es una investigación con Diseño Experimental Puro con estructura de posprueba únicamente, incluyendo un grupo de control. En este diseño uno de los grupos recibe el tratamiento experimental y el otro no (grupo de control), y la única diferencia entre los grupos es la presencia-ausencia de la variable independiente.

La Figura 8 muestra el diagrama con el diseño de la presente investigación.

Figura 8

Diagrama de diseño de posprueba y grupo de control

RGe	**X**	**O_1**
RGc	**--**	**O_2**

Donde:

R = Elección Aleatoria de los elementos del Grupo.

Ge = Grupo experimental.

Gc = Grupo de control.

O_1 = Medición posterior al estímulo, en el grupo experimental. [Resultado de aplicar las pruebas con la Arquitectura de Enrutamiento propuesta].

O_2 = Medición posterior al estímulo, en el grupo de control.

X = Tratamiento, estímulo o condición experimental. [Arquitectura de Enrutamiento].

-- = Falta de estímulo o condición experimental.

3.2 Ámbito temporal y espacial

La presente investigación contempla los años 2023 y 2024, considerando el acceso vía web a un servicio digital llamado Cambix, ofrecido por el Banco de Comercio, Lima, Perú.

3.3 Variables

3.3.1 Conceptualización

a. **Variable Independiente:** Arquitectura de Enrutamiento en Azure Front Door.

Se detalla en la Tabla 5.

Tabla 5

Conceptualización de variable independiente

Indicador: Presencia_Ausencia
Descripción: En este momento tiene el valor NO, porque aún no se ha implementado la Arquitectura de Enrutamiento en Azure Front Door para el acceso vía web al servicio digital de una entidad financiera del Perú. Cuando tome el valor SÍ, es porque ya se implementó la Arquitectura de Enrutamiento en Azure Front Door y se espera obtener mejores resultados.

b. **Variable Dependiente:** Acceso vía web al servicio digital. Se detalla en la Tabla 6.

Tabla 6

Conceptualización de variable dependiente

Indicador	Descripción
Tiempo de respuesta	Es el intervalo de tiempo que transcurre desde que se envía la solicitud al servicio hasta que se recibe la respuesta.
Número de dominios redirigidos	Es el número de dominios alternos que se redirigen hacia el dominio principal, para que el acceso vía web al servicio digital se realice únicamente a través del dominio principal.
Número de dominios expuestos hacia el navegador web del cliente	Es el número de dominios visibles en la barra de direcciones del navegador web del cliente al acceder vía web al servicio digital.
Número de dominios con redirección de HTTP a HTTPS	Es el número de dominios que redirigen las peticiones que vienen con el protocolo HTTP desde el navegador web del cliente hacia el protocolo HTTPS, para aplicar un certificado digital SSL/TLS a nivel de protocolo HTTPS en el acceso vía web al servicio digital.
Número de soluciones de seguridad WAF	Es el número de soluciones para garantizar la seguridad contra Bots y amenazas comunes en la web, como capa de seguridad a nivel de aplicación en el acceso vía web al servicio digital.

3.3.2 Operacionalización

a. **Variable Independiente:** Arquitectura de Enrutamiento en Azure Front Door. Se detalla en la Tabla 7.

Tabla 7

Operacionalización de variable independiente

Indicador	Índice
Presencia_Ausencia	No, Sí

b. **Variable Dependiente:** Acceso vía web al servicio digital. Se detalla en la Tabla 8.

Tabla 8

Operacionalización de variable dependiente

Dimensión	Indicador	Índice	Unidad de Medida	Fórmula	Unidad de Observación
Accesibilidad	Tiempo de respuesta	[0.1 s - 30 s]	Segundos	-	Revisión manual
	Número de dominios redirigidos	[0-3]	Cantidad	-	Revisión manual
Identidad corporativa	Número de dominios expuestos hacia el navegador web del cliente	[1-4]	Cantidad	-	Revisión manual
Operatividad	Número de dominios con redirección de HTTP a HTTPS	[0-4]	Cantidad	-	Revisión manual
Seguridad	Número de soluciones de seguridad WAF	[0-1]	Cantidad	-	Revisión manual

3.4 Población y muestra

La población y muestra de la presente investigación se detalla en la Tabla 9.

Tabla 9

Detalles de la Población y Muestra de la Investigación

Concepto	Detalle
Unidad Muestral:	Proceso de Acceso web a servicio digital en Entidades Financieras. Restricciones: • Entidades Financieras privadas. • Entidades Financieras del Perú.
Universo:	Todos los procesos de Acceso web a servicio digital en Entidades Financieras privadas del Perú. Debido a que no se puede conocer ni determinar la cantidad, se tiene: N = Indeterminado
Muestra:	Proceso de Acceso web al servicio digital Cambix de la Entidad Financiera Banco de Comercio. n = 30
Tipo de Muestreo:	Aleatorio

La muestra está conformada por los registros individuales del Proceso de Acceso web al servicio digital, recolectados mediante Azure Log Analytics. Cada registro representa una unidad de análisis y contiene información técnica relevante para evaluar los cinco indicadores de este estudio. Se considera un tamaño de muestra de 30 registros, en línea con los criterios estadísticos mínimos aceptables para diseños experimentales. Se utiliza un muestreo aleatorio simple. Se tienen 2 marcos muestrales, pues cada marco muestral es el conjunto de registros

para cada etapa del experimento, de este modo se trabaja con 30 registros del grupo experimental en la posprueba, así como 30 registros del grupo de control en la posprueba.

3.5 Instrumentos

3.5.1 Investigación de Campo

La técnicas e instrumentos se detallan en la Tabla 10.

Tabla 10

Técnicas e instrumentos de investigación de campo

Técnicas	Instrumentos
La Observación Directa: - Espontánea o no estructurada - Sistemática o estructurada - Participante - No participante - Individual	- Fichas de observación - Laptop - Internet - Navegador web
La Observación Indirecta: - Revisión de documentos - Consulta a base de datos y repositorios	- Laptop - Internet - Navegador web

3.5.2 Investigación Experimental

La técnicas e instrumentos se detallan en la Tabla 11.

Tabla 11

Técnicas e instrumentos de investigación experimental

Técnicas	Instrumentos
- Ejecución de experimentos - Utilización de laboratorio - Seguimiento de implementación de Arquitectura de Enrutamiento - Seguimiento de comportamiento de - redirecciones - Uso de grupos experimentales y de control - Revisión de códigos de estado de respuesta HTTP - Revisión de dominios expuestos en navegación web - Revisión de certificados digitales - Revisión de logs	- Hojas estructuradas - Fichas de Benchmarking - Laptop - Internet - Microsoft Edge DevTools - Mozilla Firefox Private Browsing - Digicert SSL Certificate Checker - Azure Portal - Azure Log Analytics - Kusto Query Language (KQL)

3.5.3 Investigación Documental

La técnicas e instrumentos se detallan en la Tabla 12.

Tabla 12

Técnicas e instrumentos de investigación documental

Técnicas	Instrumentos
Revisión de: - Libros - Revistas - Tesis - Periódicos - Documentos - Actas - Boletines - Fotografías - Equipos de cómputo - Internet	- PC - Memoria USB - Disco externo HDD - Libreta de apuntes - Laptop - Smartphone - Router - Access Point - Windows 10 - Microsoft Office 365 - Azure Portal - Azure Log Analytics - Google Chrome - Microsoft Edge - Mozilla Firefox - Mendeley - Bizagi - Microsoft Teams - Microsoft Project - Microsoft Authenticator - Google Translate - Sci-Hub - Adobe Acrobat - Minitab - Trello - Google Calendar - Samsung Calendar - Google Keep - Samsung Notes

3.5.4 Confiabilidad, validez y objetividad de instrumentos

La presente investigación utiliza como instrumentos a aplicaciones web que se ejecutan en un navegador web, al tratarse de software se garantiza la objetividad. La confiablidad y validez de los instrumentos de esta investigación se garantiza a través de la selección por juicio

de experto y la estandarización de instrumentos, ya que son instrumentos desarrollados por entidades de tecnología acreditadas y ampliamente influyentes en el contexto de esta investigación, como lo son Microsoft, Mozilla Foundation y DigiCert. Por tal motivo no es necesario revalidarlos, no aplica para la presente investigación. La Tabla 13 detalla los instrumentos y técnicas para la medición de los indicadores de la presente investigación.

Tabla 13

Detalle de instrumentos y técnicas para la medición de indicadores

Indicador	Instrumento	Técnica
Tiempo de respuesta	- Microsoft Edge DevTools - Azure Log Analytics	- Revisión de tiempos de respuesta - Revisión de logs
Número de dominios redirigidos	- Microsoft Edge DevTools - Azure Log Analytics	- Revisión de códigos de estado de respuesta HTTP - Revisión de logs
Número de dominios expuestos hacia el navegador web del cliente	- Mozilla Firefox Private Browsing - Azure Log Analytics	- Revisión de dominios expuestos en navegación web - Revisión de logs
Número de dominios con redirección de HTTP a HTTPS	- Digicert SSL Certificate Checker - Microsoft Edge DevTools - Azure Log Analytics	- Revisión de certificados digitales - Revisión de códigos de estado de respuesta HTTP - Revisión de logs
Número de soluciones de seguridad WAF	- Azure Log Analytics	- Revisión de logs

3.6 Procedimientos

La presente investigación considera el siguiente procedimiento:

1. Se realizará un diagnóstico de los componentes y configuraciones actuales en el acceso vía web al servicio digital de Cambix.
2. Se definirá un plan de trabajo con las actividades para la creación de la Arquitectura de Enrutamiento en Azure Front Door.
3. Se realizará una validación previa de las actividades en un ambiente de pruebas, antes de su implementación en el ambiente de producción.
4. Se realizará la creación de componentes y configuraciones en Azure Front Door para la implementación de la Arquitectura de Enrutamiento.
5. Se realizará un monitoreo y comprobación del acceso al servicio a través del dominio redirigido https://cambix.com.pe/ mediante un navegador web.

3.7 Análisis de datos

Etapas del Análisis de Resultados

A continuación, se detallan las 7 fases o etapas para el análisis de resultados. La Figura 9 muestra las fases en secuencia.

Fase 1.- Seleccionar un software apropiado para analizar los datos.

Fase 2.- Ejecutar el programa.

Fase 3.- Explorar los datos: a) Analizar descriptivamente los datos por variable; b) Visualizar los datos por variable.

Fase 4.- Se lleva a cabo el análisis estadístico descriptivo de cada indicador.

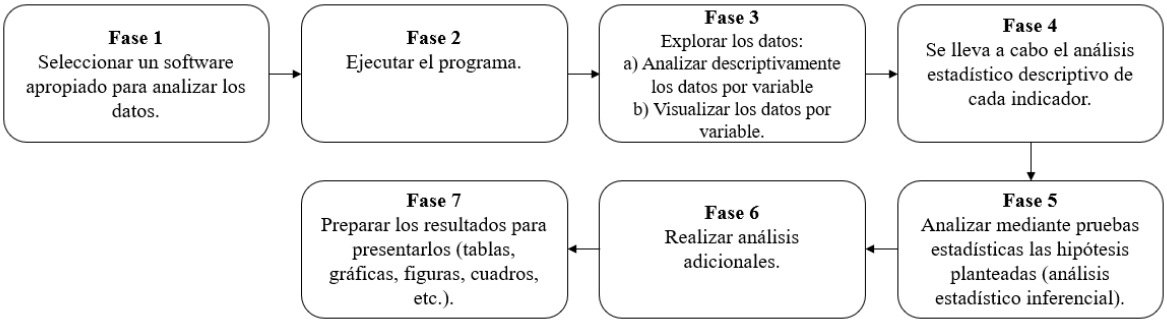
Fase 5.- Analizar mediante pruebas estadísticas las hipótesis planteadas (análisis estadístico inferencial).

Fase 6.- Realizar análisis adicionales.

Fase 7.- Preparar los resultados para presentarlos (tablas, gráficas, figuras, cuadros, etc.).

Figura 9

Etapas del análisis de resultados



Nota: Adaptado de *Proceso para efectuar análisis estadístico* (p. 312), por Hernández y Mendoza, 2018, McGraw-Hill.

3.8 Consideraciones éticas

En este proyecto de investigación se tendrán las siguientes consideraciones éticas:

- Se respetará los derechos de autor de las fuentes utilizadas, toda fuente de información será citada.
- La información recolectada es veraz.
- Toda fuente de información será referenciada al final de la investigación.
- Se cuidará la privacidad de las personas que formen parte del grupo muestral.
- Preservación de la confidencialidad.
- Revelación de información.

- **Código de Núremberg**
  - Consentimiento voluntario.

  - Beneficio de la sociedad.
  - Resultados precios justificaran la realización del experimento.
  - Evitar todo sufrimiento físico y mental innecesario.
  - No debe realizarse ningún experimento cuando exista una razón a priori que lleve a creer el que pueda sobrevenir muerte o daño que lleve a una incapacitación.
  - Riesgo vs Beneficio.
  - Preparaciones propias para proteger al sujeto.
  - Personas científicamente cualificadas.
  - Libertad de interrupción.
  - Estar preparado para terminarlo en cualquier fase.
- **Declaración de Helsinki**
- **Informe Belmont**
- **Principios Éticos Básicos**
  - Respeto a las personas.
  - Beneficencia.
  - Justicia.
- **Aplicaciones**
  - Consentimiento informado: Información, Compresión, Voluntariedad.
  - Valoración de Riesgo Beneficio.
  - Selección de sujetos.
- **Pautas de la CIOMS**
  - El respeto por las personas.
  - La beneficencia.
  - La justicia.

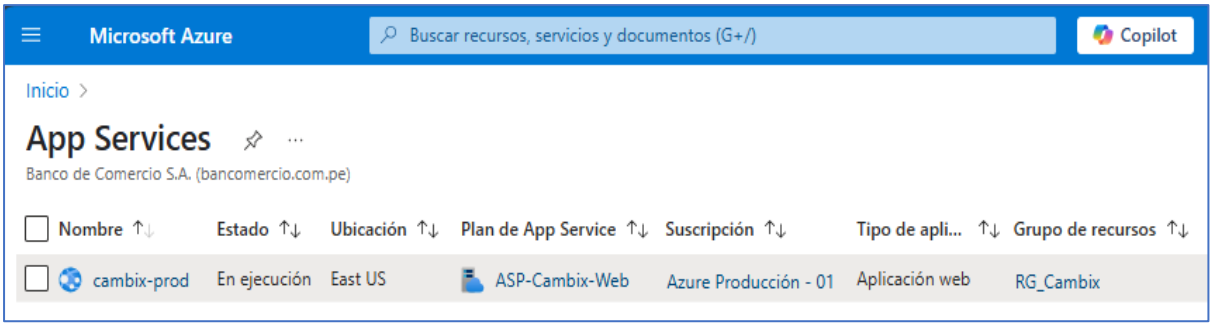
IV. RESULTADOS

4.1 Diagnóstico de componentes y configuraciones

Se dispone de un recurso de App Service nombrado cambix-prod, allí se hospeda y ejecuta el servicio de Cambix, La Figura 10 presenta este recurso.

Figura 10

Recurso cambix-prod del servicio de Cambix



Nota: Vista del recurso desde la consola de Azure Portal.

4.2 Plan de trabajo

Se adjunta Anexo C con el plan de trabajo definido para las actividades de creación de la Arquitectura de Enrutamiento en Azure Front Door.

4.3 Validación previa a producción

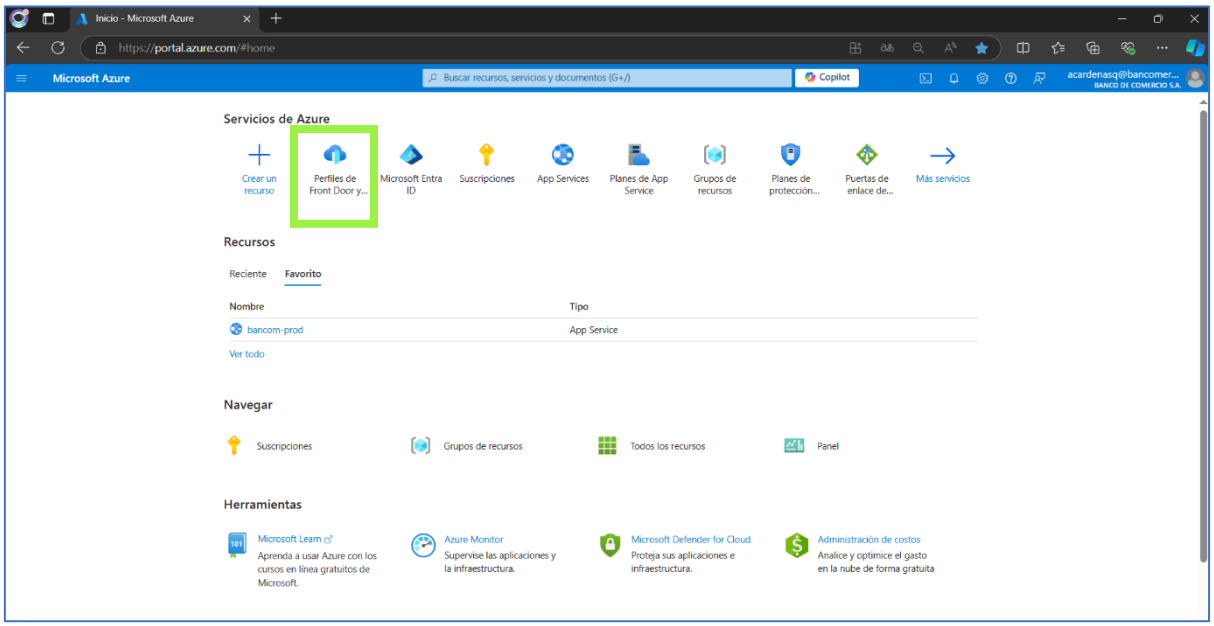
Se adjunta Anexo D con la implementación exitosa de la solución en un ambiente de pruebas (calidad), como validación previa a su implementación en el ambiente de producción. Esta validación en calidad es fundamental para asegurar que la solución técnica cumple con los requisitos funcionales antes de ser implementada en el ambiente productivo de cara a los clientes, minimizando riesgos y errores.

4.4 Creación de componentes y configuraciones en la implementación de la solución

Se describe el paso a paso para la implementación de la solución. El punto inicial es el acceso a la consola de administración de recursos de Azure Portal, suscripción de Producción del Banco, como se aprecia en la Figura 11.

Figura 11

Vista de la consola de administración de recursos de Azure Portal



Nota: Vista del punto inicial tras el inicio de sesión en Microsoft Azure, desde allí se dispone del acceso a cada servicio de Microsoft Azure en específico.

Desde Azure Portal se accede al servicio de Azure Front Door (Perfiles de Front Door y CDN), como se aprecia en las Figura 12 y Figura 13.

Figura 12

Vista de acceso al servicio de Azure Front Door

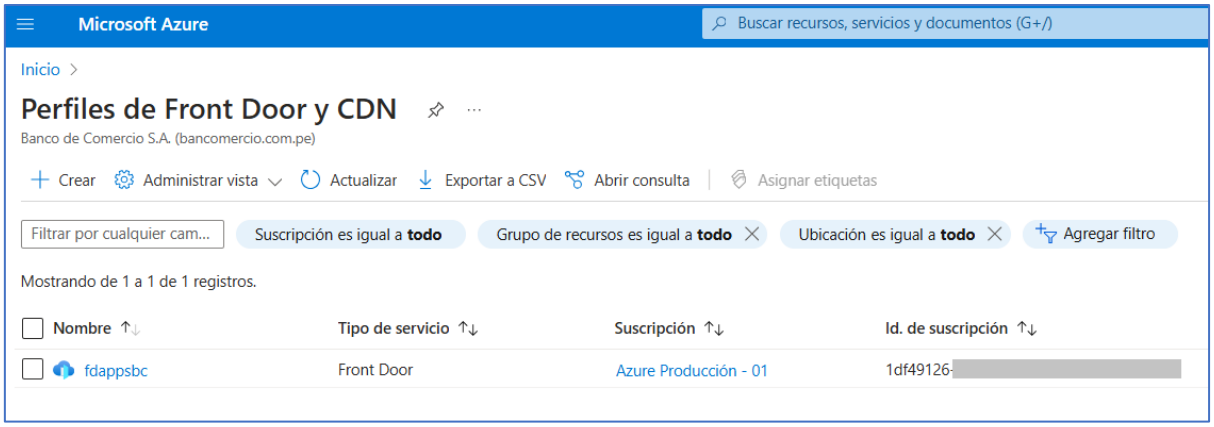
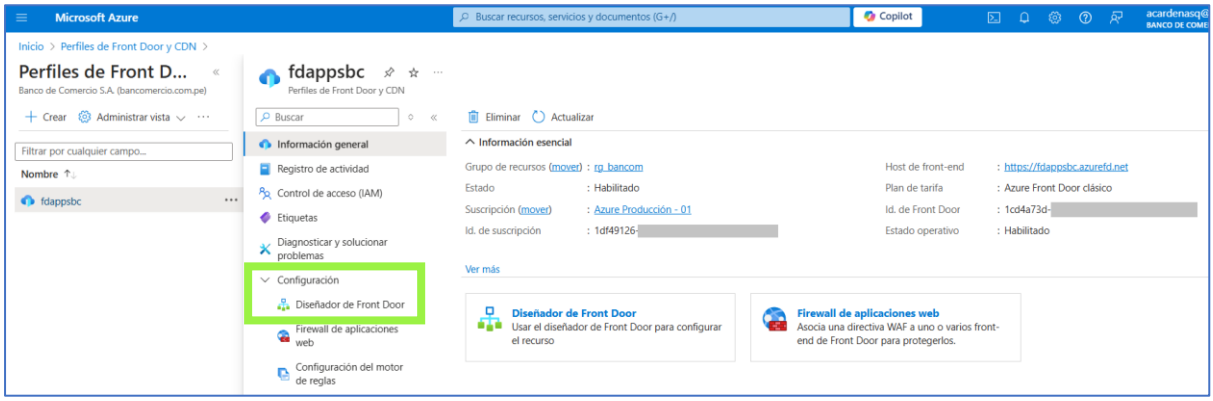


Figura 13

Información general de la instancia fdappsbc en Azure Front Door

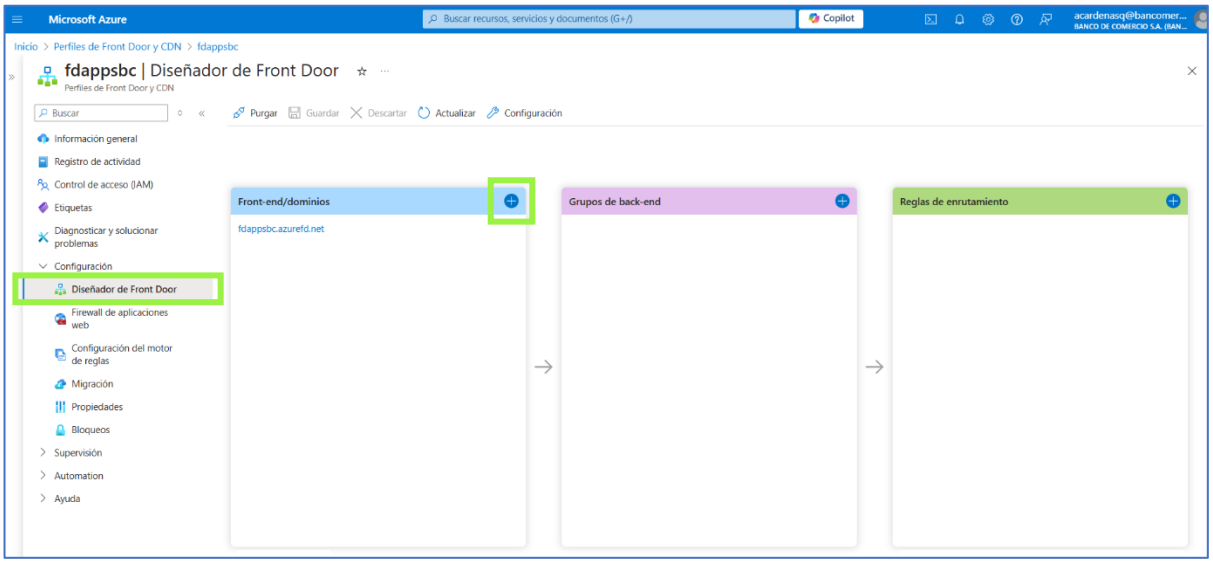


Nota: Desde aquí se dispone del acceso a la sección Diseñador de Front Door que permite la creación y configuración de componentes.

La Figura 14 muestra la vista inicial de la sección Diseñador de Front Door, aquí se crean y configuran los front-end/dominios, los grupos de back-end y las reglas de enrutamiento.

Figura 14

Vista inicial del Diseñador de Front Door



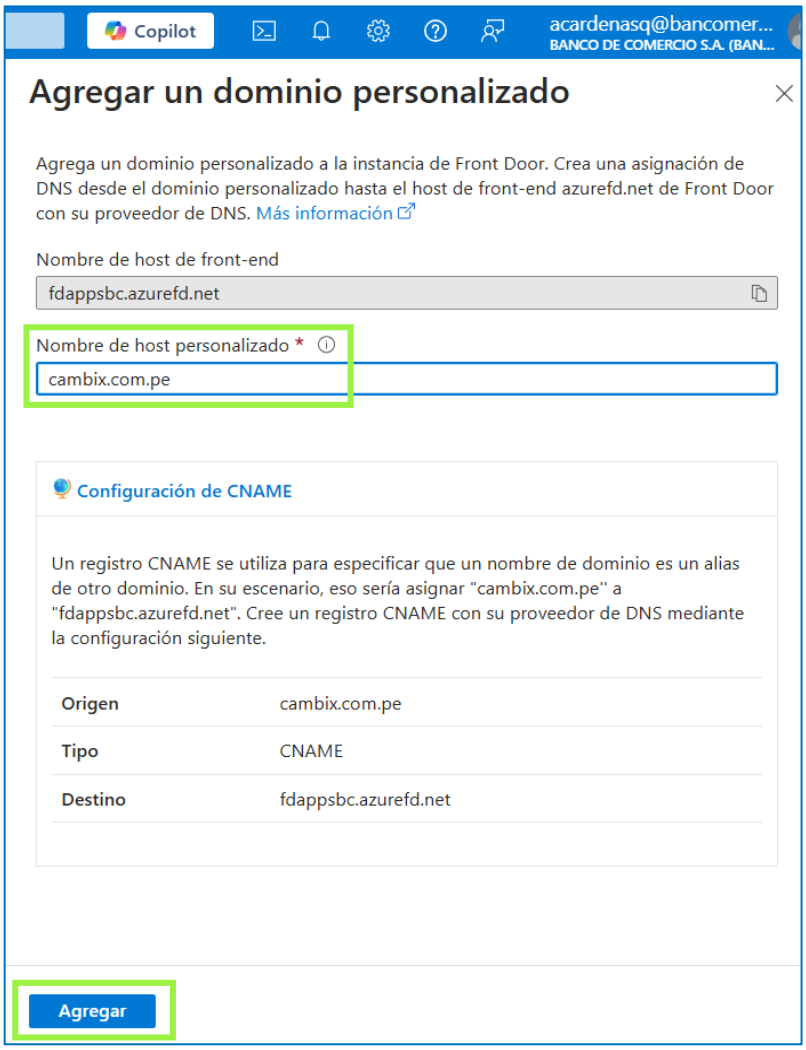
Nota: Los cuadros del Diseñador de Front Door están vacíos, pues aún no se tiene ninguna configuración para el servicio de Cambix. Se procede a pulsar el signo más (+) para iniciar la creación y configuración de cada componente.

4.4.1 Creación de front-ends

La Figura 15 y Figura 16 muestran la creación del front-end y registro DNS para el dominio principal del servicio de Cambix.

Figura 15

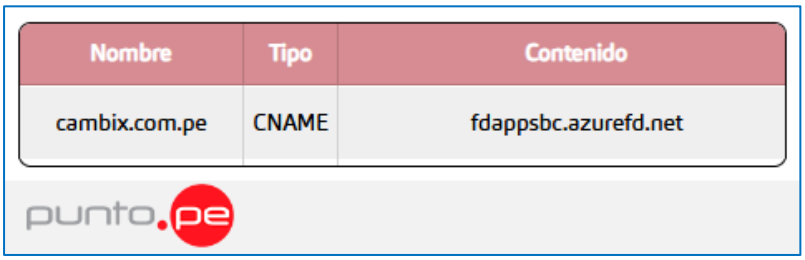
Creación de front-end para el dominio cambix.com.pe



Nota: Nombre de host personalizado es el nombre del dominio que se desea vincular al servicio de Front Door, esto permite crear un nuevo front-end para posteriormente configurar el enrutamiento del dominio.

Figura 16

Registro DNS en nic.pe para el dominio cambix.com.pe



Nota: Para vincular el dominio al servicio de Front Door se crea un registro DNS de tipo CNAME en la empresa registradora de dominios, en este caso NIC.PE (Punto Pe). Nótese además que este registro CNAME vincula el dominio cambix.com.pe a la instancia fdappsbc.azurefd.net en Front Door. Adaptado de Punto Pe. (s.f.).

Las posteriores Figuras 17, 18, 19, 20, 21 y 22 muestran la misma operación de creación del front-ends, pero para los dominios alternos, completando así la creación de front-ends para cada uno de los 4 dominios del servicio.

Figura 17

Creación de front-end para el dominio www.cambix.com.pe

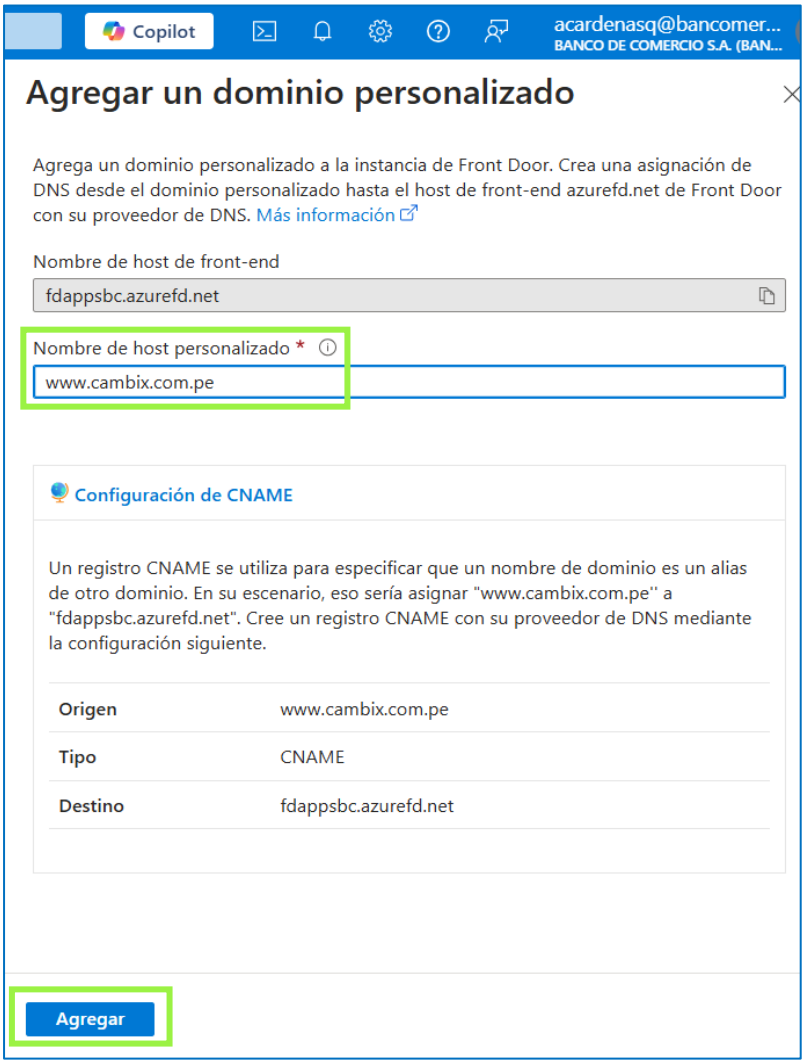
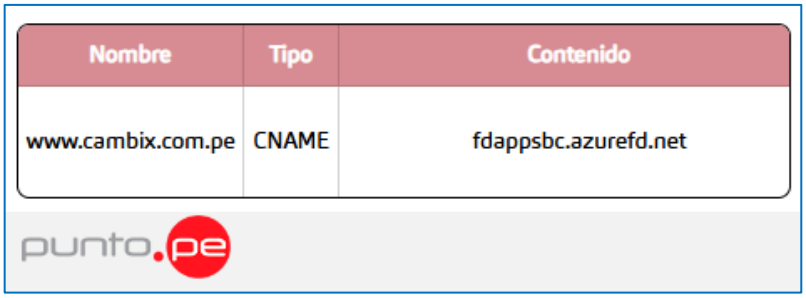


Figura 18

Registro DNS en nic.pe para el dominio www.cambix.com.pe



Nota: Adaptado de Punto Pe. (s.f.).

Figura 19

Creación de front-end para el dominio cambix.pe

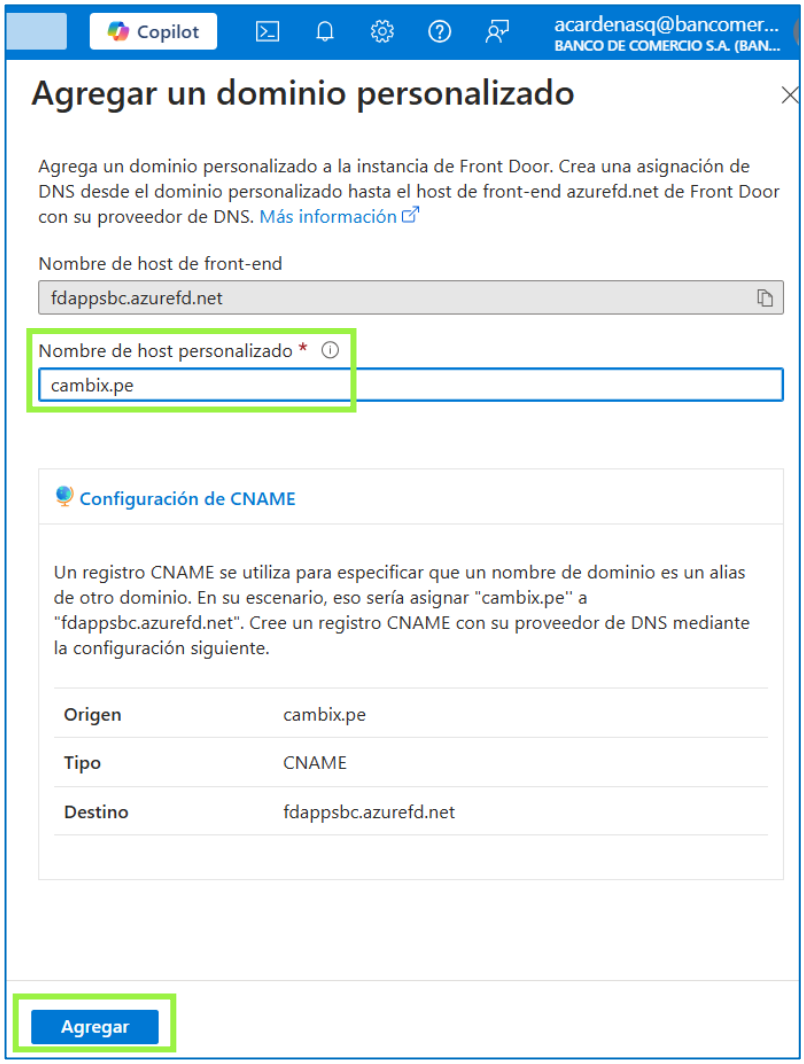
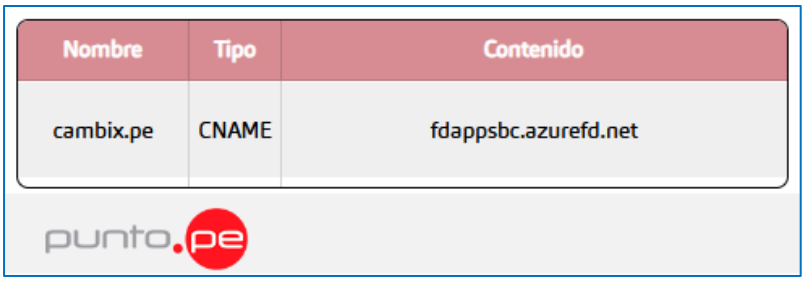


Figura 20

Registro DNS en nic.pe para el dominio cambix.pe



Nota: Adaptado de Punto Pe. (s.f.).

Figura 21

Creación de front-end para el dominio www.cambix.pe

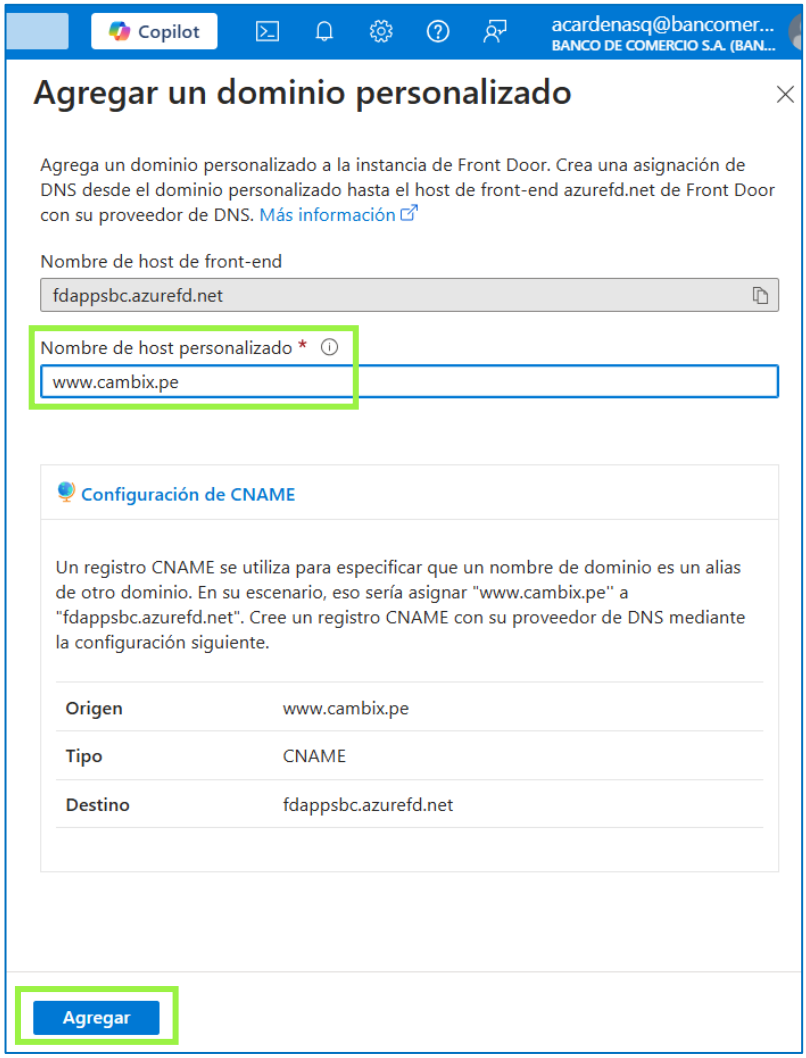


Figura 22

Registro DNS en nic.pe para el dominio www.cambix.pe

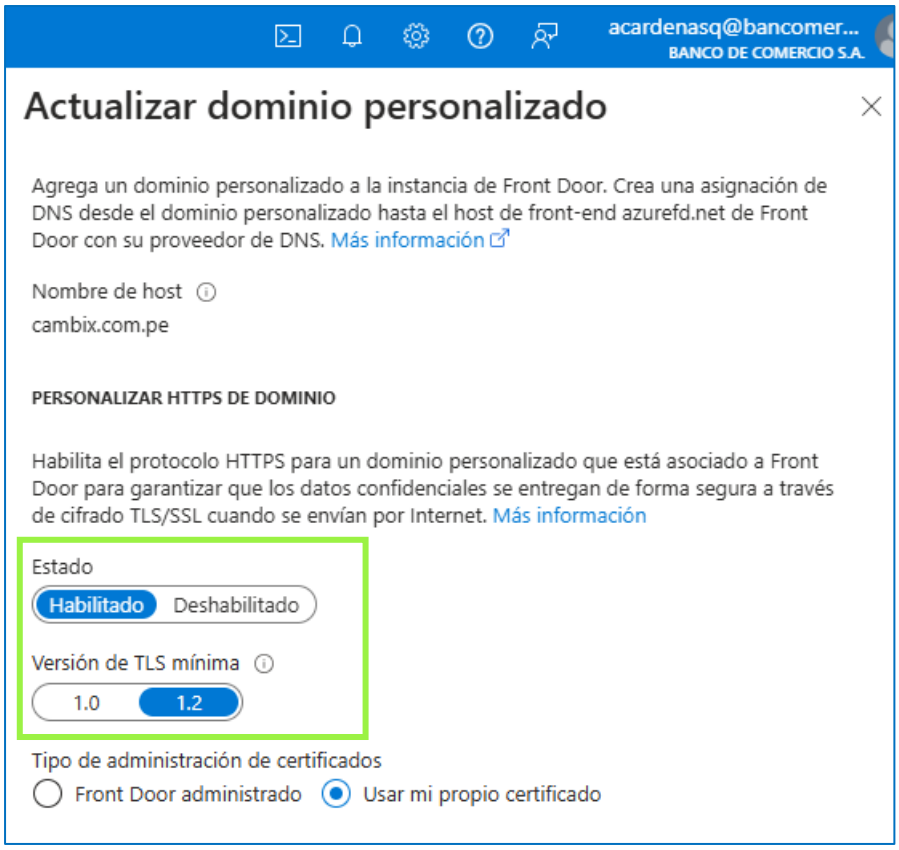
Nota: Adaptado de Punto Pe. (s.f.).

4.4.1.1 Configuración de front-end cambix.com.pe

La Figura 23, Figura 24 y Figura 25 muestran la configuración del front-end creado para el dominio principal del servicio de Cambix.

Figura 23

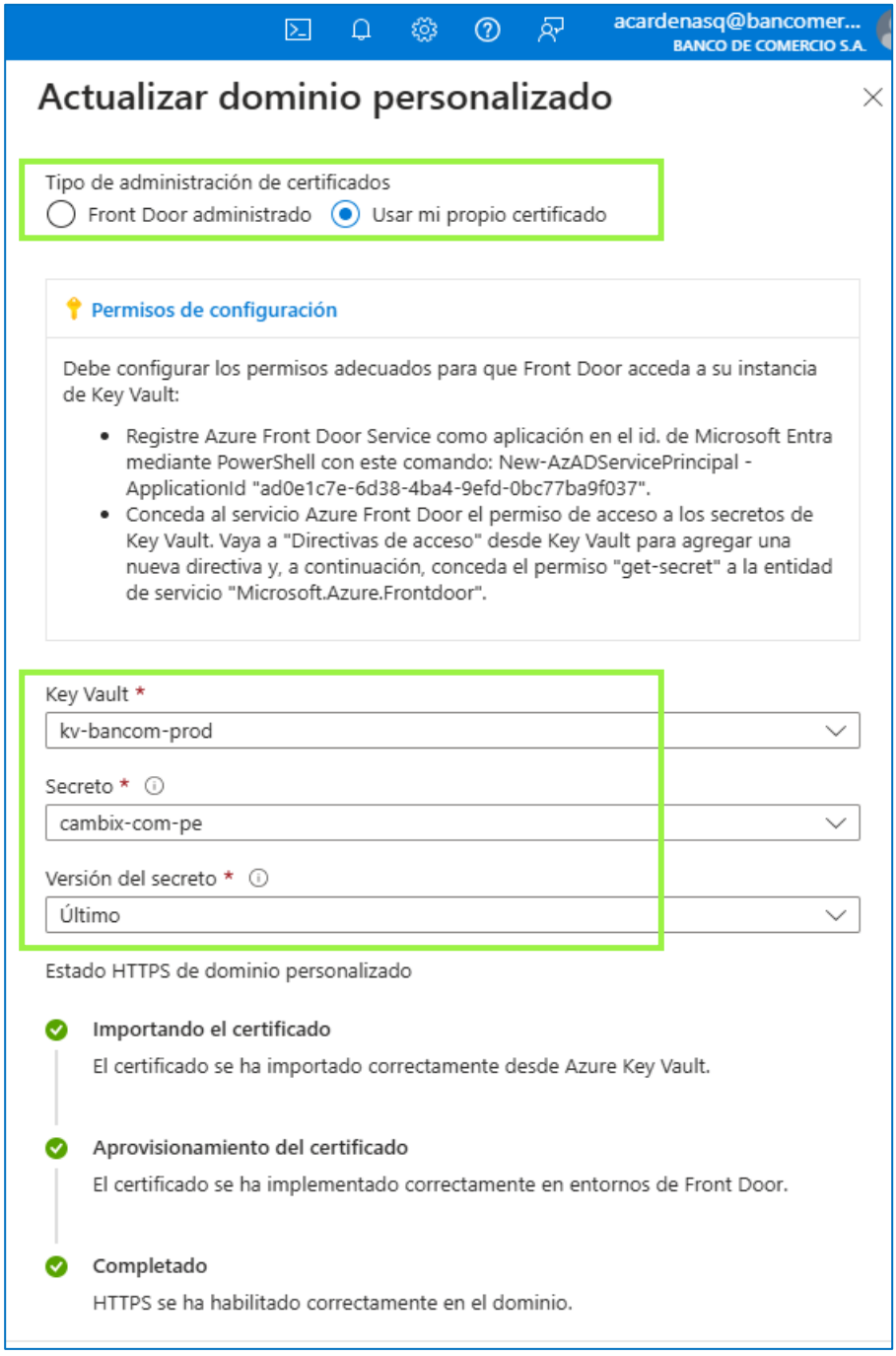
Configuración HTTPS en front-end del dominio cambix.com.pe



Nota: Esta configuración HTTPS permite habilitar un certificado digital al dominio para disponer de una conexión segura. Se recomienda la versión TLS 1.2 por ser la más segura disponible para el cifrado de la comunicación entre el cliente y el servidor.

Figura 24

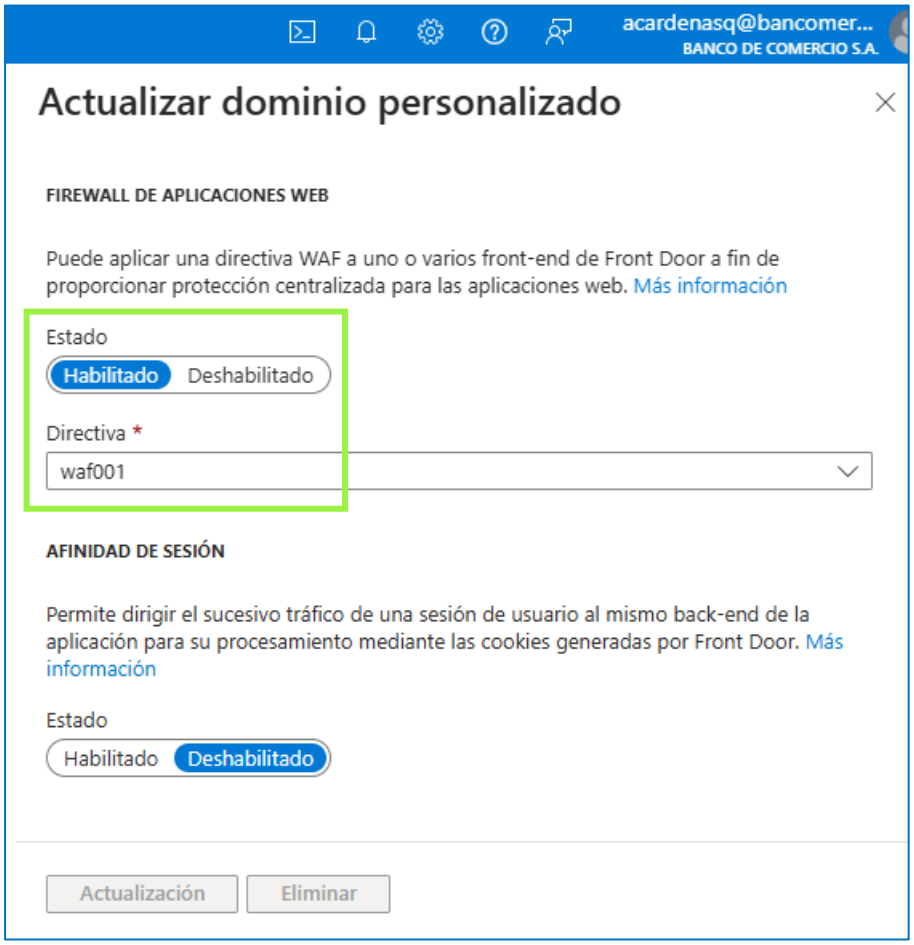
Configuración de certificado digital en front-end del dominio cambix.com.pe



Nota: Usar mi propio certificado indica que se utilizará un certificado adquirido fuera de Azure, en este caso adquirido a través del proveedor DigiCert. Luego, estos certificados se cargan y almacenan en Azure en formato PFX mediante el servicio de Azure Key Vault. La última versión del secreto permite utilizar el certificado actual en base a la fecha de carga más reciente.

Figura 25

Configuración de WAF en front-end del dominio cambix.com.pe



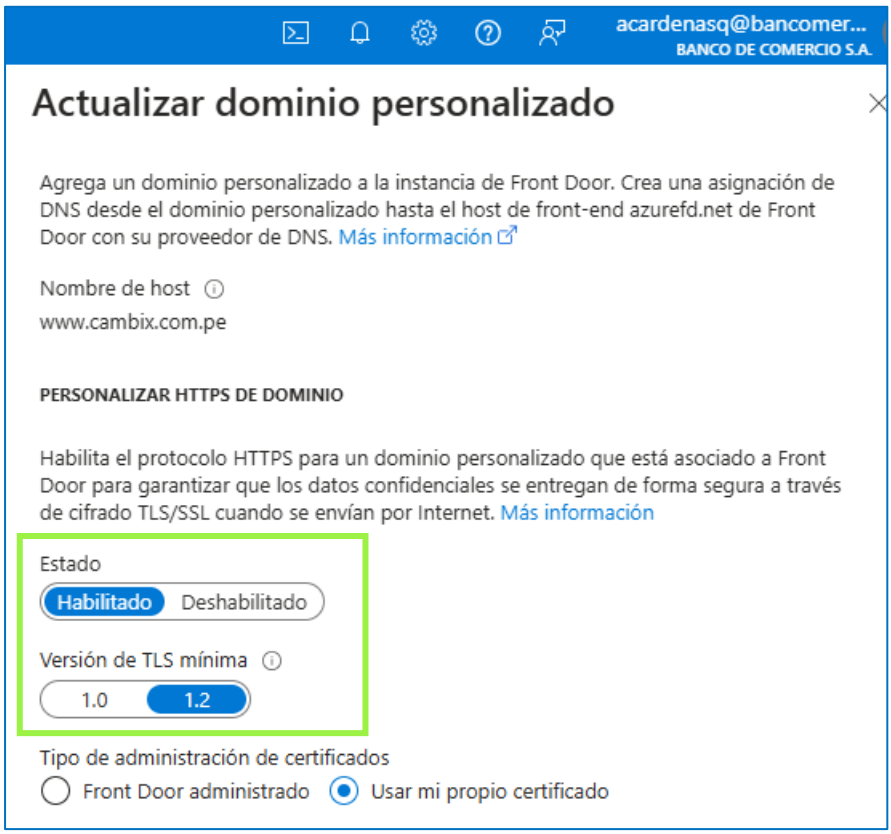
Nota: Esta configuración permite habilitar una directiva WAF en el front-end creado. La directiva waf001 se crea y administra mediante el servicio de Azure WAF. La afinidad de sesión permite que el tráfico de la sesión de un usuario se atienda siempre por un mismo App Service, esto es útil cuando se tienen dos o más back-ends, pero en esta implementación se tiene un solo back-end y no es necesario habilitarla.

4.4.1.2 Configuración de front-end www.cambix.com.pe

La Figura 26, Figura 27 y Figura 28 muestran la configuración del front-end para el dominio alterno del servicio de Cambix.

Figura 26

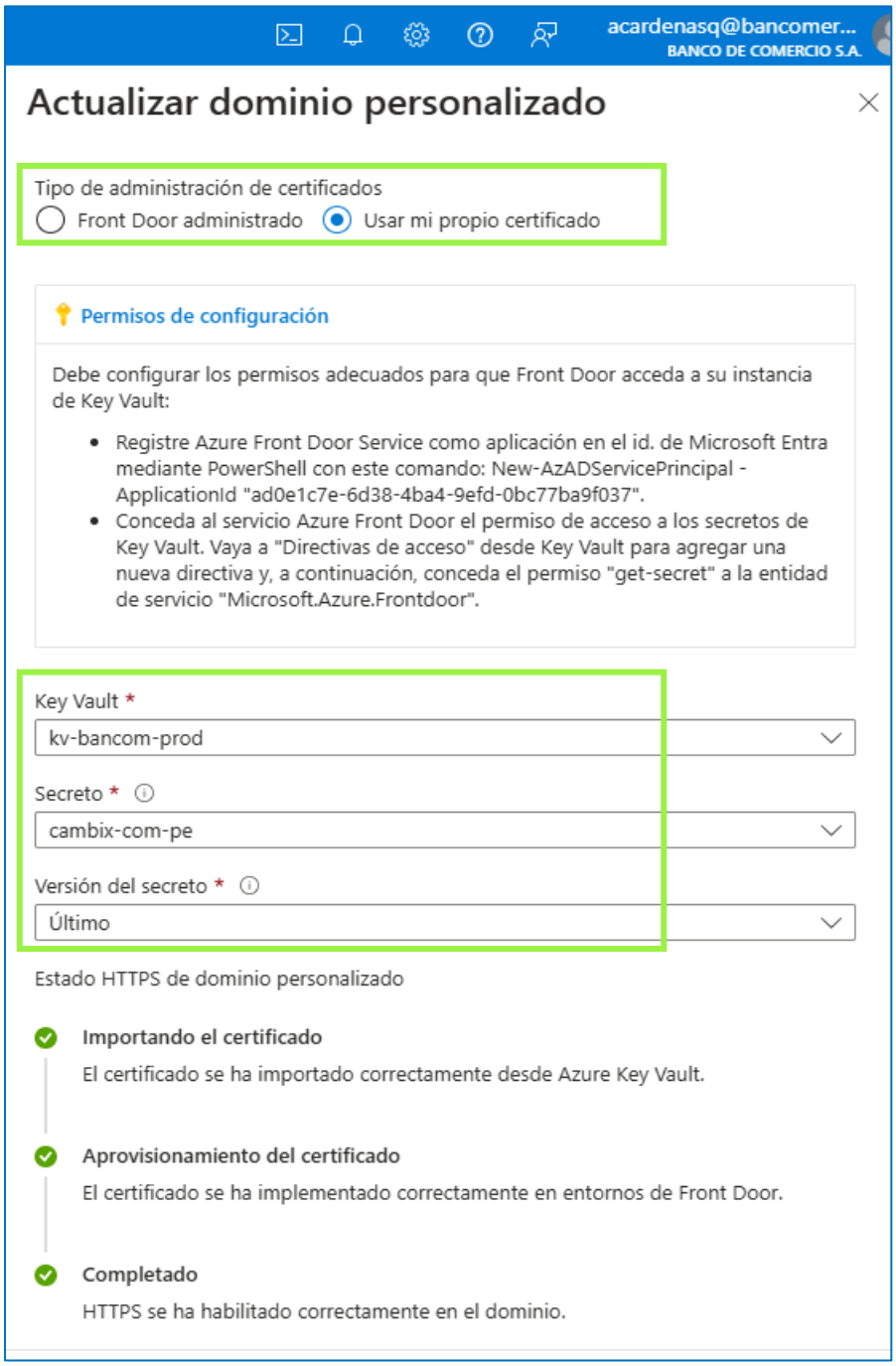
Configuración HTTPS en front-end del dominio www.cambix.com.pe



Nota: Esta configuración HTTPS permite habilitar un certificado digital al dominio para disponer de una conexión segura. Se recomienda la versión TLS 1.2 por ser la más segura disponible para el cifrado de la comunicación entre el cliente y el servidor.

Figura 27

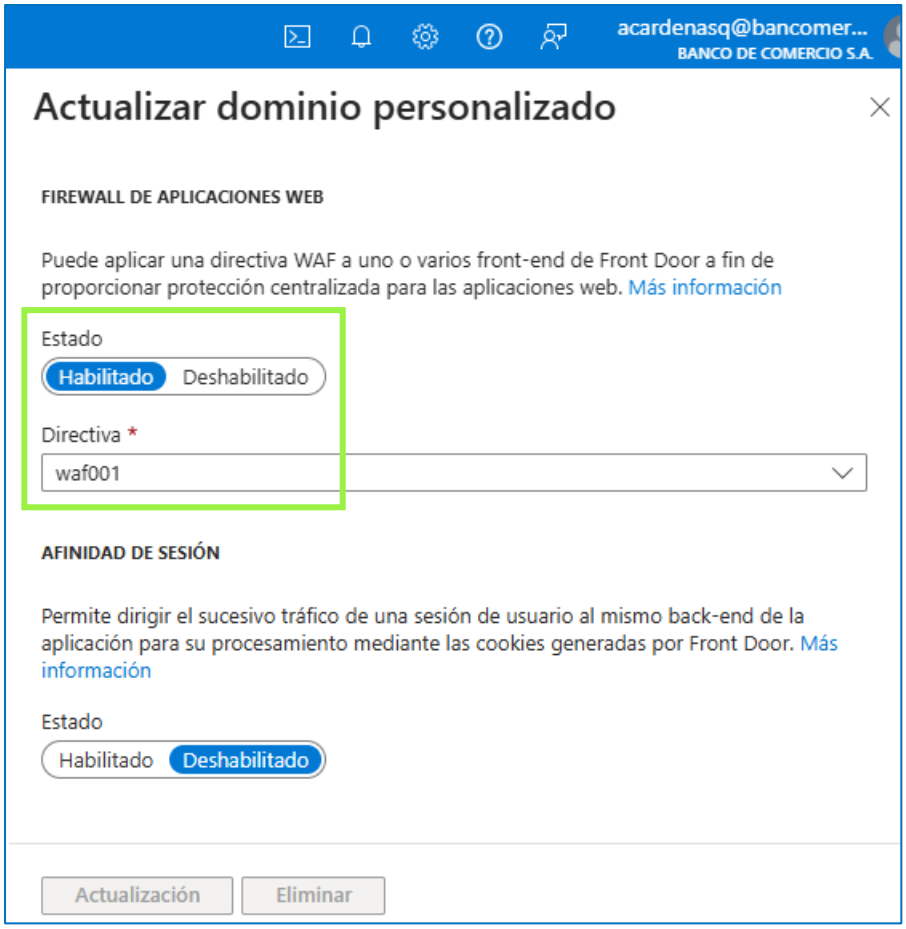
Configuración de certificado digital en front-end del dominio www.cambix.com.pe



Nota: Usar mi propio certificado indica que se utilizará un certificado adquirido fuera de Azure, en este caso adquirido a través del proveedor DigiCert. Luego, estos certificados se cargan y almacenan en Azure en formato PFX mediante el servicio de Azure Key Vault. La última versión del secreto permite utilizar el certificado actual en base a la fecha de carga más reciente.

Figura 28

Configuración de WAF en front-end del dominio www.cambix.com.pe



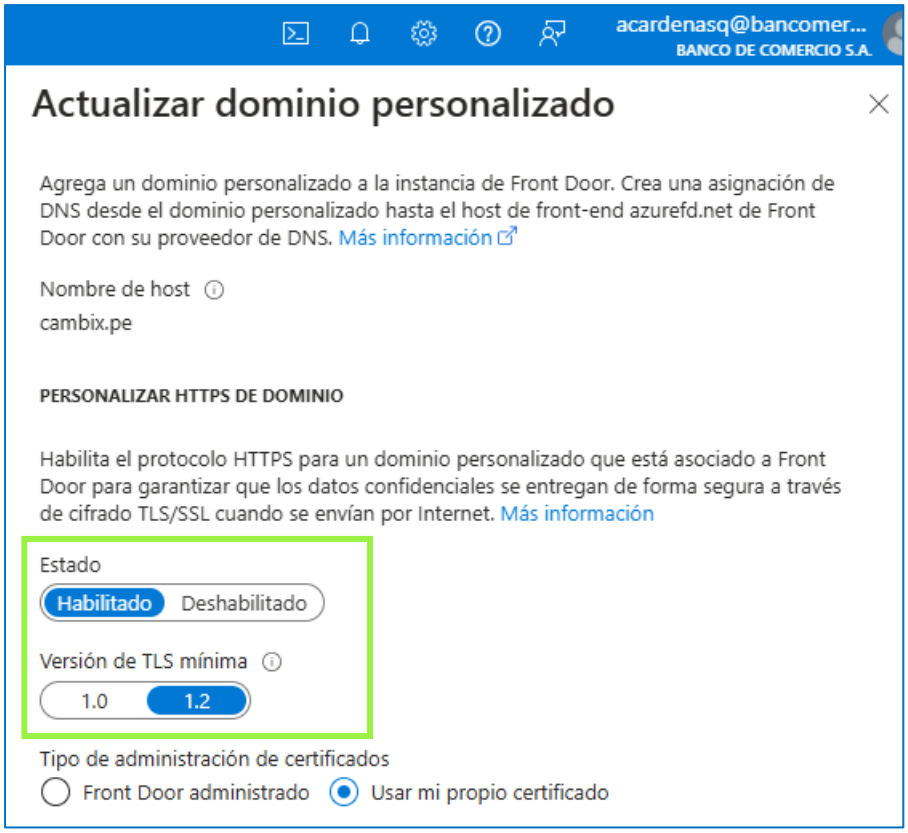
Nota: Esta configuración permite habilitar una directiva WAF en el front-end creado. La directiva waf001 se crea y administra mediante el servicio de Azure WAF. La afinidad de sesión permite que el tráfico de la sesión de un usuario se atienda siempre por un mismo App Service, esto es útil cuando se tienen dos o más back-ends, pero en esta implementación se tiene un solo back-end y no es necesario habilitarla.

4.4.1.3 Configuración de front-end cambix.pe

La Figura 29, Figura 30 y Figura 31 muestran la configuración del front-end para el dominio alterno del servicio de Cambix.

Figura 29

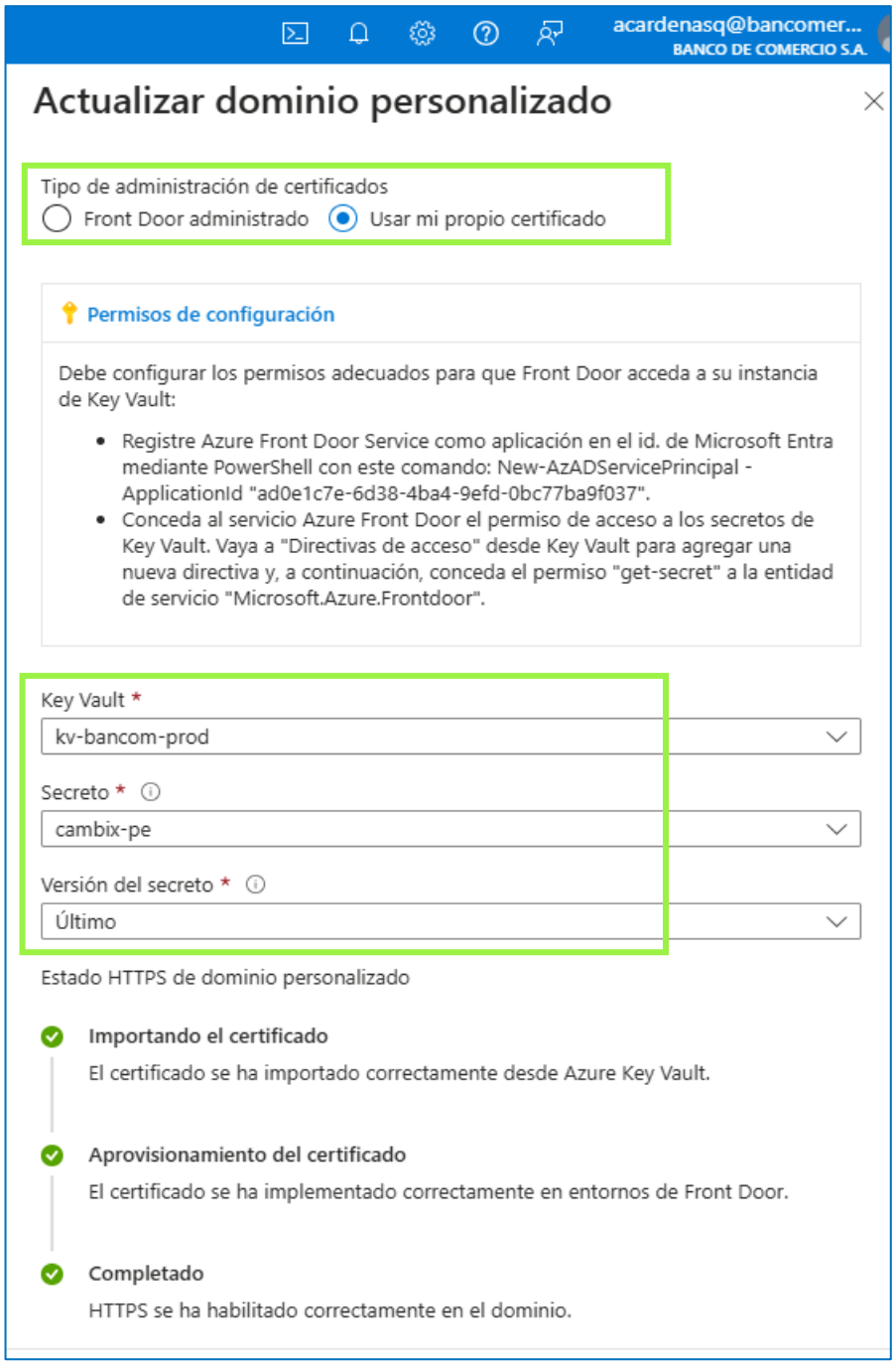
Configuración HTTPS en front-end del dominio cambix.pe



Nota: Esta configuración HTTPS permite habilitar un certificado digital al dominio para disponer de una conexión segura. Se recomienda la versión TLS 1.2 por ser la más segura disponible para el cifrado de la comunicación entre el cliente y el servidor.

Figura 30

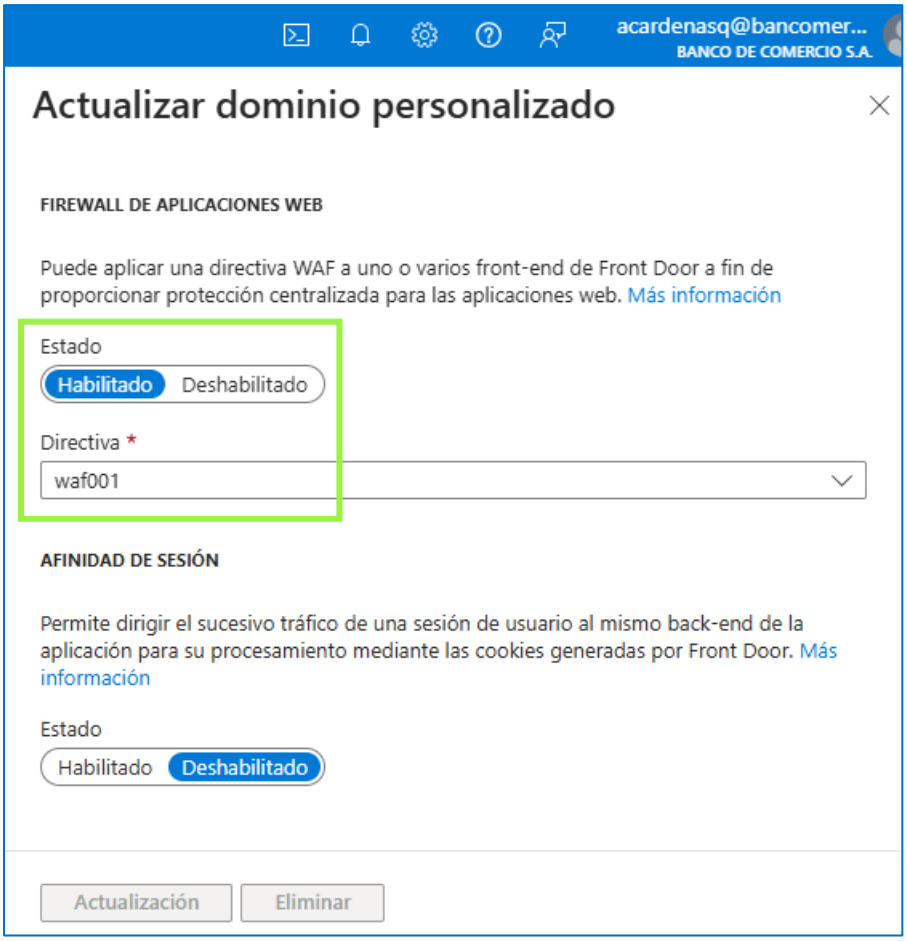
Configuración de certificado digital en front-end del dominio cambix.pe



Nota: Usar mi propio certificado indica que se utilizará un certificado adquirido fuera de Azure, en este caso adquirido a través del proveedor DigiCert. Luego, estos certificados se cargan y almacenan en Azure en formato PFX mediante el servicio de Azure Key Vault. La última versión del secreto permite utilizar el certificado actual en base a la fecha de carga más reciente.

Figura 31

Configuración de WAF en front-end del dominio cambix.pe



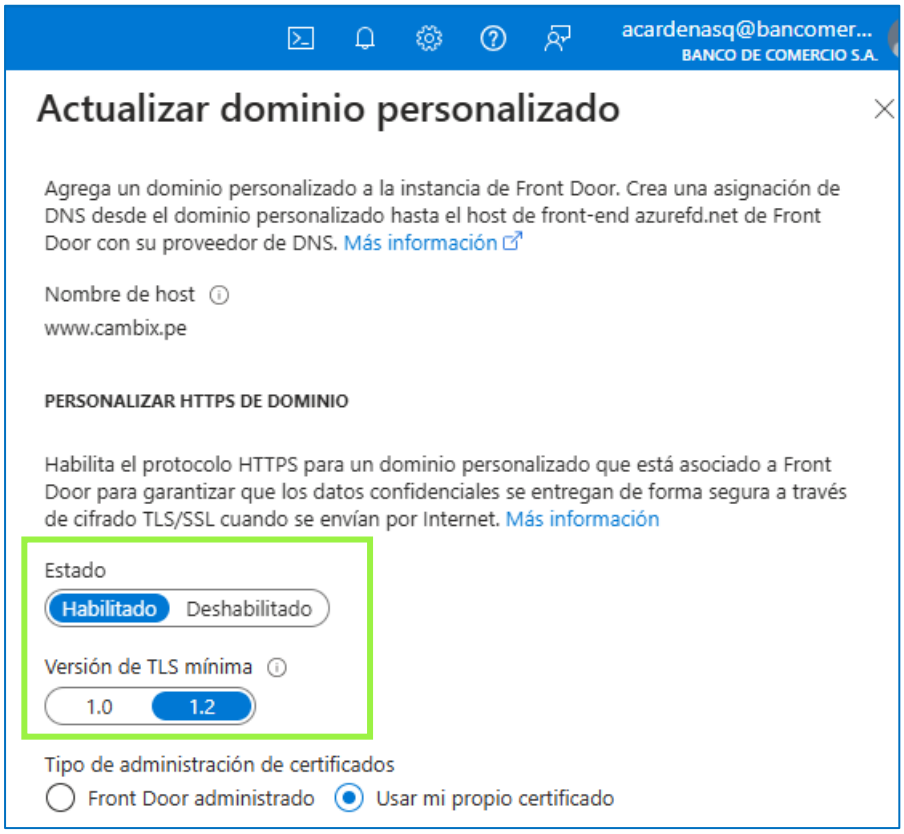
Nota: Esta configuración permite habilitar una directiva WAF en el front-end creado. La directiva waf001 se crea y administra mediante el servicio de Azure WAF. La afinidad de sesión permite que el tráfico de la sesión de un usuario se atienda siempre por un mismo App Service, esto es útil cuando se tienen dos o más back-ends, pero en esta implementación se tiene un solo back-end y no es necesario habilitarla.

4.4.1.4 Configuración de front-end www.cambix.pe

La Figura 32, Figura 33 y Figura 34 muestran la configuración del front-end para el dominio alterno del servicio de Cambix.

Figura 32

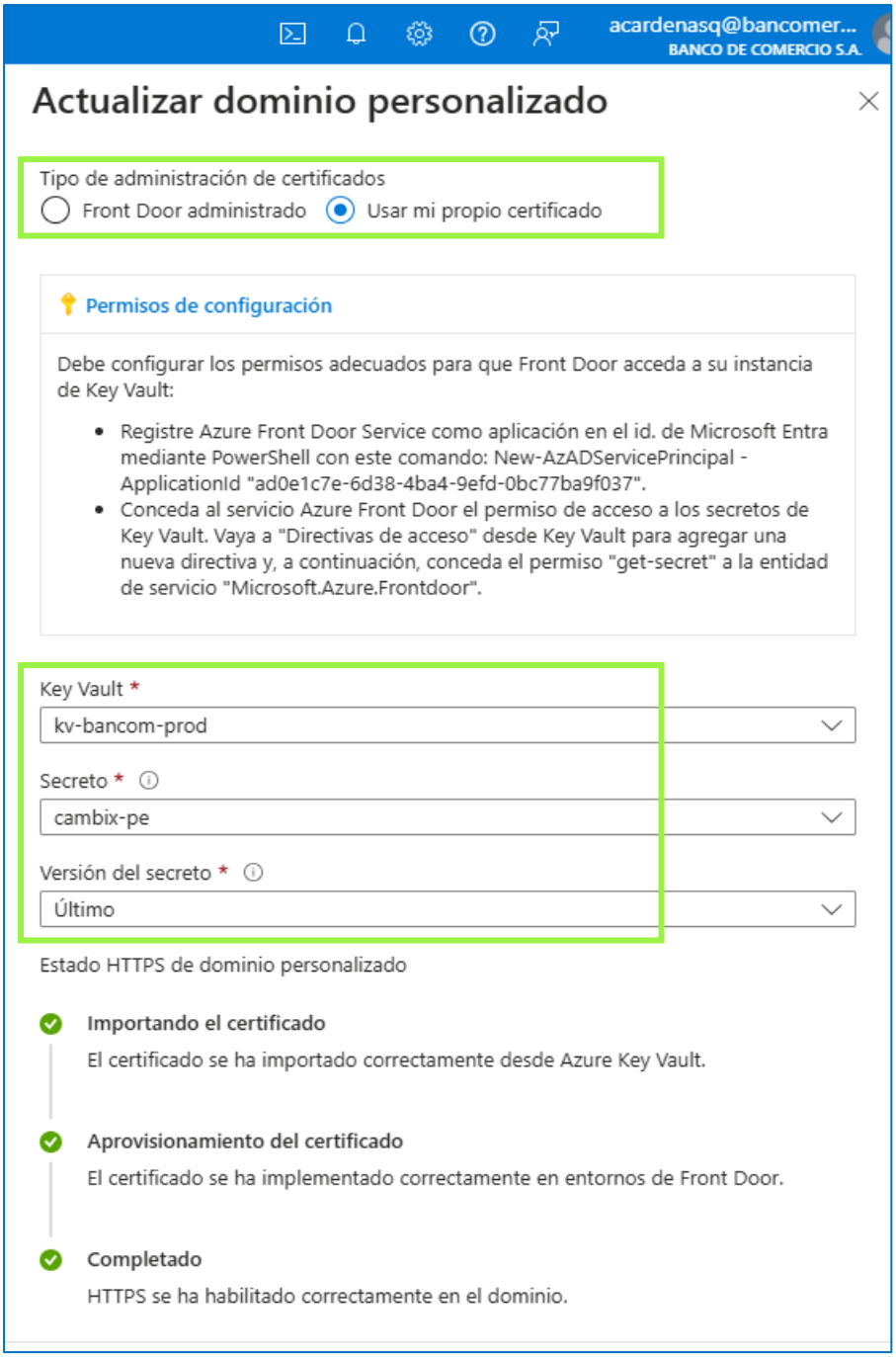
Configuración HTTPS en front-end del dominio www.cambix.pe



Nota: Esta configuración HTTPS permite habilitar un certificado digital al dominio para disponer de una conexión segura. Se recomienda la versión TLS 1.2 por ser la más segura disponible para el cifrado de la comunicación entre el cliente y el servidor.

Figura 33

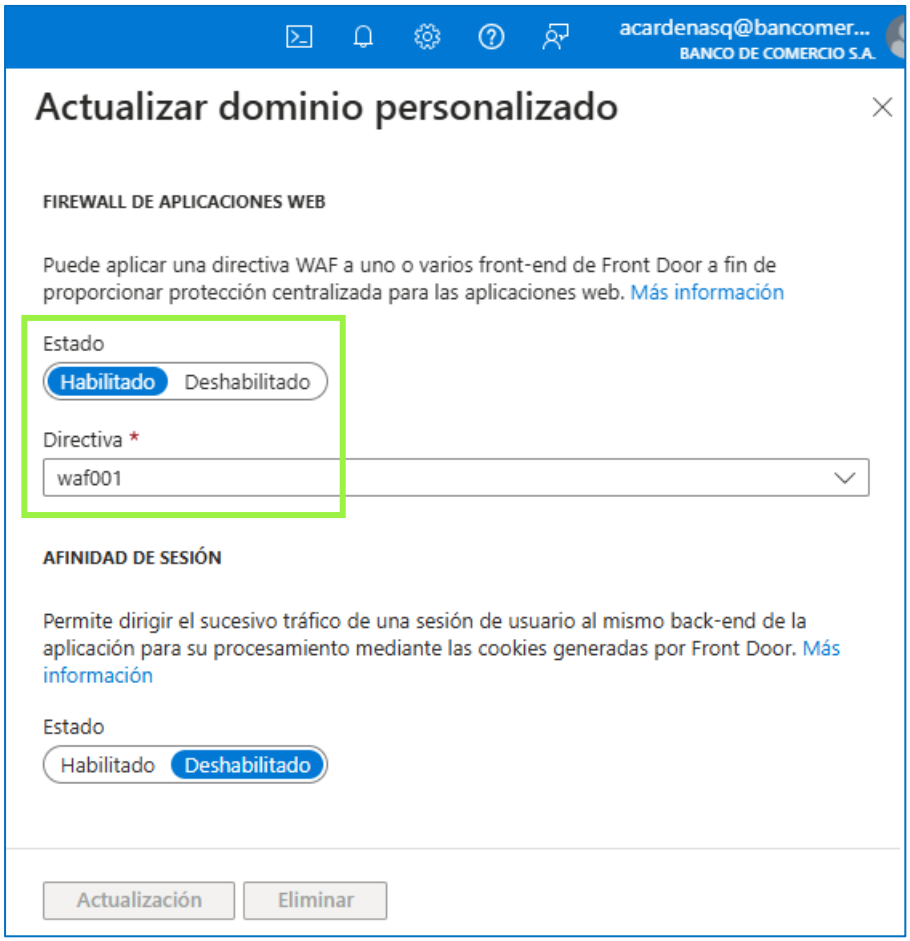
Configuración de certificado digital en front-end del dominio www.cambix.pe



Nota: Usar mi propio certificado indica que se utilizará un certificado adquirido fuera de Azure, en este caso adquirido a través del proveedor DigiCert. Luego, estos certificados se cargan y almacenan en Azure en formato PFX mediante el servicio de Azure Key Vault. La última versión del secreto permite utilizar el certificado actual en base a la fecha de carga más reciente.

Figura 34

Configuración de WAF en front-end del dominio www.cambix.pe



Nota: Esta configuración permite habilitar una directiva WAF en el front-end creado. La directiva waf001 se crea y administra mediante el servicio de Azure WAF. La afinidad de sesión permite que el tráfico de la sesión de un usuario se atienda siempre por un mismo App Service, esto es útil cuando se tienen dos o más back-ends, pero en esta implementación se tiene un solo back-end y no es necesario habilitarla.

4.4.1.5 Configuración de directiva WAF

Directiva waf001 destinada a la protección del servicio de Cambix.

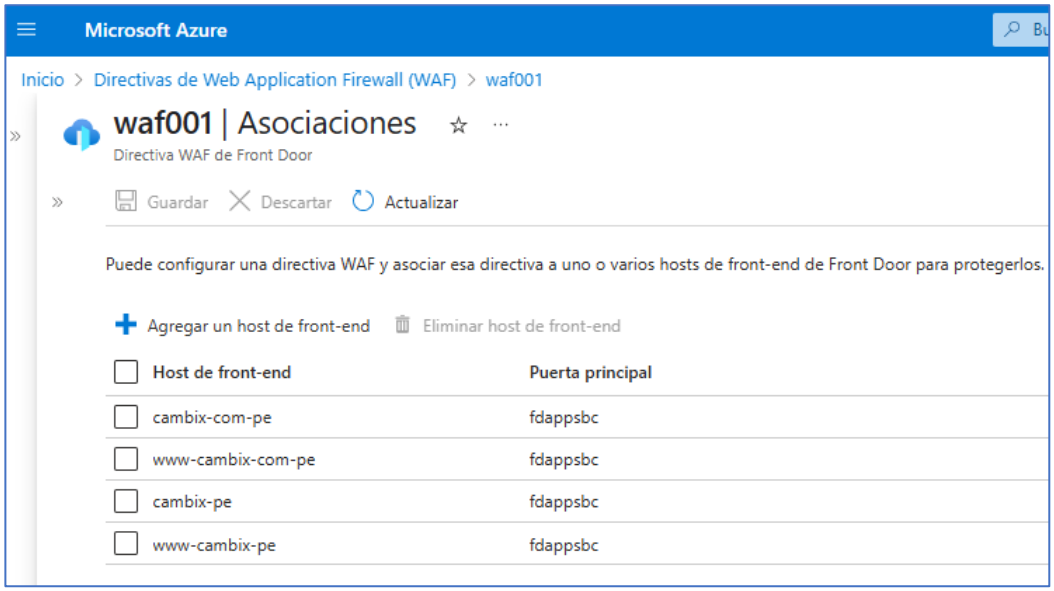
Figura 35

Directiva waf001 para la habilitación de solución de seguridad WAF

Nota: Vista del recurso desde la consola de Azure Portal.

Figura 36

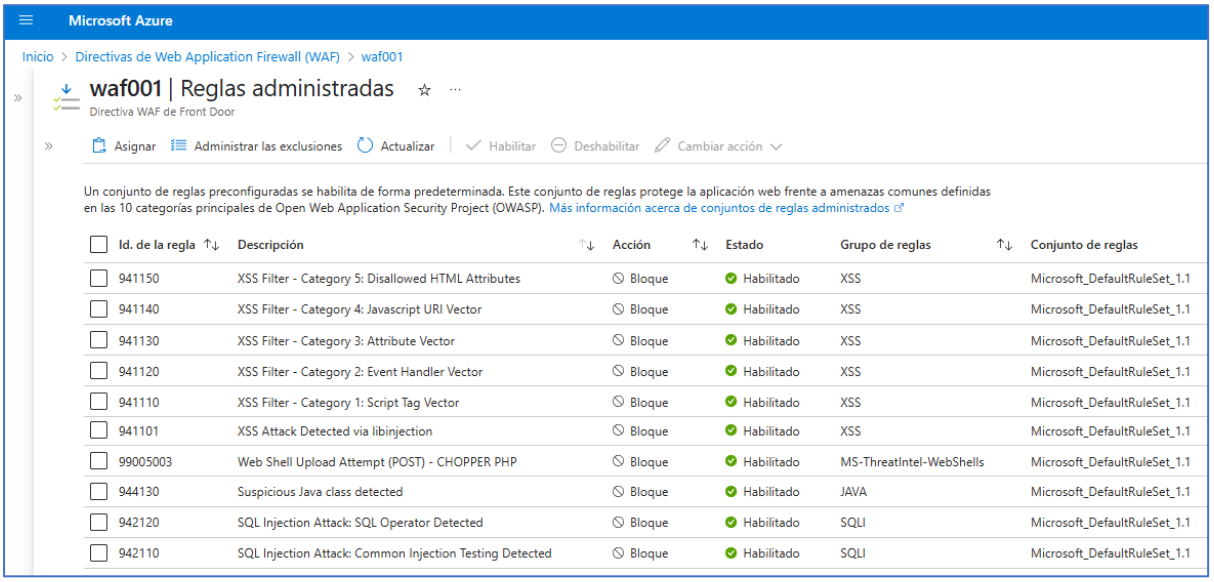
Asociaciones de directiva waf001



Nota: Nótese que la directiva está asociada a los cuatro front-ends configurados para el servicio de Cambix.

Figura 37

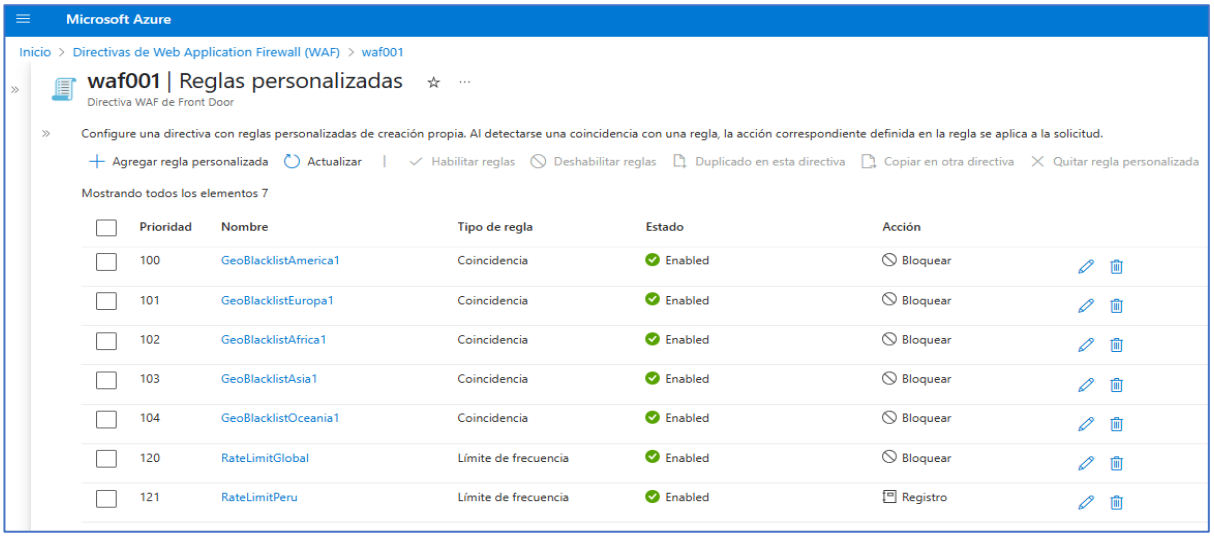
Reglas administradas de directiva waf001



Nota: Vista parcial del total de más de 130 reglas administradas. Las reglas administradas se basan en la inteligencia de amenazas global de Microsoft Azure para ofrecer protección contra vulnerabilidades y ataques comunes en la web.

Figura 38

Reglas personalizadas de directiva waf001



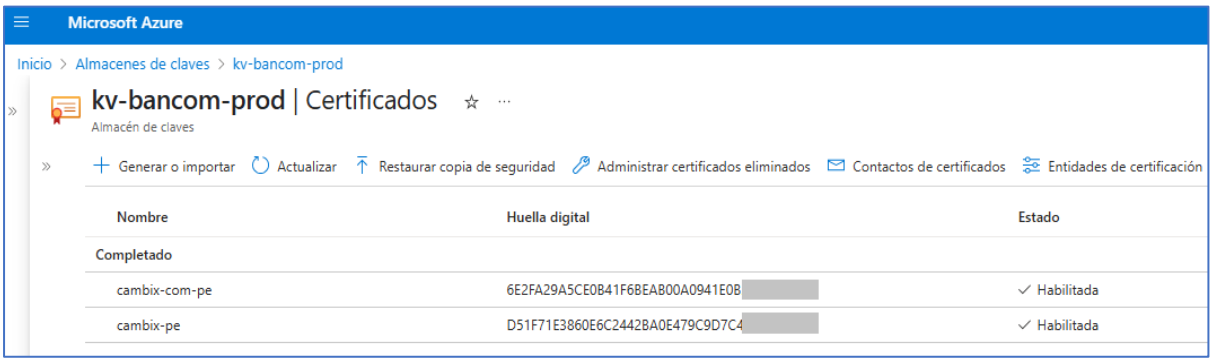
Nota: En cumplimiento con las políticas de seguridad del Banco, se restringe el tráfico proveniente de países identificados como fuentes recurrentes de actividades maliciosas, tales como Rusia, China, Corea del Norte y otros.

4.4.1.6 Configuración de almacén de claves de certificados digitales

Almacén de claves kv-bancom-prod destinado a la gestión de certificados digitales del servicio de Cambix.

Figura 39

Almacén de claves kv-bancom-prod para la gestión de certificados digitales

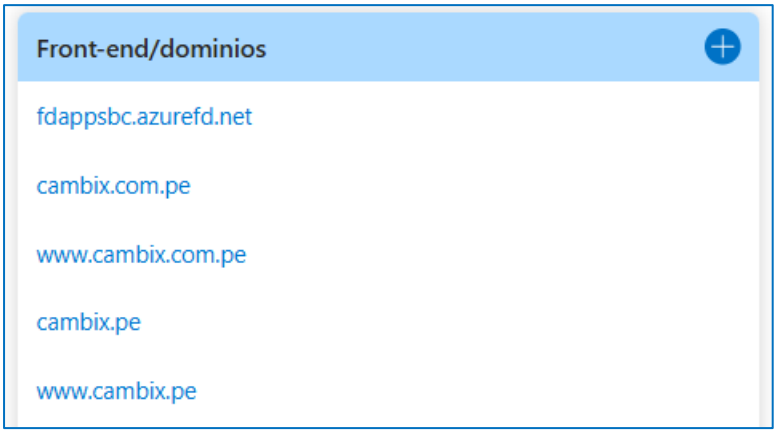


Nota: Cada certificado es válido tanto para el nombre raíz como para la versión con www. Los certificados se importan en el recurso kv-bancom-prod, el cual está asociado a los front-ends configurados para el servicio de Cambix.

En la Figura 40 se observan los 4 front-ends creados y configurados. La Figura 41 muestra la vista parcial del Diseñador de Front Door tras la creación de estos los front-ends.

Figura 40

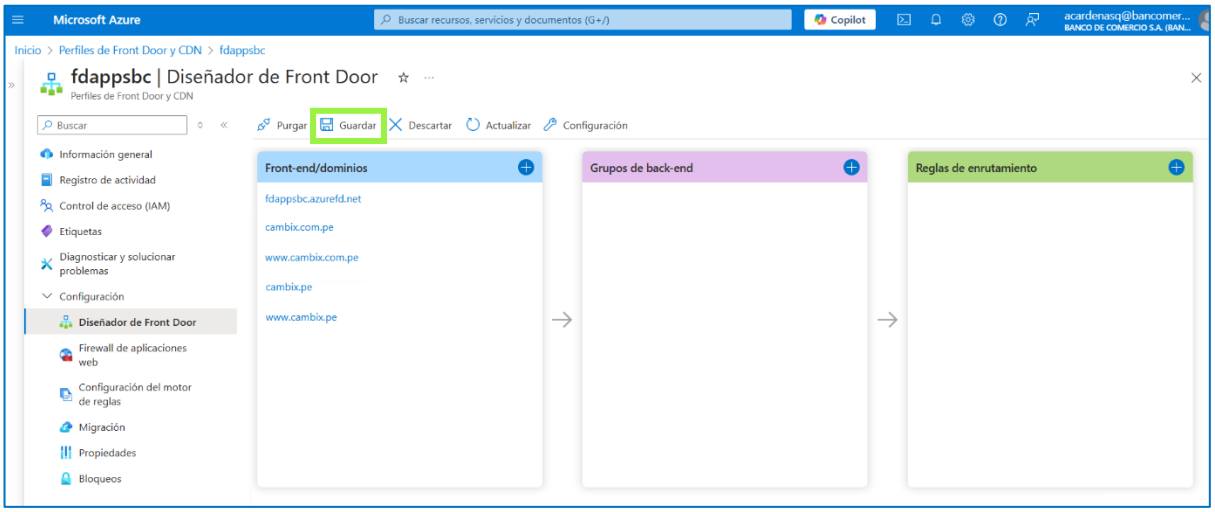
Front-ends completos



Nota: El front-end fdappsbc.azurefd.net se crea por defecto al crear la instancia. Nótese que ahora, tras el front-end por defecto, se muestran los 4 front-ends para el servicio de Cambix.

Figura 41

Vista parcial del Diseñador de Front Door con front-ends completos



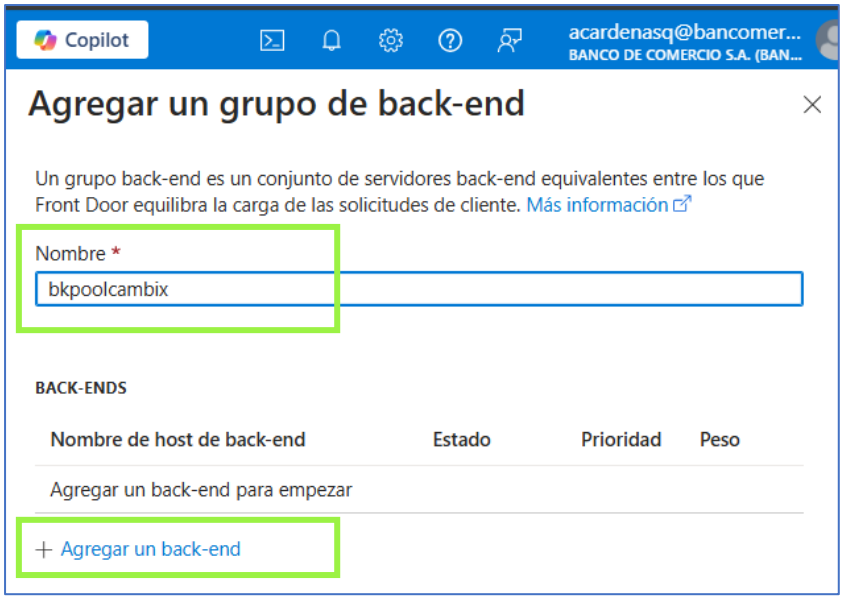
Nota: Se guarda la configuración para aplicar los cambios y finalizar.

4.4.2 Creación de grupo de back-end

La Figura 42, Figura 43 y Figura 44 muestran la creación y configuración del grupo de back-end para el servicio de Cambix.

Figura 42

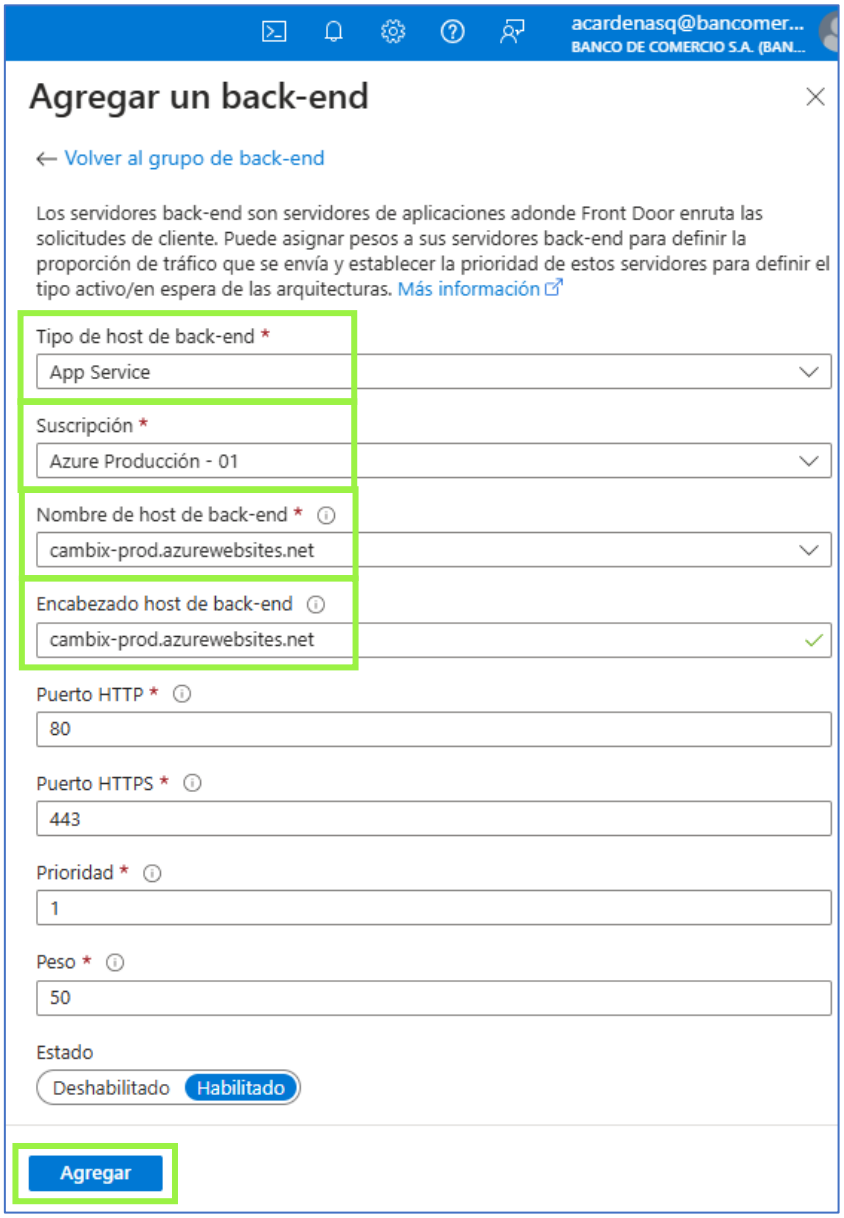
Creación del grupo de back-end bkpoolcambix



Nota: Un grupo de back-end se conforma por uno o más back-ends, en la presente implementación se conforma por un solo back-end, nótese que de momento el listado está vacío y se solicita agregar un back-end para empezar.

Figura 43

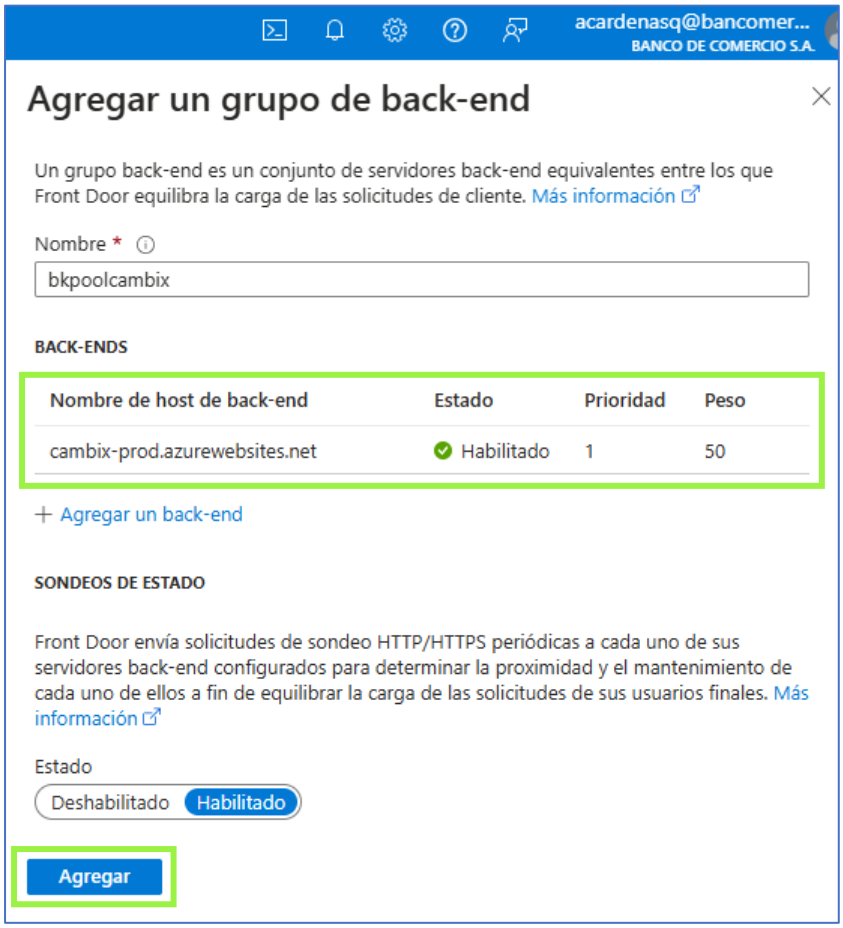
Agregar back-end cambix-prod



Nota: Nótese que se establece como back-end al recurso App Service cambix-prod del servicio de Cambix, las demás configuraciones quedan por defecto. El número de puerto para las solicitudes HTTP se queda habilitado por defecto en 80, posteriormente se configura la redirección para permitir únicamente el acceso por el puerto 443. La prioridad y el peso se asignan al trabajar con más de un back-end. La prioridad define el back-end principal y los de reserva; el peso distribuye el tráfico. En esta implementación no aplican y quedan por defecto.

Figura 44

Completar creación del grupo de back-end bkpoolcambix con back-end cambix-prod



En la Figura 45 se observa el grupo de back-end creado y configurado. La Figura 46 muestra la vista parcial del Diseñador de Front Door tras esta creación.

Figura 45

Grupo de back-end completo

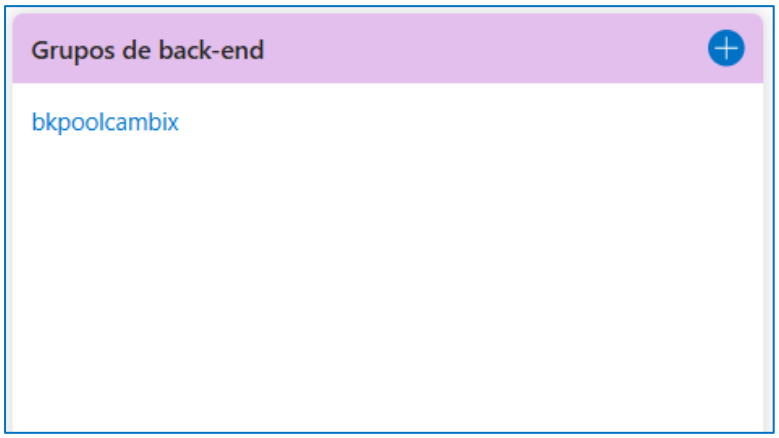
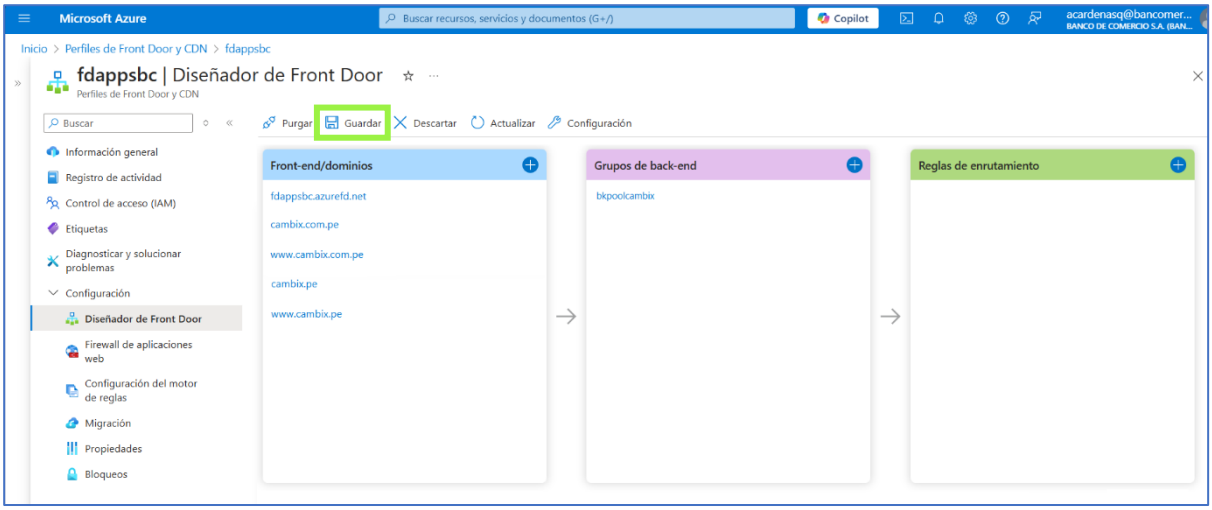


Figura 46

Vista parcial del Diseñador de Front Door con grupo de back-end completo



4.4.3 Creación de reglas de enrutamiento

4.4.3.1 Regla Rule-cambix

La configuración de la regla Rule-cambix permite habilitar el acceso al servicio, únicamente a través del dominio principal con el protocolo seguro HTTPS.

Casos:

- https://cambix.com.pe

Figura 47

Creación de regla Rule-cambix

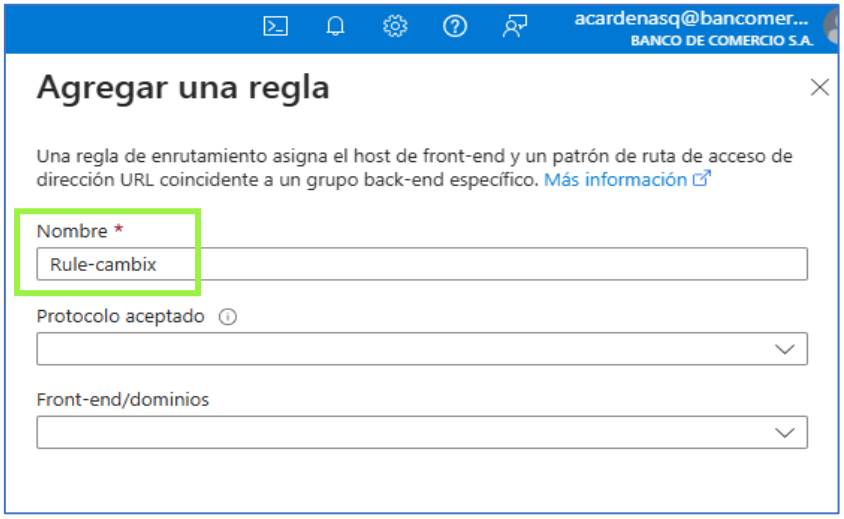
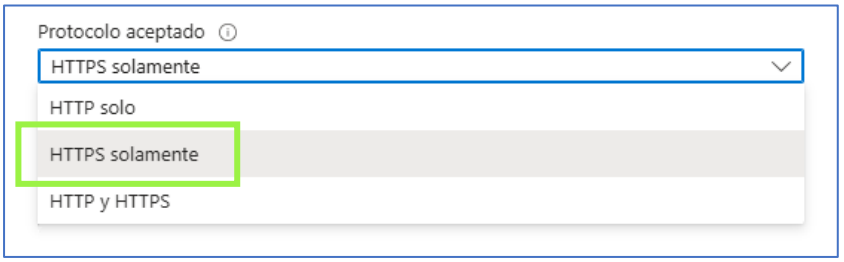


Figura 48

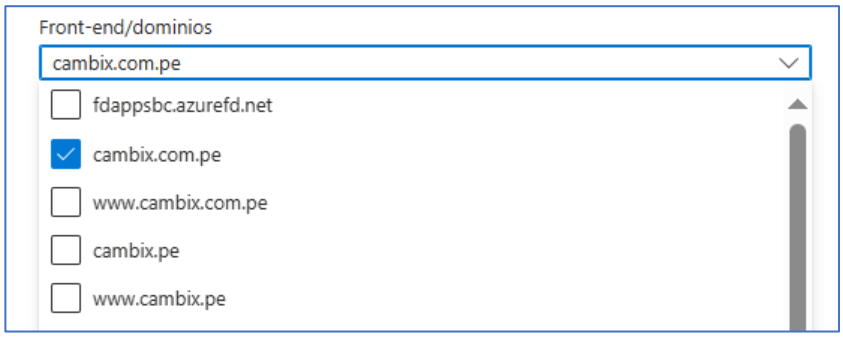
Configuración de protocolo aceptado regla Rule-cambix



Nota: Se especifica qué protocolos entrantes se permiten. Nótese que para habilitar el acceso al servicio se considera únicamente el protocolo HTTPS.

Figura 49

Configuración de front-ends en regla Rule-cambix



Nota: Se especifican los front-ends asignados a esta regla. Nótese que para habilitar el acceso al servicio se considera únicamente el front-end cambix.com.pe, correspondiente al dominio principal.

Figura 50

Configuración de back-end en regla Rule-cambix

Nota: El tipo de ruta establece como tratar las solicitudes a una ruta, en este caso al dominio principal, para definir si se reenvían a un back-end (Adelante) o si se redirecciona a los usuarios a otra dirección URL (Redireccionamiento). Nótese que para habilitar el acceso al servicio se considera reenviar (Adelante) al grupo de back-end bkpoolcambix creado para el servicio de Cambix.

4.4.3.2 Regla http-to-https

La configuración de la regla http-to-https permite redirigir las peticiones originadas con el protocolo HTTP, hacia el protocolo seguro HTTPS, en el dominio principal.

Casos:

- http://cambix.com.pe

Esta configuración considera exclusivamente el protocolo HTTP en el dominio principal, para redirigirlo y acceder únicamente mediante el protocolo HTTPS.

Figura 51

Creación de regla http-to-https

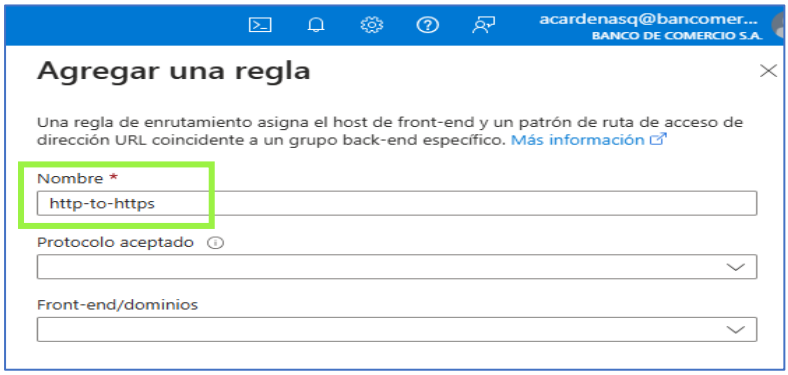
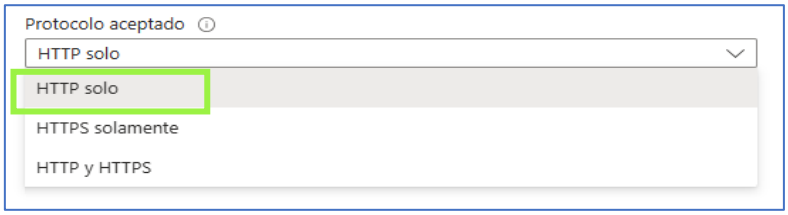


Figura 52

Configuración de protocolo aceptado regla http-to-https



Nota: Se especifica qué protocolos entrantes se permiten. Nótese que para configurar la redirección de HTTP a HTTPS en el dominio principal se considera únicamente el protocolo HTTP. Así, todas las peticiones HTTP serán automáticamente redireccionadas a la regla Rule-cambix, la cual ya está configurada para el acceso al dominio principal únicamente por el protocolo HTTPS.

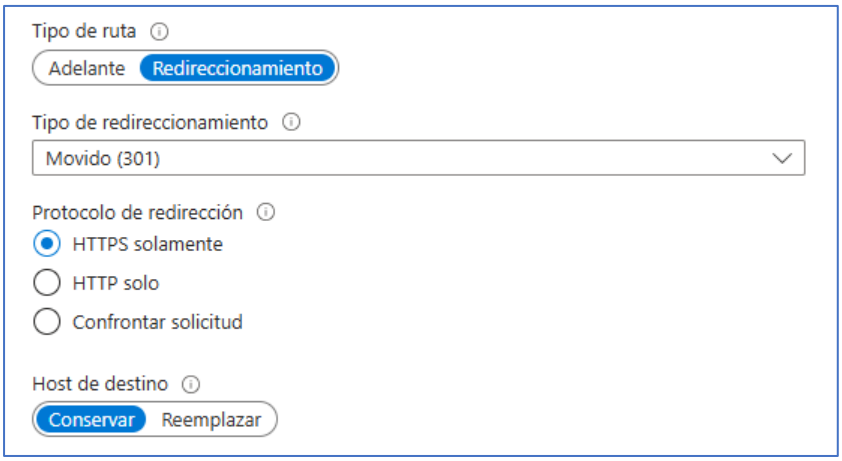
Figura 53

Configuración de front-ends en regla http-to-https

Nota: Se especifican los front-ends asignados a esta regla. Nótese que para configurar está redirección de HTTP a HTTPS también se considera el front-end cambix.com.pe, correspondiente al dominio principal.

Figura 54

Configuración de back-end en regla Rule-cambix



Nota: El tipo de ruta establece como tratar las solicitudes a una ruta, en este caso se redirecciona a los usuarios a una dirección URL (Redireccionamiento) con el mismo host (dominio), pero con distinto protocolo (esquema). Nótese que para configurar la redirección de HTTP a HTTPS en el dominio principal se considera un tipo de redireccionamiento 301, mientras se habilita conservar el host de destino; de esta manera el protocolo HTTP queda cubierto y se expone únicamente el protocolo HTTPS en el dominio principal.

4.4.3.3 Regla redirect04-cambix

La configuración de la regla redirect04-cambix permite redirigir las peticiones originadas desde los dominios alternos hacia el dominio principal.

Casos:

- https://cambix.pe
- https://www.cambix.pe
- https://www.cambix.com.pe
- http://cambix.pe
- http://www.cambix.pe
- http://www.cambix.com.pe

Esta configuración considera todos los demás casos de acceso, que son los dominios alternos mediante el protocolo HTTPS y en complemento el protocolo HTTP; para redirigir cualquiera de estos casos y acceder únicamente a través del dominio principal con el protocolo seguro HTTPS.

Figura 55

Creación de regla redirect04-cambix

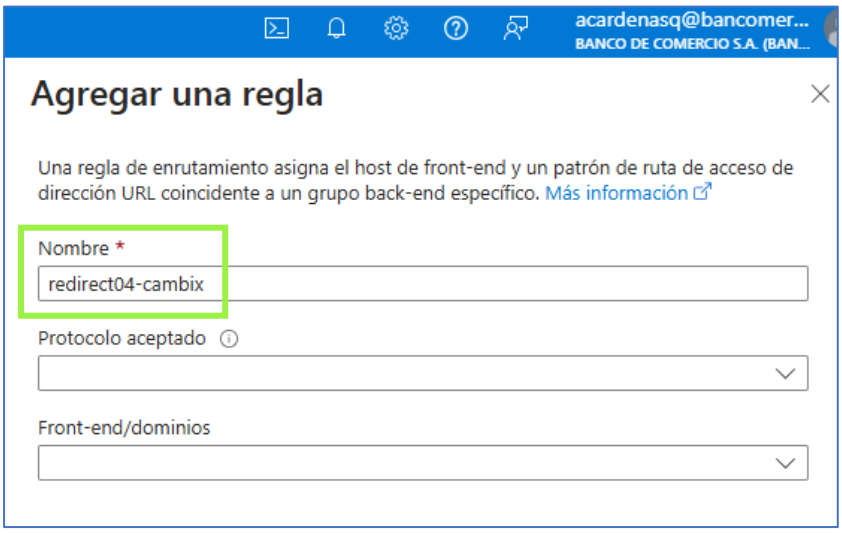
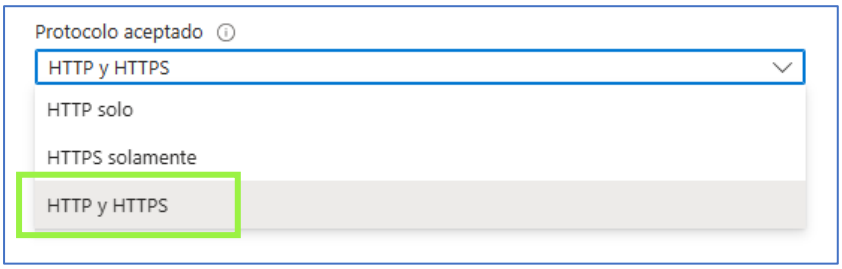


Figura 56

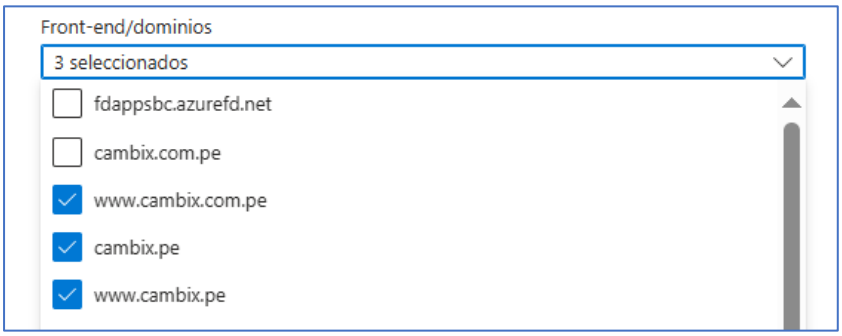
Configuración de protocolo aceptado regla redirect04-cambix



Nota: Se especifica qué protocolos entrantes se permiten. Nótese que para configurar la redirección de los dominios alternos se consideran ambos protocolos, ya que todas las peticiones alternas, sean HTTP o HTTPS, finalmente se redireccionarán a la regla Rule-cambix que ya está configurada para el acceso al dominio principal únicamente por el protocolo HTTPS.

Figura 57

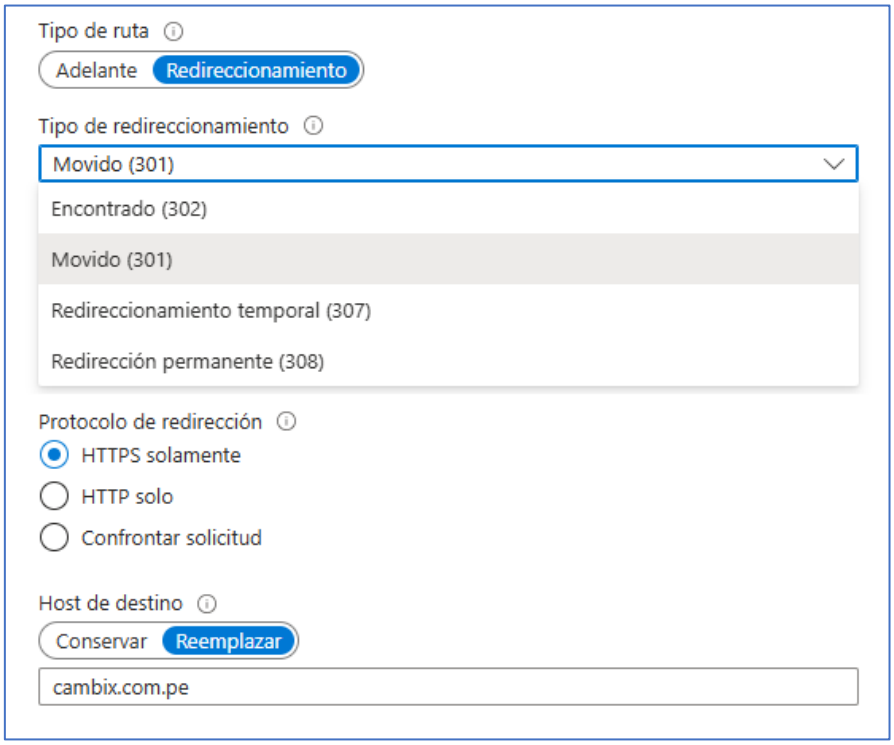
Configuración de front-ends en regla redirect04-cambix



Nota: Se especifican los front-ends asignados a esta regla. Nótese que para configurar la redirección de los dominios alternos se consideran los front-ends correspondientes a los 3 dominios alternos.

Figura 58

Configuración de back-end en regla redirect04-cambix



Nota: El tipo de ruta establece como tratar las solicitudes a una ruta, en este caso se redirecciona a los usuarios a otra dirección URL (Redireccionamiento). Nótese que para configurar la redirección de los dominios alternos se considera un tipo de redireccionamiento 301; dicha configuración permite indicar que la URL del dominio alterno ha sido cambiada permanentemente y en su reemplazo se designa una URL correspondiente al dominio principal cambix.com.pe, la cual se visualizará en el navegador web del cliente; de esta manera los dominios alternos quedan reemplazados y se expone únicamente el dominio principal.

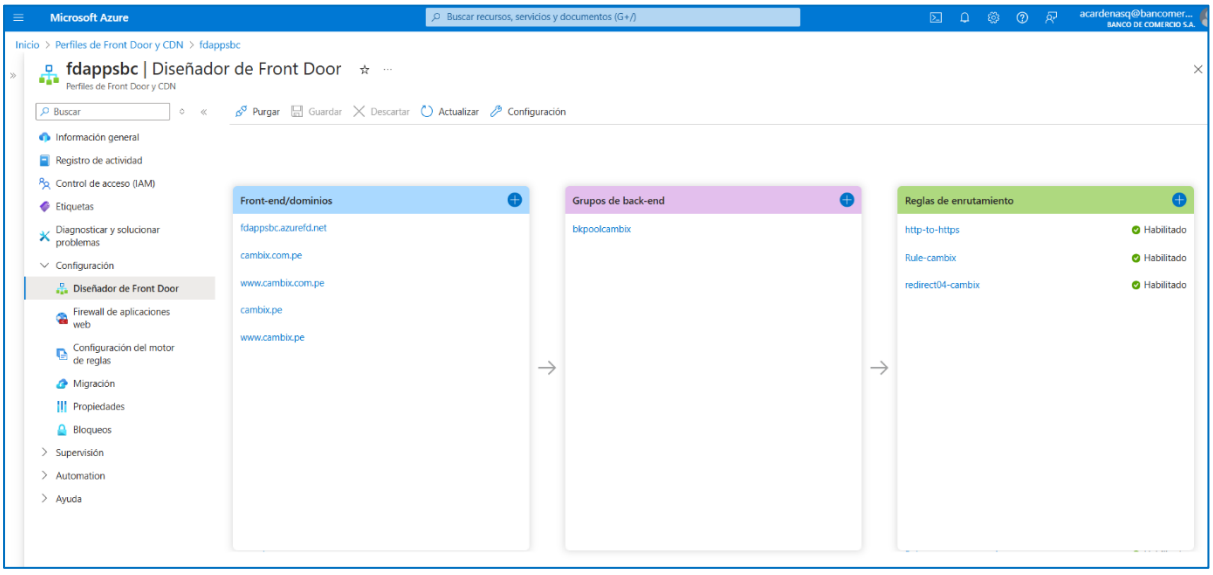
La Figura 59 muestra las reglas de enrutamiento creadas y configuradas. La Figura 60 muestra la vista final del Diseñador de Front Door.

Figura 59

Reglas de enrutamiento completas

Figura 60

Vista final del Diseñador de Front Door

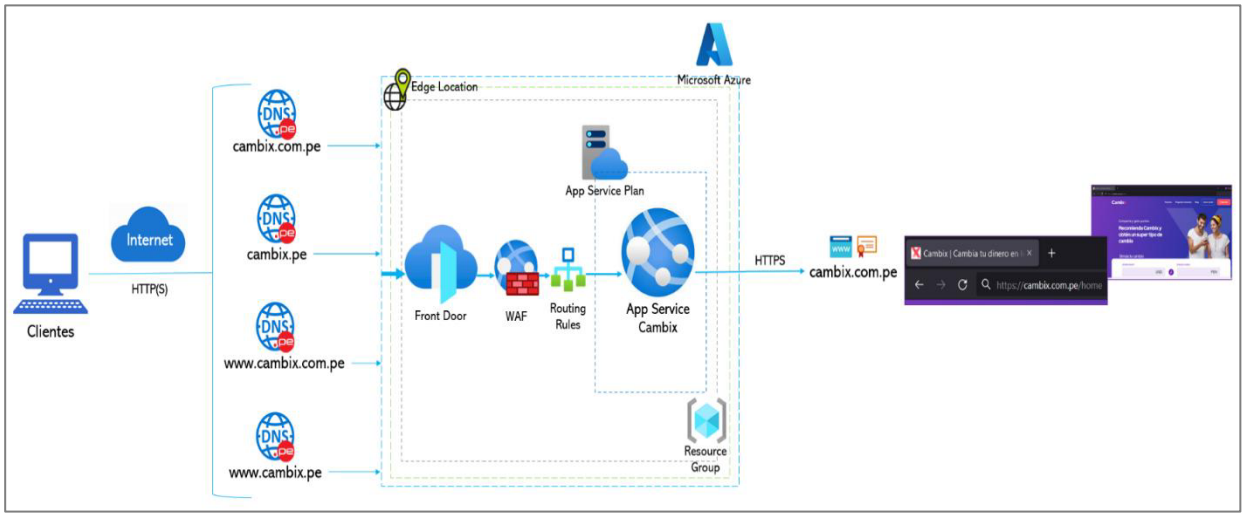


La Figura 61 muestra el nuevo flujo de navegación de los clientes para acceder vía web al servicio digital de Cambix, en donde el cliente, sea cual sea cualquiera de las 4 URL por las

que ingrese, será redirigido al servicio de Cambix a través de la URL principal, gracias a la Arquitectura de Enrutamiento en Azure Front Door implementada.

Figura 61

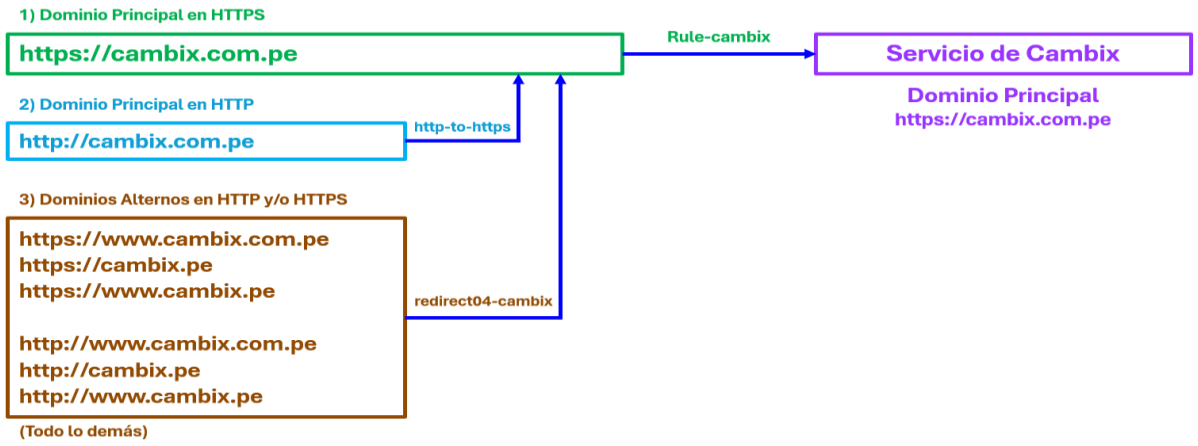
Nuevo flujo de navegación de los clientes para acceder vía web al servicio digital de Cambix



La Figura 62 representa el flujo de las reglas de enrutamiento configuradas para el acceso al servicio. La Figura 63 muestra la Arquitectura de Enrutamiento Front Door.

Figura 62

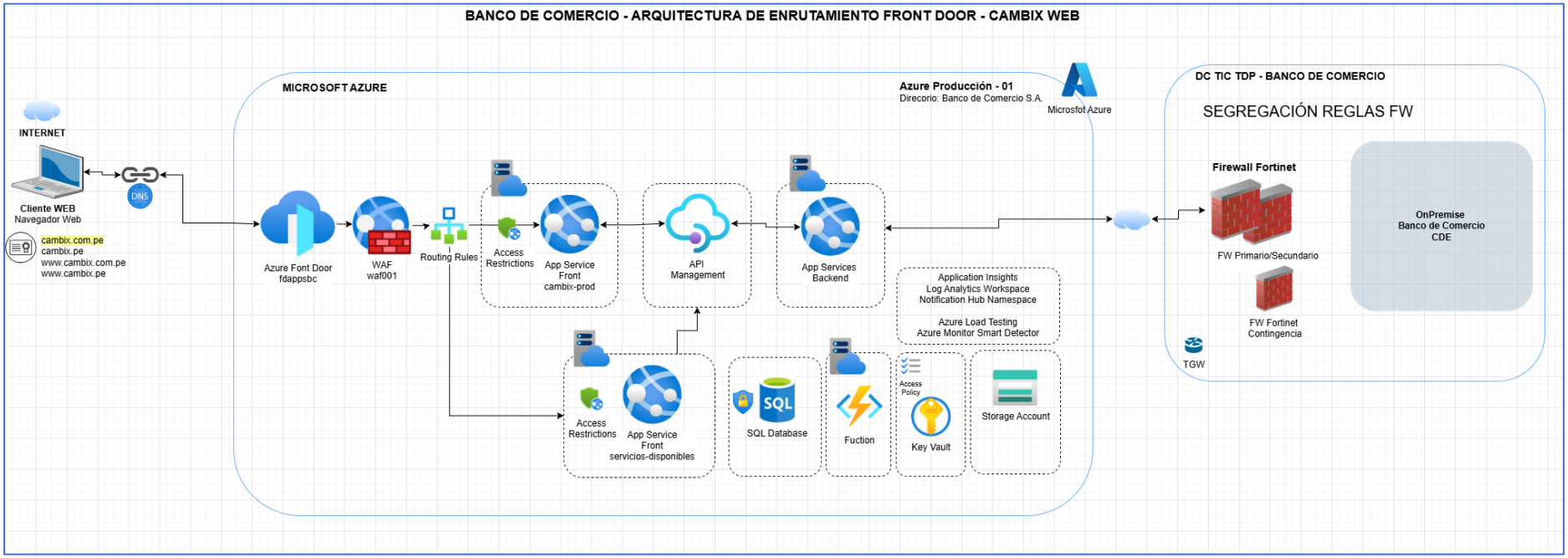
Flujo de reglas de enrutamiento para el acceso al servicio de Cambix



Nota: Cada regla de enrutamiento maneja el protocolo y dominio específico para el cual se ha configurado.

Figura 63

Arquitectura de Enrutamiento Front Door para el servicio de Cambix



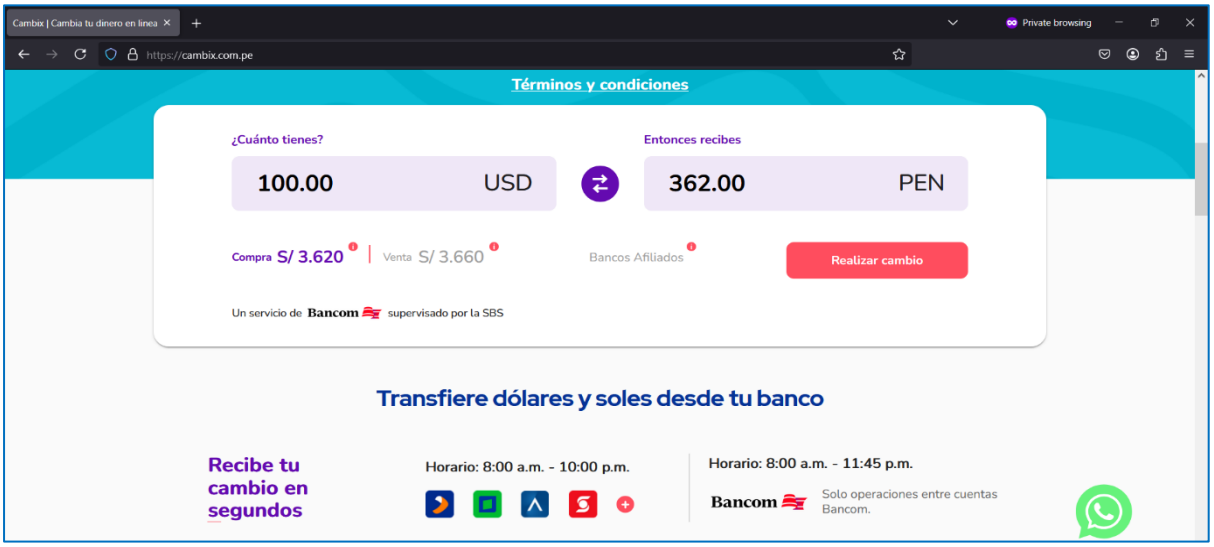
Nota: Nótese la estructura y diseño de los componentes que se utilizan para enrutar el tráfico de red del servicio de Cambix a través de la infraestructura de entrega de contenido global de Azure.

4.5 Monitoreo y comprobación del acceso al servicio

Tras completar la creación y configuración de componentes se monitorea y comprueba el acceso mediante un navegador web, como se muestra en la Figura 64.

Figura 64

Validación de acceso al servicio mediante un navegador web



Nota: Nótese que finalmente, sea cual sea el dominio o protocolo, siempre se accede al servicio únicamente a través del dominio principal con el protocolo HTTPS. Adaptado de Cambix. (s.f.).

4.6 Presentación de resultados

El objetivo principal de esta investigación fue analizar el impacto de la implementación de una Arquitectura de Enrutamiento en Azure Front Door en la mejora del acceso vía web al servicio digital de una entidad financiera del Perú. Para ello, se evaluaron indicadores clave de desempeño en el grupo de control y grupo experimental, con el fin de determinar si la arquitectura propuesta contribuyó a optimizar aspectos como la accesibilidad, identidad corporativa, operatividad y seguridad del servicio.

La Tabla 14 muestra los valores de los indicadores con los resultados de posprueba en ambos grupos para cada indicador. A continuación, la Tabla 15 muestra el promedio de los indicadores, la Figura 65 la prueba de normalidad para el primer indicador con valores continuos a través de Minitab, la Tabla 16 muestra los registros de posprueba en el grupo experimental recolectados con Log Analytics.

Tabla 14

Resultados de Posprueba del Gc y Posprueba del Ge para I_1, I_2, I_3, I_4 e I_5

	I_1: Tiempo de respuesta		I_2: Número de dominios redirigidos		I_3: Número de dominios expuestos hacia el navegador web del cliente		I_4: Número de dominios con redirección de HTTP a HTTPS		I_5: Número de soluciones de seguridad WAF	
N°	**Posprueba Gc**	**Posprueba Ge**	**Posprueba Gc**	**Posprueba Ge**	**Posprueba Gc**	**Posprueba Ge**	**Posprueba Gc**	**Posprueba Ge**	**Posprueba Gc**	**Posprueba Ge**
1	13.42	4.82	0	3	4	1	0	4	0	1
2	12.88	5.33	0	3	4	1	0	4	0	1
3	15.12	3.74	0	3	4	1	0	4	0	1
4	11.99	1.99	0	3	4	1	0	4	0	1
5	14.35	6.12	0	3	4	1	0	4	0	1
6	13.09	4.41	0	3	4	1	0	4	0	1
7	12.44	7.08	0	3	4	1	0	4	0	1
8	13.78	5.02	0	3	4	1	0	4	0	1
9	15.03	3.57	0	3	4	1	0	4	0	1
10	14.62	4.96	0	3	4	1	0	4	0	1
11	12.21	8.25	0	3	4	1	0	4	0	1
12	13.55	4.13	0	3	4	1	0	4	0	1
13	13.98	6.88	0	3	4	1	0	4	0	1
14	15.24	2.44	0	3	4	1	0	4	0	1
15	12.67	5.71	0	3	4	1	0	4	0	1
16	14.1	3.92	0	3	4	1	0	4	0	1
17	13.33	7.54	0	3	4	1	0	4	0	1
18	11.99	4.67	0	3	4	1	0	4	0	1
19	15.98	9.11	0	3	4	1	0	4	0	1
20	13.74	2.78	0	3	4	1	0	4	0	1
21	12.56	6.03	0	3	4	1	0	4	0	1
22	14.82	5.29	0	3	4	1	0	4	0	1
23	13.21	3.25	0	3	4	1	0	4	0	1
24	12.93	4.58	0	3	4	1	0	4	0	1
25	15.25	7.91	0	3	4	1	0	4	0	1
26	13.49	4.36	0	3	4	1	0	4	0	1
27	14.28	5.84	0	3	4	1	0	4	0	1
28	12.35	2.66	0	3	4	1	0	4	0	1
29	13.89	6.47	0	3	4	1	0	4	0	1
30	15.28	3.89	0	3	4	1	0	4	0	1

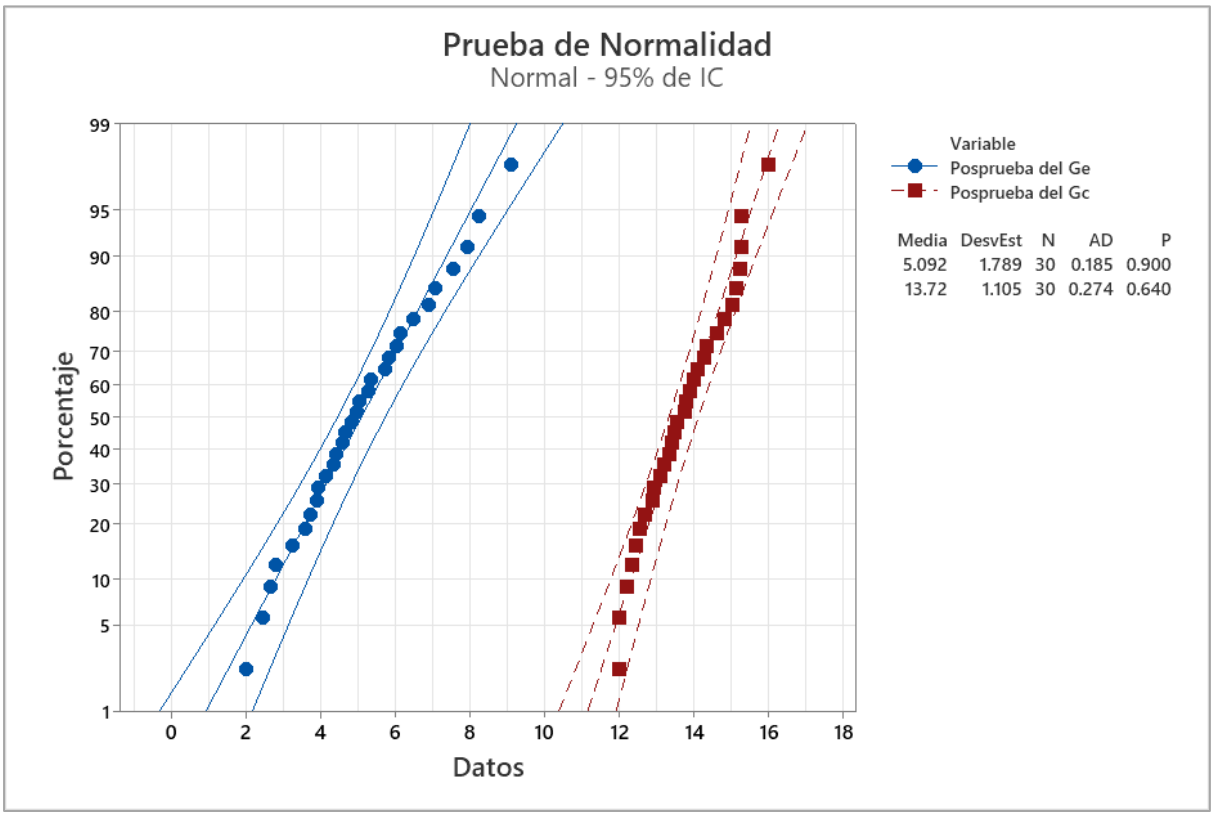
Tabla 15

Promedio de los indicadores de la Posprueba del Gc y Ge

Indicador	Posprueba Gc (Media: $\bar{X}_1$)	Posprueba Ge (Media: $\bar{X}_2$)
Tiempo de respuesta	13.72 segundos	5.09 segundos
Número de dominios redirigidos	0 dominios redirigidos	3 dominios redirigidos
Número de dominios expuestos hacia el navegador web del cliente	4 dominios expuestos	1 dominio expuesto
Número de dominios con redirección de HTTP a HTTPS	0 dominios con redirección de protocolo	4 dominios con redirección de protocolo
Número de soluciones de seguridad WAF	0 soluciones de seguridad WAF	1 solución de seguridad WAF

Figura 65

Prueba de normalidad indicador I_1



Nota: Nótese que p(0.900 y 0.640) > α(0.05). Por lo tanto, los valores tienen un comportamiento normal.

Tabla 16

Registros de posprueba en el grupo experimental recolectados con Log Analytics

N°	Request URI	Request Protocol	Routing Rule Name	Backend	HTTP Status Code
1	https://cambix.com.pe:443/	HTTPS	Rule-cambix	cambix-prod.azurewebsites.net:443	200
2	https://cambix.com.pe:443/	HTTPS	Rule-cambix	cambix-prod.azurewebsites.net:443	200
3	https://cambix.pe:443/	HTTPS	redirect04-cambix	N/A	301
4	https://cambix.pe:443/	HTTPS	redirect04-cambix	N/A	301
5	https://cambix.com.pe:443/	HTTPS	Rule-cambix	cambix-prod.azurewebsites.net:443	200
6	http://cambix.com.pe:80/	HTTP	http-to-https	N/A	301
7	https://cambix.com.pe:443/	HTTPS	Rule-cambix	cambix-prod.azurewebsites.net:443	200
8	http://cambix.com.pe:80/	HTTP	http-to-https	N/A	301
9	http://cambix.com.pe:80/	HTTP	http-to-https	N/A	301
10	https://cambix.com.pe:443/	HTTPS	Rule-cambix	cambix-prod.azurewebsites.net:443	200
11	http://cambix.pe:80/	HTTP	redirect04-cambix	N/A	301
12	https://cambix.com.pe:443/	HTTPS	Rule-cambix	cambix-prod.azurewebsites.net:443	200
13	https://cambix.com.pe:443/	HTTPS	Rule-cambix	cambix-prod.azurewebsites.net:443	200
14	https://www.cambix.com.pe:443/	HTTPS	redirect04-cambix	N/A	301
15	https://cambix.pe:443/	HTTPS	redirect04-cambix	N/A	301
16	http://cambix.com.pe:80/	HTTP	http-to-https	N/A	301
17	https://www.cambix.pe:443/	HTTPS	redirect04-cambix	N/A	301
18	https://www.cambix.com.pe:443/	HTTPS	redirect04-cambix	N/A	301
19	http://cambix.pe:80/	HTTP	redirect04-cambix	N/A	301
20	http://www.cambix.com.pe:80/	HTTP	redirect04-cambix	N/A	301
21	https://cambix.pe:443/	HTTPS	redirect04-cambix	N/A	301
22	http://cambix.com.pe:80/	HTTP	http-to-https	N/A	301
23	https://cambix.com.pe:443/	HTTPS	Rule-cambix	cambix-prod.azurewebsites.net:443	200
24	http://www.cambix.pe:80/	HTTP	redirect04-cambix	N/A	301
25	https://cambix.com.pe:443/	HTTPS	Rule-cambix	cambix-prod.azurewebsites.net:443	200
26	https://cambix.com.pe:443/	HTTPS	Rule-cambix	cambix-prod.azurewebsites.net:443	200
27	https://cambix.com.pe:443/	HTTPS	Rule-cambix	cambix-prod.azurewebsites.net:443	200
28	https://cambix.com.pe:443/	HTTPS	Rule-cambix	cambix-prod.azurewebsites.net:443	200
29	https://cambix.pe:443/	HTTPS	redirect04-cambix	N/A	301
30	https://cambix.com.pe:443/	HTTPS	Rule-cambix	cambix-prod.azurewebsites.net:443	200

4.7 Contrastación de las hipótesis

4.7.1 Contrastación de la H_1

Se llevo a cabo un análisis estadístico inferencial para la contrastación de la primera hipótesis especifica. Se menciona la Hipótesis de Investigación del presente estudio.

H_1: Si se implementa una Arquitectura de Enrutamiento en Azure Front Door, utilizando Microsoft Azure, entonces disminuye el tiempo de respuesta en el acceso vía web al servicio digital de una entidad financiera del Perú.

Hi: La implementación de una Arquitectura de Enrutamiento en Azure Front Door disminuye el tiempo de respuesta (Posprueba del Ge) con respecto a la muestra a la que no se aplicó (Posprueba del Gc).

Se realizaron mediciones sin la implementación de una Arquitectura de Enrutamiento en Azure Front Door (Posprueba del Gc) y otras con la implementación de una Arquitectura de Enrutamiento en Azure Front Door (Posprueba del Ge). La Tabla 17 muestra estos valores.

Tabla 17

Valores de las mediciones para H_1

Ge	4.82	5.33	3.74	1.99	6.12	4.41	7.08	5.02	3.57	4.96	8.25	4.13	6.88	2.44	5.71
	3.92	7.54	4.67	9.11	2.78	6.03	5.29	3.25	4.58	7.91	4.36	5.84	2.66	6.47	3.89

Gc	13.42	12.88	15.12	11.99	14.35	13.09	12.44	13.78	15.03	14.62	12.21	13.55	13.98	15.24	12.67
	14.1	13.33	11.99	15.98	13.74	12.56	14.82	13.21	12.93	15.25	13.49	14.28	12.35	13.89	15.28

a) Planteamiento de las Hipótesis Nula y Alterna:

H_0: La implementación de una Arquitectura de Enrutamiento en Azure Front Door incrementa el tiempo de respuesta (Posprueba del Ge) con respecto a la muestra a la que no se aplicó (Posprueba del Gc).

Ha: La implementación de una Arquitectura de Enrutamiento en Azure Front Door disminuye el tiempo de respuesta (Posprueba del Ge) con respecto a la muestra a la que no se aplicó (Posprueba del Gc).

μ_1 = Media Poblacional del Tiempo de respuesta en la Posprueba del Gc.

μ_2 = Media Poblacional del Tiempo de respuesta en la Posprueba del Ge.

H_0: $\mu_{1c} \leq \mu_{2e}$

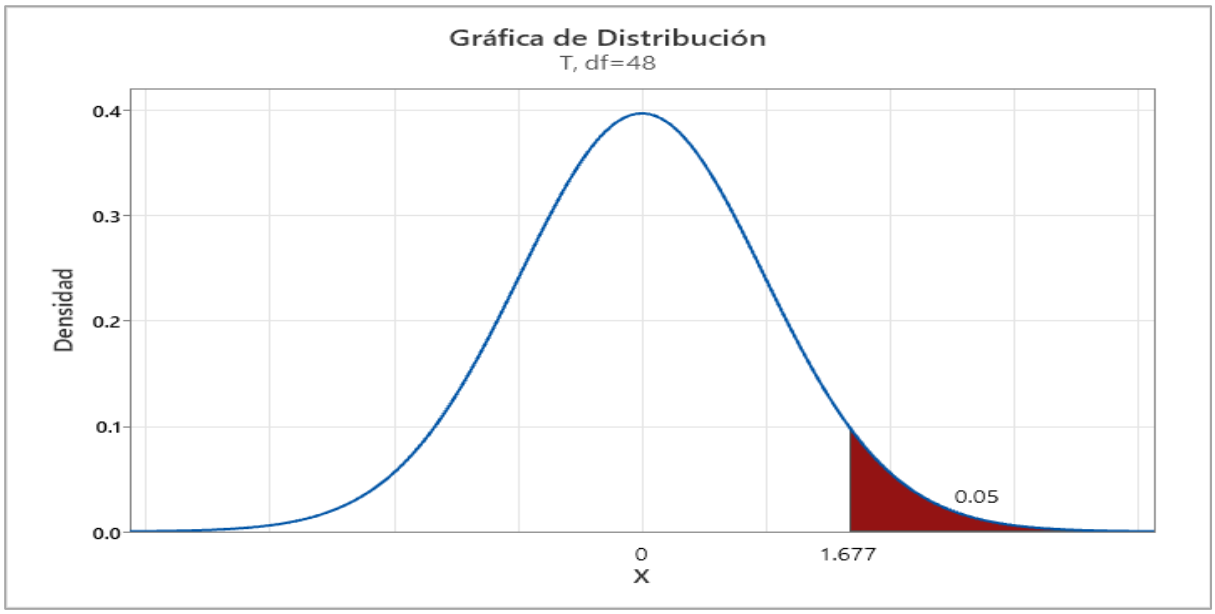
Ha: $\mu_{1c} > \mu_{2e}$

b) Criterios de decisión:

La Figura 66 muestra la gráfica de distribución para establecer el criterio de decisión; la Figura 67 muestra la fórmula Welch-Satterthwaite para el cálculo de los grados de libertad.

Figura 66

Gráfica de Distribución para H_1



Nota: El valor de grados de libertad (df) es de 48. Con el nivel de significancia del 0.05, el valor de t-crítico (t_t) resulta 1.677. Nótese que la región de rechazo de la Hipótesis Nula es el conjunto de valores de la estadística de prueba mayores al valor de t-crítico que caen en el rango de la cola derecha.

Figura 67

Fórmula Welch-Satterthwaite para calcular los grados de libertad (degrees of freedom)

$$DF = \frac{\left(\frac{s_1^2}{n_1} + \frac{s_2^2}{n_2}\right)^2}{\frac{s_1^4}{n_1^2(n_1-1)} + \frac{s_2^4}{n_2^2(n_2-1)}}$$

c) Cálculo:

El resultado del estadístico de prueba para la presente investigación se calcula mediante la prueba estadística t de Student para muestras independientes. La Figura 68 y Figura 69 muestran el cálculo mediante Minitab.

Figura 68

Cálculo del valor del Estadístico de Prueba mediante la Prueba t de Student en Minitab

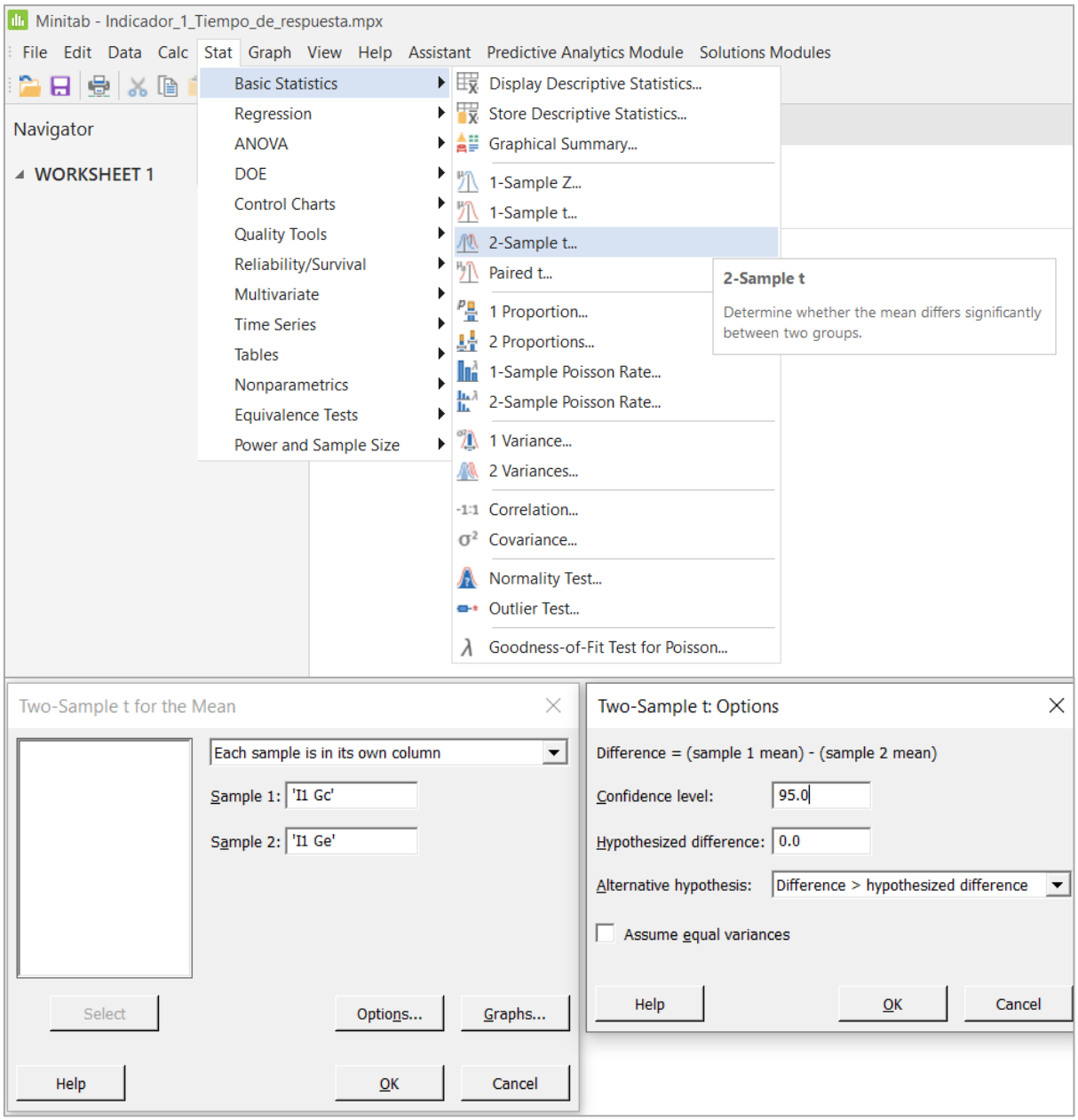
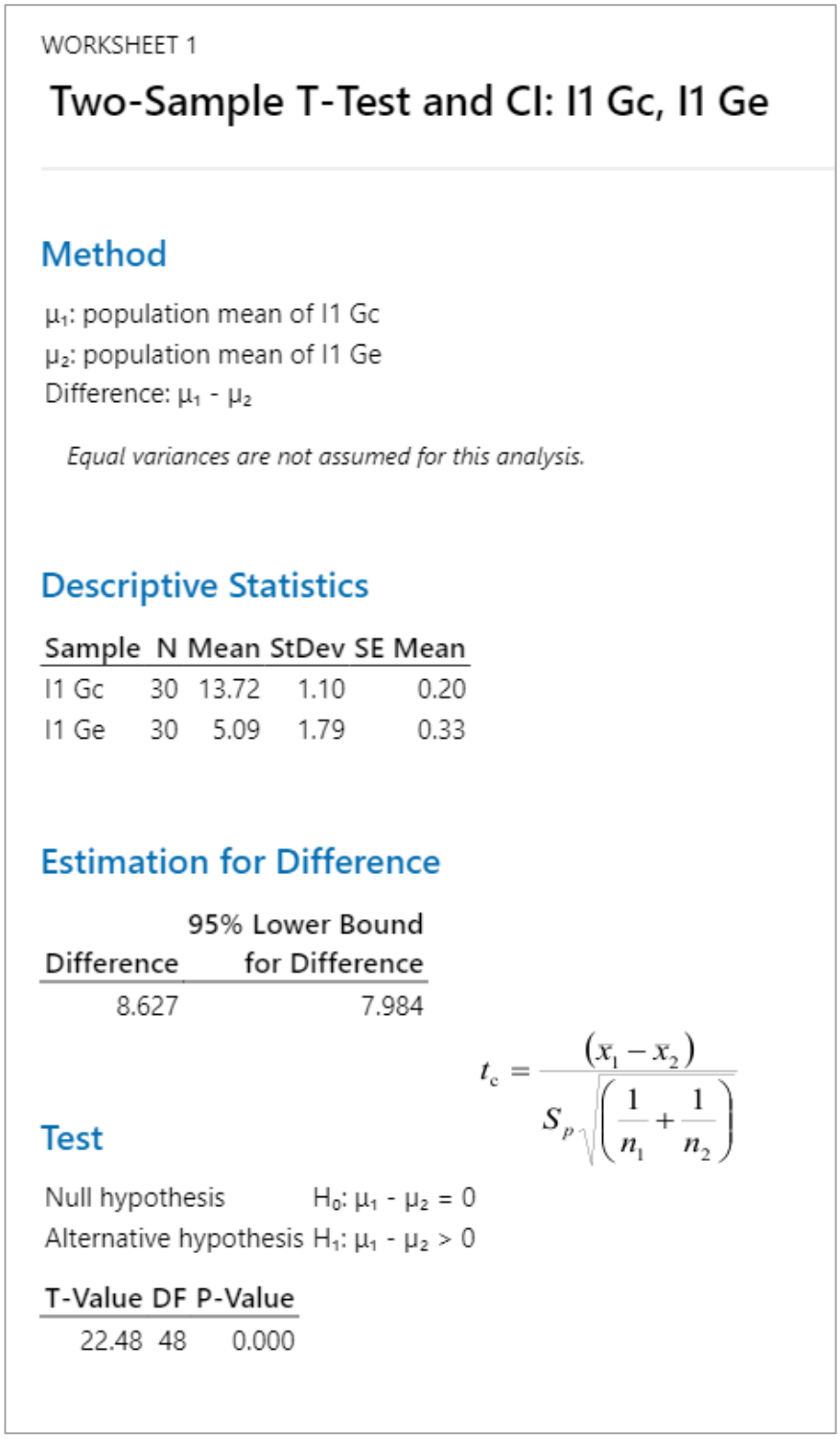


Figura 69

Resultado de la Prueba t de Student para medias de las 2 muestras en Minitab



WORKSHEET 1

Two-Sample T-Test and CI: I1 Gc, I1 Ge

Method

μ_1: population mean of I1 Gc
μ_2: population mean of I1 Ge
Difference: $\mu_1 - \mu_2$

Equal variances are not assumed for this analysis.

Descriptive Statistics

Sample	N	Mean	StDev	SE Mean
I1 Gc	30	13.72	1.10	0.20
I1 Ge	30	5.09	1.79	0.33

Estimation for Difference

Difference	95% Lower Bound for Difference
8.627	7.984

$$t_c = \frac{(x_1 - x_2)}{S_p\sqrt{\left(\frac{1}{n_1} + \frac{1}{n_2}\right)}}$$

Test

Null hypothesis H_0: $\mu_1 - \mu_2 = 0$
Alternative hypothesis H_1: $\mu_1 - \mu_2 > 0$

T-Value	DF	P-Value
22.48	48	0.000

Nota: Nótese el resultado con el t-calculado (T-Value) y el p-value (P-Value).

La Tabla 18 muestra el resumen con el resultado del cálculo del Estadístico de Prueba mediante la Prueba t de Student.

Tabla 18

Resumen del resultado del cálculo del valor del Estadístico de Prueba

	PosPrueba Gc	**PosPrueba Ge**
Media ($\bar{X}$)	13.72	5.09
Desviación Estándar (S)	1.10	1.79
Observaciones (n)	30	30
Diferencia hipotética de las medias	0	
t-calculado (t-value): t_c	22.48	
p-value (una cola)	0.000	

Nota: Se utiliza la Prueba t para saber si se rechaza la hipótesis nula o no; para ello, se calculó el p-value a partir del valor t-calculado (t-value) en Minitab.

d) Decisión estadística:

Puesto que el p-value(0.000) < α(0.05), los resultados proporcionan suficiente evidencia estadística para rechazar la hipótesis nula (H_0), y la hipótesis alterna (Ha) es cierta. La prueba resultó ser significativa.

4.7.2 Contrastación de la H_2

Se llevo a cabo un análisis estadístico inferencial para la contrastación de la segunda hipótesis especifica.

H_2: Si se implementa una Arquitectura de Enrutamiento en Azure Front Door, utilizando Microsoft Azure, entonces incrementa el número de dominios redirigidos para el acceso vía web al servicio digital de una entidad financiera del Perú.

Hi: La implementación de una Arquitectura de Enrutamiento en Azure Front Door incrementa el número de dominios redirigidos (Posprueba del Ge) con respecto a la muestra a la que no se aplicó (Posprueba del Gc).

Se realizaron mediciones sin la implementación de una Arquitectura de Enrutamiento en Azure Front Door (Posprueba del Gc) y otras con la implementación de una Arquitectura de Enrutamiento en Azure Front Door (Posprueba del Ge). La Tabla 19 muestra estos valores.

Tabla 19

Valores de las mediciones para H_2

Ge	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3

Gc	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

a) Planteamiento de las Hipótesis Nula y Alterna:

H_0: La implementación de una Arquitectura de Enrutamiento en Azure Front Door disminuye el número de dominios redirigidos (Posprueba del Ge) con respecto a la muestra a la que no se aplicó (Posprueba del Gc).

Ha: La implementación de una Arquitectura de Enrutamiento en Azure Front Door incrementa el número de dominios redirigidos (Posprueba del Ge) con respecto a la muestra a la que no se aplicó (Posprueba del Gc).

μ_1 = Media Poblacional del Número de dominios redirigidos en la Posprueba del Gc.

μ_2 = Media Poblacional del Número de dominios redirigidos en la Posprueba del Ge.

H_0: $\mu_{1c} \geq \mu_{2e}$

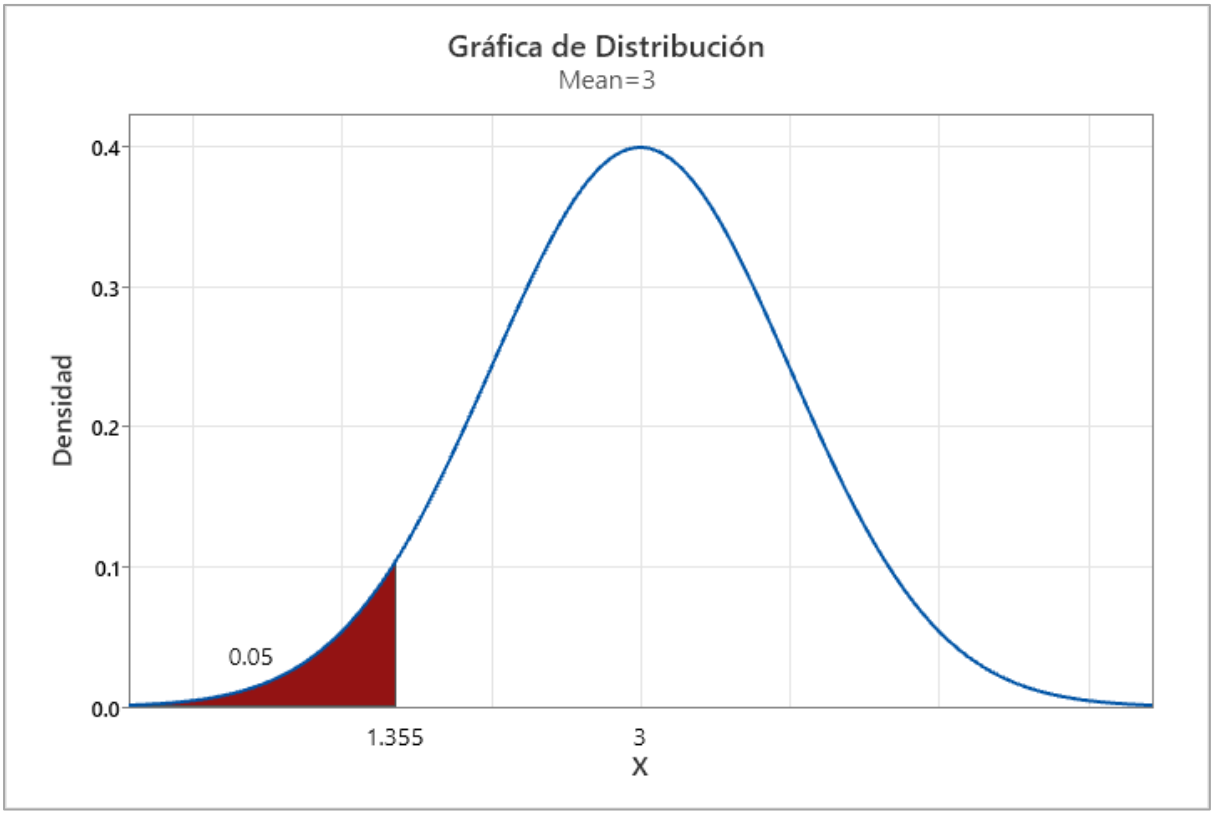
Ha: $\mu_{1c} < \mu_{2e}$

b) Criterios de decisión:

La Figura 70 muestra la gráfica de distribución para establecer el criterio de decisión.

Figura 70

Gráfica de Distribución para H_2



Nota: El valor de la media es de 3. Con el nivel de significancia del 0.05, el valor crítico resulta 1.355.

c) Cálculo:

Dado que los valores de la intervención no presentan variabilidad, el resultado del estadístico de prueba se calcula mediante la prueba estadística U de Mann-Whitney para muestras independientes. La Figura 71 y Figura 72 muestran el cálculo mediante Minitab.

Figura 71

Cálculo del valor mediante la Prueba U de Mann-Whitney en Minitab para H_2

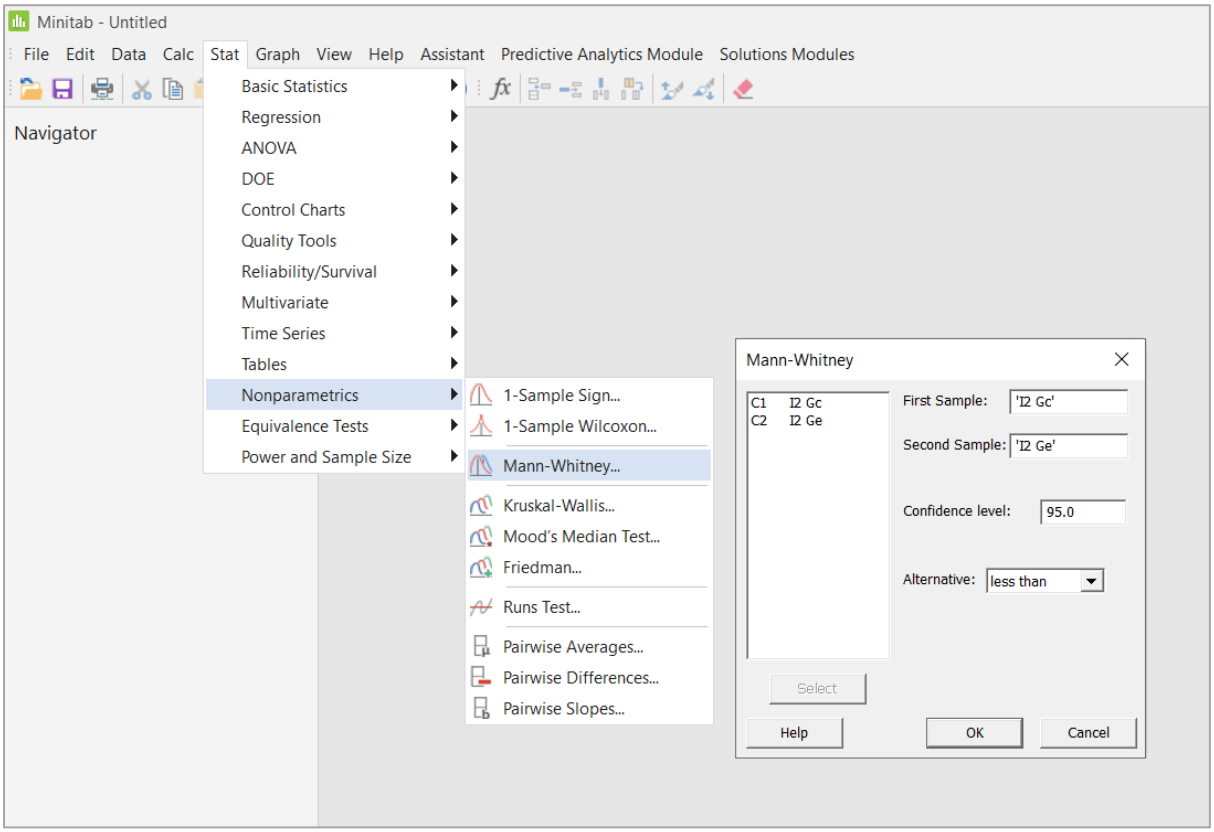
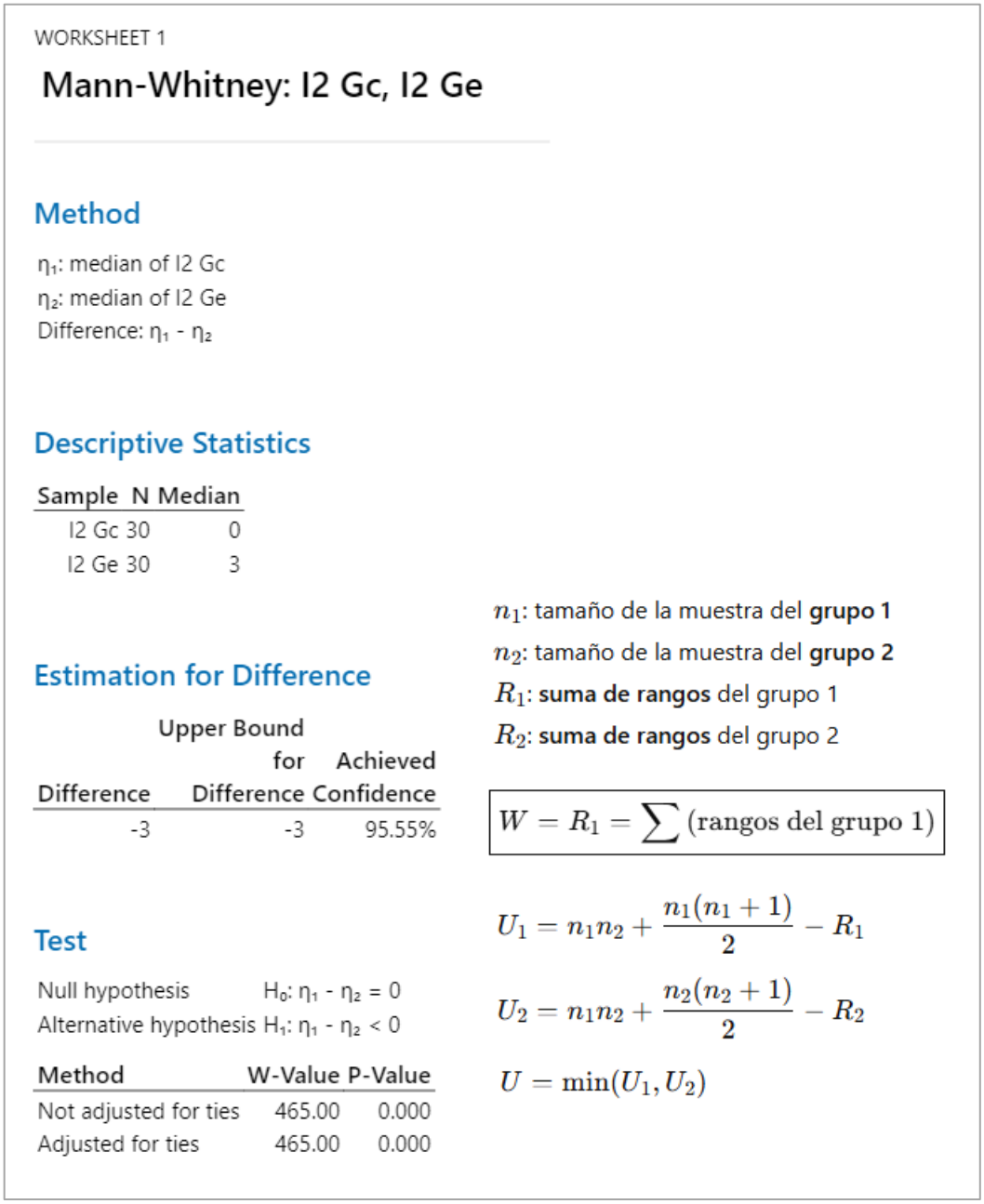


Figura 72

Resultado de la Prueba U de Mann-Whitney en Minitab para H_2



WORKSHEET 1

Mann-Whitney: I2 Gc, I2 Ge

Method

η_1: median of I2 Gc
η_2: median of I2 Ge
Difference: η_1 - η_2

Descriptive Statistics

Sample	N	Median
I2 Gc	30	0
I2 Ge	30	3

Estimation for Difference

Difference	Upper Bound for Difference	Achieved Confidence
-3	-3	95.55%

Test

Null hypothesis H_0: η_1 - η_2 = 0
Alternative hypothesis H_1: η_1 - η_2 < 0

Method	W-Value	P-Value
Not adjusted for ties	465.00	0.000
Adjusted for ties	465.00	0.000

n_1: tamaño de la muestra del **grupo 1**
n_2: tamaño de la muestra del **grupo 2**
R_1: **suma de rangos** del grupo 1
R_2: **suma de rangos** del grupo 2

$$W = R_1 = \sum (\text{rangos del grupo 1})$$

$$U_1 = n_1 n_2 + \frac{n_1(n_1+1)}{2} - R_1$$

$$U_2 = n_1 n_2 + \frac{n_2(n_2+1)}{2} - R_2$$

$$U = \min(U_1, U_2)$$

Nota: Nótese el resultado con el W-Value y el p-value (P-Value).

d) Decisión estadística:

Puesto que el p-value(0.000) < α(0.05), los resultados reflejan suficiente evidencia para rechazar la hipótesis nula (H_0) y aceptar la hipótesis alterna (Ha) como cierta. La prueba resultó ser significativa.

4.7.3 Contrastación de la H_3

Se llevo a cabo un análisis estadístico inferencial para la contrastación de la tercera hipótesis especifica.

H_3: Si se implementa una Arquitectura de Enrutamiento en Azure Front Door, utilizando Microsoft Azure, entonces disminuye el número de dominios expuestos hacia el navegador web del cliente en el acceso vía web al servicio digital de una entidad financiera del Perú.

Hi: La implementación de una Arquitectura de Enrutamiento en Azure Front Door disminuye el número de dominios expuestos hacia el navegador web del cliente (Posprueba del Ge) con respecto a la muestra a la que no se aplicó (Posprueba del Gc).

Se realizaron mediciones sin la implementación de una Arquitectura de Enrutamiento en Azure Front Door (Posprueba del Gc) y otras con la implementación de una Arquitectura de Enrutamiento en Azure Front Door (Posprueba del Ge). La Tabla 20 muestra estos valores.

Tabla 20

Valores de las mediciones para H_3

Ge	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

Gc	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4

a) Planteamiento de las Hipótesis Nula y Alterna:

H_0: La implementación de una Arquitectura de Enrutamiento en Azure Front Door incrementa el número de dominios expuestos hacia el navegador web del cliente (Posprueba del Ge) con respecto a la muestra a la que no se aplicó (Posprueba del Gc).

Ha: La implementación de una Arquitectura de Enrutamiento en Azure Front Door disminuye el número de dominios expuestos hacia el navegador web del cliente (Posprueba del Ge) con respecto a la muestra a la que no se aplicó (Posprueba del Gc).

μ_1 = Media Poblacional del Número de dominios expuestos en la Posprueba del Gc.

μ_2 = Media Poblacional del Número de dominios expuestos en la Posprueba del Ge.

H_0: $\mu_{1c} \leq \mu_{2e}$

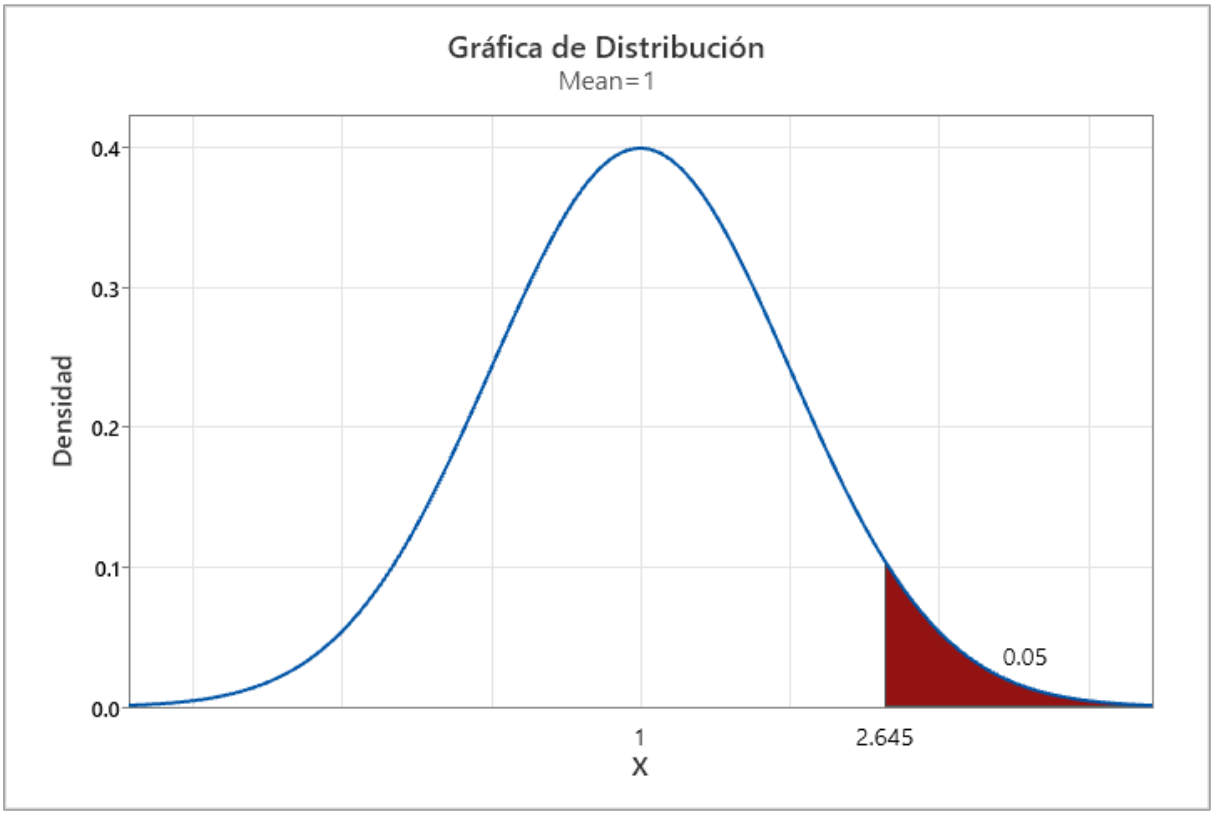
Ha: $\mu_{1c} > \mu_{2e}$

b) Criterios de decisión:

La Figura 73 muestra la gráfica de distribución para establecer el criterio de decisión.

Figura 73

Gráfica de Distribución para H_3



Nota: El valor de la media es de 3. Con el nivel de significancia del 0.05, el valor crítico resulta 2.645.

c) Cálculo:

Dado que los valores de la intervención no presentan variabilidad, el resultado del estadístico de prueba se calcula mediante la prueba estadística U de Mann-Whitney para muestras independientes. La Figura 74 y Figura 75 muestran el cálculo mediante Minitab.

Figura 74

Cálculo del valor mediante la Prueba U de Mann-Whitney en Minitab para H_3

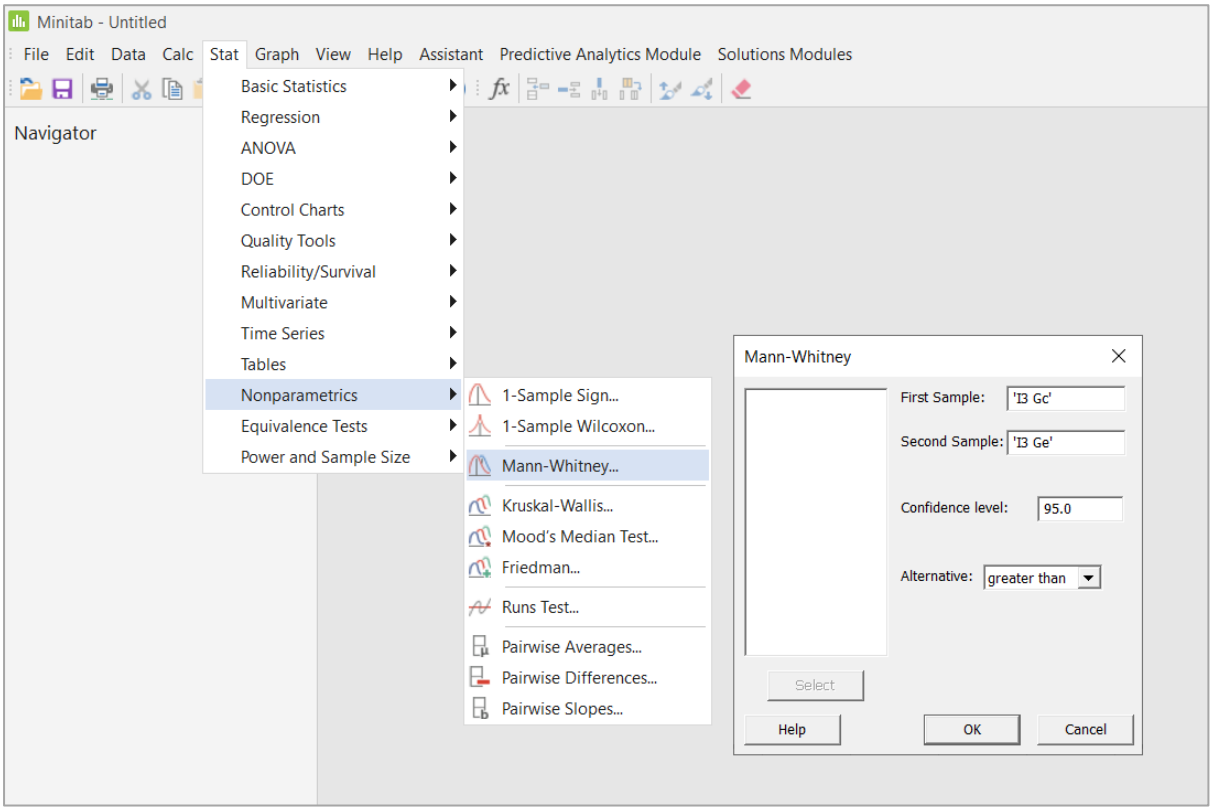


Figura 75

Resultado de la Prueba U de Mann-Whitney en Minitab para H_3

WORKSHEET 1

Mann-Whitney: I3 Gc, I3 Ge

Method

η_1: median of I3 Gc
η_2: median of I3 Ge
Difference: η_1 - η_2

Descriptive Statistics

Sample	N	Median
I3 Gc	30	4
I3 Ge	30	1

Estimation for Difference

Difference	Lower Bound for Difference	Achieved Confidence
3	3	95.55%

Test

Null hypothesis H_0: η_1 - η_2 = 0
Alternative hypothesis H_1: η_1 - η_2 > 0

Method	W-Value	P-Value
Not adjusted for ties	1365.00	0.000
Adjusted for ties	1365.00	0.000

n_1: tamaño de la muestra del **grupo 1**
n_2: tamaño de la muestra del **grupo 2**
R_1: **suma de rangos** del grupo 1
R_2: **suma de rangos** del grupo 2

$$W = R_1 = \sum (\text{rangos del grupo 1})$$

$$U_1 = n_1 n_2 + \frac{n_1(n_1+1)}{2} - R_1$$

$$U_2 = n_1 n_2 + \frac{n_2(n_2+1)}{2} - R_2$$

$$U = \min(U_1, U_2)$$

Nota: Nótese el resultado con el W-Value y el p-value (P-Value).

d) Decisión estadística:

Puesto que el p-value(0.000) < α(0.05), los resultados reflejan suficiente evidencia para rechazar la hipótesis nula (H_0) y aceptar la hipótesis alterna (Ha) como cierta. La prueba resultó ser significativa.

4.7.4 Contrastación de la H_4

Se llevo a cabo un análisis estadístico inferencial para la contrastación de la cuarta hipótesis especifica.

H_4: Si se implementa una Arquitectura de Enrutamiento en Azure Front Door, utilizando Microsoft Azure, entonces incrementa el número de dominios con redirección de HTTP a HTTPS para el acceso vía web al servicio digital de una entidad financiera del Perú.

Hi: La implementación de una Arquitectura de Enrutamiento en Azure Front Door incrementa el número de dominios con redirección de HTTP a HTTPS (Posprueba del Ge) con respecto a la muestra a la que no se aplicó (Posprueba del Gc).

Se realizaron mediciones sin la implementación de una Arquitectura de Enrutamiento en Azure Front Door (Posprueba del Gc) y otras con la implementación de una Arquitectura de Enrutamiento en Azure Front Door (Posprueba del Ge). La Tabla 21 muestra estos valores.

Tabla 21

Valores de las mediciones para H_4

Ge	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4

Gc	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

a) Planteamiento de las Hipótesis Nula y Alterna:

H_0: La implementación de una Arquitectura de Enrutamiento en Azure Front Door disminuye el número de dominios con redirección de HTTP a HTTPS (Posprueba del Ge) con respecto a la muestra a la que no se aplicó (Posprueba del Gc).

Ha: La implementación de una Arquitectura de Enrutamiento en Azure Front Door incrementa el número de dominios con redirección de HTTP a HTTPS (Posprueba del Ge) con respecto a la muestra a la que no se aplicó (Posprueba del Gc).

μ_1 = Media Poblacional del Número de dominios con redirección de HTTP a HTTPS en la Posprueba del Gc.

μ_2 = Media Poblacional del Número de dominios con redirección de HTTP a HTTPS en la Posprueba del Ge.

H_0: $\mu_{1c} \geq \mu_{2e}$

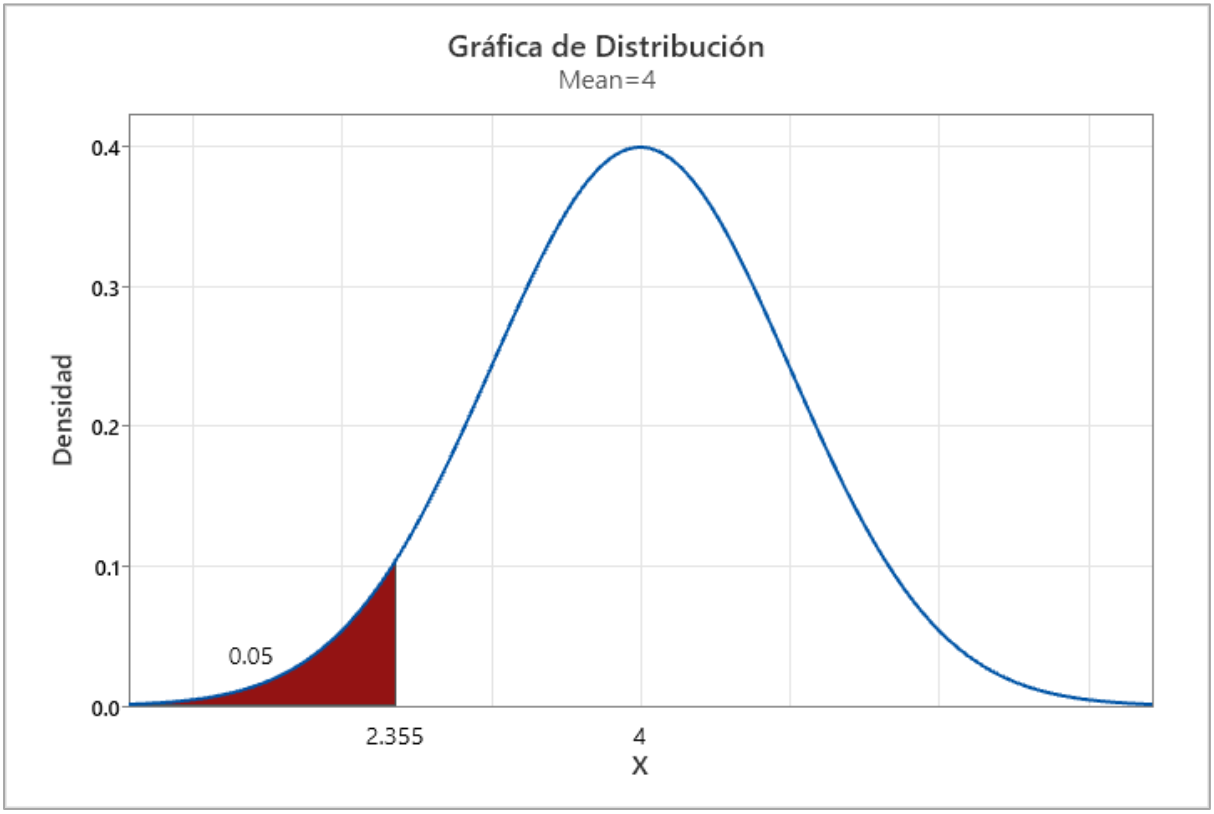
Ha: $\mu_{1c} < \mu_{2e}$

b) Criterios de decisión:

La Figura 76 muestra la gráfica de distribución para establecer el criterio de decisión.

Figura 76

Gráfica de Distribución para H_4



Nota: El valor de la media es de 4. Con el nivel de significancia del 0.05, el valor crítico resulta 2.355.

c) Cálculo:

Dado que los valores de la intervención no presentan variabilidad, el resultado del estadístico de prueba se calcula mediante la prueba estadística U de Mann-Whitney para muestras independientes. La Figura 77 y Figura 78 muestran el cálculo mediante Minitab.

Figura 77

Cálculo del valor mediante la Prueba U de Mann-Whitney en Minitab para H_4

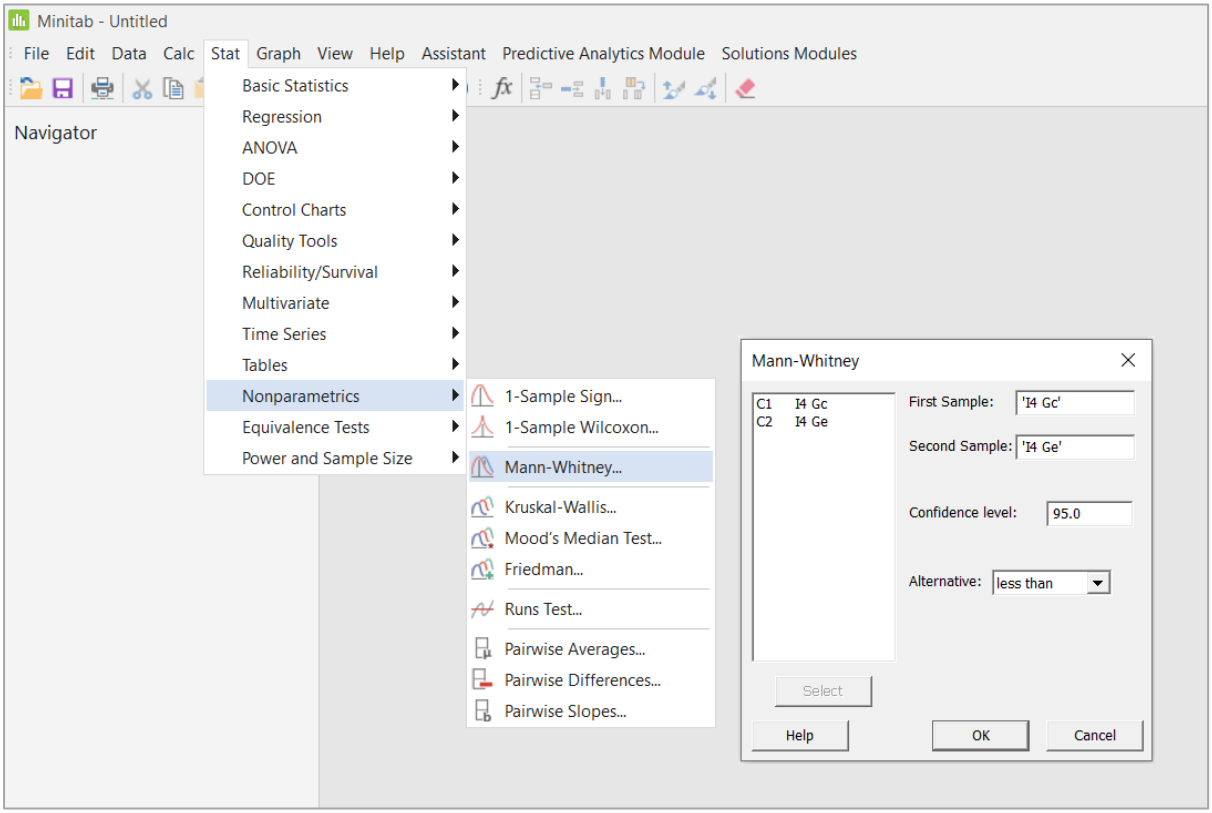


Figura 78

Resultado de la Prueba U de Mann-Whitney en Minitab para H_4

WORKSHEET 1

Mann-Whitney: I4 Gc, I4 Ge

Method

η_1: median of I4 Gc
η_2: median of I4 Ge
Difference: η_1 - η_2

Descriptive Statistics

Sample	N	Median
I4 Gc	30	0
I4 Ge	30	4

Estimation for Difference

Difference	Upper Bound for Difference	Achieved Confidence
-4	-4	95.55%

Test

Null hypothesis H_0: η_1 - η_2 = 0
Alternative hypothesis H_1: η_1 - η_2 < 0

Method	W-Value	P-Value
Not adjusted for ties	465.00	0.000
Adjusted for ties	465.00	0.000

n_1: tamaño de la muestra del **grupo 1**
n_2: tamaño de la muestra del **grupo 2**
R_1: **suma de rangos** del grupo 1
R_2: **suma de rangos** del grupo 2

$$W = R_1 = \sum (\text{rangos del grupo 1})$$

$$U_1 = n_1 n_2 + \frac{n_1(n_1+1)}{2} - R_1$$

$$U_2 = n_1 n_2 + \frac{n_2(n_2+1)}{2} - R_2$$

$$U = \min(U_1, U_2)$$

Nota: Nótese el resultado con el W-Value y el p-value (P-Value).

d) Decisión estadística:

Puesto que el p-value(0.000) < α(0.05), los resultados reflejan suficiente evidencia para rechazar la hipótesis nula (H_0) y aceptar la hipótesis alterna (Ha) como cierta. La prueba resultó ser significativa.

4.7.5 Contrastación de la H_5

Se llevo a cabo un análisis estadístico inferencial para la contrastación de la quinta hipótesis especifica.

H_5: Si se implementa una Arquitectura de Enrutamiento en Azure Front Door, utilizando Microsoft Azure, entonces incrementa el número de soluciones de seguridad WAF en el acceso vía web al servicio digital de una entidad financiera del Perú.

Hi: La implementación de una Arquitectura de Enrutamiento en Azure Front Door incrementa el número de soluciones de seguridad WAF (Posprueba del Ge) con respecto a la muestra a la que no se aplicó (Posprueba del Gc).

Se realizaron mediciones sin la implementación de una Arquitectura de Enrutamiento en Azure Front Door (Posprueba del Gc) y otras con la implementación de una Arquitectura de Enrutamiento en Azure Front Door (Posprueba del Ge). La Tabla 22 muestra estos valores.

Tabla 22

Valores de las mediciones para H_5

Ge	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

Gc	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

a) Planteamiento de las Hipótesis Nula y Alterna:

H_0: La implementación de una Arquitectura de Enrutamiento en Azure Front Door disminuye el número de soluciones de seguridad WAF (Posprueba del Ge) con respecto a la muestra a la que no se aplicó (Posprueba del Gc).

Ha: La implementación de una Arquitectura de Enrutamiento en Azure Front Door incrementa el número de soluciones de seguridad WAF (Posprueba del Ge) con respecto a la muestra a la que no se aplicó (Posprueba del Gc).

μ_1 = Media Poblacional del Número de soluciones de seguridad WAF en la Posprueba del Gc.

μ_2 = Media Poblacional del Número de soluciones de seguridad WAF en la Posprueba del Ge.

H_0: $\mu_{1c} \geq \mu_{2e}$

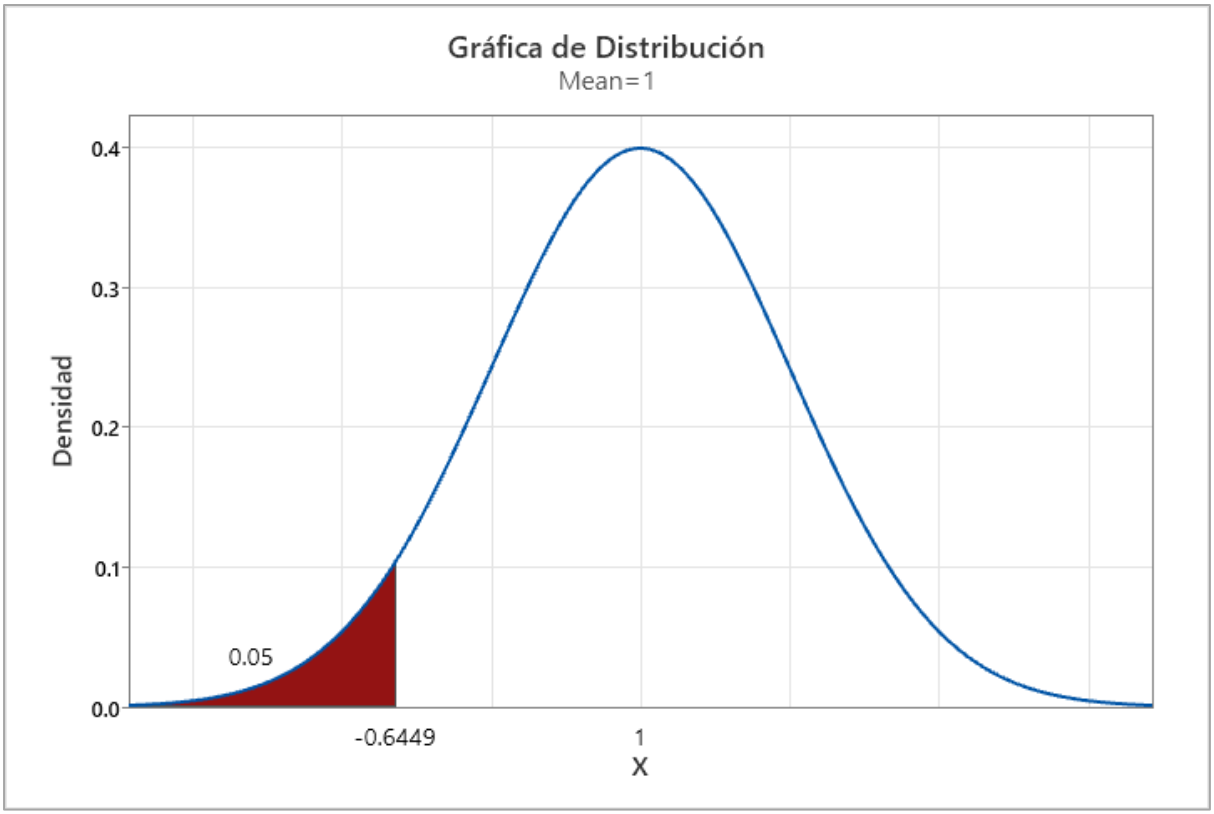
Ha: $\mu_{1c} < \mu_{2e}$

b) Criterios de decisión:

La Figura 79 muestra la gráfica de distribución para establecer el criterio de decisión.

Figura 79

Gráfica de Distribución para H_5



Nota: El valor de la media es de 1. Con el nivel de significancia del 0.05, el valor crítico resulta -0.6449.

c) Cálculo:

Dado que los valores de la intervención no presentan variabilidad, el resultado del estadístico de prueba se calcula mediante la prueba estadística U de Mann-Whitney para muestras independientes. La Figura 80 y Figura 81 muestran el cálculo mediante Minitab.

Figura 80

Cálculo del valor mediante la Prueba U de Mann-Whitney en Minitab para H_5

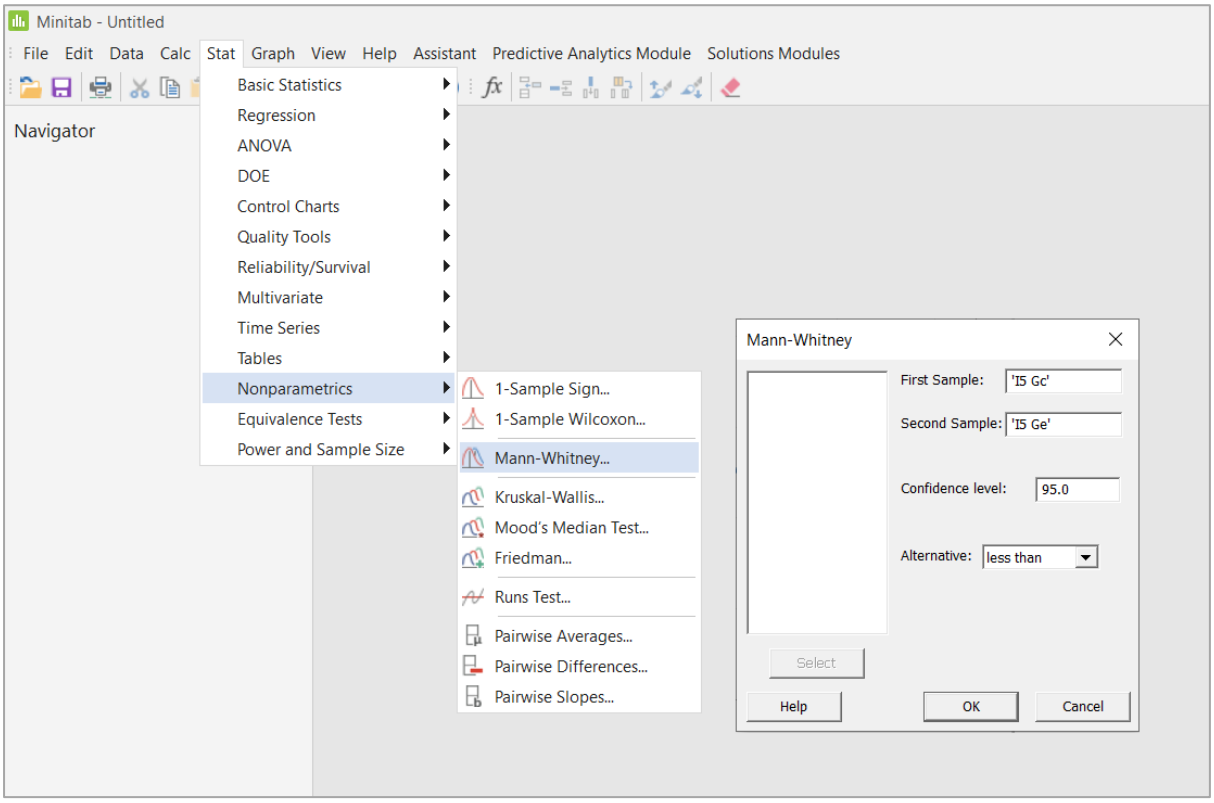


Figura 81

Resultado de la Prueba U de Mann-Whitney en Minitab para H_5

WORKSHEET 1

Mann-Whitney: I5 Gc, I5 Ge

Method

η_1: median of I5 Gc
η_2: median of I5 Ge
Difference: η_1 - η_2

Descriptive Statistics

Sample	N	Median
I5 Gc	30	0
I5 Ge	30	1

Estimation for Difference

Difference	Upper Bound for Difference	Achieved Confidence
-1	-1	95.55%

Test

Null hypothesis H_0: η_1 - η_2 = 0
Alternative hypothesis H_1: η_1 - η_2 < 0

Method	W-Value	P-Value
Not adjusted for ties	465.00	0.001
Adjusted for ties	465.00	0.000

n_1: tamaño de la muestra del **grupo 1**
n_2: tamaño de la muestra del **grupo 2**
R_1: **suma de rangos** del grupo 1
R_2: **suma de rangos** del grupo 2

$$W = R_1 = \sum (\text{rangos del grupo 1})$$

$$U_1 = n_1 n_2 + \frac{n_1(n_1+1)}{2} - R_1$$

$$U_2 = n_1 n_2 + \frac{n_2(n_2+1)}{2} - R_2$$

$$U = \min(U_1, U_2)$$

Nota: Nótese el resultado con el W-Value y el p-value (P-Value).

d) Decisión estadística:

Puesto que el p-value(0.000) < α(0.05), los resultados reflejan suficiente evidencia para rechazar la hipótesis nula (H_0) y aceptar la hipótesis alterna (Ha) como cierta. La prueba resultó ser significativa.

4.8 Análisis Estadístico Descriptivo

4.8.1 Incrementar el número de dominios redirigidos

Dado que los valores de la intervención no presentan variabilidad, se realizó el análisis estadístico descriptivo. Se aplicó el instrumento Microsoft Edge DevTools y la revisión de logs para medir el número de dominios redirigidos. La Tabla 23 presenta los resultados para este indicador. Las Figuras 82 y 83 detallan los resultados del grupo de control y grupo experimental.

Tabla 23

Resultados para número de dominios redirigidos

Indicador		
Número de dominios redirigidos		
Grupo	$\bar{X}$ **(n=30)**	**Resultado**
Gc	0	Se mantuvo el acceso al site, pero no hubo ninguna redirección.
Ge	3	Redirección de los 3 dominios alternos hacia el dominio principal.

Nota: El número de dominios redirigidos incrementó a 3. Esto significa que el 100% de las peticiones de accesos por dominios alternos son redirigidas para acceder mediante el dominio principal del servicio. La implementación de la arquitectura de enrutamiento permitió pasar de 0 a 3 dominios redirigidos en el 100% de los casos evaluados.

Figura 82

Resultados del Grupo de Control en número de dominios redirigidos

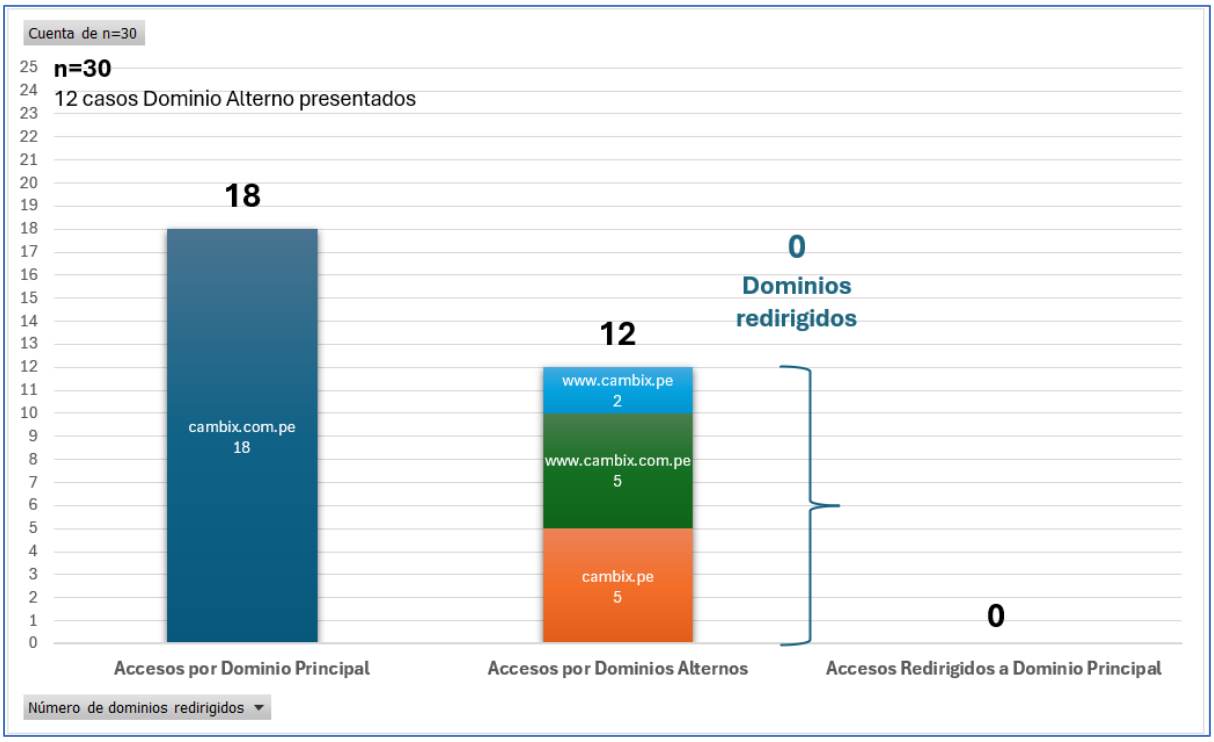
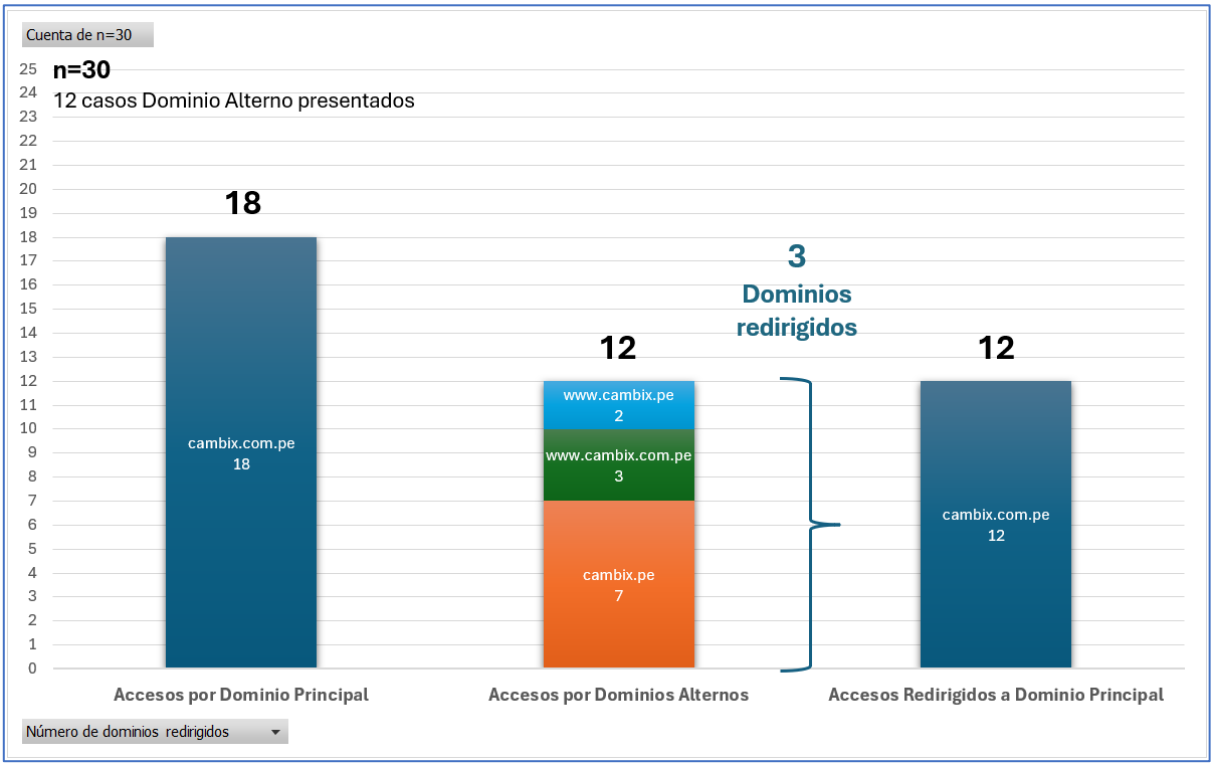


Figura 83

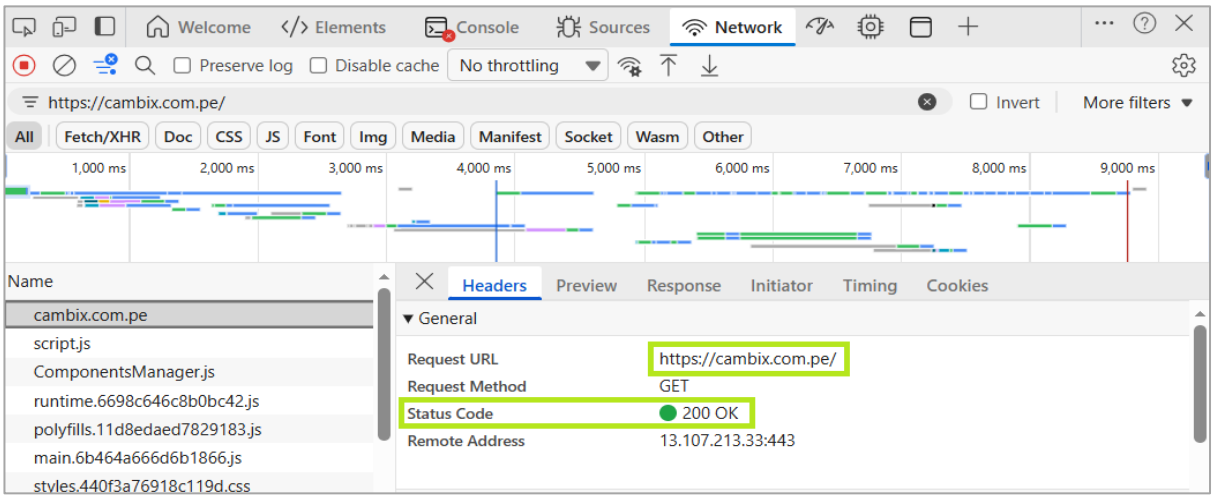
Resultados del Grupo Experimental en número de dominios redirigidos



Las Figuras 84, 85, 86 y 87 evidencian el resultado a partir de la revisión de códigos de estado de respuesta HTTP.

Figura 84

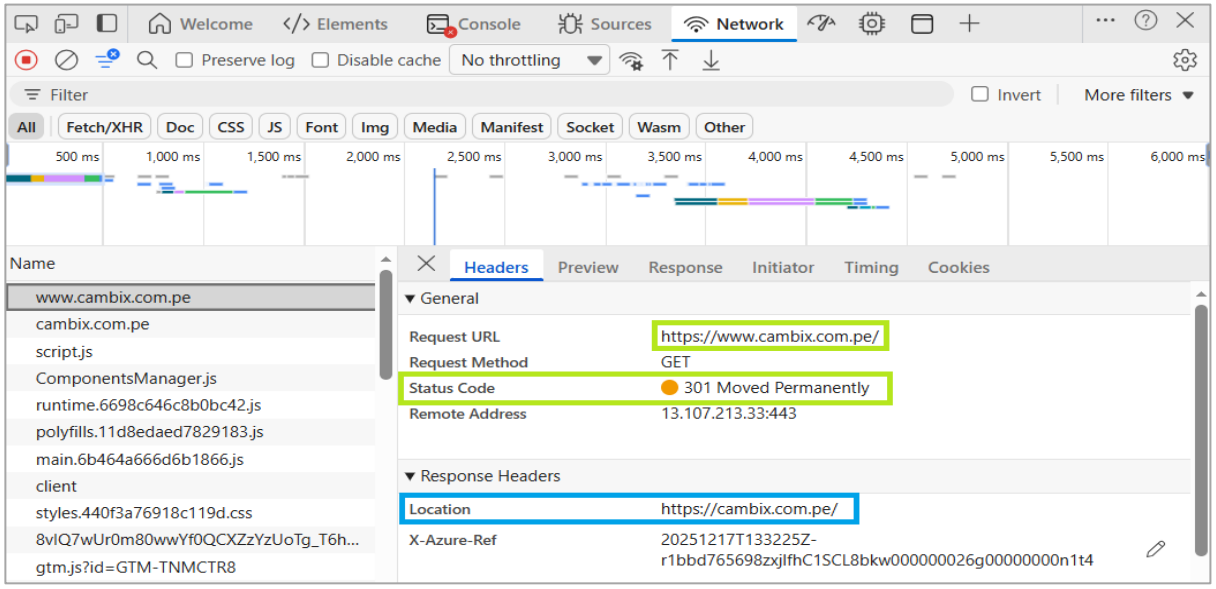
Revisión de códigos de estado de respuesta HTTP con Microsoft Edge DevTools – 1



Nota: Mediante el dominio principal el código de respuesta HTTP es 200, lo cual significa que la solicitud ha tenido éxito.

Figura 85

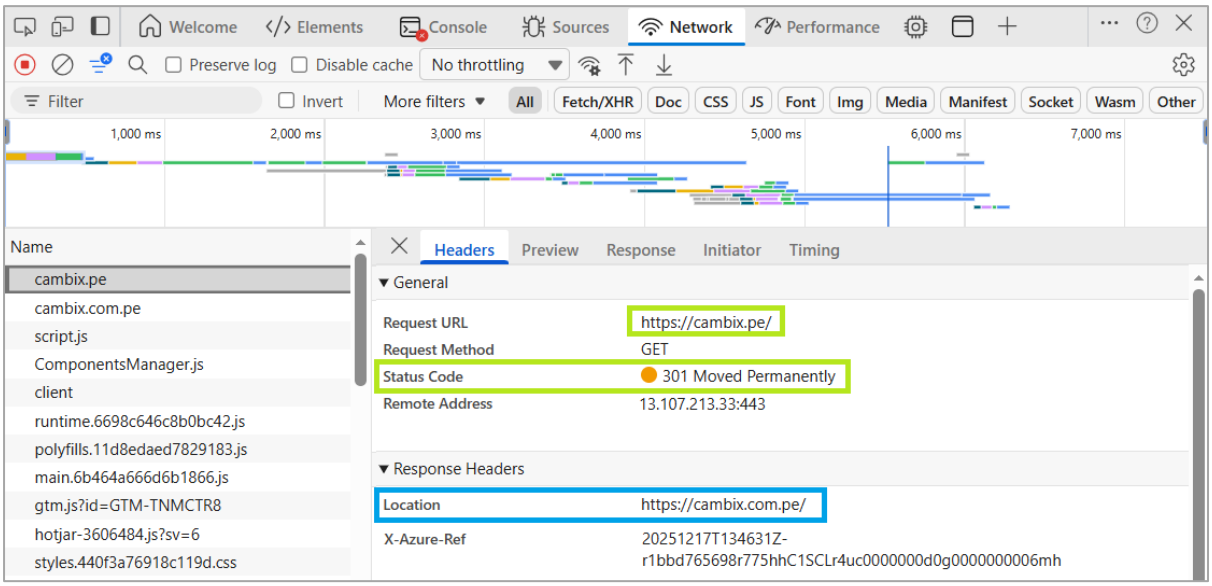
Revisión de códigos de estado de respuesta HTTP con Microsoft Edge DevTools – 2



Nota: Mediante el dominio alterno el código de respuesta HTTP es 301, lo cual significa que la solicitud ha sido redirigida con éxito al dominio principal.

Figura 86

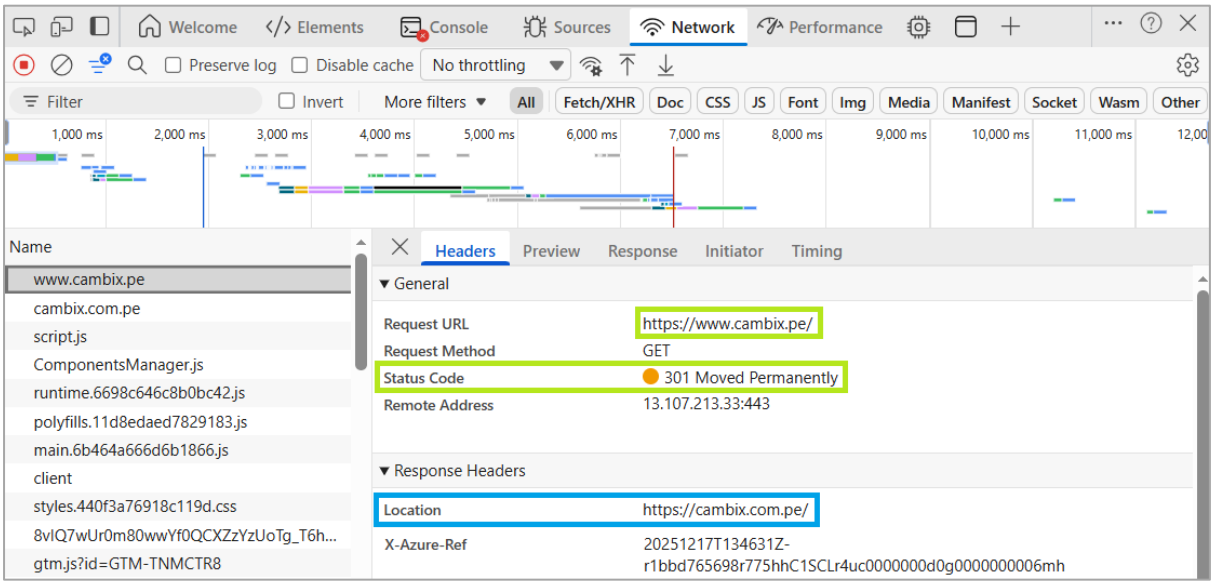
Revisión de códigos de estado de respuesta HTTP con Microsoft Edge DevTools - 3



Nota: Mediante el dominio alterno el código de respuesta HTTP es 301, lo cual significa que la solicitud ha sido redirigida con éxito al dominio principal.

Figura 87

Revisión de códigos de estado de respuesta HTTP con Microsoft Edge DevTools - 4



Nota: Mediante el dominio alterno el código de respuesta HTTP es 301, lo cual significa que la solicitud ha sido redirigida con éxito al dominio principal.

4.8.2 Disminuir el número de dominios expuestos hacia el navegador web del cliente

Dado que los valores de la intervención no presentan variabilidad, se realizó el análisis estadístico descriptivo. Se aplicó el instrumento Mozilla Firefox Private Browsing y la revisión de logs para medir el número de dominios expuestos. La Tabla 24 presenta los resultados. Las Figuras 88 y 89 detallan los resultados del grupo de control y grupo experimental. La Figura 90 evidencia el resultado a partir de la revisión de dominios expuestos en la navegación web.

Tabla 24

Resultados para número de dominios expuestos

Indicador		
Número de dominios expuestos hacia el navegador web del cliente		
Grupo	$\bar{X}$ ***(n=30)***	**Resultado**
Gc	4	Persistió la ambigüedad por múltiples dominios expuestos.
Ge	1	Focalización al exponer únicamente el dominio principal.

Nota: El número de dominios expuestos disminuyó a 1. Esto significa que para el 100% de los accesos al servicio se expone únicamente el dominio principal en la barra de direcciones del navegador web del cliente.

Figura 88

Resultados del Grupo de Control en número de dominios expuestos

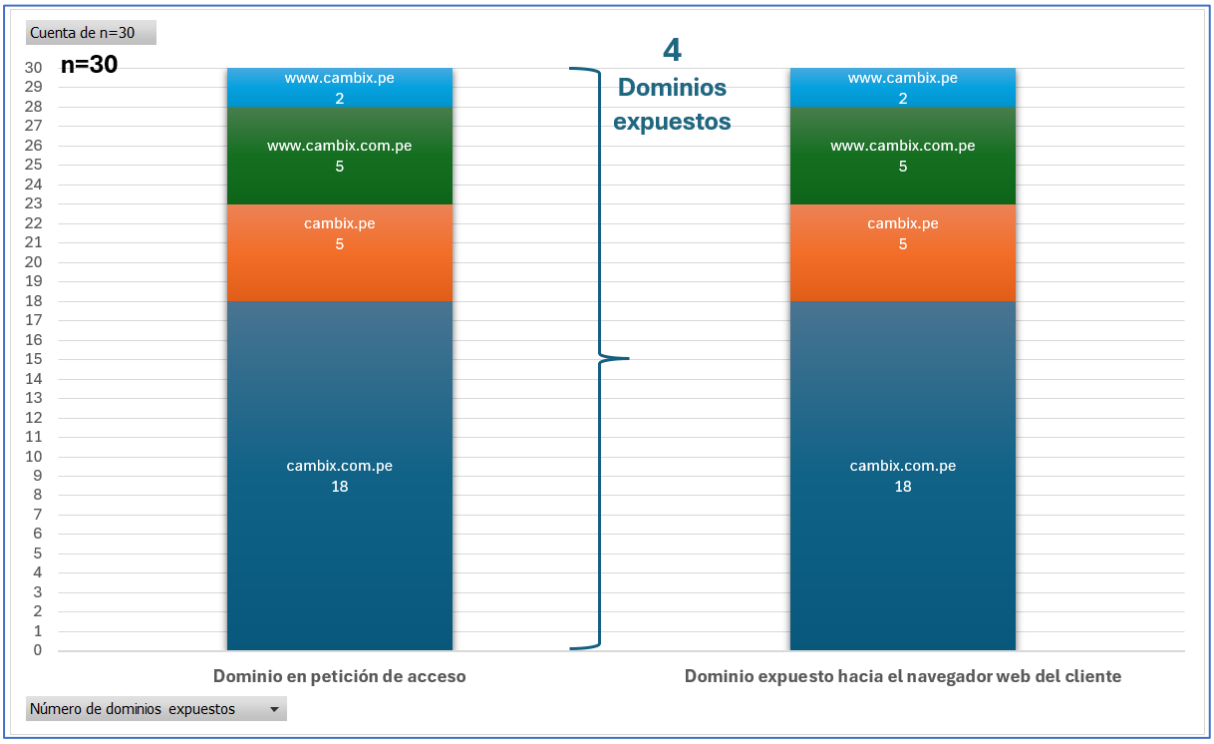


Figura 89

Resultados del Grupo Experimental en número de dominios expuestos

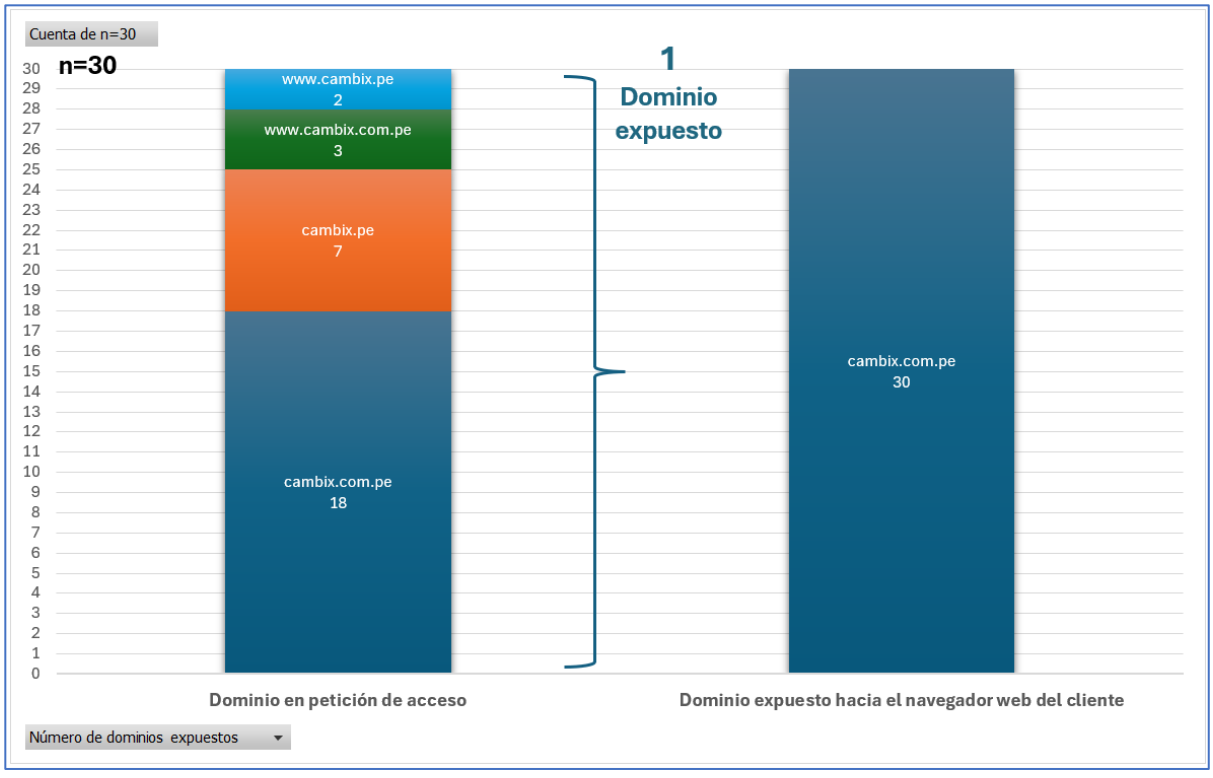
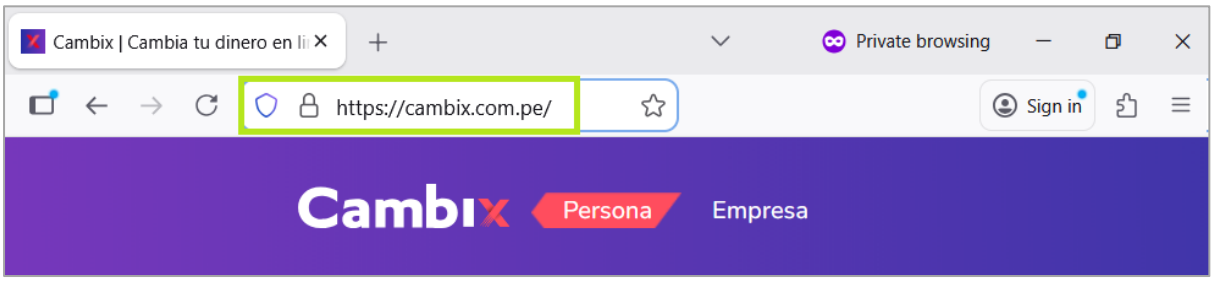


Figura 90

Revisión de dominios expuestos en navegación web con Mozilla Firefox Private Browsing



Nota: Mediante cualquier dominio, siempre se expone con éxito únicamente el dominio principal en la barra de direcciones del navegador web del cliente. Adaptado de Cambix. (s.f.).

4.8.3 Incrementar el número de dominios con redirección de HTTP a HTTPS

Dado que los valores de la intervención no presentan variabilidad, se realizó el análisis estadístico descriptivo. Se aplicaron los instrumentos Digicert SSL Certificate Checker y Microsoft Edge DevTools, así como la revisión de logs, para medir el número de dominios con redirección de HTTP a HTTPS. La Tabla 25 presenta los resultados.

Tabla 25

Resultados para número de dominios con redirección HTTPS

Indicador		
Número de dominios con redirección de HTTP a HTTPS		
Grupo	***X̄ (n=30)***	**Resultado**
Gc	0	No se presentó ninguna redirección a nivel de protocolo HTTPS.
Ge	4	Redirección de peticiones a nivel de protocolo HTTPS para forzar la navegación segura.

Nota: El número de dominios con redirección de HTTP a HTTPS incrementó a 4. El 100% de las peticiones originadas con el protocolo HTTP son redirigidas a HTTPS.

Figura 91

Resultados del Grupo de Control en número de dominios con redirección HTTPS

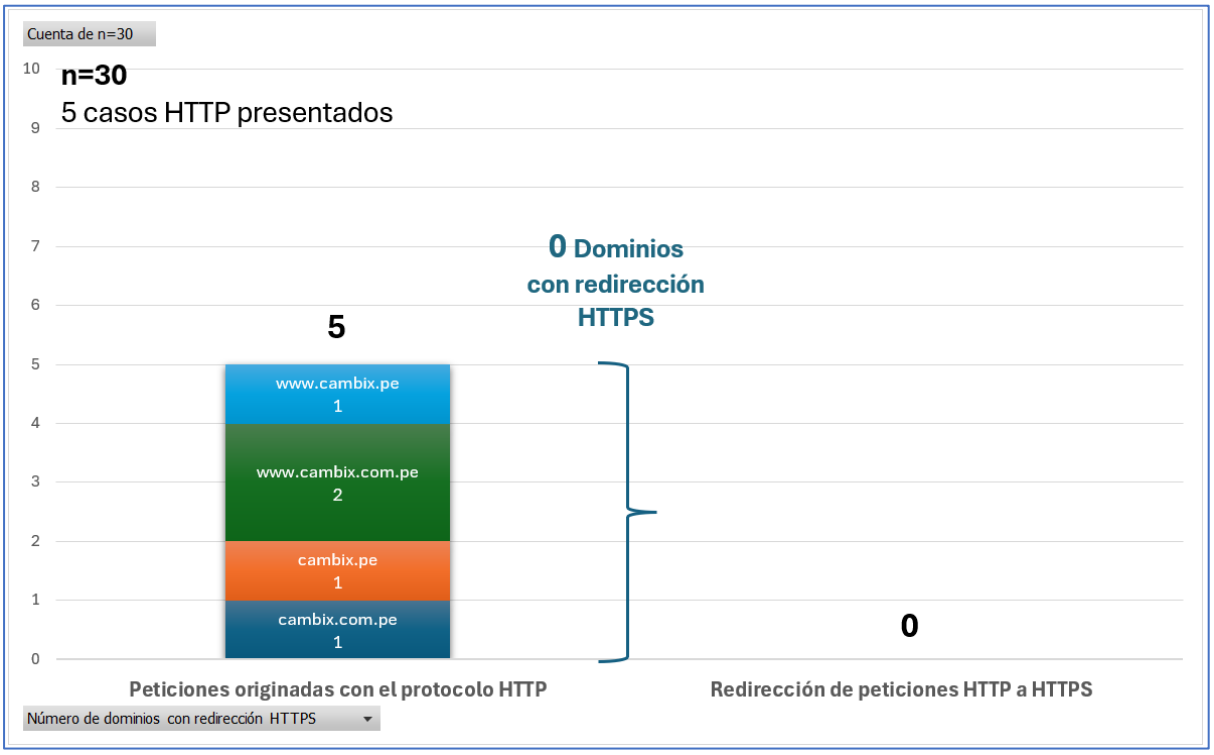
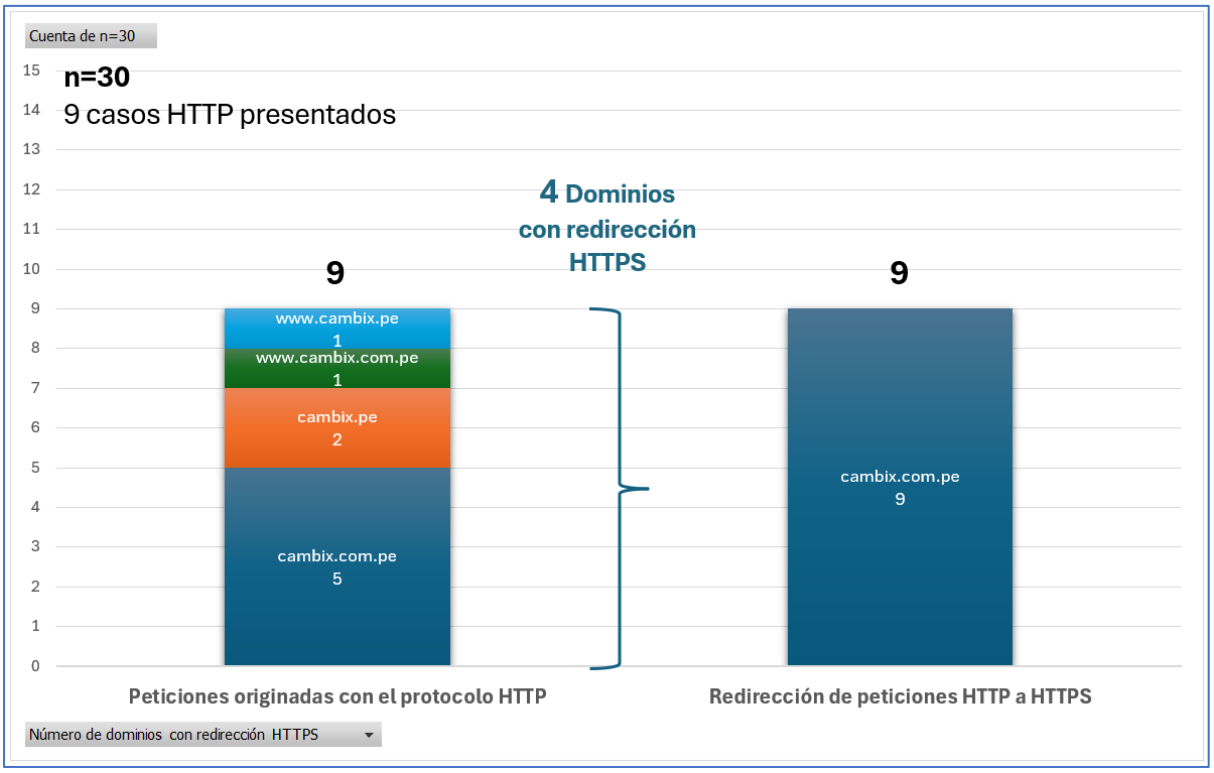


Figura 92

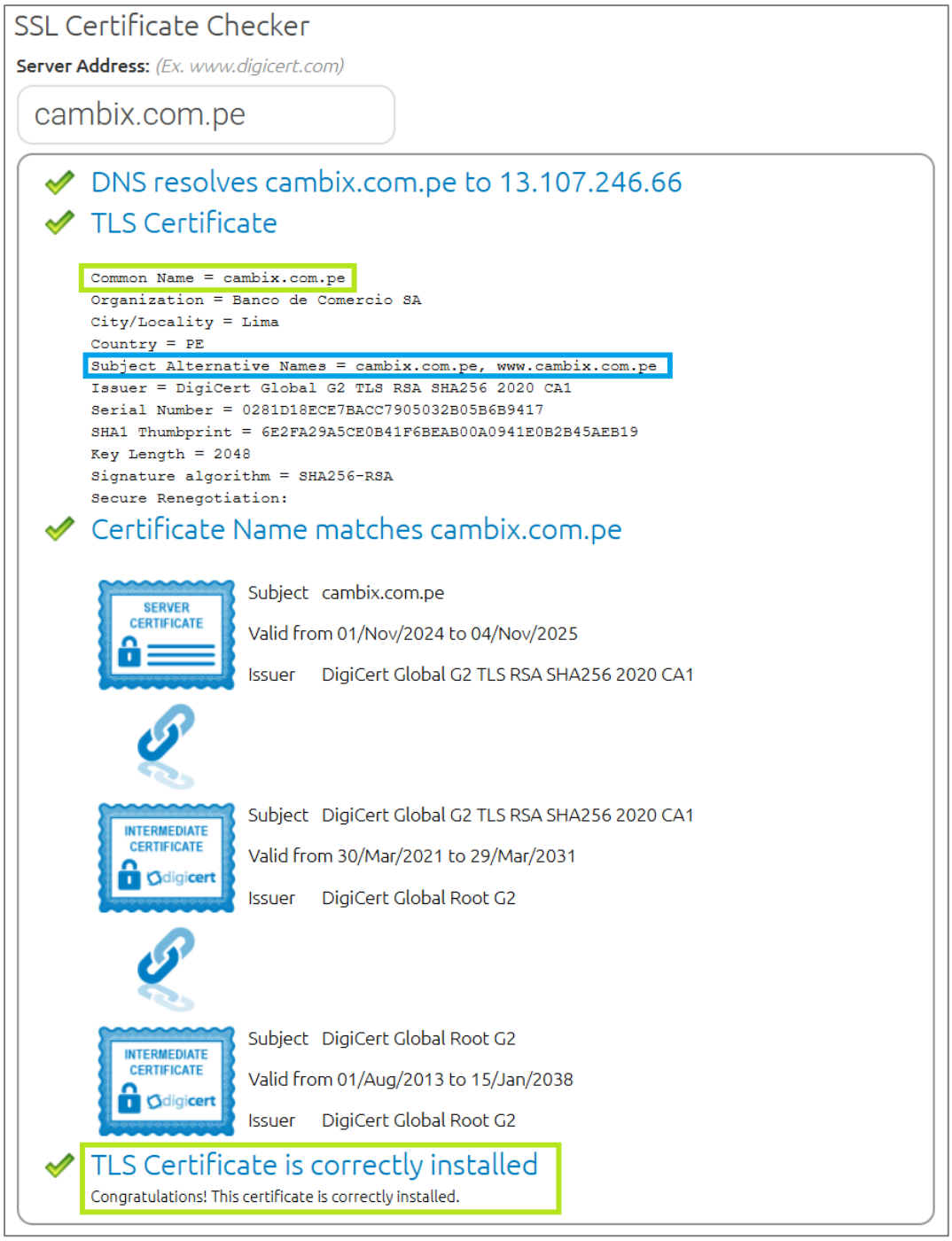
Resultados del Grupo Experimental en número de dominios con redirección HTTPS



La Figura 93 evidencia el resultado a partir de la revisión de certificados digitales, mientras la Figura 94 a partir de la revisión de códigos de estado de respuesta HTTP.

Figura 93

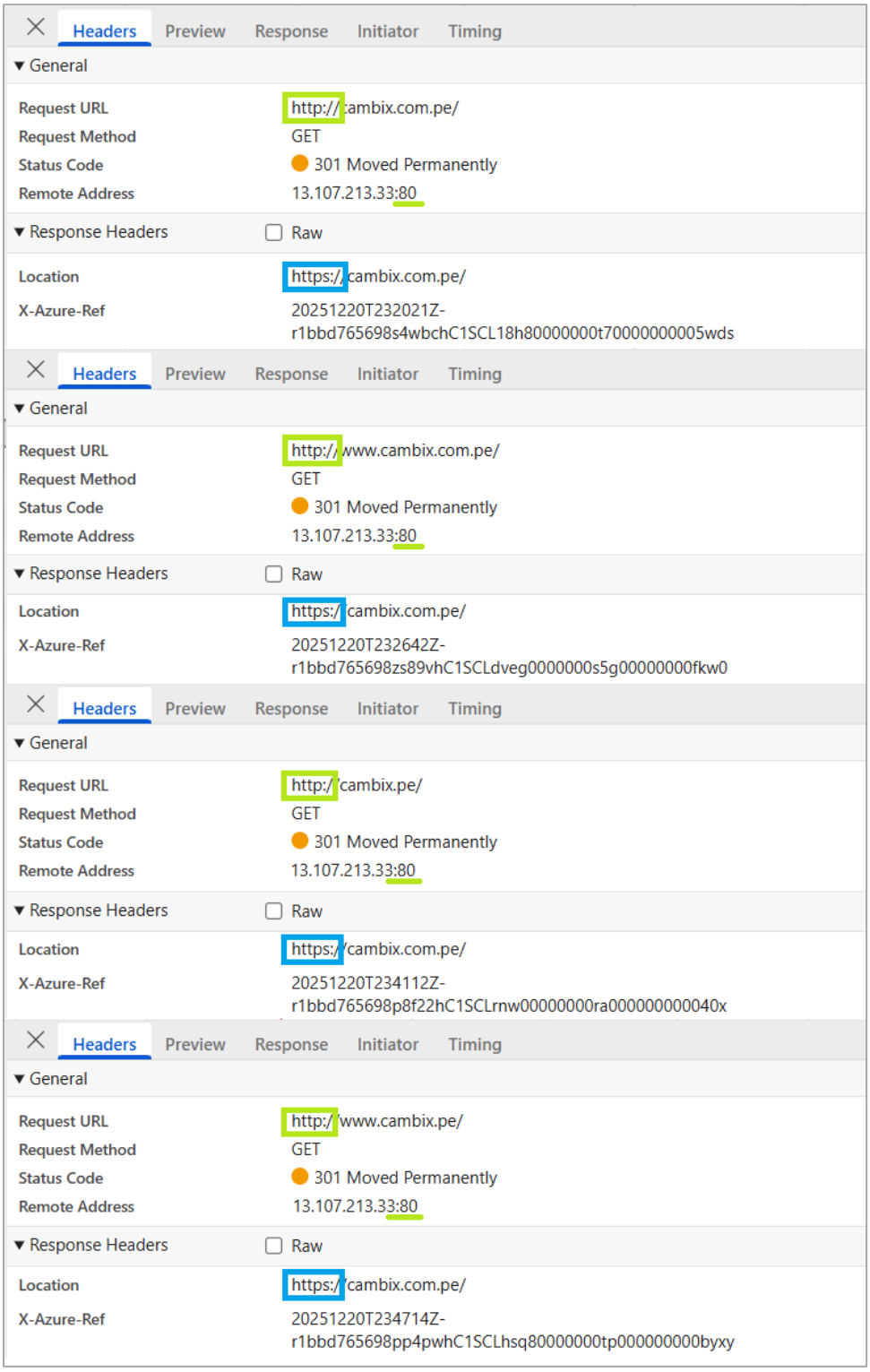
Revisión de certificados digitales con Digicert SSL Certificate Checker



Nota: Se verifica que el certificado digital está instalado correctamente. Adaptado de *SSL Installation Diagnostics Tool* por Digicert (DigiCert, Inc., s.f.-b).

Figura 94

Revisión de códigos de estado de respuesta HTTP con Microsoft Edge DevTools



Nota: Mediante el protocolo HTTP en cualquier dominio el código de respuesta es 301, lo cual significa que la petición ha sido redirigida con éxito al protocolo HTTPS.

4.8.4 Habilitar una solución de seguridad WAF

Dado que los valores de la intervención no presentan variabilidad, se realizó el análisis estadístico descriptivo. Se aplicó el instrumento Azure Log Analytics y la revisión de logs para cuantificar la habilitación de la solución de seguridad WAF. La Tabla 26 presenta los resultados para este indicador. La Figura 95 evidencia el resultado a partir de la revisión de logs.

Tabla 26

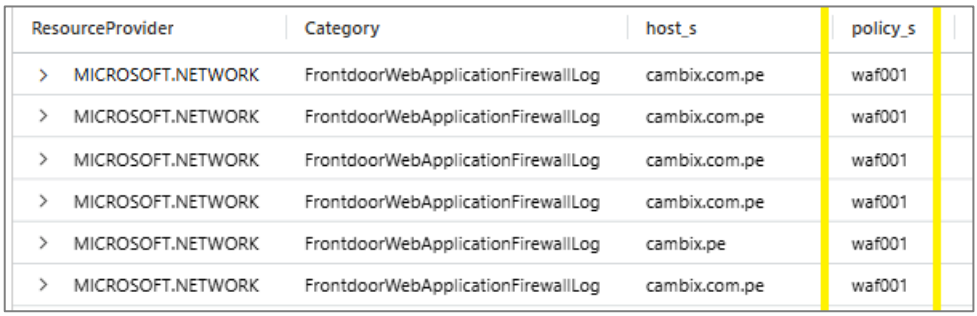
Resultados para número de soluciones de seguridad WAF

Indicador		
Número de soluciones de seguridad WAF		
Grupo Experimental	***X̄ (n=30)***	**Resultado**
Gc	0	Se mantuvo el acceso al site, pero sin ninguna solución WAF protegiéndolo.
Ge	1	Habilitación de una solución WAF como capa de seguridad a nivel de aplicación.

Nota: El número de soluciones de seguridad WAF incrementó a 1. El 100% de las solicitudes de acceso son inspeccionadas por la solución de seguridad WAF desplegada.

Figura 95

Revisión de logs con Azure Log Analytics



ResourceProvider	Category	host_s	policy_s
MICROSOFT.NETWORK	FrontdoorWebApplicationFirewallLog	cambix.com.pe	waf001
MICROSOFT.NETWORK	FrontdoorWebApplicationFirewallLog	cambix.com.pe	waf001
MICROSOFT.NETWORK	FrontdoorWebApplicationFirewallLog	cambix.com.pe	waf001
MICROSOFT.NETWORK	FrontdoorWebApplicationFirewallLog	cambix.com.pe	waf001
MICROSOFT.NETWORK	FrontdoorWebApplicationFirewallLog	cambix.pe	waf001
MICROSOFT.NETWORK	FrontdoorWebApplicationFirewallLog	cambix.com.pe	waf001

Nota: La solución WAF ha sido desplegada y se encuentra en operación, inspeccionando el tráfico web entrante para la protección del servicio. Se adjunta Anexo F con consulta KQL en Azure Logs Analytics.

Figura 96

Resultados del Grupo de Control en número de soluciones de seguridad WAF

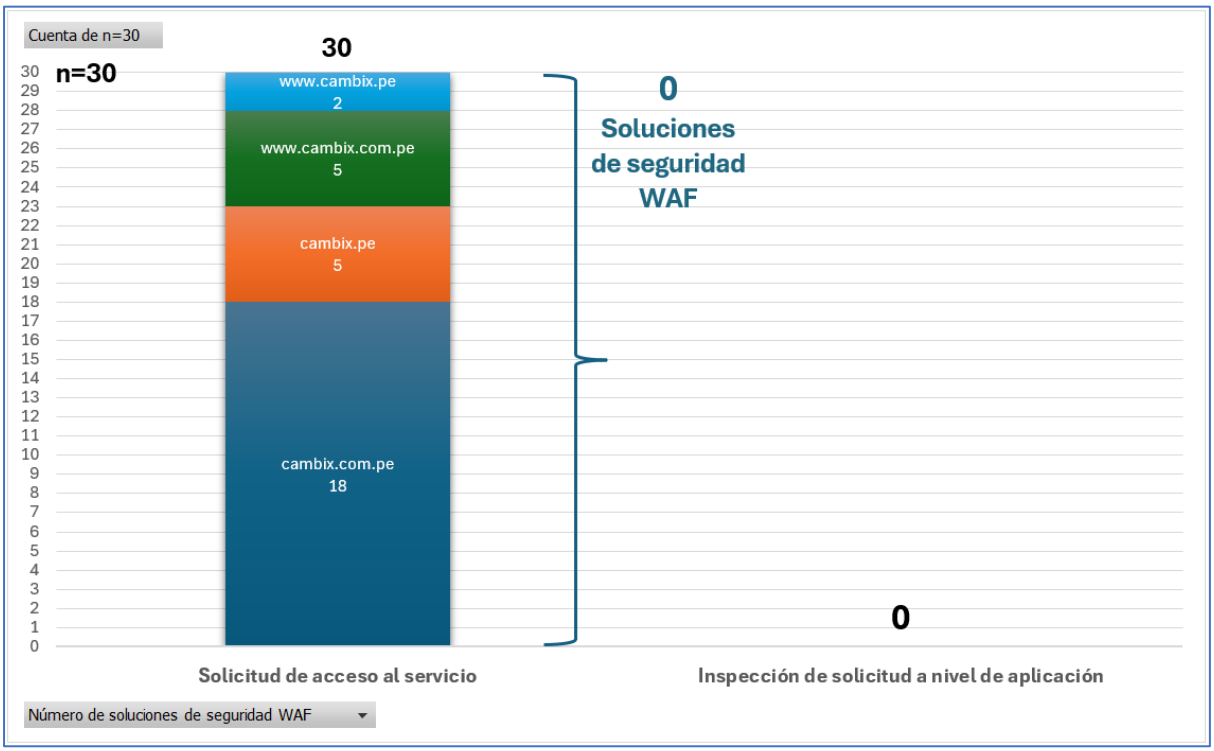
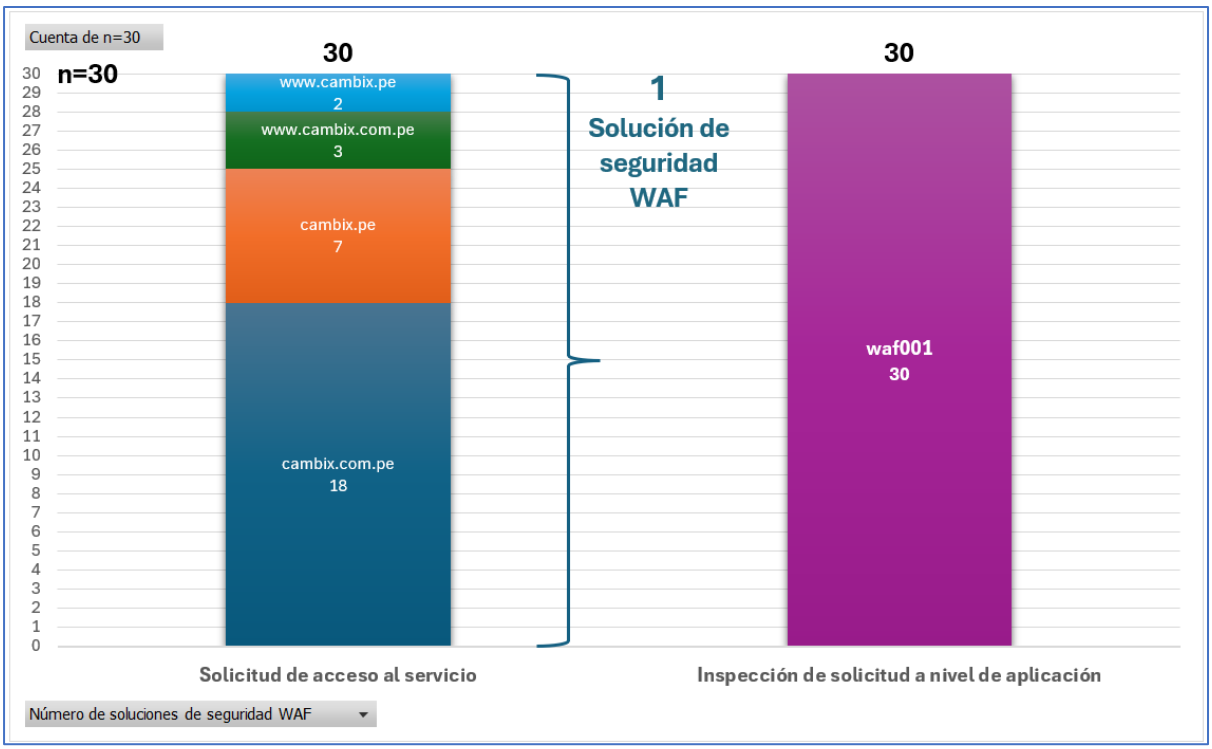


Figura 97

Resultados del Grupo Experimental en número de soluciones de seguridad WAF



Las Figuras 98, 99, 100 presentan la extracción y análisis de los eventos generados por la solución WAF, evaluando su comportamiento ante solicitudes potencialmente maliciosas.

Figura 98

Modo de operación y acción tomada en tráfico malicioso

host_s	policy_s	policyMode_s	action_s	clientIP_s
cambix.com.pe	waf001	prevention	Block	185.107.80.53
cambix.com.pe	waf001	prevention	Block	38.25.17.77
cambix.com.pe	waf001	prevention	Block	38.25.17.77
cambix.com.pe	waf001	prevention	Block	38.25.26.158
cambix.pe	waf001	prevention	Block	185.107.80.53
cambix.com.pe	waf001	prevention	Block	2800:4b0:430a:a8...

Nota: La acción “Block” indica que la solicitud fue bloqueada al ser identificada como tráfico malicioso, en base a las reglas de inteligencia de amenazas y configuración de la solución.

Figura 99

Intentos de ataques dirigidos a rutas específicas de la aplicación

action_s	clientIP_s	requestUri_s
Block	185.107.80.53	https://cambix.com.pe:443/.git/config?sR6=niOe7o8d&p3hH...
Block	38.25.17.77	https://cambix.com.pe:443/?gbraid=0AAAAApnuW_P-uK3YEC...
Block	38.25.17.77	https://cambix.com.pe:443/?gbraid=0AAAAApnuW_P-uK3YEC...
Block	38.25.26.158	https://cambix.com.pe:443/?utm_medium=cpc&utm_source=...
Block	185.107.80.53	https://cambix.pe:443/.git/config?2gWG=k8iLv6&oUk0BWSrs...
Block	2800:4b0:430a:a8...	https://cambix.com.pe:443/?utm_medium=cpc&utm_source=...
Block	154.83.103.12	http://cambix.com.pe:80/.git/HEAD
Block	154.83.103.12	http://cambix.pe:80/.git/HEAD
Block	2602:fa59:4:1d4::1	http://cambix.pe:80/.env
Block	172.184.190.202	http://cambix.pe:80/.env
Block	18.246.68.158	https://www.cambix.com.pe:443/
Block	132.251.1.143	https://cambix.com.pe:443/?utm_medium=cpc&utm_source=...
Block	200.41.86.1	https://cambix.com.pe:443/?utm_medium=cpc&utm_source=...
Block	45.142.193.251	https://cambix.com.pe:443/
Block	172.184.190.202	http://cambix.pe:80/.env

Nota: La URI de cada solicitud evidencia intentos de ataque en los dominios, incluyendo actividades de exploración de vulnerabilidades mediante el acceso a recursos potencialmente sensibles. Por ejemplo, solicitudes hacia la ruta /.env intentan acceder al archivo de variables de entorno, que puede contener credenciales y claves críticas para la seguridad.

Figura 100

Regla de seguridad activada y detalle del tipo de ataque detectado

requestUri_s	ruleName_s	details_msg_s
https://cambix.com.pe:443/.git/config?sR6=niOe7o8d&p3hH...	Microsoft_DefaultRuleSet-1.1-LFI-930130	Restricted File Access Attempt
https://cambix.com.pe:443/?gbraid=0AAAAApnuW_P-uK3YEC...	Microsoft_DefaultRuleSet-1.1-SQLI-942440	SQL Comment Sequence Detected.
https://cambix.com.pe:443/?gbraid=0AAAAApnuW_P-uK3YEC...	Microsoft_DefaultRuleSet-1.1-SQLI-942440	SQL Comment Sequence Detected.
https://cambix.com.pe:443/?utm_medium=cpc&utm_source=...	Microsoft_DefaultRuleSet-1.1-SQLI-942440	SQL Comment Sequence Detected.
https://cambix.pe:443/.git/config?2gWG=k8iLv6&oUk0BWSrs...	Microsoft_DefaultRuleSet-1.1-LFI-930130	Restricted File Access Attempt
https://cambix.com.pe:443/?utm_medium=cpc&utm_source=...	Microsoft_DefaultRuleSet-1.1-SQLI-942440	SQL Comment Sequence Detected.
http://cambix.com.pe:80/.git/HEAD	Microsoft_DefaultRuleSet-1.1-LFI-930130	Restricted File Access Attempt
http://cambix.pe:80/.git/HEAD	Microsoft_DefaultRuleSet-1.1-LFI-930130	Restricted File Access Attempt
http://cambix.pe:80/.env	Microsoft_DefaultRuleSet-1.1-LFI-930130	Restricted File Access Attempt
http://cambix.pe:80/.env	Microsoft_DefaultRuleSet-1.1-LFI-930130	Restricted File Access Attempt
https://www.cambix.com.pe:443/	Microsoft_BotManagerRuleSet-1.0-BadBots...	Malicious bots that have falsified their identity
https://cambix.com.pe:443/?utm_medium=cpc&utm_source=...	Microsoft_DefaultRuleSet-1.1-SQLI-942440	SQL Comment Sequence Detected.
https://cambix.com.pe:443/?utm_medium=cpc&utm_source=...	Microsoft_DefaultRuleSet-1.1-SQLI-942440	SQL Comment Sequence Detected.
https://cambix.com.pe:443/	Microsoft_BotManagerRuleSet-1.0-BadBots...	Malicious bots that have falsified their identity
http://cambix.pe:80/.env	Microsoft_DefaultRuleSet-1.1-LFI-930130	Restricted File Access Attempt

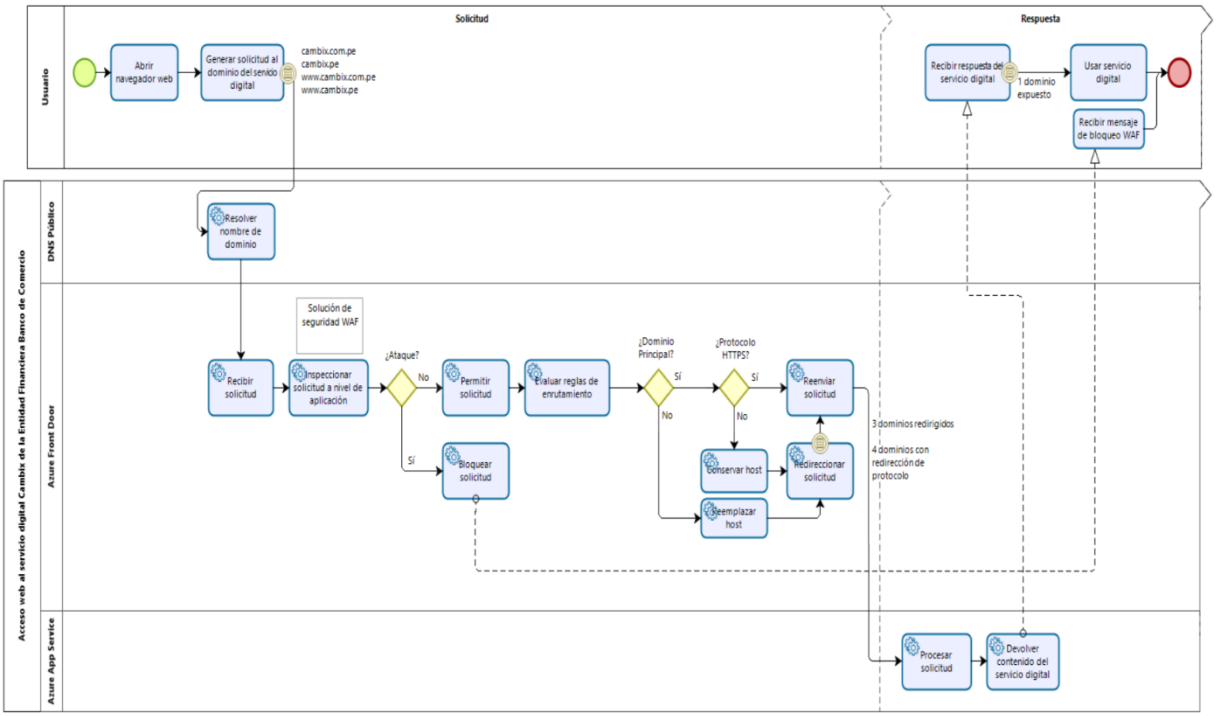
Nota: Se aprecia la regla de seguridad activada en cada evento, esto permite analizar el comportamiento del tráfico malicioso y establecer medidas que contribuyan a fortalecer la seguridad del servicio.

4.9 Nuevo proceso de acceso web al servicio digital

La Figura 101 muestra el nuevo flujograma del proceso de acceso web al servicio digital de Cambix, en donde sea cual sea el dominio o protocolo, se mejora el tiempo de respuesta, siempre se accede al servicio únicamente a través del dominio principal, con el protocolo HTTPS, y con la inspección de la capa de seguridad WAF, gracias a la Arquitectura de Enrutamiento en Azure Front Door implementada.

Figura 101

Nuevo proceso de Acceso web al servicio digital Cambix de la Entidad Financiera Banco de Comercio



Nota: Se aplica redirección de los 3 dominios alternos hacia el dominio principal, focalización al exponer únicamente el dominio principal, redirección de peticiones a nivel de protocolo HTTPS para forzar la navegación segura y una solución WAF habilitada como capa de seguridad a nivel de aplicación. Se adjunta Anexo G con una vista más amplia del presente flujograma.

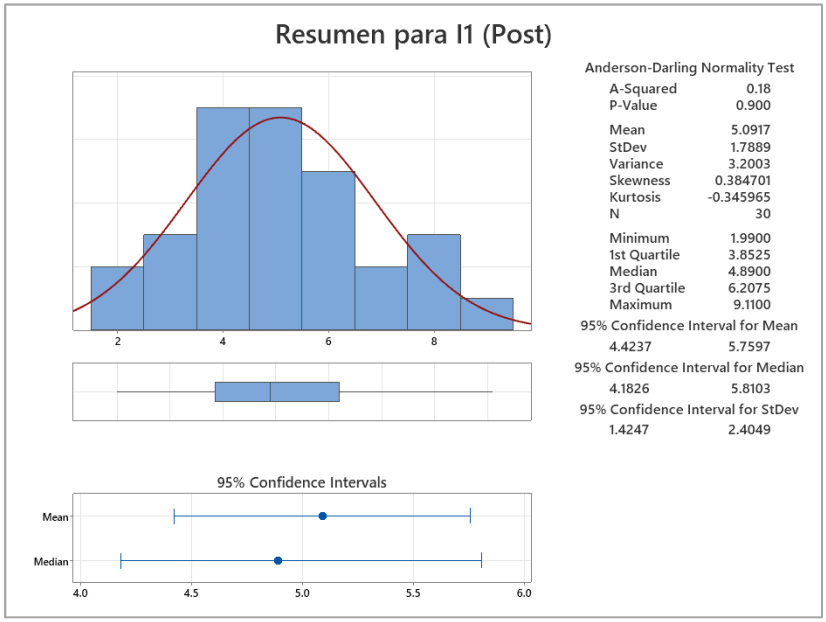
V. DISCUSIÓN DE RESULTADOS

La adopción de soluciones en la nube ha experimentado un crecimiento considerable en los últimos años, impulsando la transformación digital y la evolución de las tecnologías de comunicación empleadas por las organizaciones para la publicación de sus servicios. Esta investigación dio importancia a ese notable crecimiento, mediante una solución tecnológica enfocada en mejorar la publicación y acceso de los servicios en la nube. Los resultados obtenidos demuestran que la implementación de la Arquitectura de Enrutamiento en Azure Front Door tuvo un impacto significativo en la mejora del acceso vía web al servicio digital de Cambix del Banco de Comercio, mediante la mejora de los valores de los indicadores del Ge.

Indicador 1: Tiempo de respuesta

Figura 102

Resultados de Estadística Descriptiva



Aproximadamente el 95% de los tiempos de respuesta del servicio se ubican entre 2 desviaciones estándar del promedio (media), lo que implican que se encuentran dentro de 4.42 a 5.76 segundos, con una media de 5.09 segundos y una desviación estándar de 1.789.

Indicador 2: Número de dominios redirigidos

La implementación de la Arquitectura de Enrutamiento en Azure Front Door permitió pasar de 0 a 3 dominios redirigidos en el 100% de los casos evaluados. Este incremento en la redirección se atribuye directamente a la intervención del estímulo experimental.

Indicador 3: Número de dominios expuestos hacia el navegador web del cliente

El número de dominios expuestos disminuyó de 4 a 1 en el 100% de los casos evaluados. Esto significa que en todos los accesos al servicio se expone únicamente el dominio principal en la barra de direcciones del navegador web del cliente. La focalización del dominio en el acceso se atribuye directamente a la intervención del estímulo experimental.

Indicador 4: Número de dominios con redirección de HTTP a HTTPS

El número de dominios con redirección de HTTP a HTTPS incrementó de 0 a 4 en el 100% de los casos evaluados. La redirección al protocolo HTTPS para forzar la navegación segura se atribuye directamente a la intervención del estímulo experimental.

Indicador 5: Número de soluciones de seguridad WAF

El número de soluciones de seguridad WAF incrementó de 0 a 1 en el 100% de los casos evaluados. La habilitación de la solución WAF como capa de seguridad a nivel de aplicación se atribuye directamente a la intervención del estímulo experimental.

Estos resultados son semejantes a los de Perera (2023), quien en su investigación acerca de la mejora del rendimiento de las aplicaciones web demostró que el uso de arquitecturas integradas con tecnologías modernas mejora significativamente los tiempos de respuesta y estabilidad en la comunicación, mostrando mayor rendimiento frente a arquitecturas tradicionales que presentan tiempos de respuesta más altos. Así también, son semejantes a los resultados de Martínez (2022), quien demostró las capacidades de mecanismos de redirección de tráfico basados en nuevas tecnologías para la transparencia en el acceso y distribución de servicios. Así también, Cuiña (2021) destaca la eficacia de la implementación de un WAF

como medida efectiva y recomendable para fortalecer la seguridad de aplicaciones web frente a amenazas actuales.

Los resultados respaldan las hipótesis formuladas, validando la efectividad de la solución propuesta para mejorar el acceso al servicio digital de la entidad financiera.

Actualmente, Azure Front Door ofrece tres versiones para el despliegue de soluciones: Classic, Standard y Premium. Si bien la presente implementación se realizó utilizando la versión Classic, cabe señalar que Microsoft ha anunciado el retiro y migración de esta versión a partir del 31 de marzo de 2027 (Microsoft Learn, 2025). Esta situación no afecta los resultados obtenidos en esta investigación, sino más bien representa una consideración informada, profesional y consciente del entorno tecnológico actual y de su evolución. Por lo tanto, cualquier implementación futura deberá contemplar la migración hacia las versiones Standard o Premium, las cuales mantienen compatibilidad funcional con la arquitectura utilizada en esta investigación. Esta medida es importante para garantizar el soporte, la continuidad operativa y el mantenimiento sostenible de la solución a largo plazo.

La solución ofrece un diseño inteligente para la gestión efectiva del tráfico web y la experiencia del usuario. La implementación de reglas de enrutamiento representa una capacidad técnica clave, especialmente útil en servicios web que operan o planean operar con múltiples dominios como puntos de acceso.

VI. CONCLUSIONES

6.1. Se comprueba que la implementación de una Arquitectura de Enrutamiento en Azure Front Door, utilizando Microsoft Azure, mejora el acceso vía web al servicio digital Cambix de la entidad financiera Banco de Comercio, centralizando el tráfico de múltiples dominios en un único dominio principal, mejorando el tiempo de respuesta y fortaleciendo la seguridad del servicio mediante la integración de un Firewall de Aplicaciones Web para protegerlo contra bots y amenazas comunes en la web.

6.2. Se aprecia que la implementación de la Arquitectura de Enrutamiento en Azure Front Door disminuye significativamente el tiempo de respuesta para el acceso al servicio.

6.3. El indicador correspondiente al número de dominios redirigidos incrementó de 0 a 3, permitiendo así la redirección de tres dominios alternos hacía el dominio principal del servicio.

6.4. El indicador correspondiente al número de dominios expuestos hacia el navegador del cliente se redujo de 4 a 1, lo que permitió focalizar la marca al exponer únicamente el dominio principal.

6.5. El indicador correspondiente al número de dominios con redirección de HTTP a HTTPS incrementó de 0 a 4, alcanzando el valor esperado de redirección de peticiones a nivel de protocolo. Esto permitió forzar la navegación segura mediante HTTPS en los cuatro dominios y garantizar el acceso al servicio exclusivamente a través del dominio principal utilizando el protocolo seguro HTTPS.

6.6. El indicador correspondiente al número de soluciones de seguridad WAF mejoró al pasar de 0 a 1, tras la integración de una solución de seguridad WAF configurada para controlar el tráfico entrante al servicio digital. La solución WAF empleó reglas administradas basadas en la inteligencia de amenazas global de Microsoft Azure, proporcionando protección frente a vulnerabilidades y ataques comunes en la web. Además, se definieron

reglas personalizadas para asegurar el cumplimiento de políticas de seguridad del Banco, restringiendo el tráfico proveniente de países identificados como fuentes recurrentes de actividades maliciosas, tales como Rusia, China, Corea del Norte, entre otros.

6.7. Se confirman la hipótesis general y las hipótesis específicas formuladas, ya que la implementación de una Arquitectura de Enrutamiento en Azure Front Door mejora de forma significativa el acceso web al servicio digital.

6.8. Existe una relación de causa y efecto entre la implementación realizada y la mejora evidenciada en el acceso vía web al servicio digital Cambix de la entidad financiera Banco de Comercio del Perú.

VII. RECOMENDACIONES

7.1. Se recomienda utilizar la presente tesis de investigación como sustento para la implementación de Arquitecturas de Enrutamiento en la nube, teniendo como base los resultados obtenidos a fin de optimizar la estrategia y la infraestructura asociadas a los sistemas de publicación y acceso a servicios digitales públicos a través de Internet.

7.2. Se recomienda implementar Azure Front Door en entidades que disponen de múltiples dominios para sus servicios digitales. Cada entidad debe definir sus dominios principales, adecuar la estrategia de redirección y el tratamiento a sus dominios alternos, y configurar de forma personalizada sus soluciones de seguridad, en base a sus necesidades operativas y objetivos institucionales.

7.3. Para servicios digitales que operan con un único dominio, se recomienda comprar los dominios alternativos o similares al dominio inicial, esto como buena práctica para mantener la propiedad y el control de dominios que potencialmente pueden usarse para dar acceso al servicio, prevenir el uso no autorizado, evitar riesgos de suplantación y reforzar seguridad de la marca. Si la estrategia del servicio es mantener activos estos nuevos dominios alternos, entonces se recomienda la implementación de la solución propuesta en esta investigación.

7.4. Para servicios digitales que disponen o planean disponer de un acceso vía aplicación móvil (Android y/o iOS), se recomienda crear un subdominio específico del dominio principal (por ejemplo, apimobile.dominio.com) y vincular ese nuevo subdominio hacía el servicio de Front Door, con una nueva directiva de WAF independiente y destinada específicamente para los accesos móviles. Así también, la aplicación móvil debe ser configurada para apuntar y consumir los servicios a través de este nuevo subdominio.

7.5. Se recomienda investigar la integración de Azure Front Door con otros servicios de Microsoft Azure, como Azure API Management, Azure Virtual Network, Azure Private

Link, Azure DNS, entre otros, con el fin de deshabilitar completamente el acceso público a recursos internos como App Services. Esta integración permite establecer servicios dedicados como Azure Front Door como único punto de entrada para el consumo de servicios en la nube, reforzando la seguridad perimetral. Así mismo, se recomienda usar Azure Front Door en su versión Premium.

7.6. Se recomienda investigar la creación de consultas optimizadas en KQL, orientadas al análisis detallado de los registros de acceso y de eventos generados por el WAF mediante el servicio Azure Log Analytics, esto para mejorar el monitoreo y para optimizar el consumo de recursos que pueden generar consultas KQL más generales.

7.7. Se recomienda gestionar los registros DNS a través de NIC.PE, debido a su flexibilidad para crear registros CNAME sobre dominios apex. En caso de usar GoDaddy, se puede migrar la administración de servidores DNS a Azure DNS Zones para vincular dominios apex con Azure Front Door.

VIII. REFERENCIAS

Amazon Web Services. (s.f.). *What is routing?* https://aws.amazon.com/es/what-is/routing/

Caldas, J. (2016). *Prácticas de gestión en la mejora en la calidad de servicios de Tecnologías de la Información al adoptar Cloud Computing [Tesis de Pregrado].* Lima, Perú: Universidad Científica del Sur.

Cambix. (s.f.). *Un servicio de Banco de Comercio SA.* https://cambix.com.pe/

Carrasco, S. (2019). *Metodología de la investigación científica* (reimpresión, 2 ed.). Lima: Editorial San Marcos.

CertSuperior. (s.f.). *DigiCert.* https://www.certsuperior.com/digicert/

Cuiña, F. J. (2021). *Presentación de soluciones WAF Open Source [Tesis de Posgrado].* Buenos Aires, Argentina: Universidad de Buenos Aires.

DigiCert, Inc. (s.f.-a). *What is a Digital Certificate?* https://www.digicert.com/faq/public-trust-and-certificates/what-is-a-digital-certificate

DigiCert, Inc. (s.f.-b). *DigiCert® SSL Installation Diagnostics Tool.* https://www.digicert.com/help/

Galiveeti, S., Tawalbeh, L., Tawalbeh, M., & El-Latif, A. A. (2021). Cybersecurity Analysis: Investigating the Data Integrity and Privacy in AWS and Azure Cloud Platforms. In Y. Maleh, Y. Baddi, M. Alazab, L. Tawalbeh, & I. Romdhani, *(eds) Artificial Intelligence and Blockchain for Future Cybersecurity Applications. Studies in Big Data, vol 90.* Cham: Springer. doi:https://doi.org/10.1007/978-3-030-74575-2_17

Google Support. (s.f.-a). *Conceptos básicos de DNS.* https://support.google.com/a/answer/48090

Google Support. (s.f.-b). *Redirigir un dominio a una URL o una dirección IP.* https://support.google.com/domains/answer/4522141

Goyes, J. (2020). *Estudio de impacto del modelo cloud computing en la gestión de servicios de información gerencial en la banca privada, Caso: Banco Internacional [Tesis de Maestría].* Quito, Ecuador: Universidad Andina Simón Bolívar.

Hernández, R., & Mendoza, C. (2018). *Metodología de la investigación. Las rutas cuantitativa, cualitativa y mixta.* México D.F.: McGraw-Hill.

International Standard Serial Number. (s.f.). *URN.* https://www.issn.org/es/servicios-y-prestaciones/servicios-en-linea/urn/

Internet Assigned Numbers Authority. (s.f.). *IANA About us.* https://www.iana.org/about

Internet Corporation for Assigned Names and Numbers. (s.f.). *ICANN for Beginners.* https://www.icann.org/en/beginners

Laudon, K. C., & Laudon, J. P. (2012). *Sistemas de Información Gerencial* (12 ed.). (A. V. Romero Elizondo, Trans.) México: Pearson Education.

Llauce, M. (2020). *Implementación de una arquitectura de computación en la nube (cloud computing) diseñada para escalabilidad automática y alta disponibilidad basado en la plataforma de amazon web services (AWS) en la Universidad de Lambayeque [Tesis de Pregrado].* Lima, Perú: Universidad Pedro Ruiz Gallo.

Loaiza, R. (2021). *Cloud Security Posture Management (CSPM) in Azure [Tesis de Pregrado].* Finlandia: Metropolia University of Applied Sciences.

Martínez, D. (2022). *Desarrollo de mecanismos de redirección de tráfico en redes de campus basadas en SDN para distribución de contenido multimedia [Tesis de Maestría].* Madrid, España: Universidad Politécnica de Madrid.

Microsoft Learn. (10 de octubre de 2023d). *Azure Web Application Firewall on Azure Application Gateway bot protection overview.* https://learn.microsoft.com/en-us/azure/web-application-firewall/ag/bot-protection-overview

Microsoft Learn. (11 de julio de 2023f). *Inspect network activity.* https://learn.microsoft.com/en-us/microsoft-edge/devtools-guide-chromium/network/

Microsoft Learn. (15 de julio de 2025). *Migrate Azure Front Door (classic) to Standard or Premium tier.* https://learn.microsoft.com/en-us/azure/frontdoor/migrate-tier

Microsoft Learn. (15 de noviembre de 2023b). *What is the Azure Well-Architected Framework?* https://learn.microsoft.com/en-us/azure/well-architected/what-is-well-architected-framework

Microsoft Learn. (16 de enero de 2024). *Kusto Query Language (KQL) overview.* https://learn.microsoft.com/en-us/azure/data-explorer/kusto/query/

Microsoft Learn. (2 de agosto de 2023h). *Azure Web Application Firewall monitoring and logging.* https://learn.microsoft.com/en-us/azure/web-application-firewall/afds/waf-front-door-monitor?pivots=front-door-classic

Microsoft Learn. (28 de diciembre de 2023g). *Overview of Log Analytics in Azure Monitor.* https://learn.microsoft.com/en-us/azure/azure-monitor/logs/log-analytics-overview

Microsoft Learn. (4 de abril de 2023a). *Routing architecture overview.* https://learn.microsoft.com/en-us/azure/frontdoor/front-door-routing-architecture

Microsoft Learn. (5 de diciembre de 2023c). *What is the Azure portal?* https://learn.microsoft.com/en-us/azure/azure-portal/azure-portal-overview

Microsoft Learn. (7 de diciembre de 2023e). *Overview of DevTools.* https://learn.microsoft.com/en-us/microsoft-edge/devtools-guide-chromium/overview

Mozilla Developer Network Web Docs. (13 de noviembre de 2023c). *HTTPS.* Mozilla Foundation. https://developer.mozilla.org/es/docs/Glossary/HTTPS

Mozilla Developer Network Web Docs. (2 de agosto de 2023h). *What is a URL?* Mozilla Foundation. https://developer.mozilla.org/en-US/docs/Learn/Common_questions/Web_mechanics/What_is_a_URL

Mozilla Developer Network Web Docs. (22 de septiembre de 2023a). *Generalidades del protocolo HTTP.* Mozilla Foundation. https://developer.mozilla.org/es/docs/Web/HTTP/Overview

Mozilla Developer Network Web Docs. (24 de julio de 2023b). *HTTP.* Mozilla Foundation. https://developer.mozilla.org/es/docs/Web/HTTP

Mozilla Developer Network Web Docs. (27 de septiembre de 2023d). *Transport Layer Security (TLS).* Mozilla Foundation. https://developer.mozilla.org/en-US/docs/Web/Security/Defenses/Transport_Layer_Security

Mozilla Developer Network Web Docs. (3 de noviembre de 2023f). *HTTP response status codes.* Mozilla Foundation. https://developer.mozilla.org/en-US/docs/Web/HTTP/Status#information_responses

Mozilla Developer Network Web Docs. (5 de octubre de 2023e). *Redirections in HTTP.* Mozilla Foundation. https://developer.mozilla.org/en-US/docs/Web/HTTP/Redirections#forcing

Mozilla Developer Network Web Docs. (8 de junio de 2023g). *URI.* Mozilla Foundation. https://developer.mozilla.org/en-US/docs/Glossary/URI

Mozilla Support. (s.f.-a). *Private Browsing - Use Firefox without saving history.* Mozilla Foundation. https://support.mozilla.org/en-US/kb/private-browsing-use-firefox-without-history

Mozilla Support. (s.f.-b). *Address bar autocomplete suggestions in Firefox.* Mozilla Foundation. https://support.mozilla.org/en-US/kb/address-bar-autocomplete-firefox

National Institute of Standards and Technology. (12 de mayo de 2022). *NIST Cloud Computing Program - NCCP.* https://www.nist.gov/programs-projects/nist-cloud-computing-program-nccp

Palo Alto Networks. (s.f.). *What Is a WAF? | Web Application Firewall Explained.* https://www.paloaltonetworks.com/cyberpedia/what-is-a-web-application-firewall

Perera, Y. (2023). *Enhancing the front end web applications performance using design patterns and microservices based architecture [Tesis de Pregrado].* Kelaniya, Sri Lanka: University of Kelaniya.

Punto Pe. (s.f.). *Acerca de Punto.pe.* https://punto.pe/acerca.php

Quispe, J. (2021). *Diseño de escalamiento inteligente del Customer Relationship Management (CRM) bajo el modelo de nube hibrida entre azure y universidad privada peruana [Tesis de Pregrado].* Lima, Perú: Universidad Peruana de Ciencias Aplicadas.

Ruiz, A. (2019). *Migración de Servidores a la nube de Microsoft Azure para mejorar la Continuidad de los Servicios TI, de la Fiduciaria en el año 2018 [Tesis de Pregrado].* Lima, Perú: Universidad San Ignacio de Loyola.

Stack Overflow. (20 de junio de 2020). *What is the difference between a URI, a URL, and a URN?* Stack Exchange, Inc. https://stackoverflow.com/posts/1984225/revisions

Tapia, E. (14 de febrero de 2018). *El uso de la banca digital creció un 30% en el Ecuador el año pasado.* Revista Líderes. https://www.revistalideres.ec/lideres/banca-digital-ecuador-tecnologia-informe.html

Vara, A. (2015). *Los 7 pasos para elaborar una Tesis* (1 ed.). Lima, Perú: Editorial Macro.

Yacolca, F., & Lopez, D. (2022). *Sistema Web para el proceso de identificación biométrica con reconocimiento facial de clientes para la aseguradora Pacífico Seguros en Lima, 2021 [Tesis de Pregrado].* Lima, Perú: Universidad Ricardo Palma.

IX. ANEXOS

Anexo A. Matriz de consistencia

Título: Arquitectura de Enrutamiento Front Door, utilizando Microsoft Azure, para mejorar el acceso web al servicio digital de una entidad financiera

Problema General	Objetivo General	Hipótesis General	Variables	Indicadores	
¿De qué manera la implementación de una Arquitectura de Enrutamiento en Azure Front Door, utilizando Microsoft Azure, mejora el acceso vía web al servicio digital de una entidad financiera?	Implementar una Arquitectura de Enrutamiento en Azure Front Door, utilizando Microsoft Azure, para mejorar el acceso vía web al servicio digital de una entidad financiera.	Si se implementa una Arquitectura de Enrutamiento en Azure Front Door, utilizando Microsoft Azure, entonces mejora el acceso vía web al servicio digital de una entidad financiera.	Variable Independiente: Arquitectura de Enrutamiento en Azure Front Door	- Presencia_Ausencia	**Tipo de Investigación:** - Investigación Aplicada **Nivel de Investigación:** - Nivel Explicativo **Población:** N = Indeterminado **Muestra:** n = 30
			Variable Dependiente: Acceso vía web al servicio digital.	- Tiempo de respuesta - Número de dominios redirigidos - Número de dominios expuestos hacia el navegador web del cliente - Número de dominios con redirección de HTTP a HTTPS - Número de soluciones de seguridad WAF	

...Continuación

Variables	Indicadores	Índices	Unidades de medida	Fórmula
Variable Independiente: Arquitectura de Enrutamiento en Azure Front Door	- Presencia_Ausencia	- No, Sí	-	-
Variable Dependiente: Acceso vía web al servicio digital.	- Tiempo de respuesta	- [0.1 s - 30 s]	- Segundos	-
	- Número de dominios redirigidos	- [0-3]	- Cantidad	-
	- Número de dominios expuestos hacia el navegador web del cliente	- [1-4]	- Cantidad	-
	- Número de dominios con redirección de HTTP a HTTPS	- [0-4]	- Cantidad	-
	- Número de soluciones de seguridad WAF	- [0-1]	- Cantidad	-

Anexo B. Matriz de operacionalización de la variable dependiente

Variable dependiente: Acceso vía web al servicio digital

Variable dependiente	Definición conceptual	Definición operacional	Dimensión	Indicador	Escala
Acceso vía web al servicio digital	Capacidad de acceder a un servicio digital en Internet mediante el protocolo HTTP y un navegador web (Martínez, 2022).	Capacidad de acceder a un servicio digital únicamente a través de su dominio principal, asegurando la redirección de dominios alternos para la centralización del servicio, y la implementación de una solución de seguridad WAF para la protección del servicio en la web.	Accesibilidad	Tiempo de respuesta *Trs: Tiempo de respuesta del servicio*	Intervalo
				Número de dominios redirigidos *Qdar: Cantidad dominios alternos redirigidos*	Intervalo
			Identidad corporativa	Número de dominios expuestos hacia el navegador web del cliente *Qde: Cantidad dominios expuestos*	Intervalo
			Operatividad	Número de dominios con redirección de HTTP a HTTPS *Qdh: Cantidad dominios https*	Intervalo
			Seguridad	Número de soluciones de seguridad WAF *Qssw: Cantidad soluciones seguridad waf*	Intervalo

Anexo C. Plan de trabajo

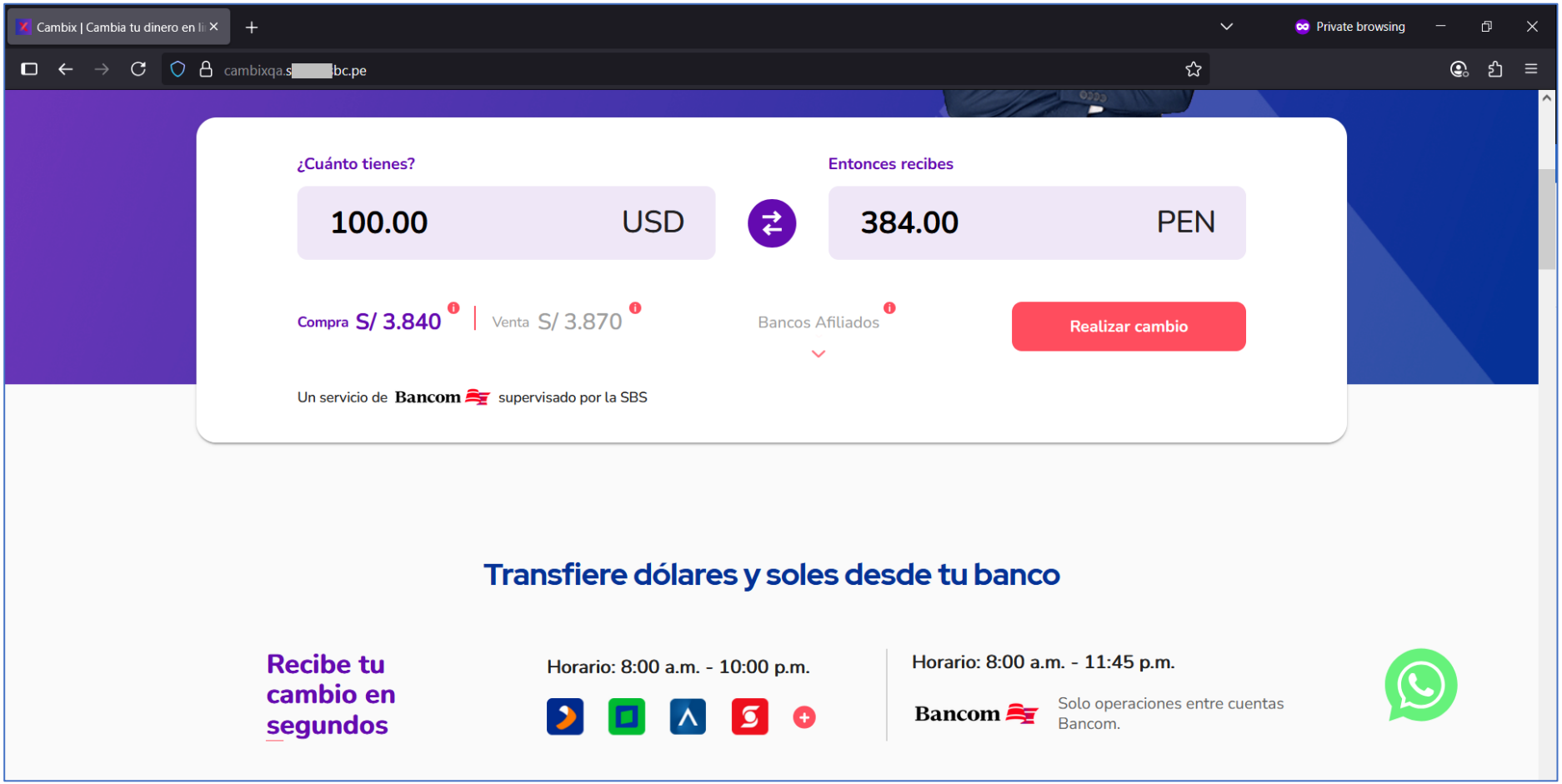
PLAN DE TRABAJO: Arquitectura de Enrutamiento en Azure Front Door para mejorar el acceso web al servicio digital Cambix - cambix.com.pe

Id.	Actividad	Detalle de actividad	Responsable de la actividad	Nombre y Apellido del ejecutor de Actividad	Impacto en Servicio (On Line / Off Line)	Observaciones /Comentarios
Actividades Previas - Certificado Digital TLS/SSL						
1	Generar certificado digital	Exportar llave privada en formato PFX para cada certificado.	GSTI	**Aléxis Cárdenas**	**On Line**	Realizado
Actividades de Ventana - Implementación Azure Front Door cambix.com.pe						
2	Crear de front-ends/dominio personalizado	Agregar dominio personalizado a Azure Front Door, y asignar registro DNS tipo CNAME en NIC.PE. Frontend: cambix.com.pe CNAME fdappsbc.azurefd.net Frontend: www.cambix.com.pe CNAME fdappsbc.azurefd.net Frontend: cambix.pe CNAME fdappsbc.azurefd.net Frontend: www.cambix.pe CNAME fdappsbc.azurefd.net	GSTI	**Aléxis Cárdenas**	**On Line**	Realizado
3	Configurar nuevo front-end/dominio personalizado	Configuración de front-ends creados: Frontend: cambix.com.pe Frontend: www.cambix.com.pe Frontend: cambix.pe Frontend: www.cambix.pe Estado: Habilitado Versión de TLS mínima: 1.2 Tipo de certificado: Propio (Key Vault) WAF: Habilitado (waf001)	GSTI	**Aléxis Cárdenas**	**On Line**	Realizado
4	Configurar directiva WAF	Validar Reglas administradas de directiva waf001. Desplegar Reglas personalizadas de directiva waf001. En base a políticas de seguridad del Banco (se restringe el tráfico proveniente de los países identificados como fuentes recurrentes de actividades maliciosas, tales como Rusia, China, Corea del Norte, etc.).	GSTI	**Aléxis Cárdenas**	**On Line**	Realizado
5	Instalar certificado en Azure Front Door	Configurar almacén de claves de certificados digitales. Subir certificado en formato PFX a almacén de claves en Azure. Enlazar certificado almacenado PFX a Front-end en Azure Front Door.	GSTI	**Aléxis Cárdenas**	**On Line**	Realizado

6	Configurar grupos de backend	Crear grupo de backend: bkpoolcambix Tipo de backend: App Service Backend: cambix-prod.azurewebsites.net Sondeos de estado: Habilitado Protocolo: HTTPS Método de sondeo: HEAD Intervalo (segundos): 30 Equilibrio de carga Tamaño de muestra: 4 Se requieren muestras correctas: 2 Sensibilidad de latencia (milisegundos): 0	GSTI	**Aléxis Cárdenas**	**On Line**	Realizado
7	Configurar reglas de enrutamiento	Crear regla de enrutamiento con las siguientes actualizaciones: Regla de enrutamiento: Rule-cambix Protocolo aceptado: HTTPS solamente Front-end: **cambix.com.pe** (seleccionar solo 1) Tipo de ruta: Adelante (Forwarding) Grupo de backend: bkpoolcambix Protocolo de reenvío: HTTPS solamente Regla de enrutamiento: http-to-https Protocolo aceptado: HTTP solamente Front-end: cambix.com.pe (seleccionar solo 1) Tipo de ruta: Redireccionamiento (Redirect) Tipo: 301 Protocolo: HTTPS solamente Host de destino: Conservar Regla de enrutamiento: redirect04-cambix Protocolo aceptado: HTTP y HTTPS Front-end: www.cambix.com.pe, cambix.pe, www.cambix.pe (seleccionar 3) Tipo de ruta: Redireccionamiento (Redirect) Tipo: 301 Protocolo: HTTPS solamente Host de destino: Reemplazar por cambix.com.pe	GSTI	**Aléxis Cárdenas**	**On Line**	Realizado
Actividades de Ventana - Registros DNS						

8	Configurar cambio de servidores DNS en NIC.PE	Baja de servidores DNS de Azure para cada dominio: ns1-04.azure-dns.com ns2-04.azure-dns.net ns3-04.azure-dns.org ns4-04.azure-dns.info Alta de servidores DNS RCP para cada dominio: ns.rcp.net.pe ns2.rcp.net.pe	GSTI	**Aléxis Cárdenas**	**Off Line** (aprox 5 min)	Realizado
9	Configurar registros DNS en NIC.PE	Alta de registros DNS de tipo CNAME para cada dominio: cambix.com.pe CNAME fdappsbc.azurefd.net cambix.pe CNAME fdappsbc.azurefd.net www.cambix.com.pe CNAME fdappsbc.azurefd.net www.cambix.pe CNAME fdappsbc.azurefd.net	GSTI	**Aléxis Cárdenas**	**Off Line** (aprox 5 min)	Realizado
Actividades de Ventana - Validaciones						
10	Comprobar el acceso al servicio	Acceso correcto mediante navegador web. Coordinación con Innovación.	GSTI / Innovación	**Aléxis Cárdenas Innovación**	**On Line**	Realizado
Actividades de Rollback						
11	Configurar cambio de servidores DNS en NIC.PE	Baja de servidores DNS RCP para cada dominio: ns.rcp.net.pe ns2.rcp.net.pe Alta de servidores DNS de Azure para cada dominio: ns1-04.azure-dns.com ns2-04.azure-dns.net ns3-04.azure-dns.org ns4-04.azure-dns.info	GSTI	**Aléxis Cárdenas**	**Off Line** (aprox 5 min)	No requerido
Actividades Post-Ventana						
12	Monitorear el acceso al servicio	Monitoreo de los eventos presentados en los logs de acceso al servicio.	GSTI / Innovación	**Aléxis Cárdenas Innovación**	**On Line**	Realizado

Anexo D. Validación previa a producción



Nota: Adaptado de Cambix. (s.f.).

Anexo E. Registros completos de grupo control y grupo experimental

O1_Posprueba_Gc

N	Category	requestUri_s	sni_s	requestProtocol_s	routingRuleName_s	backendHostname_s	httpStatusCode_s	destination_host	response_time	policy_s	userAgent_s	SourceSystem	Type
1	FrontdoorAccessLog	https://cambix.pe:443/	cambix.pe	HTTPS	N/A	cambix-prod.azurewebsites.net:443	200	cambix.pe	13.42	N/A	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)	Azure	AzureDiagnostics
2	FrontdoorAccessLog	https://cambix.com.pe:443/	cambix.com.pe	HTTPS	N/A	cambix-prod.azurewebsites.net:443	200	cambix.com.pe	12.88	N/A	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)	Azure	AzureDiagnostics
3	FrontdoorAccessLog	https://cambix.com.pe:443/	cambix.com.pe	HTTPS	N/A	cambix-prod.azurewebsites.net:443	200	cambix.com.pe	15.12	N/A	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)	Azure	AzureDiagnostics
4	FrontdoorAccessLog	https://cambix.com.pe:443/	cambix.com.pe	HTTPS	N/A	cambix-prod.azurewebsites.net:443	200	cambix.com.pe	11.99	N/A	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)	Azure	AzureDiagnostics
5	FrontdoorAccessLog	https://cambix.com.pe:443/	cambix.com.pe	HTTPS	N/A	cambix-prod.azurewebsites.net:443	200	cambix.com.pe	14.35	N/A	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)	Azure	AzureDiagnostics
6	FrontdoorAccessLog	https://cambix.com.pe:443/	cambix.com.pe	HTTPS	N/A	cambix-prod.azurewebsites.net:443	200	cambix.com.pe	13.09	N/A	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)	Azure	AzureDiagnostics
7	FrontdoorAccessLog	http://cambix.com.pe:80/	cambix.com.pe	HTTP	N/A	cambix-prod.azurewebsites.net:443	403	cambix.com.pe	12.44	N/A	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:142.0) Gecko/20100101 Firefox/142.0	Azure	AzureDiagnostics
8	FrontdoorAccessLog	http://www.cambix.com.pe:80/	www.cambix.com.pe	HTTP	N/A	cambix-prod.azurewebsites.net:443	403	www.cambix.com.pe	13.78	N/A	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:142.0) Gecko/20100101 Firefox/142.0	Azure	AzureDiagnostics
9	FrontdoorAccessLog	https://cambix.com.pe:443/	cambix.com.pe	HTTPS	N/A	cambix-prod.azurewebsites.net:443	200	cambix.com.pe	15.03	N/A	Mozilla/5.0 (iPhone; CPU iPhone OS 13_2_3 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like	Azure	AzureDiagnostics
10	FrontdoorAccessLog	https://cambix.pe:443/	cambix.pe	HTTPS	N/A	cambix-prod.azurewebsites.net:443	200	cambix.pe	14.62	N/A	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)	Azure	AzureDiagnostics
11	FrontdoorAccessLog	https://cambix.pe:443/	cambix.pe	HTTPS	N/A	cambix-prod.azurewebsites.net:443	200	cambix.pe	12.21	N/A	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)	Azure	AzureDiagnostics
12	FrontdoorAccessLog	https://cambix.com.pe:443/	cambix.com.pe	HTTPS	N/A	cambix-prod.azurewebsites.net:443	200	cambix.com.pe	13.55	N/A	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)	Azure	AzureDiagnostics
13	FrontdoorAccessLog	https://cambix.com.pe:443/	cambix.com.pe	HTTPS	N/A	cambix-prod.azurewebsites.net:443	200	cambix.com.pe	13.98	N/A	Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0	Azure	AzureDiagnostics
14	FrontdoorAccessLog	http://www.cambix.com.pe:80/	www.cambix.com.pe	HTTP	N/A	cambix-prod.azurewebsites.net:443	403	www.cambix.com.pe	15.24	N/A	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)	Azure	AzureDiagnostics
15	FrontdoorAccessLog	https://cambix.com.pe:443/	cambix.com.pe	HTTPS	N/A	cambix-prod.azurewebsites.net:443	200	cambix.com.pe	12.67	N/A	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)	Azure	AzureDiagnostics
16	FrontdoorAccessLog	https://cambix.com.pe:443/	cambix.com.pe	HTTPS	N/A	cambix-prod.azurewebsites.net:443	200	cambix.com.pe	14.1	N/A	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)	Azure	AzureDiagnostics
17	FrontdoorAccessLog	https://cambix.com.pe:443/	cambix.com.pe	HTTPS	N/A	cambix-prod.azurewebsites.net:443	200	cambix.com.pe	13.33	N/A	Mozilla/5.0 (iPhone; CPU iPhone OS 18_5 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like	Azure	AzureDiagnostics
18	FrontdoorAccessLog	https://www.cambix.com.pe:443/	www.cambix.com.pe	HTTPS	N/A	cambix-prod.azurewebsites.net:443	200	www.cambix.com.pe	11.99	N/A	Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0	Azure	AzureDiagnostics
19	FrontdoorAccessLog	https://www.cambix.com.pe:443/	www.cambix.com.pe	HTTPS	N/A	cambix-prod.azurewebsites.net:443	200	www.cambix.com.pe	15.98	N/A	Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0	Azure	AzureDiagnostics
20	FrontdoorAccessLog	https://cambix.com.pe:443/	cambix.com.pe	HTTPS	N/A	cambix-prod.azurewebsites.net:443	200	cambix.com.pe	13.74	N/A	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)	Azure	AzureDiagnostics
21	FrontdoorAccessLog	https://cambix.com.pe:443/	cambix.com.pe	HTTPS	N/A	cambix-prod.azurewebsites.net:443	200	cambix.com.pe	12.56	N/A	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)	Azure	AzureDiagnostics
22	FrontdoorAccessLog	http://cambix.pe:80/	cambix.pe	HTTP	N/A	cambix-prod.azurewebsites.net:443	403	cambix.pe	14.82	N/A	Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0	Azure	AzureDiagnostics
23	FrontdoorAccessLog	https://cambix.com.pe:443/	cambix.com.pe	HTTPS	N/A	cambix-prod.azurewebsites.net:443	200	cambix.com.pe	13.21	N/A	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)	Azure	AzureDiagnostics
24	FrontdoorAccessLog	https://cambix.com.pe:443/	cambix.com.pe	HTTPS	N/A	cambix-prod.azurewebsites.net:443	200	cambix.com.pe	12.93	N/A	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)	Azure	AzureDiagnostics
25	FrontdoorAccessLog	https://www.cambix.com.pe:443/	www.cambix.com.pe	HTTPS	N/A	cambix-prod.azurewebsites.net:443	200	www.cambix.com.pe	15.25	N/A	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko)	Azure	AzureDiagnostics
26	FrontdoorAccessLog	http://www.cambix.pe:80/	www.cambix.pe	HTTP	N/A	cambix-prod.azurewebsites.net:443	403	www.cambix.pe	13.49	N/A	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)	Azure	AzureDiagnostics
27	FrontdoorAccessLog	https://www.cambix.pe:443/	www.cambix.pe	HTTPS	N/A	cambix-prod.azurewebsites.net:443	200	www.cambix.pe	14.28	N/A	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)	Azure	AzureDiagnostics
28	FrontdoorAccessLog	https://cambix.com.pe:443/	cambix.com.pe	HTTPS	N/A	cambix-prod.azurewebsites.net:443	200	cambix.com.pe	12.35	N/A	Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0	Azure	AzureDiagnostics
29	FrontdoorAccessLog	https://cambix.pe:443/	cambix.pe	HTTPS	N/A	cambix-prod.azurewebsites.net:443	200	cambix.pe	13.89	N/A	Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0	Azure	AzureDiagnostics
30	FrontdoorAccessLog	https://cambix.com.pe:443/	cambix.com.pe	HTTPS	N/A	cambix-prod.azurewebsites.net:443	200	cambix.com.pe	15.28	N/A	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)	Azure	AzureDiagnostics

O2_Posprueba_Ge													
N	Category	requestUri_s	sni_s	requestProtocol_s	routingRuleName_s	backendHostname_s	httpStatusCode_s	destination_host	response_time	policy_s	userAgent_s	SourceSystem	Type
1	FrontdoorAccessLog	https://cambix.com.pe:443/	cambix.com.pe	HTTPS	Rule-cambix	cambix-prod.azurewebsites.net:443	200	cambix.com.pe	04.82	waf001	Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko)	Azure	AzureDiagnostics
2	FrontdoorAccessLog	https://cambix.com.pe:443/	cambix.com.pe	HTTPS	Rule-cambix	cambix-prod.azurewebsites.net:443	200	cambix.com.pe	05.33	waf001	Mozilla/5.0 (iPhone; CPU iPhone OS 18_5 like Mac OS X) AppleWebKit/605.1.15	Azure	AzureDiagnostics
3	FrontdoorAccessLog	https://cambix.pe:443/	cambix.pe	HTTPS	redirect04-cambix	N/A	301	cambix.com.pe	03.74	waf001	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like	Azure	AzureDiagnostics
4	FrontdoorAccessLog	https://cambix.pe:443/	cambix.pe	HTTPS	redirect04-cambix	N/A	301	cambix.com.pe	01.99	waf001	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like	Azure	AzureDiagnostics
5	FrontdoorAccessLog	https://cambix.com.pe:443/	cambix.com.pe	HTTPS	Rule-cambix	cambix-prod.azurewebsites.net:443	200	cambix.com.pe	06.12	waf001	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like	Azure	AzureDiagnostics
6	FrontdoorAccessLog	http://cambix.com.pe:80/	cambix.com.pe	HTTP	http-to-https	N/A	301	cambix.com.pe	04.41	waf001	Mozilla/5.0 (iPhone; CPU iPhone OS 13_2_3 like Mac OS X) AppleWebKit/605.1.15	Azure	AzureDiagnostics
7	FrontdoorAccessLog	https://cambix.com.pe:443/	cambix.com.pe	HTTPS	Rule-cambix	cambix-prod.azurewebsites.net:443	200	cambix.com.pe	07.08	waf001	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like	Azure	AzureDiagnostics
8	FrontdoorAccessLog	http://cambix.com.pe:80/	cambix.com.pe	HTTP	http-to-https	N/A	301	cambix.com.pe	05.02	waf001	Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko)	Azure	AzureDiagnostics
9	FrontdoorAccessLog	http://cambix.com.pe:80/	cambix.com.pe	HTTP	http-to-https	N/A	301	cambix.com.pe	03.57	waf001	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like	Azure	AzureDiagnostics
10	FrontdoorAccessLog	https://cambix.com.pe:443/	cambix.com.pe	HTTPS	Rule-cambix	cambix-prod.azurewebsites.net:443	200	cambix.com.pe	04.96	waf001	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like	Azure	AzureDiagnostics
11	FrontdoorAccessLog	http://cambix.pe:80/	cambix.pe	HTTP	redirect04-cambix	N/A	301	cambix.com.pe	08.25	waf001	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like	Azure	AzureDiagnostics
12	FrontdoorAccessLog	https://cambix.com.pe:443/	cambix.com.pe	HTTPS	Rule-cambix	cambix-prod.azurewebsites.net:443	200	cambix.com.pe	04.13	waf001	Mozilla/5.0 (iPhone; CPU iPhone OS 18_3 like Mac OS X) AppleWebKit/605.1.15	Azure	AzureDiagnostics
13	FrontdoorAccessLog	https://cambix.com.pe:443/	cambix.com.pe	HTTPS	Rule-cambix	cambix-prod.azurewebsites.net:443	200	cambix.com.pe	06.88	waf001	Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko)	Azure	AzureDiagnostics
14	FrontdoorAccessLog	https://www.cambix.com.pe:443/	www.cambix.com.pe	HTTPS	redirect04-cambix	N/A	301	cambix.com.pe	02.44	waf001	Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko)	Azure	AzureDiagnostics
15	FrontdoorAccessLog	https://cambix.pe:443/	cambix.pe	HTTPS	redirect04-cambix	N/A	301	cambix.com.pe	05.71	waf001	Mozilla/5.0 (iPhone; CPU iPhone OS 18_5 like Mac OS X) AppleWebKit/605.1.15	Azure	AzureDiagnostics
16	FrontdoorAccessLog	http://cambix.com.pe:80/	cambix.com.pe	HTTP	http-to-https	N/A	301	cambix.com.pe	03.92	waf001	Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko)	Azure	AzureDiagnostics
17	FrontdoorAccessLog	https://www.cambix.pe:443/	www.cambix.pe	HTTPS	redirect04-cambix	N/A	301	cambix.com.pe	07.54	waf001	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like	Azure	AzureDiagnostics
18	FrontdoorAccessLog	https://www.cambix.com.pe:443/	www.cambix.com.pe	HTTPS	redirect04-cambix	N/A	301	cambix.com.pe	04.67	waf001	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like	Azure	AzureDiagnostics
19	FrontdoorAccessLog	http://cambix.pe:80/	cambix.pe	HTTP	redirect04-cambix	N/A	301	cambix.com.pe	09.11	waf001	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like	Azure	AzureDiagnostics
20	FrontdoorAccessLog	http://www.cambix.com.pe:80/	www.cambix.com.pe	HTTP	redirect04-cambix	N/A	301	cambix.com.pe	02.78	waf001	Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko)	Azure	AzureDiagnostics
21	FrontdoorAccessLog	https://cambix.pe:443/	cambix.pe	HTTPS	redirect04-cambix	N/A	301	cambix.com.pe	06.03	waf001	Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko)	Azure	AzureDiagnostics
22	FrontdoorAccessLog	http://cambix.com.pe:80/	cambix.com.pe	HTTP	http-to-https	N/A	301	cambix.com.pe	05.29	waf001	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like	Azure	AzureDiagnostics
23	FrontdoorAccessLog	https://cambix.com.pe:443/	cambix.com.pe	HTTPS	Rule-cambix	cambix-prod.azurewebsites.net:443	200	cambix.com.pe	03.25	waf001	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like	Azure	AzureDiagnostics
24	FrontdoorAccessLog	http://www.cambix.pe:80/	www.cambix.pe	HTTP	redirect04-cambix	N/A	301	cambix.com.pe	04.58	waf001	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like	Azure	AzureDiagnostics
25	FrontdoorAccessLog	https://cambix.com.pe:443/	cambix.com.pe	HTTPS	Rule-cambix	cambix-prod.azurewebsites.net:443	200	cambix.com.pe	07.91	waf001	Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko)	Azure	AzureDiagnostics
26	FrontdoorAccessLog	https://cambix.com.pe:443/	cambix.com.pe	HTTPS	Rule-cambix	cambix-prod.azurewebsites.net:443	200	cambix.com.pe	04.36	waf001	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like	Azure	AzureDiagnostics
27	FrontdoorAccessLog	https://cambix.com.pe:443/	cambix.com.pe	HTTPS	Rule-cambix	cambix-prod.azurewebsites.net:443	200	cambix.com.pe	05.84	waf001	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like	Azure	AzureDiagnostics
28	FrontdoorAccessLog	https://cambix.com.pe:443/	cambix.com.pe	HTTPS	Rule-cambix	cambix-prod.azurewebsites.net:443	200	cambix.com.pe	02.66	waf001	Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko)	Azure	AzureDiagnostics
29	FrontdoorAccessLog	https://cambix.pe:443/	cambix.pe	HTTPS	redirect04-cambix	N/A	301	cambix.com.pe	06.47	waf001	Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko)	Azure	AzureDiagnostics
30	FrontdoorAccessLog	https://cambix.com.pe:443/	cambix.com.pe	HTTPS	Rule-cambix	cambix-prod.azurewebsites.net:443	200	cambix.com.pe	03.89	waf001	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like	Azure	AzureDiagnostics

Anexo F. Consulta KQL en Azure Logs Analytics para la extracción y análisis de eventos WAF

```
AzureDiagnostics
| extend geo = geo_info_from_ip_address(clientIP_s)
| extend geo2 = geo_info_from_ip_address(clientIp_s)
| extend Waf_clientIP_s = clientIP_s
| extend Access_clientIp_s = clientIp_s
| where host_s contains "cambix"
| where action_s == "Block"
| project TimeGenerated, ResourceProvider, Category, host_s, policy_s, policyMode_s, action_s, clientIP_s, requestUri_s, ruleName_s, details_msg_s, trackingReference_s,
Waf_clientIP_s, Waf_Country = tostring(geo.country), Access_clientIp_s, Access_Country = tostring(geo2.country), sni_s, requestProtocol_s, routingRuleName_s,
httpStatusCode_s, userAgent_s, SourceSystem, Type
```

Versión comentada:

```
AzureDiagnostics //Fuente de datos de diagnóstico de Microsoft Azure. Es utilizada para consultar métricas, logs y eventos relacionados con el monitoreo y la seguridad.
| extend geo = geo_info_from_ip_address(clientIP_s) //Se crea la columna geo, con el valor de la función geo, para extraer el país de la IP Cliente de los registros de WAF.
| extend geo2 = geo_info_from_ip_address(clientIp_s) //Se crea la columna geo2, con el valor de la función geo, para extraer el país de la IP Cliente de los registros de Acceso.
| extend Waf_clientIP_s = clientIP_s //Se crea la columna Waf_clientIP_s, con el valor de la IP Cliente de los registros de WAF.
| extend Access_clientIp_s = clientIp_s //Se crea la columna Access_clientIp_s, con el valor de la IP Cliente de los registros de Acceso.
| where host_s contains "cambix" //Se filtra los registros, para mantener únicamente los que contienen la cadena cambix en el host.
| where action_s == "Block" //Se filtra los registros, para mantener únicamente aquellos cuya acción en WAF fue de bloqueo.
| project TimeGenerated, ResourceProvider, Category, host_s, policy_s, policyMode_s, action_s, clientIP_s, requestUri_s, ruleName_s, details_msg_s, trackingReference_s,
Waf_clientIP_s, Waf_Country = tostring(geo.country), Access_clientIp_s, Access_Country = tostring(geo2.country), sni_s, requestProtocol_s, routingRuleName_s,
httpStatusCode_s, userAgent_s, SourceSystem, Type //Se seleccionan las columnas específicas para visualizar en el resultado de la consulta KQL. La consulta puede variar
para ajustarse al propósito del análisis.
```

Nota: Consulta KQL para extraer y analizar los eventos registrados por la solución WAF. Se ha comentado cada línea.

Anexo G. Nuevo proceso de acceso web al servicio digital Cambix de la Entidad Financiera Banco de Comercio