FACULTAD DE POSTGRADO
TRABAJO FINAL DE GRADUACIÓN

PROYECTO DE IMPLEMENTACIÓN DE MECANISMOS DE AUTENTICACIÓN DE DOBLE FACTOR EN SISTEMAS FINANCIEROS EN EL BANCO CENTRAL DE HONDURAS

SUSTENTADO POR:

AARON ISMAEL ELVIR ROSALES
GINSBERG YAMIR RODRIGUEZ IRIAS

PREVIA INVESTIDURA AL TÍTULO DE

MÁSTER EN
ADMINISTRACIÓN DE PROYECTOS

TEGUCIGALPA, FRANCISCO MORAZAN, HONDURAS, C.A.

ENERO, 2019

UNIVERSIDAD TECNOLÓGICA CENTROAMERICANA

UNITEC

FACULTAD DE POSTGRADO

AUTORIDADES UNIVERSITARIAS

RECTOR
MARLON ANTONIO BREVÉ REYES

VICERRECTORA ACADÉMICA
DESIREE TEJADA CALVO

SECRETARIO GENERAL
ROGER MARTÍNEZ MIRALDA

DECANA DE LA FACULTAD DE POSTGRADO
CLAUDIA MARÍA CASTRO VALLE

PROYECTO DE IMPLEMENTACIÓN DE MECANISMOS DE AUTENTICACIÓN DE DOBLE FACTOR EN SISTEMAS FINANCIEROS EN EL BANCO CENTRAL DE HONDURAS

TRABAJO PRESENTADO EN CUMPLIMIENTO DE LOS REQUISITOS EXIGIDOS PARA OPTAR AL TÍTULO DE

MÁSTER EN

ADMINISTRACIÓN DE PROYECTOS

ASESOR METODOLÓGICO

MINA CECILIA GARCIA LEZCANO

MIEMBROS DE LA TERNA:

HENRY JAVIER OVIEDO URBIBA
PABLO ABRAHAM MOYA GAITAN
JORGE A. CENTENO SARMIENTO

FACTULTAD DE POSTGRADO

PROYECTO DE IMPLEMENTACIÓN DE MECANISMOS DE AUTENTICACIÓN DE DOBLE FACTOR EN SISTEMAS FINANCIEROS EN EL BANCO CENTRAL DE HONDURAS

AARON ISMAEL ELVIR ROSALES
GINSBERG YAMIR RODRIGUEZ IRIAS

RESUMEN

El presente documento refleja el estudio efectuado en Banco Central de Honduras, donde se desarrolló la implementación de un mecanismo adicional de autenticación para los sistemas financieros, en base a buenas prácticas, nivel de seguridad informática; haciendo uso de metodologías para el desarrollo del proyecto como lo es la gestión del alcance y gestión de la calidad de la guía del PMBOK, apoyados sobre la metodología de desarrollo ágil de SCRUM, se busca alcanzar el objetivo del proyecto. Considerando que este estudio desea alcanzar en la institución implementar un mecanismo adicional de autenticación de usuarios, utilizando principalmente los insumos que ya posee a nivel de aplicaciones e infraestructura tecnológica, se aplicaron dos instrumentos a personal experto en temas de seguridad y telecomunicaciones a nivel de la Institución. Por lo tanto, el análisis efectuado considera un enfoque mixto de variables cualitativas y cuantitativas, que satisfacen el objetivo del proyecto de investigación; el instrumento utilizado en el estudio fue la entrevista aplicada a personal especializado, por esta razón, no se tuvo una muestra significativa de observación.

Palabras claves: Gestión de la calidad, Gestión del alcance, PMBOK, SCRUM.

GRADUATE SCHOOL

PROJECT OF IMPLEMENTATION OF DOUBLE FACTOR AUTHENTICATION MECHANISMS IN FINANCIAL SYSTEMS IN CENTRAL BANK OF HONDURAS

AARON ISMAEL ELVIR ROSALES
GINSBERG YAMIR RODRIGUEZ IRIAS

ABSTRACT

This document reflects the study carried out at Banco Central de Honduras, where the implementation of an additional authentication mechanism for financial systems was developed, based on good practices, level of computer security; Making use of methodologies for the development of the project as it is the management of the scope and management of the quality of the guide of the PMBOK, supported on the Agile development Methodology of SCRUM, seeks to achieve the objective of the project. Considering that this study wants to achieve in the institution to implement an additional mechanism of user authentication, using mainly the inputs that it already has at the level of applications and technological infrastructure, two instruments were applied to Expert staff in security and telecommunications issues at the institution level. Therefore, the analysis carried out considers a mixed approach of qualitative and quantitative variables, which meet the objective of the research project; The instrument used in the study was the interview applied to specialized personnel, for this reason, there was not a significant sample of observation.

Keywords: PMBOK, Quality management, Scope management, SCRUM

AGRADECIMIENTO

Quiero agradecer principalmente a Dios, quien ha sido la inspiración y fuente de sabiduría en estos 2 años de estudio, a mi esposa e hijos que son la inspiración para seguir adelante sin importar las adversidades, a mis padres que siempre se han esforzado para que siempre pueda cumplir con mis metas. Ra: Aaron Ismael Elvir Rosales

Agradezco a todas las personas mencionadas en mi dedicatoria ya que fueron la base para que lograra llegar a esta nueva etapa de la vida y darles las gracias por brindarme su apoyo y comprensión en estos estudios, muchas gracias y de la forma más sincera reconozco que sin ellos hubiera sido imposible lograr lo que hoy en día estoy compartiendo con mucha alegría con ellos. Ra: Ginsberg Yamir Rodríguez Irías

DEDICATORIA

Dedico el presente documento a mi familia, quienes han tomaron un rol activo en todo este proceso de educación que comenzó en octubre de 2016. A los maestros que brindaron de su tiempo y sabiduría para formar lo que en este momento soy y parte de su conocimiento se ve reflejado en este documento. A todos ellos les gracias de todo corazón. Ra: Aaron Ismael Elvir Rosales

Dedico esta tesis en primera instancia a Dios Padre, Dios Hijo y Dios Espíritu Santo quien en todo momento estuvo a mi lado, brindándome sabiduría, fortaleza, consejo y temor; a mis padres con me concibieron y dieron a luz, educación, consejos durante todo este tiempo; a la institución en la que laboro por brindarme facilidades para continuar mis estudios; a mi compañero de proyecto que con su ayuda a sido posible lograr la culminación del proyecto de investigación y en general a todos los que me apoyaron a los largo de este logro que considero de todos los que ayudaron. A todos ellos les gracias de todo corazón. Ra: Ginsberg Yamir Rodríguez Irías

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURÁS

ÍNDICE DE TABLAS

CAPÍTULO I. PLANTEAMIENTO DE LA INVESTIGACIÓN

1.1 Introducción

En este capítulo se describe de manera ordenada los principales elementos del planteamiento de la investigación, los cuales ayudaran a entender y razonar el objetivo del estudio, en la cual se incluye la introducción, antecedentes del proyecto, definición del problema que servirá para analizar y crear la estructura que contiene el proyecto de investigación, concibiendo una idea que permitirá brindar respuesta a las preguntas de investigación, objetivos, variables y su respectiva justificación. “Plantear el problema no es sino afinar y estructurar más formalmente la idea de investigación” (Sampieri & Lucio, Metodología de la Investigación, 2003) (p. 9).

La autenticación tradicional de los sistemas informáticos se realiza mediante el ingreso de un usuario y contraseña, con el paso del tiempo los atacantes han mejorado sus prácticas para violentar el acceso a software lo cual nos lleva a identificar que no siempre las mejores metodologías son suficientes, ya que pese a todos los esfuerzos que hagamos siempre nuestra contraseña así como el usuario se verá expuesta ante factores que escapan de nuestro control, en busca de una solución a este problema, se desarrolló una medida adicional de seguridad surgiendo así la autenticación a doble factor.

“Hoy en día tener un usuario y una clave pareciera no ser suficiente, por lo que utilizar factores de doble autenticación se vuelven más relevantes.” (Financiero, 2017). Actualmente las empresas invierten gran cantidad de tiempo y recursos para poder respaldas sus sistemas informáticos, así como mejorar sus niveles de seguridad de ciber ataques. (Financiero, 2017)

1.2 Antecedentes del problema

Desde tiempo atrás los sistemas tradicionales de autenticación que emplean usuario y contraseña han incrementado su frecuencia, volviéndose más refinados y fáciles de utilizar. Un atacante denominado Hacker tarda “Para una clave de 9 caracteres, que contiene únicamente minúscula, un hacker se demoraría 4 meses en descifrarla; si lleva mayúsculas 178 años y con símbolos y números 44,530 años” (Clarín, 2014). Lo cual explica la razón de definir contraseñas no menores a 8 caracteres y que se mezclen entre: minúsculas, mayúsculas, números y símbolos.

Ante este dato podemos considerar que la información de usuarios y contraseñas representar un valor monetario para las instituciones, así lo expresa Miguel Angel Mendoza, security researcher de ESET explico que muchas personas e incluso empresas creen que su información no es valiosa o que ningún ciber delincuente los atacara, sin embargo, esta creencia es falsa.

"El valor de una contraseña de Gmail en la Deep web cuesta $1, una de Twitter $2, de Uber $8 y una de PayPal más $80, entonces toda información tiene su valor", afirmo Mendoza.

Considerando la cita anterior y el hecho de que uno de los activos más importantes en el BCH es la información tanto la que se almacena de forma física como electrónica, esta última usualmente almacenada en bases de datos la cuales se protegen de ataques en lo posible considerando como ejemplo sencillo si a una persona se le daña una memoria Universal Serial Bus (USB por sus siglas en ingles) en lo primero que se piensa es en recuperar el contenido mas no el dispositivo de hardware como tal y por ello comprendemos que toda información tiene su precio el cual es definido o establecido por los interesados.

1.3 Definición del problema

En esta sección se describe el enunciado y formulación del problema y las preguntas de investigación.

1.3.1 Enunciado del problema

Basados en la existencia de la autenticación a doble factor como método adicional de seguridad, hoy por hoy ha sido de mucha ayuda, para frustrar los intentos de los atacantes que buscan de forma incansable violentar la seguridad de los usuarios, las empresas que requieren de su uso necesitan comprar infraestructura adicional denominada Token, el cual les genera al presionar un botón o simplemente al conectarlo a un ordenador que a su vez son sincronizados con los servidores de la institución mediante software especializado para efectuar dicha labor, un valor numérico en una pantalla pero el precio de esta infraestructura "RSA securid sid700 – Hardware Token" (RSA - AMAZON, 2007). Es de $. 596.23 por cada 10 dispositivos aproximadamente L. 14,293.72 considerando una "tasa de cambio de L. 23.9735 por $. 1.00" (BCH, 2018). Lo cual al considerar un dispositivo por usuario generaría a la institución muchos gastos en adquirir los Tokens que le generen el código.

En base a la cita anterior se concluye que no todos los clientes tienen la capacidad económica para costearse mecanismos adicionales de seguridad, aunque los sistemas que utilicen manejen o controlen dinero y aunque el cliente tenga el recurso económico para comprarlo, les causa cierto malestar el estar comprando hardware para incrementar la seguridad en los sistemas que de igual forma a ellos les beneficia.

1.3.2 Formulación del problema

La planificación es uno de los pasos más importantes que puede tomar y más cuando se trata de seguridad en uno de los activos más importantes para la institución, misma que convierte

a los sistemas de información más robustos contra atacantes. Reuniendo el personal adecuado en temas de desarrollo, telecomunicaciones y bases de datos logrando determinar prioridades a nivel de seguridad y que cumplan con las normas de la institución. La planificación genera un gran esfuerzo, pero produce grandes resultados si se hace de la mejor forma posible y siguiente estándares mundialmente aceptados o mejores prácticas en entorno de sistemas de información.

En vista que implementar medidas de seguridad adicionales genera un costo para la institución, mismas que no todos los proyectos que se implementan a lo interno cuentan con el recurso o presupuesto necesario para adquirir infraestructura para los clientes que utilizaran los sistemas de información con el mecanismo adicional de autenticación.

1.3.3 Preguntas de investigación

Las preguntas que a continuación se detallan representan la guía para la evaluación y solución al problema de investigación:

a) ¿Los clientes del BCH presentaran resistencia al cambio con la implementación del proyecto?

b) ¿Cómo se supliría la necesidad en los proyectos que no dispongan de mucho presupuesto para adquirir un dispositivo adicional de seguridad?

1.4 Objetivos del proyecto

1.4.1 Objetivo General

Implementar un mecanismo de autenticación de doble factor en sistemas financieros en el Banco Central de Honduras.

1.4.2 Objetivos Específicos

a) Suplir la necesidad de generación de un código mediante un Token, con recursos internos que ya cuenta la institución.

b) Implementar un mecanismo seguro que supla los requerimientos de adicionar seguridad a la autenticación tradicional de usuario y contraseña.

c) Innovar en el desarrollo de un procedimiento tecnológico que pueda ser aceptado como nuevo mecanismo de seguridad en la institución a un mínimo costo.

1.5 Justificación

La seguridad en toda institución es importante ya que por falta de ella se puede incurrir en problemas administrativos, civiles y judiciales; en tal caso las organizaciones se ven en la necesidad de crear Departamentos que se encarguen de la seguridad y riesgo de la empresa ya que los activos que poseen son de vital importancia e inclusive hasta para sus clientes o interesados de forma general.

Con lo cual esta investigación se desarrolla debido a la necesidad de la institución de suplir sus necesidades protegiéndose a sí misma y a sus clientes o interesados, por lo cual se requiere de un nuevo mecanismo de seguridad que supla las necesidades actuales logrando disminuir costos de mantenimiento, licenciamiento o infraestructura. Implementando de forma integral una solución de software que mediante el conocimiento y experiencias adquiridas en el tiempo y con la ayuda de juicio de expertos en el tema de seguridad, logre el cumplimiento del proyecto que se elabore de manera concreta y transparente, la cual muestre mediante sus objetivos alcanzados mejorar la seguridad del sistema financiero, además de seguir la filosofía de Arquitectura Empresarial (AE) en cuanto a:

a) Protección de la base de activos existente mediante la maximización de la reutilización de los componentes arquitectónicos existentes.

b) Reutilización de procesos, conceptos y componentes en todas las unidades de negocios de la organización. (The Open Group, 2018)

Se concluye que a lo largo de este capítulo se identificó la necesidad de implementar un mecanismo de seguridad que fortalezca la autenticación tradicional de los usuarios en los sistemas de información, definiendo los objetivos del proyecto de investigación para cumplir con requisitos de seguridad del BCH.

CAPÍTULO II. MARCO TEÓRICO

El presente capítulo de marco teórico consiste en mostrar la información referente al tema de investigación en Banco Central de Honduras (BCH). Además, brinda el soporte y comprensión de las teorías que proporcionaran un sistema coordinado y coherente para el proyecto que permitirá abordar el problema, considerando las mejores prácticas e información adicional que se desarrolle hoy por hoy, por lo que en la (Fig. 1) Del mapa conceptual se muestran los marcos de trabajo elegidos que se detallaran a lo largo de este capítulo, permitiendo respaldar el documento con información bibliográfica que expone un panorama más amplio sobre el tema y un apoyo para el análisis e interpretación de los resultados obtenidos con los instrumentos considerando los 1niveles de seguridad digital en sistemas financieros.

[1] Niveles de seguridad digital en sistemas financieros: se refiere a protección de datos y del dinero digital

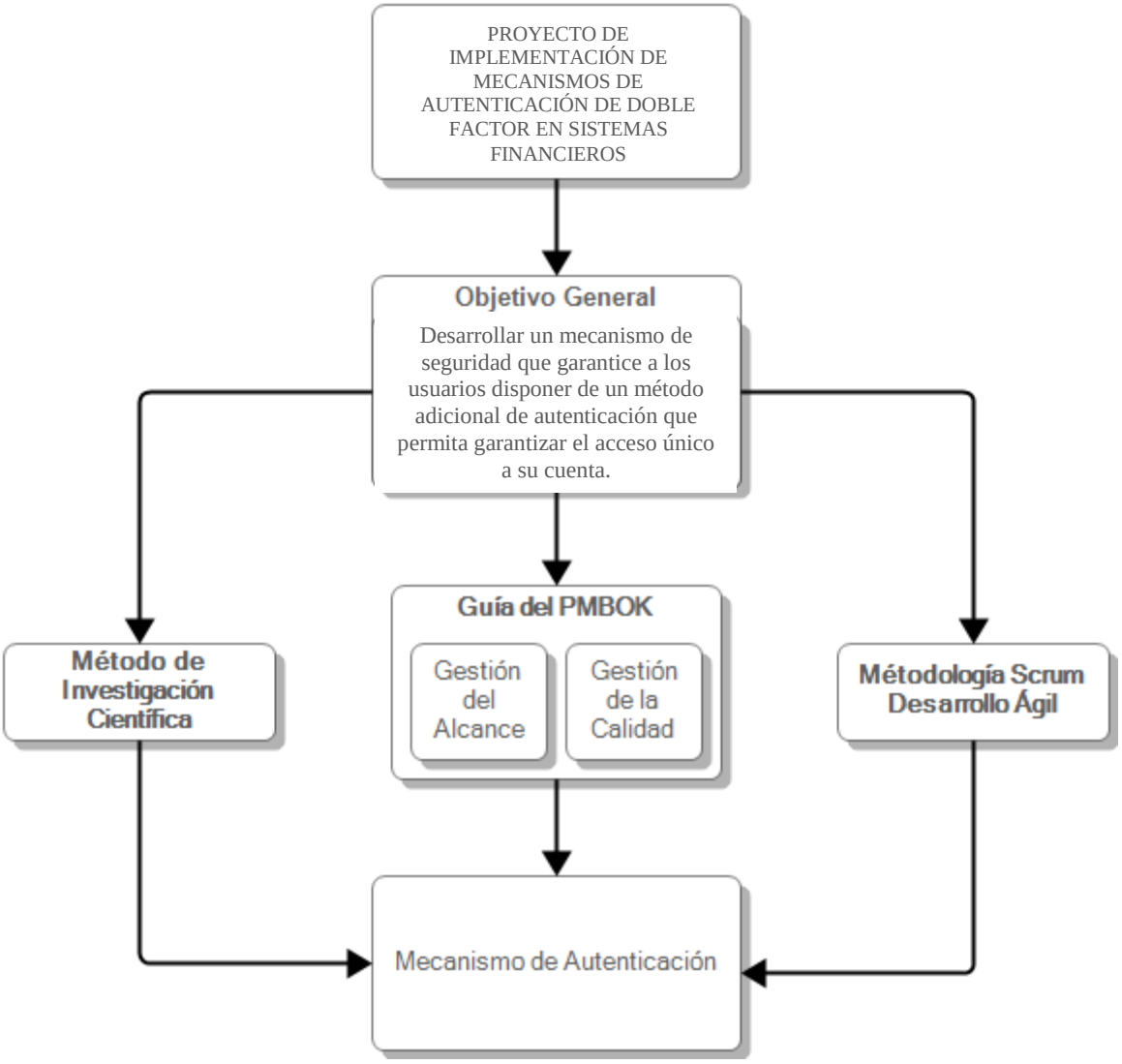


Figura 1 Mapa conceptual

Fuente: Propia.

2.1 Análisis de la situación actual

Permite examinar de forma general los sistemas informáticos que pertenecen al selecto grupo de principales activos de las organizaciones y así tener una visión actual, volviéndose un factor crítico para alcanzar el éxito y cumplir sus objetivos organizacionales, además del esfuerzo económico que se invierte en implementarlos. Los hackers hoy están desarrollando sus habilidades técnicas para encontrar las vulnerabilidades en los sistemas informáticos y poder

causar daños significativos a las organizaciones. Scambray & McClure (2002) afirma "Tan poco glamuroso como suena, adivinar las contraseñas 2SMB es un método antiguo, pero probablemente el más efectivo para obtener acceso a Windows"(p. 98). A pesar de existir muchos métodos para la suplantación de identidades a nivel informático, se continúan utilizando los métodos tradicionales como probar contraseñas de forma aleatoria en los usuarios.

"La seguridad en internet es, sin duda, uno de los temas más debatidos del momento. Sin embargo, las medidas que tomamos para protegernos de la actividad de los hackers no siempre son suficientes." (Redacción, 2017). La mejor barrera que se puede diseñar para mitigar el ataque de los piratas informáticos, es la creación de contraseñas robustas y eficientes, las cuales deben contener un mínimo de caracteres incorporando números, letras mayúsculas y minúsculas, caracteres especiales.

Según estudios publicados por la BBC, (2017) afirma que el mayor error que comenten los usuarios en internet es asignar las mismas contraseñas en diferentes sitios de navegación.

Considerando que la mejor forma de proteger nuestra contraseña es no tener una sola, sino que contar con una para cada sitio web, lo recomendable sería incluir el nombre del sitio web como parte de la contraseña con ello garantizaríamos que tenemos una contraseña para cada sitio en el que navegamos.

2.2 Teoría de sustento.

En la actualidad se busca reforzar los mecanismos de seguridad de los sistemas informáticos. (Sobh, 2008) refiere que las contraseñas de un solo uso o OTP (del vocablo ingles One Time Password) será una contraseña que se podrá utilizar una sola vez. Estas contraseñas

[2] Server Message Block (SMB): es un protocolo de red por el cual se pueden compartir archivos, impresoras y otros activos informáticos en las organizaciones

mejoran notablemente la seguridad con las que cuentan los métodos tradicionales de solo usuario y contraseña. De las principales diferencias es que no son vulnerables a los ataques de fuerza bruta que efectúan los atacantes, los cuales su objetivo fundamente es obtener la contraseña que le corresponde al usuario y para ello buscan en una base de datos previamente configurada las posibles opciones de contraseña de mayor uso por los usuarios. En el siguiente cuadro se muestran las principales contraseñas actualizadas al 2017:

1. 123456	14. login
2. password	15. abc123
3. 12345678	16. starwars
4. qwerty	17. 123123
5. 12345	18. dragon
6. 123456789	19. passw0rd
7. letmein	20. master
8. 1234567	21. hello
9. football	22. freedom
10. iloveyou	23. whatever
11. admin	24. qazwsx
12. welcome	25. trustno1
13. monkey	

Figura 2 Lista de contraseñas de mayor uso

Fuente: (BBC, 2017)

El beneficio que se obtiene al utilizar las tecnologías OTP contra atacantes, se presenta cuando un pirata informático o hacker logre descubrir nuestro código, probablemente este ya estará vencido y por lo tanto debe volver a comenzar para verificar la contraseña, lo cual lo llevaría a un ciclo sin fin de intentos originando desmotivación de los atacantes para continuar.

Según estudio realizado por la BBC, (2017) más del 10% de los usuarios de internet tiene una contraseña del tipo 123456, en muchas ocasiones los usuarios deciden utilizar este tipo de contraseñas ya que son más fáciles de recordar, el problema radica al optar por el uso de estas

contraseñas en diferentes sitios para no olvidarla, incrementando con ello el riesgo de sufrir ataques por los hackers.

2.2.1 Análisis de las metodologías

En esta sección se profundizará en las metodologías a utilizar para desarrollar el proyecto de investigación, mediante las cuales se logrará el cumplimiento de los objetivos del tema de investigación.

2.2.1.1 Metodología SCRUM

El ciclo de vida de desarrollo de un sistema de software, está comprendido por las fases de planificación, análisis, diseño e implementación. Al considerar SCRUM como una metodología de desarrollo ágil la cual ha tenido mucha aceptación en las empresas por brindar resultados rápidos y de forma exitosa la cual será de mucha ayuda en el proyecto.

La metodología SCRUM al utilizarla como marco de administración para el desarrollo de proyectos el cual reduce los tiempos de entrega entre un 30% - 40%, lo cual permite mejorar la calidad del producto, así como aumentar la satisfacción del cliente por el constante contacto que se tiene con ellos al presentarles avances del proyecto y conocer sus opiniones y necesidades. Este método se concentra en resolver situaciones en las que no se entrega al cliente el producto que él está necesitando o cuando se tiene una alta rotación en el equipo, o cuando sea necesario entregar un producto especializado para el cliente final, logrando así que está metodología logre resolver esas necesidades.

> SCRUM was initiated by Ken Swaber in 1995. It was included in agile methodology since it con tains the same concepts of agile. A SCRUM is a team pack, where everyone in the team acts together. It delivers the project within time and with minimal cost. Mahalakshmi & Sundararajan (2013, p. 1)

En comparación con otros modelos de desarrollo de software diferentes a SCRUM, como

la Estructura en Cascada, Mahalakshmi & Sundararajan (2013, p. 1) afirma que en este modelo se debe seguir un orden secuencial, el cual fluye de principio a fin, y por lo tanto el cliente no puede realizar cambios ya que la estructura no lo permite, esto al finalizar el desarrollo lleva a enfrentar grandes problemas en cuanto al alcance, tiempo y costo del proyecto, ya que el cliente no estará satisfecho y aún se tendrán requisitos pendientes.

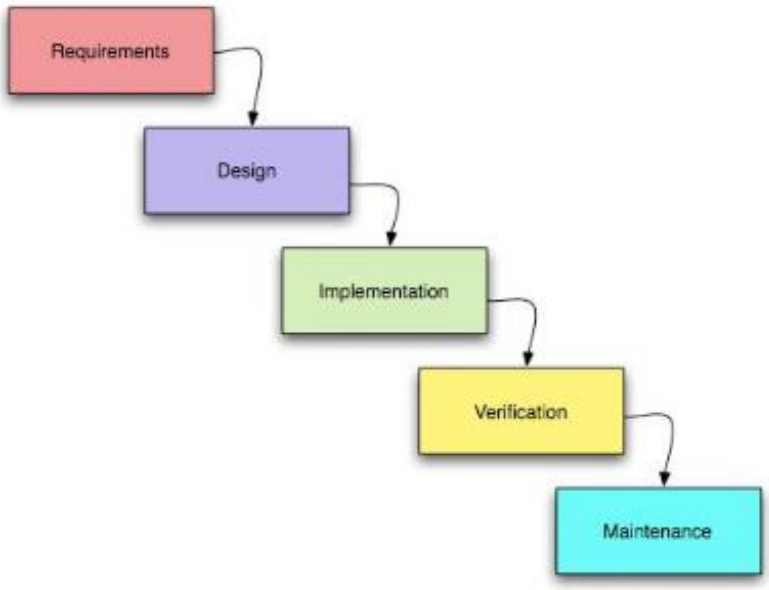


Figura 3 Modelo Tradicional
Fuente: Mahalakshmi & Sundararajan (2013)

En la imagen mostrada en la figura 3, se observa el ciclo tradicional de desarrollo de sistemas, en el cual lo requisitos se definen al iniciar el proyecto con la ayuda de documentación recopilada antes de ser un proyecto, es decir cuando era una iniciativa de proyecto utilizando los casos de negocio para recopilar toda la información preliminar al proyecto y una vez al convertirse en proyecto, se validan hasta que el mismo este por finalizar.

Por lo tanto, la metodología SCRUM implementa un enfoque para mejorar la flexibilidad de incorporar nuevos requerimientos mediante pequeñas entregas del producto de forma

consecutiva a los usuarios, mismos que al inicio del proyecto no contaban con una visión clara de lo que necesitan y de qué forma lo requerirían. A través del tiempo se han probado muchos enfoques para mejorar la administración de los proyectos de software, la mayoría han fallado Grady (1994, p. 8) afirma "A menudo llamamos a esta condición la crisis del software, pero, francamente, una enfermedad que ha continuado durante tanto tiempo debe ser llamada normal." Una gran porción de los procesos de los sistemas no está claramente estructurada que posiblemente se deba a procesos desactualizados o procesos que necesiten ser mejorados, pero el usuario los trata como si estuvieran bien, SCRUM afronta estos procesos como cajas negras controladas, desarrollando un nuevo enfoque para el desarrollo de sistemas basado en la definición de requerimientos y en cajas negras.

> SCRUM is a management, enhancement and maintenance methodology for an existing system or production prototype. It assumes existing design and code which is virtually always the case in object-oriented development due to the presence of class libraries. SCRUM will address totally new or re-engineered legacy systems development efforts at a later date. Schwaber K. (1997)

2.2.1.1.1 ¿Cómo se diferencia SCRUM del método en Cascada?

La diferencia entre las metodologías radica en: roles diferentes, enfoque diferente en las reuniones, diferentes características, diferentes actores, lenguaje de proyectos diferente. La metodología SCRUM define tres roles principales: Propietario del producto, SCRUM Master y SCRUM Team.

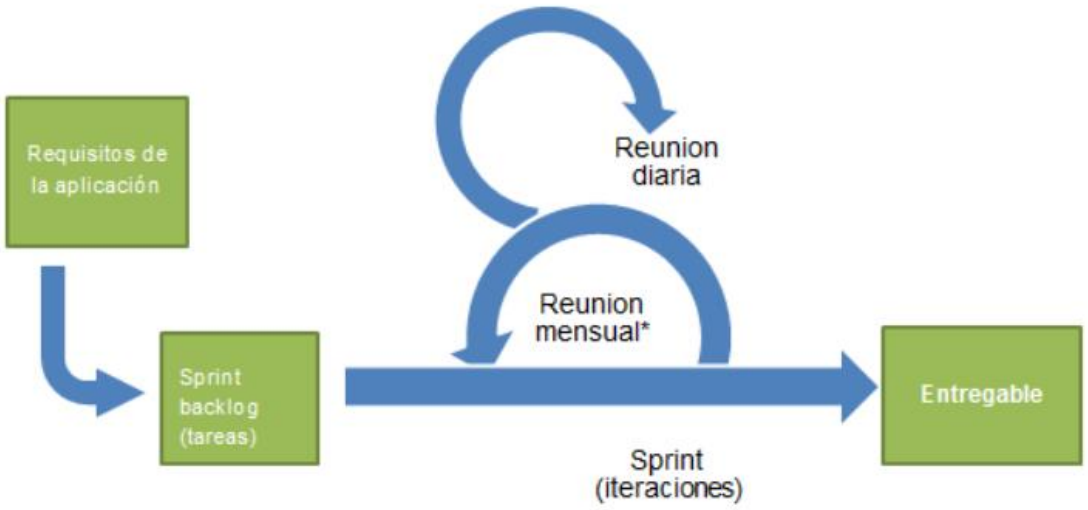


Figura 4 Proceso SCRUM

Fuente: Holgado (2013)

En la figura 4 se muestra el ciclo de la metodología SCRUM, la cual define los requerimientos al inicio del proyecto, luego se desarrolla un plan de tareas el cual se estará produciendo constantemente, en la ejecución del proyecto se desarrollan reuniones diarias de 15 a 20 minutos como máximo para validar los avances y realizar ajustes cuando sea necesario, al finalizar se tiene un entregable validado y aprobado por el cliente de principio a fin garantizando con ello su satisfacción y buen funcionamiento de la parte del producto final que al finalizar el proyecto se le estará entregando.

Tabla 1 Diferencias entre el método tradicional y SCRUM

Cascada	SCRUM
Se enfoca en el proyecto	Se enfoca en el producto
El modelo tradicional consta de diferentes fases.	La metodología SCRUM consiste en diferentes sprint.
No espera cambios	Espera cambios y acepta los
Mas documentación	Menos documentación
El costo del proyecto se determina en la planificación	El costo del proyecto se establece en el proyecto
La probabilidad de éxito es baja	La probabilidad de éxito es alta
La flexibilidad y creatividad del equipo es limitada	La flexibilidad y creatividad del equipo es ilimitada.
Secuencial	Actividades superpuestas

Fuente: Mahalakshmi & Sundararajan (2013)

2.2.1.2 Metodología del PMBOK

El PMBOK del PMI en lenguaje castellano se define como la Guía de Fundamentos para la Dirección de Proyectos, este libro fue publicado por el Instituto de Dirección de Proyectos por sus siglas en ingles PMI (Project Management Institute), en este libro se define una pauta metodológica para la administración de proyectos. Esta metodología está siendo aplicada a nivel mundial pero principalmente en América ya que en Europa se conoce también el PRINCE 2, y por ser el PMBOK una guía, se puede adoptar primeramente y adaptar a las necesidades de las organizaciones y los grupos de procesos necesarios ya que brinda una metodología para alcanzar el éxito de los proyectos indistintamente su naturaleza.

El PMI es una organización sin fines de lucro, la cual se dedica a recolectar y documentar las mejoras prácticas desarrolladas a nivel mundial en materia de administración de proyectos, para luego ser incorporadas al PMBOK después de revisiones rigurosas. Tiene su sede en Estados Unidos, Pensilvania y cuenta con una gran cantidad de asociados tanto personas naturales como jurídicas.

Para la versión 5 de la guía del PMBOK se definen 47 procesos la cual contienen entradas, herramientas y salidas; 9 áreas de conocimiento y 5 grupos de procesos.

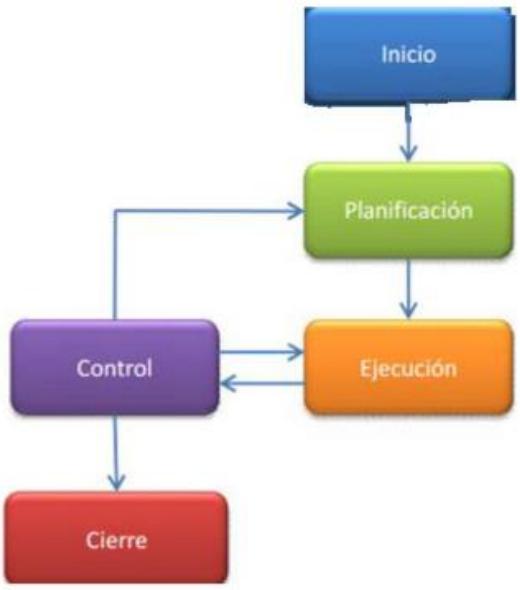


Figura 4 Fases de Proyecto PMI
Fuente Guía de Fundamentos para la Administración de Proyectos PMBOK

Para enfocar el análisis e implementación de proyectos, la guía del PMBOK plantea la administración del proyecto desde 3 perspectivas conocidas como la triple restricción: alcance, tiempo y costo; aunque hoy por hoy ya se han incorporado otras perspectivas como riesgos y calidad.

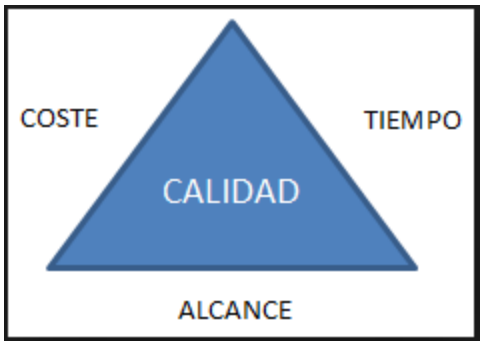


Figura 5 Triple restricción de proyectos

Fuente (PROJECT MANAGEMENT INSTITUTE, 2013).

Dinsmore and Silveira Neto (2005, p.1) afirma:

> Un proyecto es un esfuerzo temporal realizado para crear un producto o servicio único, a diferencia de cualquier otro, de todos los demás productos y servicios, con principio y fin, definido, que utiliza recursos, es administrado por personas y obedece a los parámetros de costo, tiempo y calidad.

Entre los elementos destacados definidos en la guía del PMBOK, se encuentra la división del proyecto en un grupo de fases, el cual es llamado ciclo de vida del proyecto que a su vez, tienen fases que se vinculan al principio y el final de un proyecto. “Las transiciones que ocurren entre fases generalmente involucran algún tipo de entrega, o una transferencia técnica. Por lo general, los ciclos de vida del proyecto definen qué trabajo se realizará en cada fase, así como los involucrados y los procedimientos relacionados con el control y la aprobación de cada fase” (PROJECT MANAGEMENT INSTITUTE, 2013).

2.2.1.3 Diferencias entre la metodología SCRUM y PMBOK

La metodología SCRUM para el desarrollo de sistemas de software, es diferente al estilo de gestión de proyectos que propone la guía del PMBOK, ya que este último es un enfoque altamente definido. Cada metodología de administración de proyectos, tienen como objetivo principal alcanzar el éxito del proyecto supliendo la necesidad que lo origino, pero utilizan

enfoques diferentes, además de fortalezas.

SCRUM se enfoca en completar el trabajo mediante actividades altamente interactivas (diarias y mensuales), las cuales van siendo aprobadas por el propietario del producto. Este enfoque busca entregar un producto lo más pronto posible en base a los requerimientos solicitados por el cliente y cuando sea necesario, realizar los ajustes requeridos mediante las iteraciones para lograr su aceptación y avanzar en la siguiente actividad. SCRUM puede ser una metodología muy fácil de aprender y entender, pero en campo su aplicación se puede volver un desafío para el equipo del proyecto, ya que se necesita mucho apoyo por parte de la organización, así como la aceptación de roles para el desarrollo de actividades.

El PMBOK utiliza un periodo de ejecución proyecto tradicional, SCRUM se centra en periodos cortos e intensos de trabajo para alcanzar el objetivo final, a diferencia del PMBOK que debe esperar largos periodos para ver los primeros resultados desde el inicio del proyecto.

Otra diferencia entre las metodologías, es que las lecciones aprendidas se discuten antes y después de cada reunión de trabajo en SCRUM, en cambio la guía del PMBOK la realiza en cada fase o al final del proyecto. Para el desarrollo ágil es de mucha importancia las lecciones aprendidas ya que refleja si las actividades se están desarrollando según lo planificado y bajo el criterio de aceptación del cliente, además que estas reuniones ayudan a mejorar los puntos débiles en cada semana y no se espera la finalización del proyecto.

El PMBOK brinda una guía para el entendimiento de los procesos y áreas de conocimiento, por lo cual deja poco a la interpretación, en cambio SCRUM se enfoca diferente forma brindando prioridad a las solicitudes personalizadas del cliente. Una gran diferencia entre ambos métodos está en el tamaño de su documentación la guía del PMBOK consta de 450 páginas y SCRUM 17 páginas, lo cual nos indica que la guía del PMBOK es más robusta a nivel

de administración de proyectos.

La guía del PMBOK como SCRUM tienen un enfoque para la administración de los riesgos del proyecto. El PMBOK detalla una serie de pautas para la gestión del riego desde la iniciación hasta el cierre, mediante la aceptación, traslado o cualquier método que deba emplear; en cambio SCRUM ataca directamente los riesgos en cada ciclo de trabajo, aceptando el riesgo y resolviendo al mismo tiempo, ya que su objetivo es entregar un producto bajo los criterios del cliente lo más pronto posible.

2.2.1.4 Puntos de encuentro entre SCRUM y el PMBOK

Así como lo mostrado en el apartado anterior, existen muchas diferencias entre ambas metodologías de trabajo, pero también tienen similitudes las cuales ayudan a complementar los procesos del proyecto.

Ghosh, Forrest, DiNetta, Wolfe, & Lambert, (2015) afirma:

> Tanto SCRUM como el PMBOK afirman ser una metodología, que al ser implementada da solución a los problemas que se enfrentan en los proyectos sin importar su complejidad, además que cada método tiene su propio esquema para solución de inconveniente.

Ambos métodos proporcionan importancia a que el equipo de trabajo conozca los mismos términos, o manejo del mismo idioma de Proyecto. Se definen palabras claves y se encargan que todos los miembros del proyecto las conozcan logrando así una comunicación efectiva y así conocer el norte o dirección a seguir del proyecto para lograr su éxito.

Ghosh, Forrest, DiNetta, Wolfe, & Lambert, (2015) afirma:

> Hay muchas cosas en PMBOK que ni siquiera se intentaron cubrir en Scrum. La mayor fortaleza y la mayor debilidad de Scrum es su simplicidad. Scrum puede alinearse y compararse con PMBOK en muy pocas categorías, pero en general PMBOK supera ampliamente a Scrum. Agregar más detalles a Scrum lo haría como cualquier otra guía. Sin embargo, la guía Scrum quizás podría mejorarse para que sus prácticas y estructura centrales puedan aplicarse más allá del equipo de proyecto de bajo nivel. Este tipo de práctica tal vez ya esté ocurriendo, pero puede ser útil modificar la guía para que sea más vaga en su implantación o incluir una lista de implementaciones sugeridas.

2.2.1.5 Contraseña de un solo uso (OTP)

Cuando se cuenta con sistemas que tienen un solo factor de autenticación, se posee un único punto de vulnerabilidad, por lo tanto, si ese único factor de seguridad se ve comprometido cualquier persona puede realizar transacciones en nombre del titular de cuenta.

Al implementar una autenticación de dos factores, se crea un nuevo nivel de seguridad para frenar a las personas que no han sido autorizadas, el esquema de autenticación por OTP, se basa en la creación de contraseñas generadas aleatoriamente en cada transacción que realice un usuario, sin importar su ubicación.

(Hwang, 2015) afirma: que, ahora las personas utilizan el internet para realizar un sin número de actividades en la red como ser: compra de artículos, transacciones financieras, buscar nueva información en portales y sitios web, considerando todos estos aspectos se vuelve critico que los proveedores de servicios de internet garanticen a los usuarios que su acceso al sistema es único e impenetrable. Las contraseñas tradicionales se han vuelto sencillas e inseguras, es en este momento que las contraseñas de un solo uso vienen a fortalecer la seguridad de los métodos tradicionales de autenticación.

Las contraseñas de un solo uso se vuelve un método seguro y eficiente ya que está generando caracteres numéricos de forma aleatoria, los cuales tienen un vencimiento no muy prolongado y para poder realizar una nueva transacción, los usuarios deben solicitar un nuevo código.

Actualmente, la autenticación de doble factor sigue siendo, a pesar de la era tecnológica actualmente, altamente limitado en alcance y costo para las instituciones, en este sentido se sigue confiando en las contraseñas tradicionales, sin importante la cantidad de amenazas o riesgos que pueden encontrar en internet; otro factor que afecta altamente la implementación es la

incompatibilidad entre el hardware y software.

> The lack of interoperability among hardware and Software technology Vendors has been a limiting factor in the adoption of two-factor authentication technology. In particular, hardware and Software components are often tightly coupled through proprietary technology, resulting in high cost Solutions, poor adoption and limited innovation. In the last two years, the rapid rise of network threats has exposed the inadequacies of static passwords as the primary mean of authentication on the Internet. At the same time, the current approach that requires an end-user to carry an expen sive, single-function device that is only used to authenticate to the network is clearly not the right answer. For two factor authentication to propagate on the Internet, it will have to be embedded in more flexible devices that can work across a wide range of applications. (United States Patente nº US 8,087,074 B2, 2006)

La autenticación de doble factor, es un tema que se está desarrollando día a día y por lo tanto las empresas desean implementar esta metodología para mejorar su seguridad informática y su imagen comercial ante sus clientes.

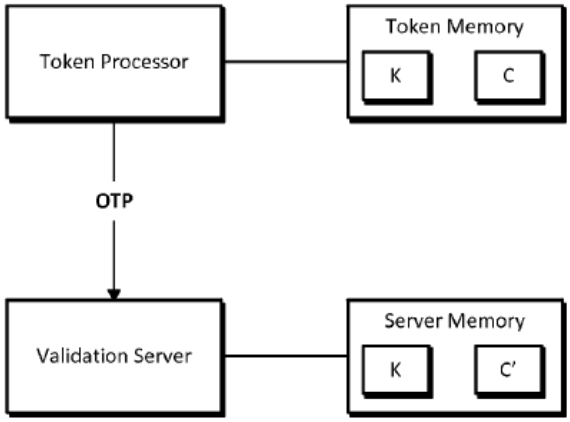


Figura 5 Esquema de autenticación OTP
Fuente (United States Patente nº US 8,087,074 B2, 2006)

En la imagen se muestra el proceso que se debe realizar para solicitar un código numérico de token para la autenticación en un sistema, en el cual existe un agente que genera los valores (Token Processor) y otro agente que realiza la validación (Validation Server) del código ingresado en el sistema, cuando el acceso solicitado por el usuario no es permitido el sistema niega la autorización al usuario. El OTP generado debe leerse fácilmente, se recomienda que sea

un valor numérico de al menos 6 caracteres.

2.2.1.6 Criptografía como elemento de seguridad informática

La criptografía es la ciencia que se encargada del cifrado o codificado de mensajes, cuyo objetivo principal es alterar los textos originales legibles, haciéndolos ilegibles a receptores no autorizados.

El surgimiento de las tecnologías informáticas, peculiarmente el internet, ha implementado todos los métodos para compartir información en diferentes niveles. Con toda la era tecnológica en auge, las amenazas a la seguridad informática son cada día mayores. Es necesario garantizar la confiabilidad y autenticidad tanto de los usuarios como los documentos que comparten. Entre las principales finalidades de la criptografía se encuentra:

- Verificar la identidad de usuarios
- Autenticar y proteger comunicaciones personales, así como transacciones comerciales y bancarias
- Proteger la integridad de transferencias electrónicas

2.2.1.7 Criptografía simétrica

Franco, Sarasa Lopez, & Salazar Riaño, (2001) menciona que la criptografía simétrica utiliza una única clave para cifrar y descifrar el texto, esta clave la debe conocer el emisor y el receptor previamente y es en este punto donde se vuelve vulnerable, ya que resulta más fácil interceptar una clave que se ha transmitido sin seguridad. Según estudios debe ser más fácil conocer la clave interceptándola que utilizando el método por fuerza bruta, teniendo en cuenta que la seguridad de un mensaje cifrado debe recaer sobre la clave y nunca sobre el algoritmo.

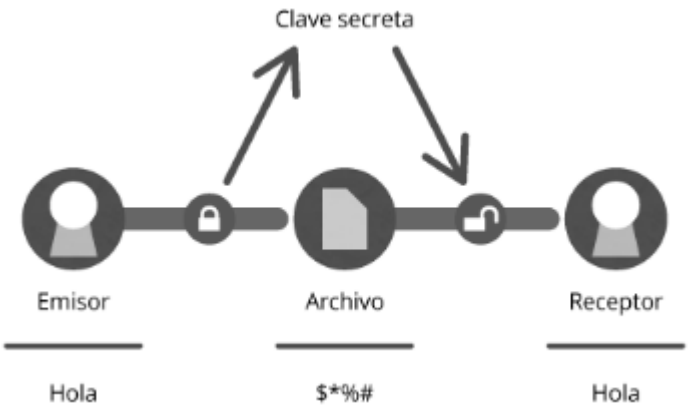


Figura 6 Encriptación Simétrica

Fuente: Franco, Sarasa Lopez, & Salazar Riaño, (2001)

2.2.1.8 Criptografía asimétrica

Franco, Sarasa Lopez, & Salazar Riaño, (2001) menciona que la criptografía asimétrica se basa en el uso de dos contraseñas: la pública (esta se puede difundir sin ningún problema a todas las personas que necesiten enviar algún mensaje cifrado) y la privada (esta clave nunca se debe de revelar). En base a lo anterior, si queremos que tres compañeros de trabajo nos manden un archivo cifrado debemos de mandarle nuestra clave pública (que está vinculada a la privada) y nos podrán enviar de forma confidencial ese archivo que solo nosotros podremos descifrar con la clave privada.

Puede parecer a simple vista un sistema un poco simple ya que podríamos pensar que sabiendo la clave pública podríamos deducir la privada, pero este tipo de sistemas criptográficos usa algoritmos bastante complejos que generan a partir de la frase de paso (la contraseña) la clave privada y pública pueden tener un tamaño de 2048 bits, lo cual lo torna imposible de descifrar.

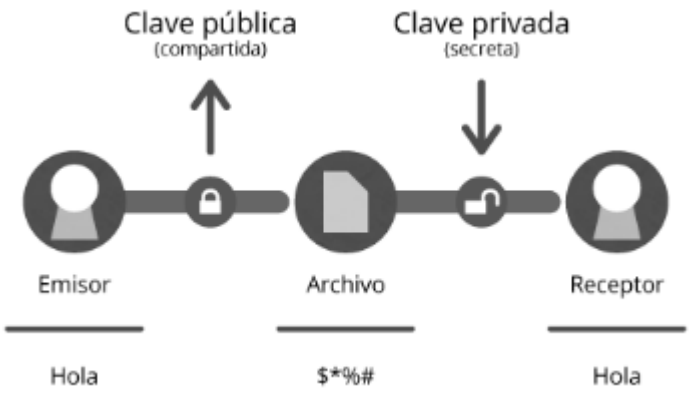


Figura 7 Encriptación Asimétrica

Fuente: Franco, Sarasa Lopez, & Salazar Riaño, (2001)

2.2.2 Análisis crítico de las metodologías a emplear en el trabajo final de investigación

El actual proceso para la recolección de información antes de implementar el trabajo final del proyecto de investigación, consta de lo siguiente:

a) Alcance
    a. Crear un mecanismo adicional de seguridad.
    b. Mejorar el proceso vigente de captura o recepción de información.
    c. No se contempla la adquisición de hardware o infraestructura para los dispositivos de seguridad OTP.
    d. Uso de correo electrónico empresarial para él envió del código OTP generado por el proyecto de implementación.

b) Limitaciones
    a. Procesos administrativos a lo interno del BCH largos, los cuales pueden dificultar la puesta en marcha del proyecto final, la cual se puede mejorar con entregas parciales en base a lo indicado por la metodología SCRUM arriba descrita.

b. Resistencia al cambio por parte del personal del BCH, por la implementación de un mecanismo adicional de autenticación, la cual puede superarse con capacitaciones las cuales revelen las ventajas de implementar tecnologías adicionales de seguridad.

2.2.3 Análisis a nivel de base de datos ORACLE en su versión 11g edición empresarial en la implementación del proyecto de investigación.

2.2.3.1 Subprograma DBMS_CRYPTO

Se utilizará para cifrar o descifrar la información almacenada ya que es compatible con varios algoritmos de cifrado y hash estándar del sector de seguridad informática.

2.2.3.2 Tabla PROPS$

Se utiliza como diccionario de datos en donde se almacena el set de caracteres propios de la base de datos a ser utilizados para cifrar o descifrar.

2.2.3.3 Lenguaje de programación / lenguaje estructurado de consulta (PL/SQL, por sus siglas en ingles)

Se utilizará como un lenguaje de programación incorporado en la base de datos ORACLE que soporta todas las consultas que se puedan generar y manipulación de datos a nivel general.

2.3 Conceptualización

En la siguiente sección se detallarán algunas definiciones que se utilizarán a lo largo del estudio de investigación del proyecto final.

a) OTP: Es un método cuyo nombre que se le brinda a un código de una longitud usualmente de 8 números generado mediante un algoritmo de software de forma aleatoria y que solo es una vez valido en un tiempo determinado usualmente 30 segundos, lo cual incrementa la seguridad en sistemas de información principalmente los financieros.

Menezo & De (2017) afirma que en el mundo actual, al solventar los problemas se comunicación, es cada vez más relevante poder garantizar la identidad de la persona que solicita acceso a la información. Existen muchos métodos que se están implementando para llevar a cabo esta labor, la forma tradicional de usuario y contraseña, más un algoritmo generado aleatoriamente. Estos métodos por si solos pueden llegar a generar deficiencias en el uso de la autenticación, pero cuando son utilizados en conjunto, se obtienen sistemas informáticos más robustos y difíciles de violentar.

b) SCRUM: Es el nombre que le fue establecido a la metodología para desarrollar aplicaciones de forma más rápida o ágil en comparación con el ciclo de vida tradicional de desarrollo de los sistemas de información, que pasan por todo un proceso de análisis, diseño, desarrollo e implementación que si bien es cierto funciona, pero no en todos los casos es la mejor opción.

"Aquellas compañías que han comenzado a usar Scrum, han experimentado cambios significativos en la calidad de sus productos y su entrega oportuna. Los programadores son más productivos ya que las tareas son divididas en partes pequeñas, mucho más manejables" (Dimes, 2015, p. 8).

c) PMBOK: Es una guía general para la buena administración de los proyectos de forma general indistintamente de la naturaleza o tipo de cada uno de ellos, considerando que en las instituciones para evitar cambios muy drásticos que pongan en riesgo su funcionamiento, se debería adoptar en primera instancia la metodología y poco a poco adaptarla a las necesidades de las empresas ya que cada una es distinta a las demás.

> La Guía del PMBOK contiene el estándar, reconocido a nivel global y la guía para la profesión de la dirección de proyectos. Por estándar se entiende un documento formal que describe normas, métodos, procesos y prácticas establecidos. Al igual que en otras profesiones, el conocimiento contenido en este estándar evolucionó a partir de las buenas

> prácticas reconocidas de los profesionales dedicados a la dirección de proyectos que han contribuido a su desarrollo. (PMI, 2013, p. 28)

Se concluye que a lo largo de este capítulo se mostró la importancia de implementar un mecanismo adicional de seguridad al proceso tradicional de autenticación. Mediante la metodología SCRUM y PMBOK podemos implementar un código generado OTP el cual contara con las características y estándares necesarios para certificar el acceso único de los usuarios a los sistemas de información.

CAPÍTULO III. METODOLOGÍA DE LA INVESTIGACION

En este capítulo se desarrollará el procedimiento a seguir mediante las metodologías de investigación seleccionadas, así mismo, los argumentos requeridos para dar respuesta a la pregunta de investigación y a los objetivos del proyecto.

3.1 Congruencia Metodológica

Dadas las características de nuestro proyecto, la investigación es de tipo exploratoria, para ofrecer un primer acercamiento al problema de investigación, lo cual permitirá familiarizarse con metodologías de seguridad, brindando un panorama o conocimiento general en relación al acceso único de usuarios.

3.1.1 Matriz Metodológica

En la siguiente sección se muestra la matriz metodológica a ser utilizada en el proyecto de investigación.

Tabla 2 Matriz Metodológica

MATRIZ METODOLÓGICA							
OBJETIVO GENERAL	PREGUNTA DE INVESTIGACIÓN	VARIABLE INDEPENDIENTE X (Variables independientes en las que se divide "X")	NIVEL DE MEDICIÓN DE LA VARIABLE INDEPENDIENTE	VARIABLE DEPENDIENTE	NIVEL DE MEDICIÓN DE LA VARIABLE DEPENDIENTE	OBJETIVOS ESPECIFICOS	PREGUNTAS DE INVESTIGACIÓN
Desarrollar un mecanismo de seguridad que garantice a los usuarios disponer de un método adicional de autenticación que permita garantizar el acceso único a su cuenta.	¿Cómo se supliría la necesidad en los proyectos que no dispongan de mucho presupuesto para adquirir un dispositivo adicional de seguridad?	Definir el código generado	Razón	Certificar el Acceso Unico	Nominal	Determinar si "Definir el código generado" incide en "Certificar el Acceso Unico"	¿Existe una relación / diferencia entre "Definir el código generado" y "Certificar el Acceso Unico"?
		Establecer el mecanismo seguro	Nominal			Determinar si "Establecer el mecanismo seguro" incide en "Certificar el Acceso Unico"	¿Existe una relación / diferencia entre "Establecer el mecanismo seguro" y "Certificar el Acceso Unico"?
		Gestionar el proceso de seguridad	Ordinal			Determinar si "Gestionar el proceso de seguridad" incide en "Certificar el Acceso Unico"	¿Existe una relación / diferencia entre "Gestionar el proceso de seguridad" y "Certificar el Acceso Unico"?

Fuente: Propia

3.1.2 Operacionalización de las Variables.

En esta sección se plantea la descripción de las variables dependientes e independientes de forma gráfica y lógica, a ser utilizadas en el proyecto, que a continuación se detallan:

a) Acceso único (variable dependiente): garantizar el ingreso genuino del cliente a los sistemas de información mediante usuario y contraseña que es la forma tradicional o estática, añadiendo un mecanismo de autenticación de un solo uso mediante la generación de códigos secreto de forma dinámica mediante la solución de OTP.

b) Generar código (variable independiente): crear un número identificador para una sesión de usuario, que expire en un tiempo determinado (usualmente 30 segundos), en los sistemas de información a utilizar.

c) Mecanismo seguro (variable independiente): es un instrumento que, por su dinamismo y privacidad para cada cliente, brinda un nivel de seguridad superior.

d) Procedimiento tecnológico (variable independiente): tareas o pasos a seguir de forma secuencial a nivel de tecnologías de información para lograr un objetivo o fin, que responda a la pregunta de investigación.

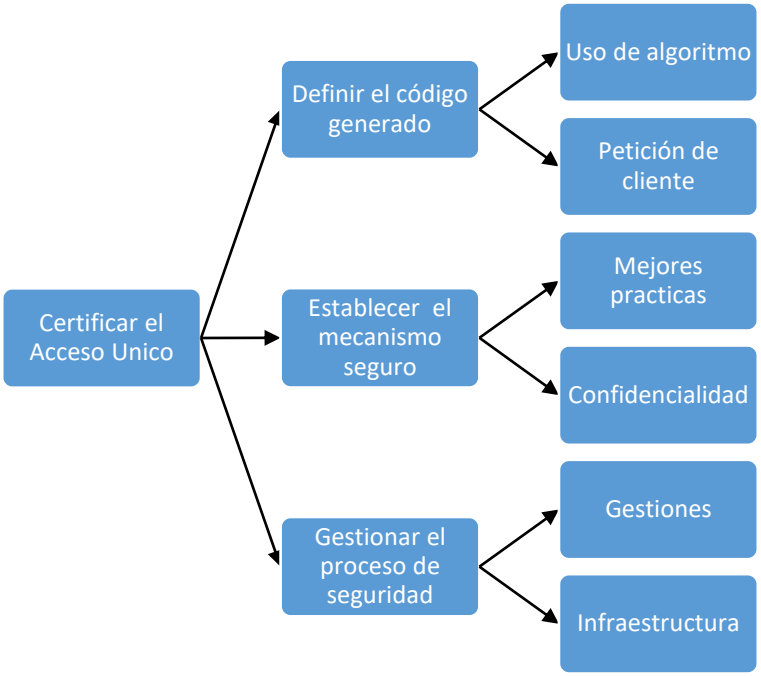


Figura 8 Diagrama de Variables

Fuente: Propia

Tabla 3 Operacionalización de las variables

Variable Independient	Definición		Dimensiones	Escala
	Conceptual	Operacional		
Definir el código generado	Crear un número identificador para una sesión de usuario, que expire en un tiempo determinado (usualmente 30 segundos), en los sistemas de información a utilizar.	Resultado de la implementación de un algoritmo que crea un numero identificador de sesión	Uso de algoritmo Petición de Cliente	Razón
Establecer el mecanismo seguro	Es un instrumento que por su dinamismo y privacidad para cada cliente, brinda un nivel de seguridad superior.	Aplicar mejores practicas desarrolladas a nivel mundial, que ayuden a reforzar la seguridad	Mejores practicas Confidencialidad	Nominal
Gestionar el proceso de seguridad	Tareas o pasos a seguir de forma secuencial a nivel de tecnologías de información para lograr un objetivo o fin, que responda a la pregunta de investigación.	Aplicación de un proceso se seguridad, mediante el uso de infraestructura que ayude a incrementar la confidencialidad del cliente	Gestiones Infraestructura	Ordinal

Variable Dependiente	Definición		Dimensiones	Escala
	Conceptual	Operacional		
Certificar el Acceso Unico	Garantizar el ingreso genuino del cliente a los sistemas de información mediante usuario y contraseña que es la forma tradicional o estática, añadiendo un mecanismo de autenticación de un solo uso mediante la generación de códigos secreto de forma dinámica mediante la solución de OTP.	Ingreso al sistema de información, sin duplicidad de sesiones del cliente	Generar código Mecanismo seguro Procedimiento tecnológico	Nominal

Fuente: Propia

3.1.3 Definición de variables de Hipótesis

En esta sección se define la hipótesis nula y alternativa de la investigación a considerarse para el análisis de correlación.

H0: No existe relación entre el código generado, mecanismo seguro y gestionar el proceso de seguridad.

H1: Existe relación entre el código generado, mecanismo seguro y gestionar el proceso de seguridad.

3.2 Enfoque y Métodos

Con la finalidad de lograr los objetivos propuestos de la investigación que tiene un enfoque mixto de tipo exploratorio, se utilizará encuestas y entrevistas como método principal para recopilar datos, en la que participará personal especializado en temas de seguridad y telecomunicaciones para lograr el cumplimiento de los objetivos y brindar respuesta a la pregunta de investigación planteada en el proyecto.

3.3 Diseño de la Investigación

Se considerará un enfoque mixto para recopilar la información de los pasos a seguir de forma general de los expertos en seguridad y telecomunicaciones para desarrollar el proceso de investigación y cumplir con los objetivos planteados, mediante el uso de entrevistas o encuestas.

3.3.1 Población

La investigación se orientará hacia expertos en el BCH en temas de seguridad y telecomunicaciones, en las diferentes dependencias de la institución que en la actualidad se cuenta con tres (3) expertos en el tema, siendo ellos nuestra población total a ser entrevistados o encuestados y por ser evaluada el total de la población con la que se cuenta, no existe o no se

considera una muestra.

3.3.2 Unidad de Análisis

Se tomará en cuenta lo siguiente:

a) Infraestructura del BCH (equipo de hardware).

b) Aplicativos (producto que ve el cliente final).

c) Software (programas requeridos para administrar la infraestructura).

3.4 Instrumentos, técnicas y procedimientos aplicados

El instrumento principal mediante el cual se recopilará la información del juicio de expertos, será mediante el uso de entrevista y como fuente secundaria el uso de encuestas a personal del BCH especializado en temas de seguridad y telecomunicaciones, además de consultar libros, revistas científicas y otros.

3.5 Fuentes de información

En esta sección se indicarán las fuentes de información a ser utilizadas en nuestro proyecto para dar respuesta a la pregunta de investigación y así cumplir con los objetivos planteados

3.5.1 Fuentes Primarias

Como fuente de primaria de información se toma en consideración el juicio de personal experto del BCH, relacionado con temas de infraestructura de telecomunicaciones y seguridad de la información

3.5.2 Fuentes Secundarias

Se implementará el uso de encuestas a personal específico de la institución, además de

revisar publicaciones en revistas científicas o libros relacionados a temas de seguridad y otros.

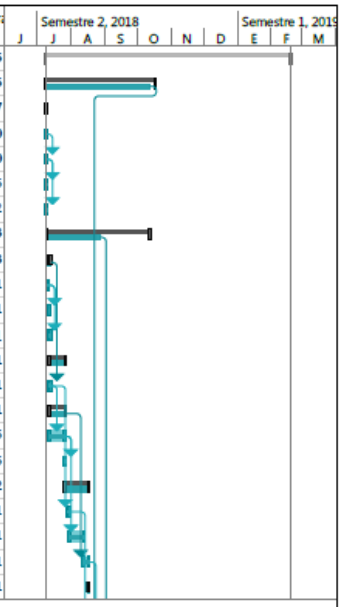
Se concluye que a lo largo de este capítulo se ha definido la variable dependiente e independientes, así como la matriz metodológica junto con su diagrama sagital, definiendo la operacionalización de las variables que servirá para formular la encuesta que irá dirigida a la población identificada, ya que no se tiene una muestra, debido a una población pequeña en cantidad, pero grande y especializada en conocimientos tecnológicos y de seguridad a lo interno del BCH, las cuales serán aplicadas mediante entrevistas a fuentes primarias de información o secundarias según sea el caso, para lograr el cumplimiento del proyecto final.

3.6 Implementación de las metodologías aplicadas en el proyecto

3.6.1 Guía de los fundamentos para la dirección de proyectos (PMBOK, por sus siglas en inglés)

Para la ejecución del proyecto de implementación se enfocaron esfuerzos en la Gestión del Alcance y Gestión del tiempo, logrando de esa forma implementarlo como sigue:

Id	EDT	Nombre de tarea	Comienzo	Fin	Ponderá
0	**0**	**STIRECFIS**	**lun 09/07/18**	**lun 18/02/19**	**53.5**
1	**1**	**Planificación**	**lun 09/07/18**	**mié 17/10/18**	**5**
2	**1.1**	**Iniciación**	**lun 09/07/18**	**mar 10/07/18**	**0.7**
3	1.1.1	Caso de Negocio (Entregable)	lun 09/07/18	lun 09/07/18	0
4	1.1.2	Acta de Constitución del Proyecto (Entregable)	lun 09/07/18	lun 09/07/18	0
5	1.1.3	Notificación del inicio de Proyecto	mar 10/07/18	mar 10/07/18	0.5
6	1.1.4	Registro de Interesados (Entregable)	mar 10/07/18	mar 10/07/18	0.2
7	**1.2**	**Plan del Proyecto**	**mié 11/07/18**	**vie 12/10/18**	**3.3**
8	**1.2.1**	**Gestión de Alcance**	**mié 11/07/18**	vie 13/07/18	**0.3**
9	1.2.1.1	Plan de Gestión del Alcance (Entregable)	mié 11/07/18	mié 11/07/18	0.1
10	1.2.1.2	Plan de Gestión de Requisitos (Entregable)	jue 12/07/18	jue 12/07/18	0.1
11	1.2.1.3	Estructura Detallada de Trabajo (Entregable)	vie 13/07/18	vie 13/07/18	0.1
12	**1.2.2**	**Gestión de Tiempo**	vie 13/07/18	vie 27/07/18	**1.1**
13	1.2.2.1	Plan de Gestión de Tiempo (Entregable)	vie 13/07/18	vie 13/07/18	0.1
14	**1.2.2.2**	**Cronograma del Proyecto (Entregable)**	**vie 13/07/18**	vie 27/07/18	**1**
15	1.2.2.2.1	Elaboración Preliminar del Cronograma	vie 13/07/18	jue 26/07/18	0.5
16	1.2.2.2.2	Revisión Preliminar del Cronograma	jue 26/07/18	vie 27/07/18	0.5
17	**1.2.3**	**Gestión de Riesgos**	vie 27/07/18	vie 17/08/18	**1.2**
18	1.2.3.1	Plan de Gestión de Riesgos (Entregable)	lun 30/07/18	lun 30/07/18	0.1
19	1.2.3.2	Identificación de Riesgos del Proyecto (Entregable)	mar 31/07/18	lun 13/08/18	0.1
20	1.2.3.3	Plan de Respuesta de Riesgos (Entregable)	lun 13/08/18	vie 17/08/18	1
21	**1.2.4**	**Gestión de Calidad**	vie 17/08/18	**vie 17/08/18**	**0.1**

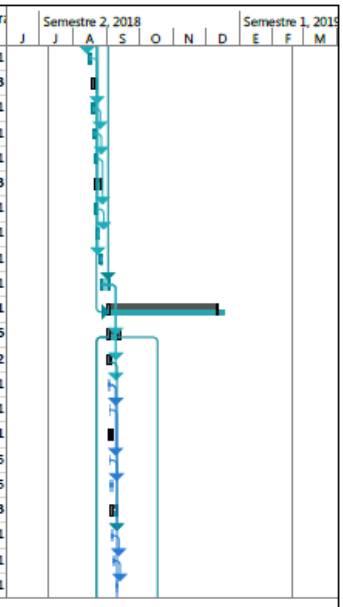


Proyecto: STIRECFIS
Fecha: jue 24/01/19

Tarea	Resumen inactivo	Tareas externas
División	Tarea manual	Hito externo
Hito	solo duración	Fecha límite
Resumen	Informe de resumen manual	Tareas críticas
Resumen del proyecto	Resumen manual	División crítica
Tarea inactiva	solo el comienzo	Progreso
Hito inactivo	solo fin	Progreso manual

Página 1

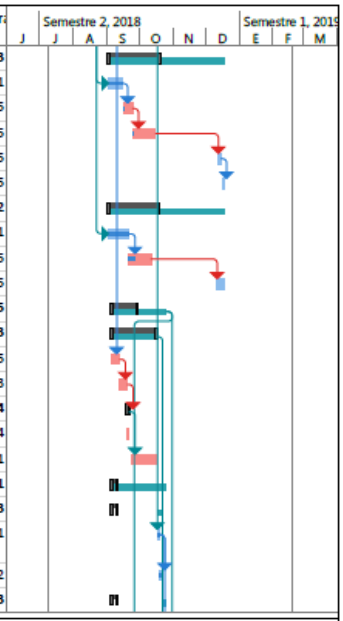
Id	EDT	Nombre de tarea	Comienzo	Fin	Ponderá
22	1.2.4.1	Plan de Gestión de Calidad (Entregable)	vie 17/08/18	vie 17/08/18	0.1
23	**1.2.5**	**Gestión de Comunicaciones**	**lun 20/08/18**	**mié 22/08/18**	**0.3**
24	1.2.5.1	Plan de Gestión de Comunicaciones (Entregable)	lun 20/08/18	lun 20/08/18	0.1
25	1.2.5.2	Matriz de Comunicaciones del Proyecto (Entregable)	mar 21/08/18	mar 21/08/18	0.1
26	1.2.5.3	Glosario de Terminología del Proyecto (Entregable)	mié 22/08/18	mié 22/08/18	0.1
27	**1.2.6**	**Gestión de Recurso Humano**	**jue 23/08/18**	lun 27/08/18	**0.3**
28	1.2.6.1	Plan de Gestión de Personal (Entregable)	jue 23/08/18	jue 23/08/18	0.1
29	1.2.6.2	Organigrama del Proyecto (Entregable)	vie 24/08/18	vie 24/08/18	0.1
30	1.2.6.3	Matriz de Asignación de Responsabilidades (Entregable)	lun 27/08/18	lun 27/08/18	0.1
31	1.3	Aprobación del Plan de Trabajo	mar 28/08/18	lun 03/09/18	1
32	**2**	**Definición**	lun 03/09/18	**mar 11/12/18**	**11**
33	**2.1**	**Análisis de Requerimientos**	lun 03/09/18	**mié 12/09/18**	**6**
34	**2.1.1**	**Análisis de Procesos**	lun 03/09/18	**mar 04/09/18**	**2**
35	2.1.1.1	Elaboración de la Presentación de Procesos Actuales	lun 03/09/18	lun 03/09/18	1
36	2.1.1.2	Elaboración de la Presentación de Procesos Propuestos	mar 04/09/18	mar 04/09/18	1
37	**2.1.2**	**Análisis de Medidas de Seguridad**	**mar 04/09/18**	jue 06/09/18	**1**
38	2.1.2.1	One Time Password	**mar 04/09/18**	mar 04/09/18	0.5
39	2.1.2.2	Aplicativo Web	**mié 05/09/18**	jue 06/09/18	0.5
40	**2.1.3**	**Análisis de Reportes**	jue 06/09/18	lun 10/09/18	**3**
41	2.1.3.1	Análisis de Reportes Actuales	jue 06/09/18	jue 06/09/18	1
42	2.1.3.2	Definición de Reportes para Entes Externos	vie 07/09/18	vie 07/09/18	1
43	2.1.3.3	Definición de Reportes para Uso de Departamento Servicios Fisc	lun 10/09/18	lun 10/09/18	1



Proyecto: STIRECFIS
Fecha: jue 24/01/19

Tarea
División
Hito
Resumen
Resumen del proyecto
Tarea inactiva
Hito inactivo
Resumen inactivo
Tarea manual
solo duración
Informe de resumen manual
Resumen manual
solo el comienzo
solo fin
Tareas externas
Hito externo
Fecha límite
Tareas críticas
División crítica
Progreso
Progreso manual

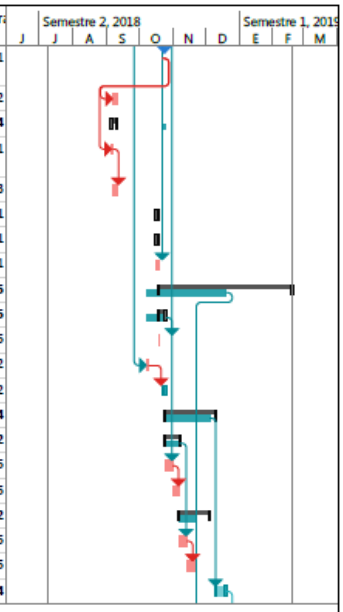
Id	EDT	Nombre de tarea	Comienzo	Fin	Ponderi
44	**2.2**	**Arquitectura de Datos**	lun 03/09/18	vie 19/10/18	3
45	2.2.1	Definición de la Arquitectura de Datos	lun 03/09/18	vie 14/09/18	1
46	2.2.2	Validación del Modelo de Datos	lun 17/09/18	lun 24/09/18	0.5
47	2.2.3	Documentación del Modelo de Datos (Entregable)	mar 25/09/18	lun 15/10/18	0.5
48	2.2.4	Socialización de la Arquitectura de Datos	jue 13/12/18	vie 14/12/18	0.5
49	2.2.5	Implementación del Modelo Físico	lun 17/12/18	mar 18/12/18	0.5
50	**2.3**	**Arquitectura de Aplicación**	lun 03/09/18	jue 18/10/18	2
51	2.3.1	Definición de la Arquitectura de Aplicación	lun 03/09/18	vie 21/09/18	1
52	2.3.2	Documento de Arquitectura de Aplicación (Entregable)	vie 21/09/18	jue 11/10/18	0.5
53	2.3.3	Socialización de la Arquitectura de Aplicación	mié 12/12/18	mar 18/12/18	0.5
54	**3**	**Construcción**	jue 06/09/18	**vie 28/09/18**	15
55	**3.1**	**Desarrollo de la Solución**	jue 06/09/18	mar 16/10/18	13
56	3.1.1	Código Fuente del Módulo Administrativo (Entregable)	jue 06/09/18	mié 12/09/18	5
57	3.1.2	Código Fuente del Capturador (Entregable)	jue 13/09/18	mié 19/09/18	3
58	**3.1.3**	**Código Fuente del Módulo de Reportes (Entregable)**	jue 20/09/18	**vie 21/09/18**	4
59	3.1.3.1	Desarrollo de Reportes del Aplicativo	jue 20/09/18	vie 21/09/18	4
60	3.1.4	Desarrollo de Programas One Time Password	**lun 24/09/18**	mar 16/10/18	1
61	**3.2**	**Implementación y Configuración**	jue 06/09/18	**lun 10/09/18**	1
62	**3.2.1**	**Configuración del Ambiente de Desarrollo**	jue 06/09/18	**lun 10/09/18**	0.3
63	3.2.1.1	Solicitud de Creación de los Ambientes de Desarrollo (Base de Datos y Aplicación)	jue 18/10/18	jue 18/10/18	0.1
64	3.2.1.2	Seguimiento y Verificación de Creación del Ambiente de Desarro	vie 19/10/18	lun 22/10/18	0.2
65	**3.2.2**	**Configuración del Ambiente de Pruebas**	jue 06/09/18	**lun 10/09/18**	0.3



Proyecto: STIRECFIS
Fecha: jue 24/01/19

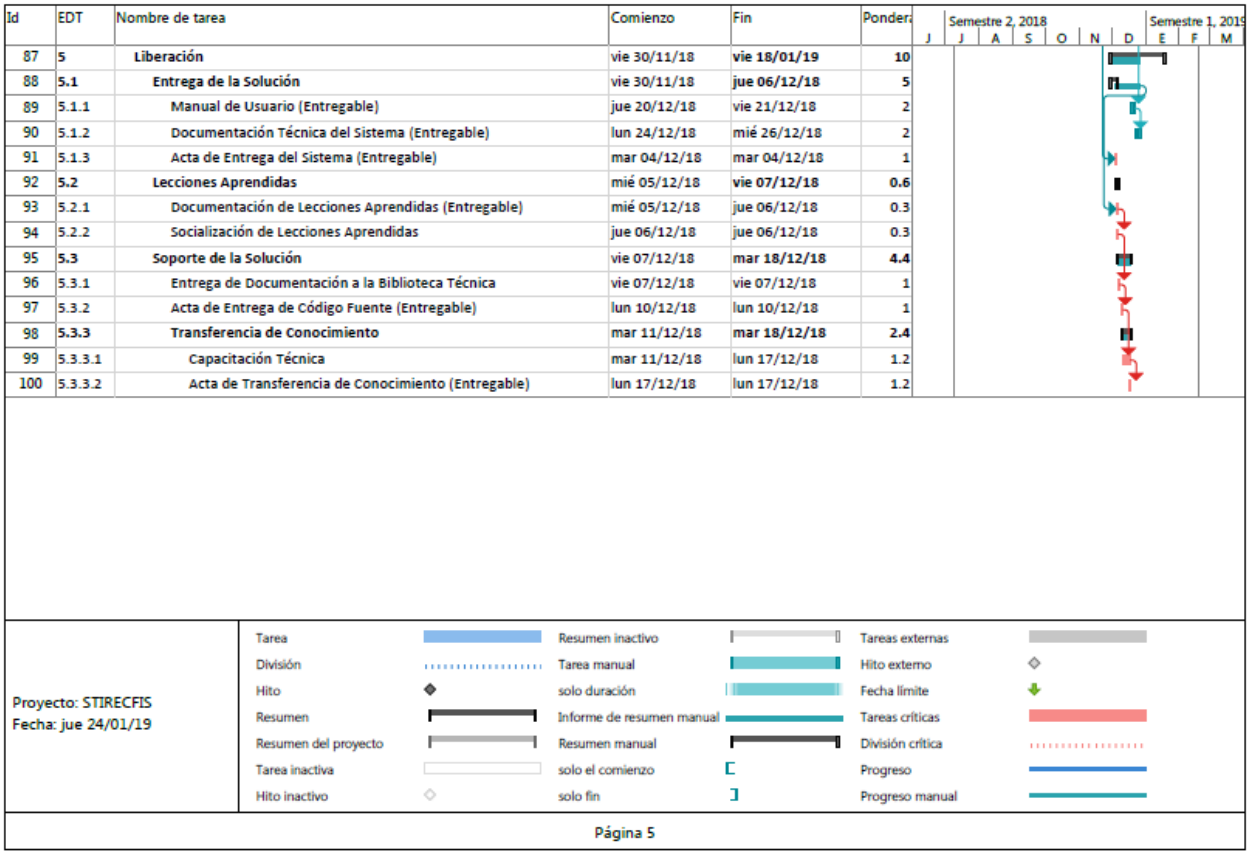
Tarea
División
Hito
Resumen
Resumen del proyecto
Tarea inactiva
Hito inactivo
Resumen inactivo
Tarea manual
solo duración
Informe de resumen manual
Resumen manual
solo el comienzo
solo fin
Tareas externas
Hito externo
Fecha límite
Tareas críticas
División crítica
Progreso
Progreso manual

Id	EDT	Nombre de tarea	Comienzo	Fin	Ponderá
66	3.2.2.1	Solicitud de Creación de los Ambientes de Pruebas (Base de Datos y Aplicación)	lun 22/10/18	lun 22/10/18	0.1
67	3.2.2.2	Seguimiento y Verificación de Creación del Ambiente de Pruebas	vie 07/09/18	lun 10/09/18	0.2
68	**3.2.3**	**Configuración del Ambiente de Producción y Contingencia**	jue 06/09/18	**lun 10/09/18**	**0.4**
69	3.2.3.1	Solicitud de Creación de los Ambientes de Producción (Base de Datos y Aplicación)	jue 06/09/18	jue 06/09/18	0.1
70	3.2.3.2	Seguimiento y Verificación de Creación del Ambiente de Producc	vie 07/09/18	lun 10/09/18	0.3
71	**3.3**	**Pruebas Técnicas**	**mié 17/10/18**	**jue 18/10/18**	1
72	**3.3.1**	**Pruebas Internas**	**mié 17/10/18**	**jue 18/10/18**	1
73	3.3.1.1	Formatos de Pruebas Técnicas (Entregable)	**mié 17/10/18**	jue 18/10/18	1
74	**4**	**Estabilización**	**vie 19/10/18**	**lun 18/02/19**	12.5
75	**4.1**	**Preparación del Despliegue**	**vie 19/10/18**	**jue 25/10/18**	4.5
76	4.1.1	Notificación de Inicio de Prueba con los Agentes Cambiarios	vie 19/10/18	vie 19/10/18	0.5
77	4.1.2	Capacitación de Usuarios Funcionales (Acompañamiento de DST)	lun 08/10/18	mar 09/10/18	2
78	4.1.3	Capacitación a Agentes Cambiarios (Acompañamiento de DST)	mié 24/10/18	jue 25/10/18	2
79	**4.2**	**Pruebas de Usuario**	jue 25/10/18	**lun 10/12/18**	4
80	**4.2.1**	**Pruebas de Usuario Clave**	jue 25/10/18	**mié 07/11/18**	2
81	4.2.1.1	Formatos de Pruebas de Usuario (Entregable)	jue 25/10/18	mié 31/10/18	0.5
82	4.2.1.2	Ejecución de Pruebas de Usuario (Acompañamiento de DST)	jue 01/11/18	mié 07/11/18	1.5
83	**4.2.2**	**Pruebas de Agentes Cambiarios**	mié 07/11/18	**mar 04/12/18**	2
84	4.2.2.1	Formatos de Pruebas de Certificación (Entregable)	mié 07/11/18	mar 13/11/18	0.5
85	4.2.2.2	Ejecución de Pruebas de Certificación (Acompañamiento de DST	mié 14/11/18	mar 20/11/18	1.5
86	**4.3**	**Aceptación del a Solución**	mar 11/12/18	**mié 19/12/18**	4



Proyecto: STIRECFIS
Fecha: jue 24/01/19

Tarea		Resumen inactivo		Tareas externas	
División		Tarea manual		Hito externo	
Hito		solo duración		Fecha límite	
Resumen		Informe de resumen manual		Tareas críticas	
Resumen del proyecto		Resumen manual		División crítica	
Tarea inactiva		solo el comienzo		Progreso	
Hito inactivo		solo fin		Progreso manual	



Id	EDT	Nombre de tarea	Comienzo	Fin	Ponder.
87	5	**Liberación**	vie 30/11/18	vie 18/01/19	10
88	5.1	**Entrega de la Solución**	vie 30/11/18	jue 06/12/18	5
89	5.1.1	Manual de Usuario (Entregable)	jue 20/12/18	vie 21/12/18	2
90	5.1.2	Documentación Técnica del Sistema (Entregable)	lun 24/12/18	mié 26/12/18	2
91	5.1.3	Acta de Entrega del Sistema (Entregable)	mar 04/12/18	mar 04/12/18	1
92	5.2	**Lecciones Aprendidas**	mié 05/12/18	vie 07/12/18	0.6
93	5.2.1	Documentación de Lecciones Aprendidas (Entregable)	mié 05/12/18	jue 06/12/18	0.3
94	5.2.2	Socialización de Lecciones Aprendidas	jue 06/12/18	jue 06/12/18	0.3
95	5.3	**Soporte de la Solución**	vie 07/12/18	mar 18/12/18	4.4
96	5.3.1	Entrega de Documentación a la Biblioteca Técnica	vie 07/12/18	vie 07/12/18	1
97	5.3.2	Acta de Entrega de Código Fuente (Entregable)	lun 10/12/18	lun 10/12/18	1
98	5.3.3	**Transferencia de Conocimiento**	mar 11/12/18	mar 18/12/18	2.4
99	5.3.3.1	Capacitación Técnica	mar 11/12/18	lun 17/12/18	1.2
100	5.3.3.2	Acta de Transferencia de Conocimiento (Entregable)	lun 17/12/18	lun 17/12/18	1.2

Página 5

Se incluyen anexos del 1 al 12 utilizados indicados en color amarillo en el cronograma de actividades del proyecto de implementación.

3.6.2 Scrum

Para la ejecución del proyecto de implementación en la parte de desarrollo de software, se enfocaron esfuerzos utilizando los formatos adaptados en la metodología ágil de desarrollo de Scrum, definidos en la sección de anexos a partir del anexo 13.

CAPÍTULO VI. RESULTADOS Y ANÁLISIS

Considerando los resultados obtenidos mediante la aplicación del instrumento de la encuesta y uso de entrevistas a nuestra población en el Banco Central de Honduras en la ciudad de Tegucigalpa en el Centro Cívico Gubernamental del Boulevard Fuerzas Armadas, del Departamento de Tecnología y Comunicaciones en la División de Operaciones y Telecomunicaciones, obteniendo respuestas de los cuestionarios de preguntas como instrumento y expresando su detalle mediante gráficos de la información, así mismo los resultados determinan una correlación entre las variables de investigación.

4.1 Resultados

4.1.1 Análisis descriptivo de la encuesta a personal especializado en seguridad y telecomunicaciones del BCH

Definir el código generado

1 ¿Considera que los clientes del BCH estarían anuentes a utilizar un token que genere un OTP sin el uso de un dispositivo de infraestructura?

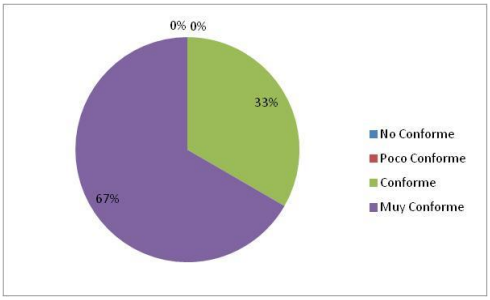


Figura 9 Gráfico de resultados de la pregunta No. 1, apartado 1
Fuente Propia

La gráfica anterior indica, que el 67% de la población está muy de acuerdo en utilizar software para la generación de un código OTP.

2 ¿Considera que el código generado por el dispositivo de infraestructura token se puede reemplazar a nivel de software?

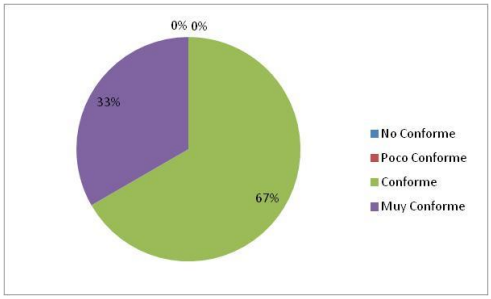


Figura 10 Gráfico de resultados de la pregunta No. 2, apartado 1
Fuente Propia

La gráfica anterior indica, que el 67% de la población está de acuerdo en generar un OTP a nivel de software, reemplazando el dispositivo de infraestructura token.

3 ¿Conoce si existe alguna norma o política que impida el uso de software que genere un código OTP en sustitución del dispositivo token a nivel de infraestructura?

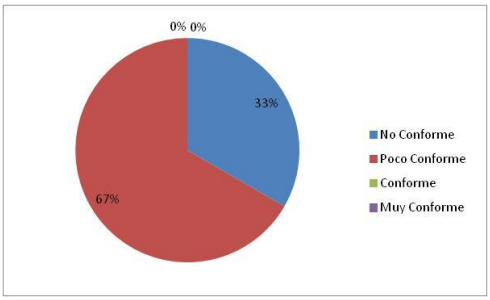


Figura 11 Gráfico de resultados de la pregunta No. 3, apartado 1
Fuente Propia

La gráfica anterior indica, que el 67% de la población no conoce si existe alguna política que impida la generación de OTP mediante software.

4 ¿Conoce si todos los clientes del BCH que usan sus sistemas de información utilizan dispositivos de infraestructura token?

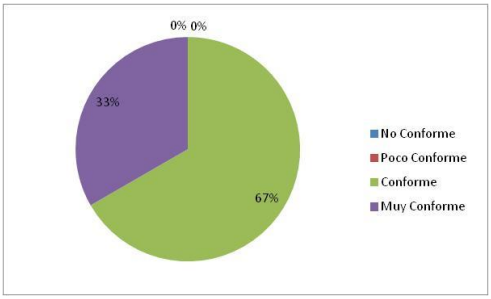


Figura 12 Gráfico de resultados de la pregunta No. 4, apartado 1
Fuente Propia

La gráfica anterior indica, que el 67% de la población utiliza un dispositivo de infraestructura token.

5 ¿Estaría conforme si para el reemplazo del token que genera el OTP se utilizara la infraestructura que el BCH posee?

El 100% de la población indico que está de acuerdo en reutilizar la infraestructura del BCH para generar un mecanismo alterno.

6 ¿Conoce si el BCH cuenta con alguna restricción en la cantidad mínima de dígitos que el OTP debe tener?

El 100% de la población considera que no existe una restricción en la cantidad mínima de dígitos que el código OTP tiene que contener.

7 ¿Conoce si el BCH cuenta con alguna restricción en el tiempo de vigencia el código OTP generado?

El 100% de la población considera que no existe una restricción en el tiempo de vigencia del código OTP generado.

Establecer el mecanismo seguro

1 ¿Actualmente el BCH cuenta con presupuesto para el uso de dispositivos token?

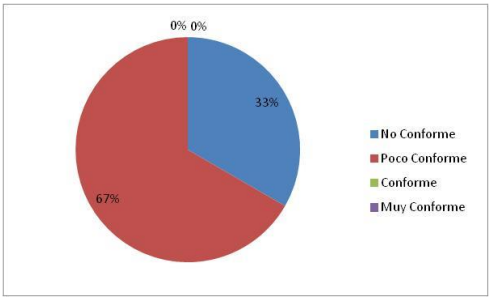


Figura 13 Gráfico de resultados de la pregunta No. 1, apartado 2
Fuente Propia

La gráfica anterior indica, que el 67% de la población considera desconocer si existe presupuesto para compra de dispositivos de infraestructura token.

2 ¿Seleccione el nivel de conformidad o de su preferencia, que considera que el uso de token a nivel de infraestructura suple en el BCH?

El 100% de la población considera que el token a nivel de infraestructura, suple las necesidades de seguridad como mecanismo adicional de autenticación.

3 ¿El BCH cuenta con formatos para el uso o asignación de token?

El 100% de la población conoce que el BCH cuenta con formatos o políticas para la asignación de token.

4 ¿Considera que en el BCH se puede incorporar el uso a nivel de software de token y no mediante el dispositivo de infraestructura?

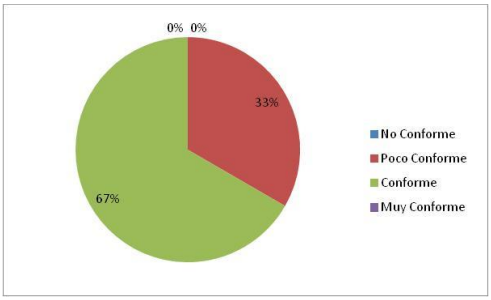


Figura 14 Gráfico de resultados de la pregunta No. 4, apartado 2
Fuente Propia

La gráfica anterior indica, que el 67% de la población considera que se podría sustituir la generación del código OTP a nivel de infraestructura, con la generación del código OTP a nivel de software.

5 ¿Estaría conforme con el uso del correo corporativo del BCH para el uso del OTP?

El 100% de la población considera que se puede enviar el código OTP por medio del correo corporativo.

6 ¿Conoce si en el BCH es factible el uso de base de datos en temas de seguridad?

El 100% de la población considera que el uso de la base de datos en temas de seguridad es factible.

7 ¿Conoce si en el BCH es factible el uso de aplicativos desarrollados en lenguaje .NET en temas de seguridad?

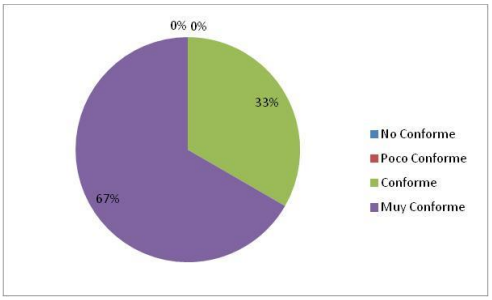


Figura 15 Gráfico de resultados de la pregunta No. 7, apartado 2
Fuente Propia

La gráfica anterior indica, que el 67% de la población considera que el uso de .NET en temas de seguridad es factible.

Gestionar el proceso de seguridad

1 ¿Tiene conocimiento de políticas o normas de seguridad en el BCH que apoyen el uso del token y OTP?

El 100% de la población considera conocer la existencia de políticas y normas que apoyan el uso de un mecanismo adicional de autenticación.

2 ¿El BCH cuenta con un plan o guía de mejora continua en la seguridad de sistemas de información?

El 100% de la población considera que el BCH cuanta con un plan de mejora continua para la seguridad en sistemas informáticos.

3 ¿Se cuenta con documentación del proceso para habilitar los token a los clientes del BCH?

El 100% de la población considera conocer los procesos de documentación para gestionar la habilitación de token a usuarios.

4 ¿Es usted el encargado de autorizar, definir, implementar o sugerir mejorar en temas de seguridad o telecomunicaciones del BCH?

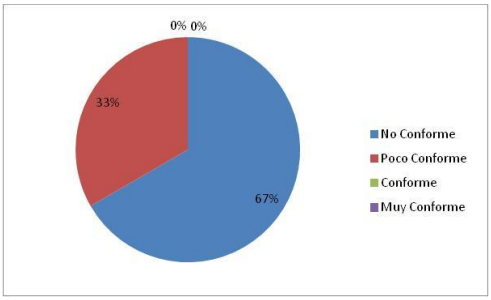


Figura 16 Gráfico de resultados de la pregunta No. 4, apartado 3
Fuente Propia

La gráfica anterior indica, que el 67% de la población no cuenta con la potestad para gestionar mejoras en temas de seguridad o telecomunicaciones, y el 33% de la población puede sugerir mejorar en niveles de seguridad.

5 ¿Conoce si el BCH utiliza herramientas que le faciliten la administración de los códigos OTP que generan los dispositivos de infraestructura token?

El 100% de la población conoce que existen herramientas para la administración de dispositivos de infraestructura token.

6 ¿Conoce si en el BCH se cuenta con procesos que controlen los cambios a nivel de infraestructura y sistemas de información?

La gráfica anterior indica, que el 100% de la población conoce que en el BCH existen procesos que controlan el cambio a nivel de infraestructura y sistemas de información.

7 ¿Conoce si el BCH brinda a sus clientes informes de auditoría a nivel de seguridad relacionados con el uso del OTP?

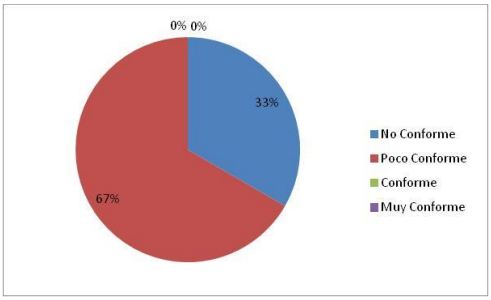


Figura 17 Gráfico de resultados de la pregunta No. 7, apartado 3
Fuente Propia

La gráfica anterior indica, que el 67% de la población considera desconocer si se brinda informes de auditoría por el uso de OTP a los clientes del BCH.

4.1.2 Análisis de confianza del instrumento.

En esta sección se muestra a través del coeficiente Alpha de Cronbach, la consistencia de puntuaciones obtenidas, que los encuestados han definido acorde a su criterio; Celina Oviedo & Campo Arias(2005) menciona que el valor mínimo aceptable para el coeficiente es de 0.70, por

su parte el valor máximo debería ser de 0.90 por encima de este valor hay redundancia o duplicidad, usualmente se prefieren valores entre 0.80 y 0.90.

La confiabilidad del instrumento utilizado como encuesta en las entrevistas realizadas al personal especialista en el BCH en el Departamento de Tecnología y Comunicaciones en la División de Operaciones y Telecomunicaciones, se muestra a continuación:

Tabla 4 Resultado de Entrevistas

Encuestados	P 1	P 2	P 3	P 4	P 5	P 6	P 7	P 8	P 9	P 10	P 11	P 12	P 13	P 14	P 15	P 16	P 17	P 18	P 19	P 20	P 21	Total
1	4	4	2	4	4	2	2	2	4	4	3	4	4	4	4	4	4	2	4	4	2	71
2	4	3	2	3	4	2	2	1	4	4	3	4	4	4	4	4	4	1	4	4	2	67
3	3	3	1	3	4	2	2	2	4	4	2	4	4	3	4	4	4	1	4	4	1	63
Varianza	0.3	0.3	0.3	0.3	0.0	0.0	0.0	0.3	0.0	0.0	0.3	0.0	0.0	0.3	0.0	0.0	0.0	0.3	0.0	0.0	0.3	

Escala de medición: 1-No Conforme, 2-Poco Conforme, 3-Conforme, 4-Muy Conforme

K	21	Sección 1	1.05	
Vi	3.0	Sección 2	0.813	
Vt	16.00	Absoluto S2	0.813	
		a	0.85	Nivel de confianza

$$\propto = \frac{K}{K-1}\left[1 - \frac{\sum Vi}{Vt}\right]$$

Fuente: Propia

Logrando con el ello al final del cálculo del coeficiente de Alfa de Cronbach un resultado del 85%, siendo superior al 80% y menor que el 90% establecido como preferido para ser confiable, con lo cual se considera consistente el instrumento aplicado a la población definida.

Virla,(2010) menciona que los factores que se buscan reducir mediante la aplicación del coeficiente de Alfa de Cronbach son los siguientes: instrucciones no estandarizadas, instrucciones dadas por el encuestador oralmente sin contar con un conjunto estándar de instrucciones que pueda leerse sin variaciones, errores en el registro de puntajes, errores debido al ambiente de medición , relacionados a condiciones ambientales distintas (iluminación, niveles de ruido, confort, etc.).

4.1.3 Comprobación de la hipótesis

En esta sección se hace el análisis de variables utilizando el método de Coeficiente de Correlación de Pearson, el cual tiene por objetivo medir la asociación o interdependencia entre dos variables estadísticas.

Parameters

- Método: Correlación de momento-producto de Pearson
- Omitir valores no presentes: en parejas

Coeficiente	var1 (Definir el código generado)	var2 (Establecer el mecanismo seguro)	var3 (Gestionar el proceso de seguridad)
var1 (Definir el código generado)	1.0000000	0.9538210	0.9971765
var2 (Establecer el mecanismo seguro)	0.9538210	1.0000000	0.9285714
var3 (Gestionar el proceso de seguridad)	0.9971765	0.9285714	1.0000000

los valores de p y el tamaño de la muestra

n \ p	var1 (Definir el código generado)	var2 (Establecer el mecanismo seguro)	var3 (Gestionar el proceso de seguridad)
var1 (Definir el código generado)	NA	0.1942241	0.04785132
var2 (Establecer el mecanismo seguro)	3	NA	0.24207544
var3 (Gestionar el proceso de seguridad)	3	3.0000000	NA

Figura 18 Matriz de correlación

Fuente Propia

En la matriz anterior se muestran los datos obtenidos de relacionar las variables de investigación utilizando una herramienta de software llamada RKward, misma que revela que contamos con un coeficiente de correlación de 0.99 obteniendo una relación positiva ya que el valor se acerca a uno, por lo tanto, podemos afirmar que la correlación entre las variables es positiva.

Prueba de hipótesis

H^0: No existe relación entre el código generado, mecanismo seguro y gestionar el proceso de seguridad.

H^1: Existe relación entre el código generado, mecanismo seguro y gestionar el proceso de

seguridad.

Criterio de decisión:

El valor de índice de correlación varía en el intervalo -1 y 1 indicando el signo de la relación. Si $0 < r < 1$, existe una fuerza de correlación positiva.

Con un nivel de significación del 0.05 ($\alpha=0.05$) se rechaza H0 a favor de H1 siempre que

$r < 0.05$

Considerando que el valor r de las variables de investigación es de 0.04 siendo menor a 0.05 y considerando los factores positivos reflejados en el instrumento de investigación aplicado a los expertos en seguridad informática del BCH, además de un nivel de 95% de confianza, se acepta la hipótesis alternativa que indica que existe relación entre las variables de investigación, rechazando la hipótesis nula.

4.2 APLICABILIDAD DEL PROYECTO

Cuando se trata de seguridad en sistemas informáticos, no existe distinción entre ambientes web o programas de escritorio, todas las empresas sin importar el rubro, requieren mecanismos informáticos de seguridad para proteger sus datos, ya que la evolución y surgimiento de nuevas tecnologías de comunicaciones, impulsa a que se mejoren los sistemas tradicionales de seguridad.

Molero Escobar, (2011) afirma: “Uno de los grandes aliados de la seguridad informática es la criptografía gracias a la utilización de funciones hash. Las funciones hash se utilizan en las comunicaciones para almacenar contraseñas, para verificar la integridad de mensajes, etc.”

Una función hash se utiliza como una huella que identifica de forma única un conjunto de datos. Ante la implementación de este método, los hackers han logrado romper las funciones criptográficas con ataques de fuerza bruta y utilización de tablas de consulta. Los ataques de fuerza bruta consisten en generar algoritmos de forma aleatoria hasta encontrar el carácter deseado, mientras que las tablas de consulta son algoritmos hash ya almacenados previamente y se consultan según sea la necesidad.

Las funciones hash son funciones que se encargan de resumir una cadena binaria, se conoce como pre imagen, da como resultado una huella o imagen de sí misma. Estas imágenes o huellas son algoritmos complejos, los cuales se pueden identificar inequívocamente con un gran porcentaje de probabilidad. Molero Escobar, (2011) afirma: “si se introducen diferentes informaciones a la misma función hash, la probabilidad de que devuelva el mismo resultado es ínfima”

4.2.1 Desarrollo librería de clases .NET

Figura 19 Algoritmo Criptográfico
Fuente: Molero Escobar, (2011)

En la figura anterior se muestra el funcionamiento básico de un algoritmo de cifrado el cual consta de los siguientes elementos:

- **Texto plano**: es el mensaje enviado por el receptor, resultando ininteligible para cualquier usuario.
- **Texto cifrado**: respuesta de codificar el texto plano.
- **Función de cifrado**: es el mecanismo a través del cual a partir de un texto claro se obtiene un texto cifrado, y a partir de un texto cifrado se consigue un texto en claro.
- **Contraseña, llave o clave**: es la información compartida entre el emisor y el receptor mediante la cual es posible cifrar y descifrar.

Para implementar el OTP, se desarrolló un proyecto de librerías de clases en la herramienta Visual Studio .Net 2018. La metodología a utilizar es Hash Sha-1, este método fue

creado por National Institute of Standars and Technology (NIST) en 1994, su tamaño de resumen es de 160 bits, es decir para encontrar el mensaje se requieren 80 pasos con una probabilidad de 2 elevado a 160 (2^160).

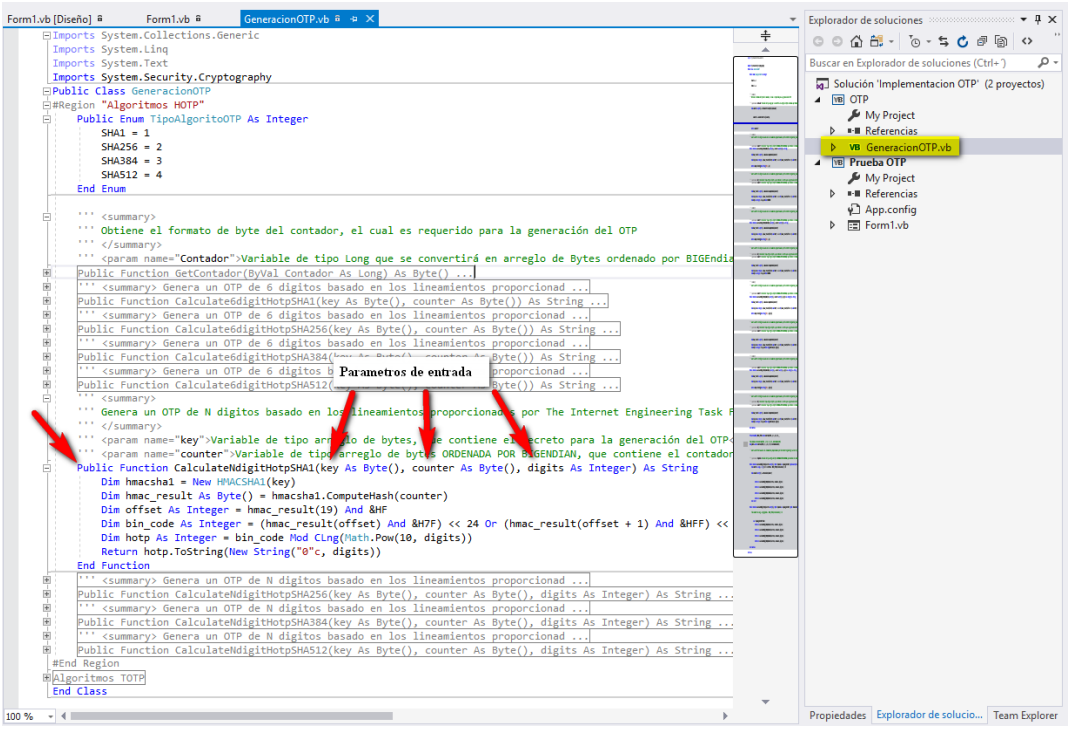


Figura 20 Implementación Clase OTP

Fuente: Propia

Para utilizar las funciones criptográficas existentes en Visual Studio, se realizó la importación de la librería de clases Cryptography, la cual contiene encapsulados las funciones generadas y autorizadas por el IETF.

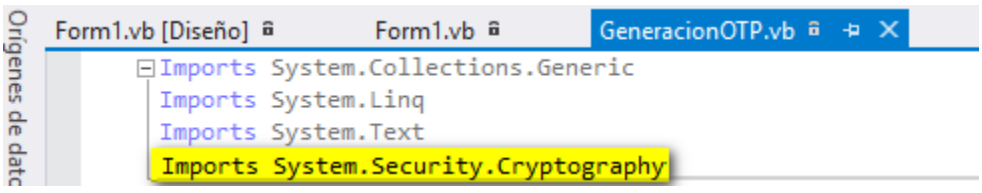


Figura 21 Importación librerías de clases criptográficas

Fuente: Propia

```
''' <summary>
''' Genera un OTP de N digitos basado en los lineamientos proporcionados por The Internet Engineering Task Force (IETF®) y utilizando un algoritmo de H
''' </summary>
''' <param name="key">Variable de tipo arreglo de bytes, que contiene el secreto para la generación del OTP</param>
''' <param name="counter">Variable de tipo arreglo de bytes ORDENADA POR BIGENDIAN, que contiene el contador para la generación del OTP</param>
Public Function CalculateNdigitHotpSHA1(key As Byte(), counter As Byte(), digits As Integer) As String
    Dim hmacsha1 = New HMACSHA1(key)
    Dim hmac_result As Byte() = hmacsha1.ComputeHash(counter)
    Dim offset As Integer = hmac_result(19) And &HF
    Dim bin_code As Integer = (hmac_result(offset) And &H7F) << 24 Or (hmac_result(offset + 1) And &HFF) << 16 Or (hmac_result(offset + 2) And &HFF) <<
    Dim hotp As Integer = bin_code Mod CLng(Math.Pow(10, digits))
    Return hotp.ToString(New String("0"c, digits))
End Function
```

Figura 22 Función que genera clave OTP

Fuente: Propia

En la 32 se muestra una función de tipo texto la cual recibe 3 parámetros de entrada, los cuales se detallan a continuación:

- Key (llave): parámetro que recibe el secreto generado por el sistema.
- Counter: variable de tipo arreglo que almacena la cantidad de caracteres a ser generados por el OTP
- Digits: parámetro que define el tamaño a generar de la contraseña.

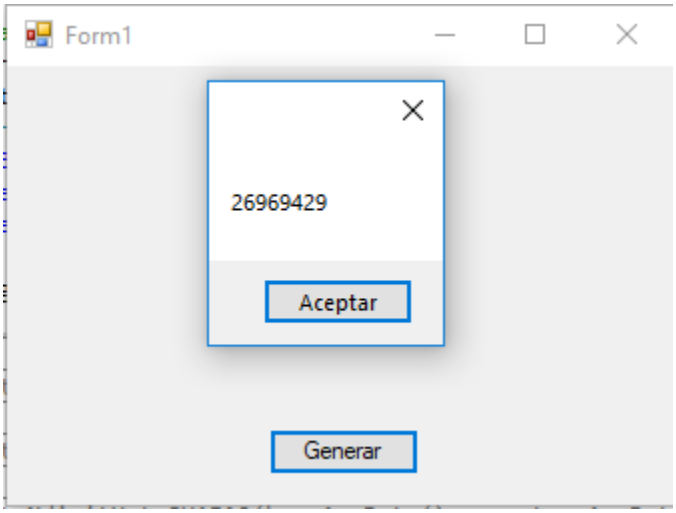


Figura 23 Implementación código OTP

Fuente: Propia

```
Public Class Form1
    Dim otp As New OTP.GeneracionOTP
    Private Sub Button1_Click(sender As Object, e As EventArgs) Handles Button1.Click
        Dim encoding As New System.Text.UTF8Encoding()
        Dim secretKey As Byte() = encoding.GetBytes("12345678901234567890")
        MessageBox.Show(otp.CalculateNdigitHotpSHA1(secretKey, otp.GetContador(3), 8))
    End Sub
End Class
```

Figura 24 Uso clase OTP

Fuente: Propia

En la figura 34 se muestra la forma de hacer un llamado a la biblioteca de clases generada, así como la generación del OTP. Debido a que el secreto es un parámetro de entrada, este será un valor que se estará generando dinámicamente por la base de datos.

4.2.2 Desarrollo a nivel de base de datos ORACLE 11g edición empresarial

En la base de datos se crea un usuario que como ejemplo será “USRRECFIS” que es un usuario para recaudación fiscal con el rol de “CONNECT” para que logre ingresar a la base de datos y el rol de “RESOURCE” para que se puedan crear algunos objetos propios de base de datos, este usuario será reemplazado por cada uno de los esquemas (usuario pero con objetos) de base de datos que los sistemas financieros en producción utilizan en Banco Central de Honduras.

Ahora se procede a la autorización del nuevo usuario creado “USRRECFIS” para que pueda hacer uso del subprograma “DBMS_CRYPTO” y de la tabla “PROPS$” mediante el usuario administrador de la base de datos “SYS” que a continuación se muestra:

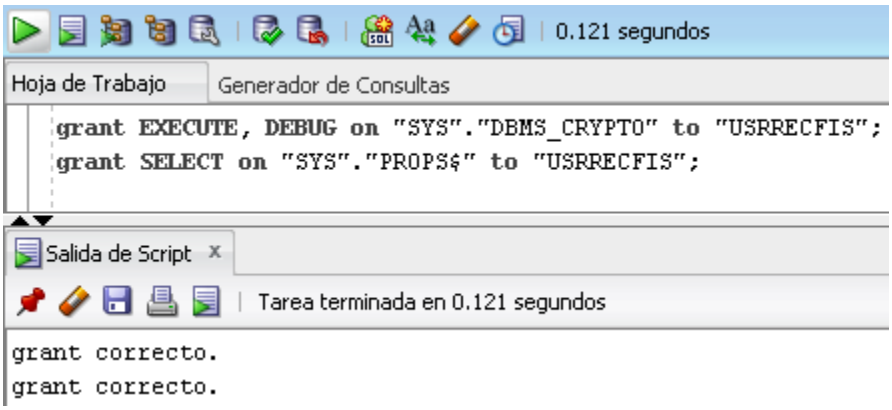


Figura 25 Autorización para uso de objetos

Fuente: Propia

En la figura anterior podemos observar como se ha efectuado el proceso faltando solo confirmar la operación mediante la ejecución del comando “COMMIT” con lo cual el privilegio otorgado al usuario USRRECFIS quedará confirmado para su uso en el momento y forma que requiera.

Seguidamente se procede a crear la función responsable de encriptar o cifrar la información que se brinde acorde a los parámetros establecidos de entrada como se muestra a continuación:

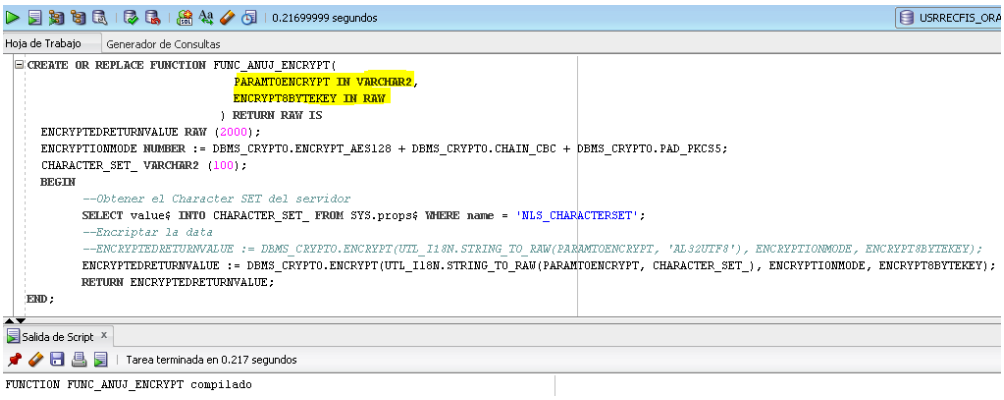


Figura 26 Creación función de cifrado de información

Fuente: Propia

En la figura anterior podemos observar que la función ha sido compilada o creada

exitosamente presentando dos parámetros de entrada, el primero solicita se le brinde el valor a encriptar o cifrar y el segundo le solicita la llave de encriptación siendo los insumos para que la función efectué su labor, como se puede observar utiliza el Estándar Avanzado de Cifrado (AES, por sus siglas en ingles) que es una encriptación simétrica que es utilizada por los Algoritmos de Hash Seguros (SHA) principalmente utilizado para contraseñas o información importante.

También podemos observar como la función obtiene el set de caracteres que el servidor de base de datos utiliza para ser implementado en la encriptación o cifrado de la información que se le proporciona a la función; notando que al final ejecuta el subprograma para encriptar con toda la información que le solicita antes de iniciar el proceso y una vez ejecutado el resultado obtenido es devuelto como producto al terminar.

De forma muy similar se crea la función encargada de desencriptar o descifrar la información que se le b rinda como insumo como se muestra a continuación:

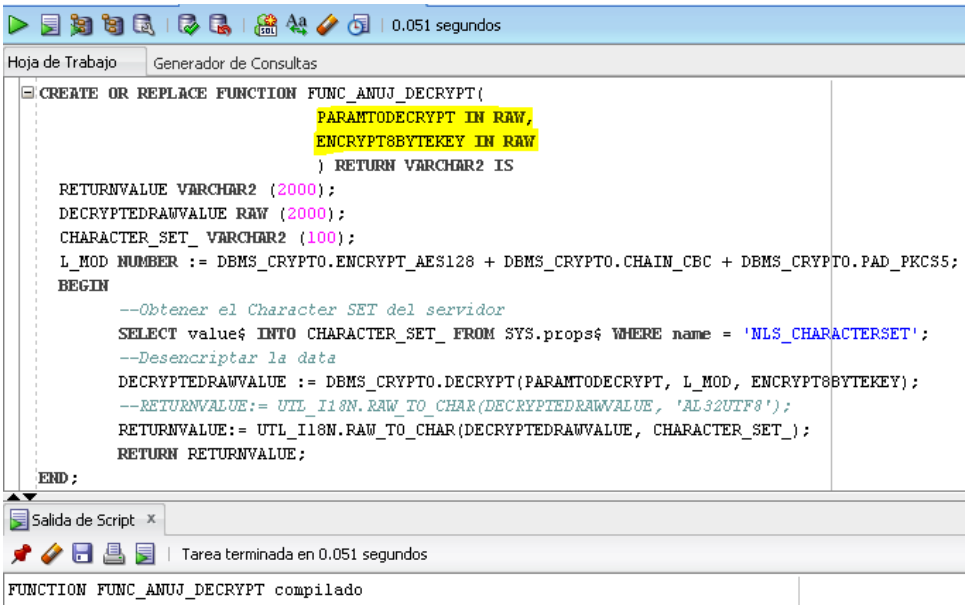


Figura 27 Creación de función de descifrado de información

Fuente: Propia

Como se muestra en la figura anterior, podemos observar que requiere dos campos de entrada el primero se refiere a la información encriptada y el segundo solicita la llave de encriptación; de forma similar a la función anterior en esta también es requerido obtener el set de caracteres que el servidor de base de datos utiliza, después se procede a desencriptar o descifrar la información proporcionada devolviendo así la información de forma legible.

4.2.3 Implementación del OTP

El desarrollo del algoritmo se implementó en El Departamento de Servicios Fiscales del Banco Central de Honduras, dicha dependencia es responsable de realizar las operaciones de recepción, revisión y de registro estadístico y contable de los ingresos Tributarios, aduaneros y no Tributarios del Estado, en vista de lo anterior, y con el propósito de automatizar el proceso de Recaudaciones Fiscales, se implementó el Sistema de Transferencia de Información de Recaudaciones Fiscales (STI-RECFIS), sistema diseñado para brindar a los Bancos del Sistema Financieros Nacional autorizados, un sitio web que permita agilizar la transmisión de los archivos electrónicos y documentos soportes de las Recaudaciones Fiscales del Estado.

4.2.4 Arquitectura de acceso al STI-RECFIS

Por la finalidad de las transacciones que se realizaran en el STI-RECFIS, se implementó una serie de mecanismos de seguridad los cuales se detallan a continuación:

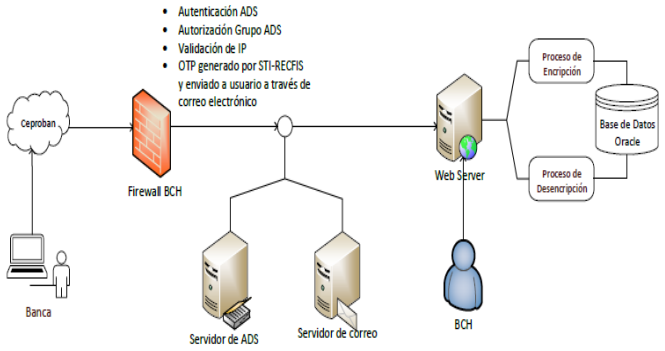


Figura 28 Uso de arquitectura OTP

Fuente: Propia

- **Banca**: usuario financiero que tendrá accesos al aplicativo.
- **CEPROBAN**: red privada del sistema financiero diseñada para proteger las transacciones y operaciones entre las instituciones bancarias.
- **Firewall BCH (muro de fuego)**: el muro de fuego está diseñado para permitir únicamente el acceso a los usuarios y entidades propiamente autorizados.
- **Servidor ADS**: servidor del directorio activo del BCH en el cual se registran las personas autorizadas para hacer uso de las aplicaciones.
- **Servidor de Correo**: servidor que usa la aplicación para envió de notificaciones generadas en el sistema.
- **BCH**: usuario funcional del Departamento de Servicios Fiscales, los cuales tienen como principal actividad, aprobar las recaudaciones fiscales.
- **Web Server**: servidor físico donde se publicará el sistema al cual tendrán accesos las instituciones financieras.
- **Proceso de encriptación y desencriptación**: método seguro para certificar a los usuarios financieros que su información y accesos son seguros.
- **Base de Datos Oracle**: servidor donde se almacena la información enviada por los usuarios, así como el almacenamiento de las llaves privadas para cada sesión generada por el usuario.

4.2.5 Esquema de autenticación y autorización

La autenticación al sistema se genera por 2 caminos:

- **Generación del OTP**: el usuario por medio de una dirección IP valida, ingresa a la aplicación, por medio de su usuario y contraseña solicita el OTP para ingresar al sistema. El usuario y contraseña se valida en el directorio activo y cuando es válido y está dentro del grupo de usuarios autorizados, se envía mediante correo electrónico el código de la sesión.

- **Ingreso a la aplicación**: el usuario por medio de una dirección IP valida, ingresa a la aplicación, por medio de usuario y contraseña más el OTP generado por el sistema, realizando sus validaciones en el directorio activo. A continuación, se detalla en el siguiente diagrama.

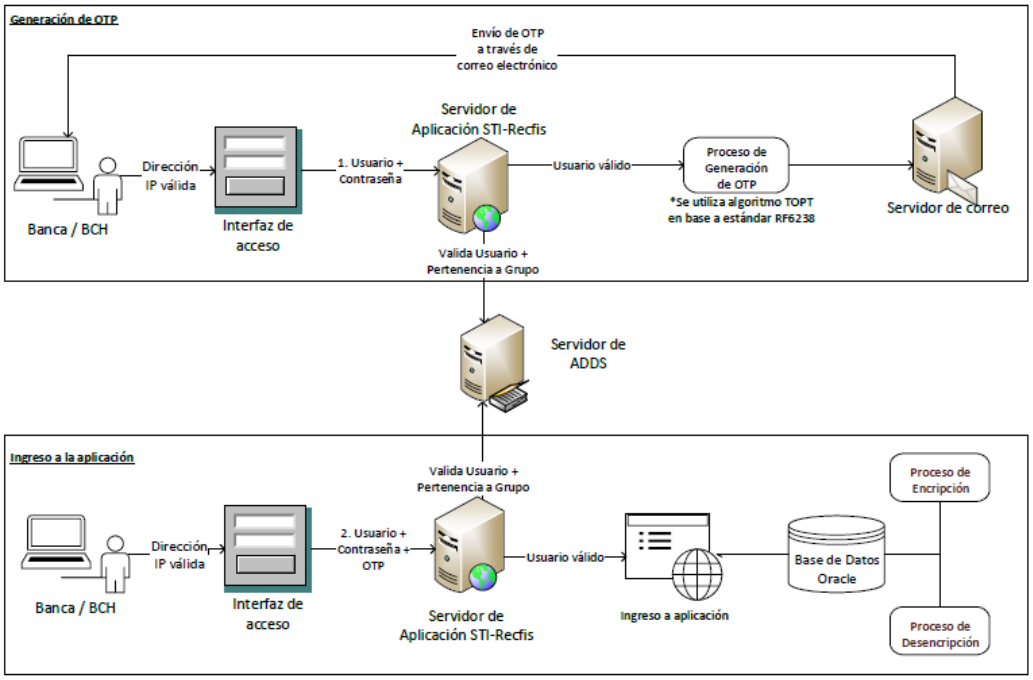


Figura 29 Esquema autenticación y autorización

Fuente: Propia

4.2.6 Implementación Sistema STI-RECFIS

Para la implementación en el sistema, primero se debe agregar la referencia al proyecto de la clase OTP creada.

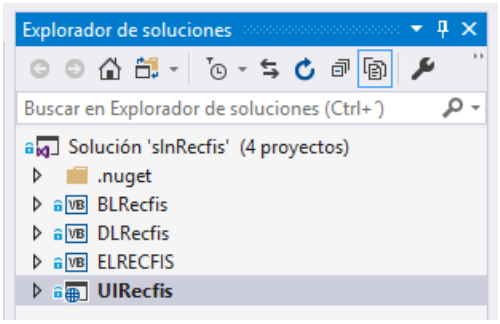


Figura 30 Solución STI-RECFIS

Fuente: Propia

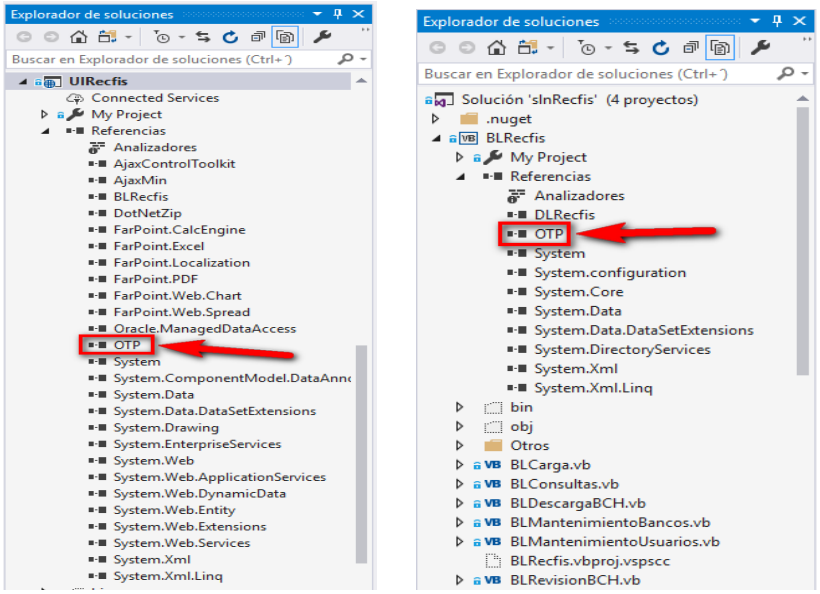
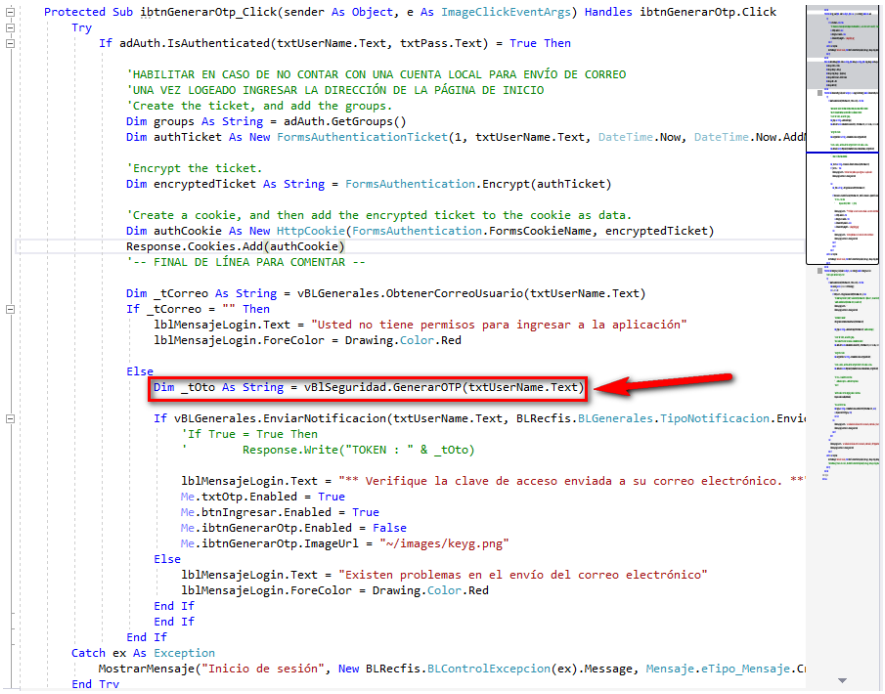


Figura 31 Referencia Clase OTP Interfaz de usuario y clase de reglas de negocio

Fuente: Propia

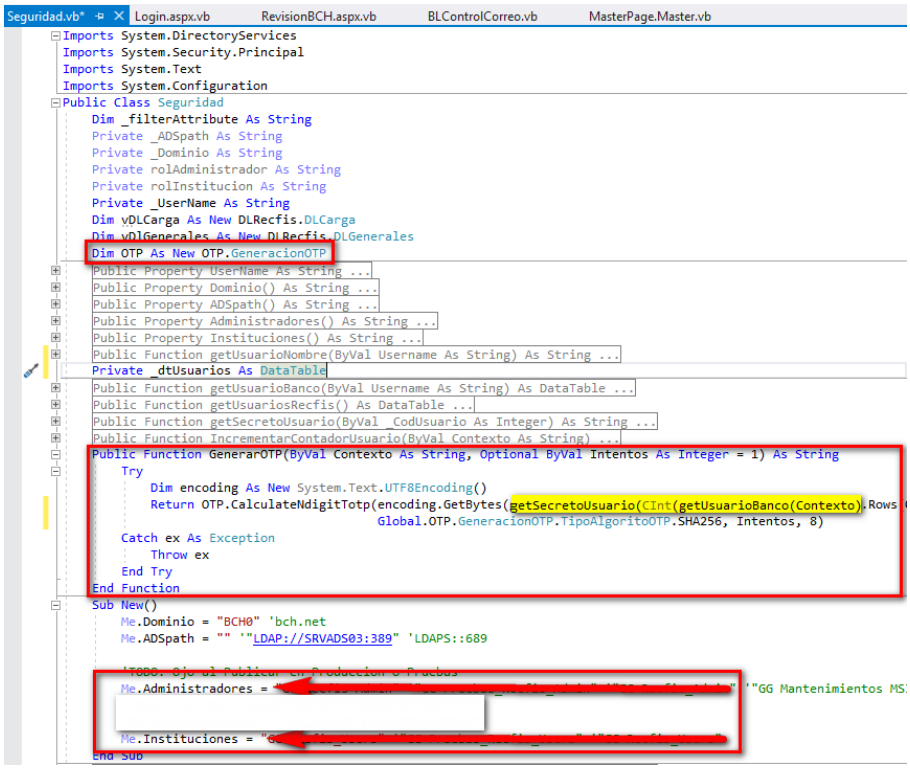
Se agregó el código fuente necesario para que en el botón de inicio de sesión solicite el OTP, a continuación, se detalla el código generado:



```
Protected Sub ibtnGenerarOtp_Click(sender As Object, e As ImageClickEventArgs) Handles ibtnGenerarOtp.Click
    Try
        If adAuth.IsAuthenticated(txtUserName.Text, txtPass.Text) = True Then

            'HABILITAR EN CASO DE NO CONTAR CON UNA CUENTA LOCAL PARA ENVÍO DE CORREO
            'UNA VEZ LOGEADO INGRESAR LA DIRECCIÓN DE LA PÁGINA DE INICIO
            'Create the ticket, and add the groups.
            Dim groups As String = adAuth.GetGroups()
            Dim authTicket As New FormsAuthenticationTicket(1, txtUserName.Text, DateTime.Now, DateTime.Now.Add

            'Encrypt the ticket.
            Dim encryptedTicket As String = FormsAuthentication.Encrypt(authTicket)

            'Create a cookie, and then add the encrypted ticket to the cookie as data.
            Dim authCookie As New HttpCookie(FormsAuthentication.FormsCookieName, encryptedTicket)
            Response.Cookies.Add(authCookie)
            '-- FINAL DE LÍNEA PARA COMENTAR --

            Dim _tCorreo As String = vBLGenerales.ObtenerCorreoUsuario(txtUserName.Text)
            If _tCorreo = "" Then
                lblMensajeLogin.Text = "Usted no tiene permisos para ingresar a la aplicación"
                lblMensajeLogin.ForeColor = Drawing.Color.Red

            Else
                Dim _tOto As String = vBlSeguridad.GenerarOTP(txtUserName.Text)

                If vBLGenerales.EnviarNotificacion(txtUserName.Text, BLRecfis.BLGenerales.TipoNotificacion.Envi
                    'If True = True Then
                    '        Response.Write("TOKEN : " & _tOto)

                    lblMensajeLogin.Text = "** Verifique la clave de acceso enviada a su correo electrónico. **"
                    Me.txtOtp.Enabled = True
                    Me.btnIngresar.Enabled = True
                    Me.ibtnGenerarOtp.Enabled = False
                    Me.ibtnGenerarOtp.ImageUrl = "~/images/keyg.png"
                Else
                    lblMensajeLogin.Text = "Existen problemas en el envío del correo electrónico"
                    lblMensajeLogin.ForeColor = Drawing.Color.Red
                End If
                End If
            End If
    Catch ex As Exception
        MostrarMensaje("Inicio de sesión", New BLRecfis.BLControlExcepcion(ex).Message, Mensaje.eTipo_Mensaje.C
    End Try
```

Figura 32 Invocar clase OTP

Fuente: Propia



```
Seguridad.vb*  Login.aspx.vb  RevisionBCH.aspx.vb  BLControlCorreo.vb  MasterPage.Master.vb

Imports System.DirectoryServices
Imports System.Security.Principal
Imports System.Text
Imports System.Configuration
Public Class Seguridad
    Dim _filterAttribute As String
    Private _ADSpath As String
    Private _Dominio As String
    Private rolAdministrador As String
    Private rolInstitucion As String
    Private _UserName As String
    Dim vDLCarga As New DLRecfis.DLCarga
    Dim vDLGenerales As New DLRecfis.DLGenerales
    Dim OTP As New OTP.GeneracionOTP
    Public Property UserName As String ...
    Public Property Dominio() As String ...
    Public Property ADSpath() As String ...
    Public Property Administradores() As String ...
    Public Property Instituciones() As String ...
    Public Function getUsuarioNombre(ByVal Username As String) As String ...
    Private _dtUsuarios As DataTable
    Public Function getUsuarioBanco(ByVal Username As String) As DataTable ...
    Public Function getUsuariosRecfis() As DataTable ...
    Public Function getSecretoUsuario(ByVal _CodUsuario As Integer) As String ...
    Public Function IncrementarContadorUsuario(ByVal Contexto As String) ...
    Public Function GenerarOTP(ByVal Contexto As String, Optional ByVal Intentos As Integer = 1) As String
        Try
            Dim encoding As New System.Text.UTF8Encoding()
            Return OTP.CalculateNdigitTotp(encoding.GetBytes(getSecretoUsuario(CInt(getUsuarioBanco(Contexto)).Rows
                                           Global.OTP.GeneracionOTP.TipoAlgoritoOTP.SHA256, Intentos, 8)
        Catch ex As Exception
            Throw ex
        End Try
    End Function
    Sub New()
        Me.Dominio = "BCH0" 'bch.net
        Me.ADSpath = "" '"LDAP://SRVADS03:389" 'LDAPS::689

        'TODO: Ojo al Publicar en Producción o Pruebas
        Me.Administradores = "                                                    "GG Mantenimientos MS

        Me.Instituciones = "
    End Sub
```

Figura 33 Clase de seguridad, capa reglas de negocio

Fuente: Propia

En la imagen anterior se muestra el llamado a la OTP referenciada al proyecto, el algoritmo de generación es SHA256, además se muestra el constructor de la clase en el cual se crearon grupos de usuarios para elevar el nivel de seguridad por medio del ADS.

```
''' <summary>
''' Función que devuelve el secreto de usuario.
''' </summary>
''' <param name="_CodigoUsuario"></param>
''' <returns></returns>
''' <remarks></remarks>
Public Function ObtenerSecreto(ByVal _CodigoUsuario As Integer) As DataTable
    Try
        Return AccesoDatos.TraerDataTable("PAQRECFIS.FU_SEGURIDADRECFISGET", "", _CodigoUsuario)
    Catch ex As Exception
        Throw ex
    End Try
End Function
```

Figura 34 Obtener secreto generado en la base de datos

Fuente: Propia

Esta función invoca el procedimiento almacenado que se encarga de sincronizar el secreto generado aleatoriamente en la base de datos, para cada sesión valida por usuario.

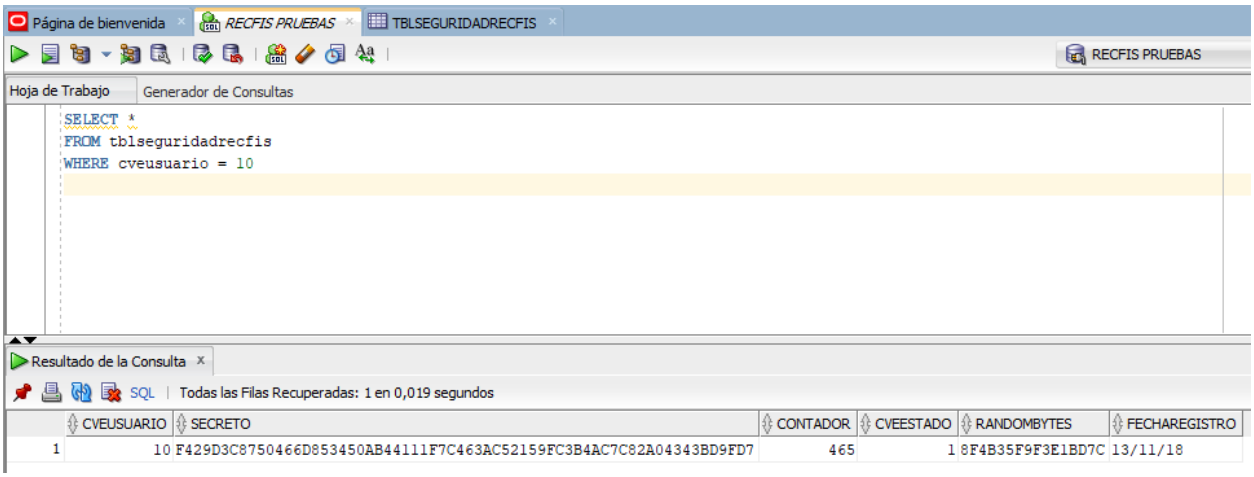


Figura 35 Tabla de almacenamiento en la base de datos

Fuente: Propia

En la figura anterior se muestra la tabla que almacena el secreto generado en la base de datos para cada sesión de usuario valida.

4.2.7 Ingreso al STI-RECFIS

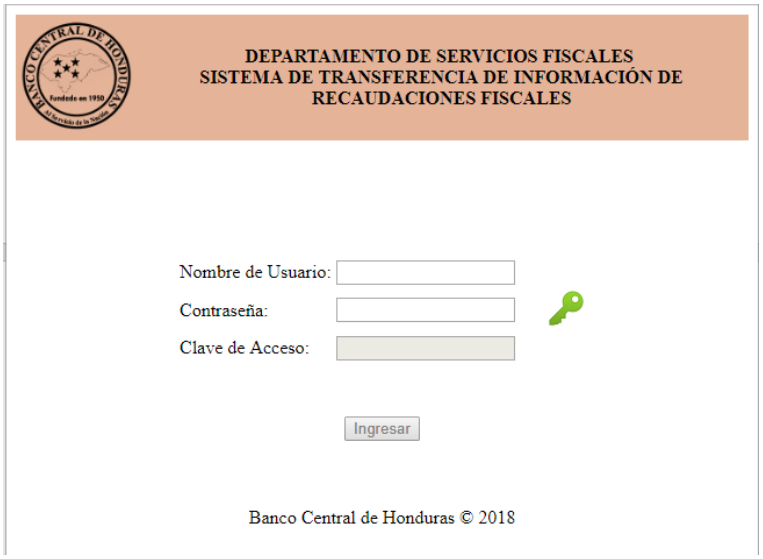


Figura 36 Pantalla de ingreso al sistema

Fuente: Propia

Esta pantalla le permitirá al usuario financiero autenticarse, de acuerdo al Nombre de Usuario y Contraseña, datos que serán proporcionados previamente por el personal del Banco Central de Honduras

Para generar la clave de acceso se realizan los pasos siguientes:

1. Ingresar nombre de usuario.
2. Ingresar contraseña.
3. Presionar el icono de llave para generar la clave de acceso.
4. Revisar correo electrónico para verificar la clave de acceso.

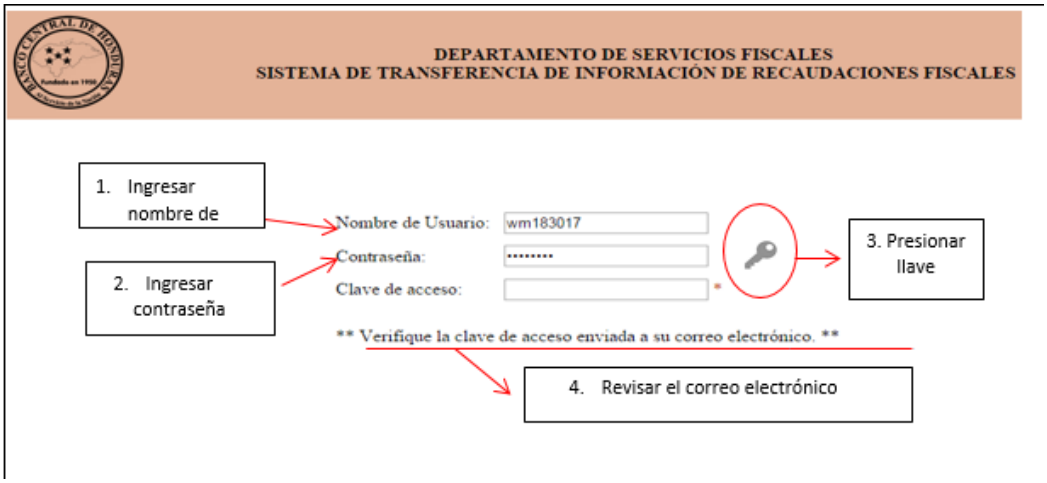
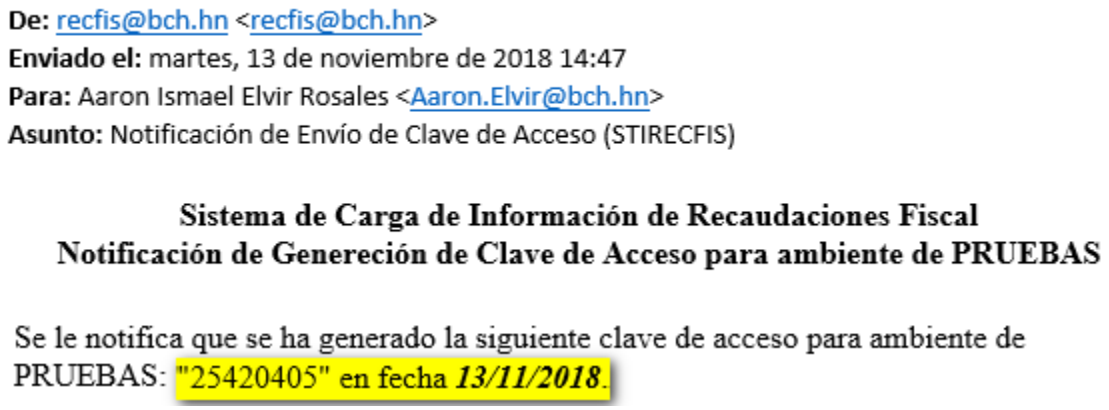


Figura 37 Pasos para ingresar al sistema

Fuente: Propia



De: recfis@bch.hn <recfis@bch.hn>
Enviado el: martes, 13 de noviembre de 2018 14:47
Para: Aaron Ismael Elvir Rosales <Aaron.Elvir@bch.hn>
Asunto: Notificación de Envío de Clave de Acceso (STIRECFIS)

Sistema de Carga de Información de Recaudaciones Fiscal
Notificación de Genereción de Clave de Acceso para ambiente de PRUEBAS

Se le notifica que se ha generado la siguiente clave de acceso para ambiente de PRUEBAS: "25420405" en fecha ***13/11/2018***.

Figura 38 Notificación de generación de clave de acceso

Fuente: Propia

Después de presionar el icono en forma de llave, el sistema enviará una Notificación de Generación de Clave de Acceso al correo electrónico del usuario.

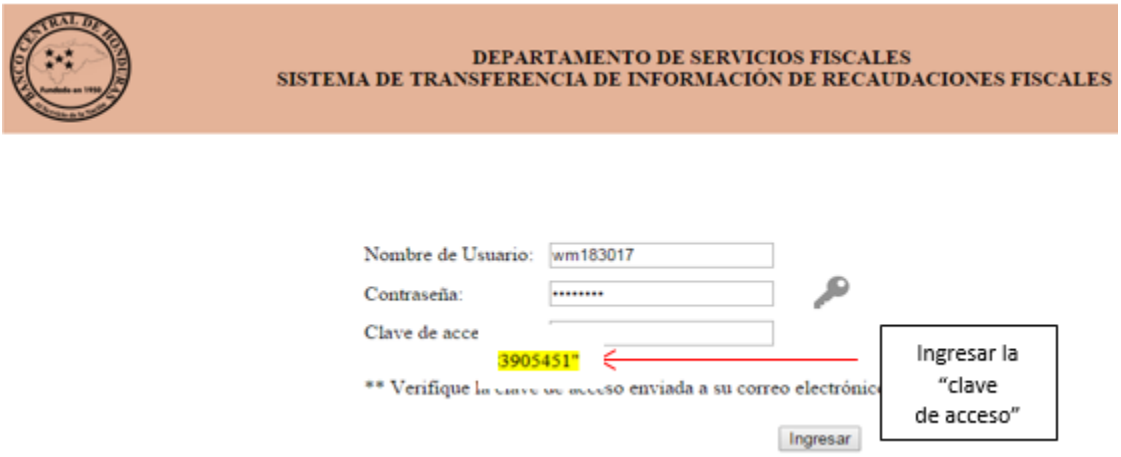


Figura 39 Ingreso al Sistema

Fuente: Propia

Por motivos de seguridad, la clave de acceso único OTP es válida por cinco (5) minutos; por lo que, si no es utilizada en este lapso de tiempo pierde su vigencia y se deberá generar una nueva clave de acceso al sistema.

Finalmente se concluye que el proceso de generación de un mecanismo adicional de autenticación, fue completado satisfactoriamente, entregando al cliente lo requerido y cumpliendo con los niveles de seguridad propuestos por los expertos en seguridad del BCH.

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

La creación de un mecanismo adicional de autenticación en los sistemas financieros, se ha vuelto una de los principales factores de éxito en las instituciones, ya que lograr la no vulnerabilidad de sus sistemas garantiza la continuidad del negocio; al utilizar componentes ya adquiridos por la institución, se logra potenciar las habilidades técnicas del equipo de informática, así como las áreas funcionales del negocio. A continuación, se presentan las conclusiones objeto del análisis de investigación mediante el estudio realizado:

- Los clientes del BCH estaban escépticos con la innovación de la nueva forma de infraestructura token que se les proponía, misma que al momento de verla y utilizar en ambiente de pruebas y producción consideraron un éxito el uso del método adicional de autenticación de doble factor, ya que les brindaba el nivel de seguridad esperado y a un mínimo costo, lo cual origina mejorar la imagen del BCH ante sus cuentahabientes logrando con ello cumplir con nuestros objetivos.
- La necesidad de seguridad en los proyectos que carezcan de recursos se suplirá, mediante el uso del servicio de correo corporativo del BCH, el cual enviará el valor numérico (OTP) al usuario que necesite ingresar y que haya cumplido con todas las validaciones anteriores de usuario, grupo de usuarios, contraseña y dirección de Protocolo de Internet (IP, por sus siglas en inglés).

5.2 Recomendaciones

- Se recomienda al Banco Central de Honduras reutilizar el nuevo mecanismo de seguridad adicional que posee con la culminación del trabajo de investigación, incorporándolo en nuevos proyectos o a los ya existentes.
- Se recomienda al Banco Central de Honduras, continuar utilizando los dispositivos token que ya fueron adquiridos por sus clientes en otros sistemas, e incorporar como contingencia o de forma alterna el uso del nuevo mecanismo de seguridad que le brindo la culminación de este proyecto y habilitarlo para los usuarios que lo requieran.

ANEXOS

Anexo 1: Caso de Negocio

CASO DE NEGOCIO DEL SISTEMA DE TRANSFERENCIA DE INFORMACIÓN DE RECAUDACIONES FISCALES (STI-RECFIS)

DATOS GENERALES DEL SISTEMA:

Nombre del sistema	Sistema de Transferencia de Información de Recaudaciones Fiscales.
Nombre corto del Sistema	STI-RECFIS
Objetivo del Sistema	Permitir mediante la extranet entre BCH y CEPROBAN la transmisión electrónica de archivos y documentos soportes que el sistema bancario requiere enviar diariamente a BCH para respaldar las recaudaciones fiscales del estado de Honduras, procesadas por las instituciones bancarias autorizadas.
Dependencia Usuaria	Departamento de Servicios Fiscales
Clientes Externos	Usuarios del Sistema Financiero Nacional
Horarios de alta disponibilidad del servicio WEB:	Horario de 8:00 a.m. a 2:00 p.m. La no disponibilidad implicaría una multa para BCH- *Conforme al ANEXO OPERATIVO I del "Contrato Marco de Recaudación Bancaria" Inciso "c" del apartado 1.8 indica: "Hasta las 14 horas (catorce horas) del día hábil siguiente al del efectivo cobro,* Las sanciones que se aplicaran a los bancos se encuentra en los apartados 3.1, 3.2, 3.3 y 3.4 de la sección 3 del ANEXO OPERATIVO donde se detalla el "Régimen de Sanciones"
Horarios no críticos:	Horario de 2:05 p.m. a 4:30 pm. Horario en el que los usuarios de las instituciones bancarias pueden subir archivos al sistema. Y personal de Servicios Fiscales puede continuar atendiendo a las instituciones bancarias.
Red Utilizada:	BCH-CEPROBAN
URL:	Ambiente Desarrollo: http://172.21.11.120/Recfisdes/Login.aspx?ReturnUrl=%2frecfisdes Ambiente Pruebas: http://srvappts01.bch.net/RecfisTest/Login.aspx?ReturnUrl=%2fRecfisTest Ambiente Producción **PENDIENTE**
Tipos de archivos a ser cargados:	Archivos PDF y ZIP encriptado de FENIX.
Máximo de archivos por instituciones bancarias:	No hay límite en el tamaño en los archivos que se cargan al sistema.
Nombre de la Cuenta de Correo	recfis@bch.hn, es utilizada para él envió de los siguientes tipos de notificaciones: a. Notificación de carga a usuario financiero b. Notificación de carga a usuario BCH c. Notificación de aceptación de datos d. Notificación de rechazo de datos e. Notificación de generación de contraseñas generadas por TOTP, para permitir acceso al sistema.
Responsable de la administración de cuenta de correo:	Personal de Servicios Fiscales.
Administración de usuarios del BCH:	A cargo de personal de Servicios Fiscales
Recursos Críticos:	a) Red de CEPROBAN b) Correo electrónico BCH

	c) Servicio Web del Sistema
Contingencia Operativa	El mecanismo de contingencia que utilizara el Departamento de Servicios Fiscales, será notificar mediante correo electrónico y/o llamada telefónica, a los encargados de la Recaudación Fiscal de los Bancos Autorizados, que tienen que enviar la información de forma manual, tal como se hace en este momento, (que el delegado bancario, venga al BCH antes de las 2:00 p.m., con la USB y las PA's Impresas)

ASPECTOS TÉCNICOS DEL SISTEMA:

Arquitectura de desarrollo:	Web (Capa de acceso a datos, capa de reglas del negocio, capa de entidades y la capa de interface de usuarios).
Lenguaje de Desarrollo:	ASP.NET 2013
Navegadores Soportados:	a) Internet Explorer (de preferencia) b) Google Chrome c) Mozilla Firefox
Requisitos del servidor de aplicaciones:	a) IIS 7 o superior b) Windows server 2008 o superior c) ODAC Oracle 12 o superior
Ambientes Creados:	a. Desarrollo (Anexo 1) a. BD: 192.49.4.22 b. APP: 172.21.11.120 b. Pruebas (Anexo 2) a. BD: 172.21.43.3 b. APP: 172.21.43.3 c. Producción (Anexo 3) a. PENDIENTE
Crecimiento de la BD:	Las instituciones cargaran diario un promedio de 3 archivos, en base a esto se genera el siguiente cálculo promedio para por banco: a. Diario: 126 Kb b. Semanal: 630 Kb c. Mensual: 2,520 Kb. (2.46 Mb) d. Anual: 30,240 Kb (29.53 Mb) Para las 13 instituciones bancarias, el cálculo seria el siguiente: a. Diario: 1,638 Kb (1.60 Mb) b. Semanal: 8,193 Kb (8.00 Mb) c. Mensual: 32,760 Kb (31.99 Mb) d. Anual: 393,120 KB (393.91 Mb)
Seguridad:	Para la autenticación de los usuarios se desarrolló una combinación de las siguientes características: a. Autenticación: uso de ADS a. Creación de grupos de usuarios para ingresar a la aplicación: i. "GG Recfis_Admin" ii. "GG Recfis_Users"

	b. Se manejan 2 perfiles de acuerdo al grupo que pertenece: i. Usuarios Administradores ii. Usuarios de la banca **b.** Autorización: uso de **TOTP (exclusivo para los bancos)** c. Altas y bajas de los usuarios de los bancos a cargo de los usuarios de STI-RECFIS d. Cuenta de Correo: recfis@bch.hn e. Procedimiento para cambio de contraseña: El usuario deberá de realizar la cita con el Departamento de Riesgos al menos un (1) día antes de vencer la contraseña y posteriormente presentarse a las instalaciones del BCH a realizar su cambio de contraseña. f. Bitácoras del sistema: registra la información de las transacciones realizadas por el usuario y los mensajes del sistema en la tabla **"TBLBITACORARECFIS"**. g. Horarios de respaldos: lunes a sábado a las 2:30 PM para así poder mantener toda la información histórica del día anterior, además guardar el respaldo en cinta para tener varios métodos de recuperación. h. Datos en línea: La información debe estar disponible para consultar en línea los últimos 2 años. i. Mantenimiento de datos históricos: este proceso se va a realizar por el personal técnico del BCH
Contingencia:	El encargado de mantenimiento del Departamento de TyC deberá notificar la caída del STI-RECFIS, mediante correo electrónico y/o llamada telefónica al Jefe de Sección de Recaudación Fiscal del Departamento de Servicios Fiscales. El tiempo máximo de espera ante una eventual caída del Sistema STI-RECFIS, es de Dos (2) horas, considerando que se tiene que avisar a los encargados de la Recaudación Fiscal de los que bancos que tendrán que enviar la información de forma manual; asimismo, considerando que el tiempo de recibir la información en el BCH es antes de las 2:00 p.m. Las dos horas se establecen considerando que el sistema se carga durante el transcurso de las 8:30 a.m. que es la hora de entrada al BCH y las 2:00 p.m. que es el tiempo máximo para la entrega de la información de Recaudación Fiscal por parte de los bancos autorizados

ASPECTOS FUNCIONALES DEL SISTEMA

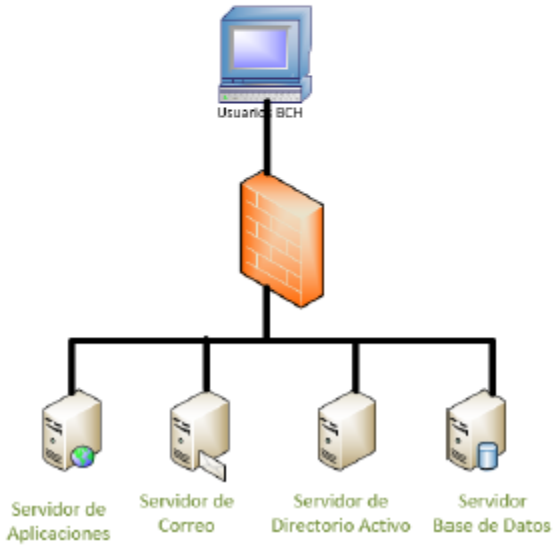
Módulo de Descarga:	Permite a los usuarios de recaudación fiscal bajar los documentos enviados por las instituciones bancarias.
Módulo de Revisión:	Permite al usuario de recaudación fiscal revisar los archivos enviados por las instituciones bancarias, para finalmente aceptar o rechazar los archivos
Módulo de Consultas:	Opción para poder verificar toda la información cargada por los usuarios
Módulo de Usuarios:	Permite al usuario de recaudación fiscal administrar los usuarios internos de BCH y de los bancos que tendrán accesos a la aplicación así como definir el banco al cual estarán asignados.
Módulo de Carga:	Habilitada desde la interface WEB para las instituciones bancarias a través de la cual realizan el envió de los datos.
Módulos de Información:	a. Normativa: permite consultar todos los documentos relacionados con los acuerdo para él envió de la información por parte de los bancos, así como las penalidades que serán establecidas por no cumplir cada una de estas normas. b. Contacto: Muestra información sobre a quién consultar en caso de tener un problema con el Sistema. c. Ayuda: opción del programa en la cual pueden descargar el manual de usuario a nivel de consulta y descarga.

CASO DE NEGOCIO DEL SISTEMA DE TRANSFERENCIA DE INFORMACIÓN DE RECAUDACIONES FISCALES (STI-RECFIS)

Anexos

Anexo 1

DIAGRAMA AMBIENTE DE DESARROLLO



Anexo 2: Plan de Gestión de Requisitos

PLAN DE GESTIÓN DE REQUISITOS

Código: STIRECFIS -PGRE-01
Versión 1.1

Proyecto:	Sistema de Transferencia de Recaudaciones Fiscales	**Siglas:**	STIRECFIS
Entregable:	Plan de Gestión de Comunicaciones (PGCO)	**Total Páginas:**	2
Elaborado por:	**Gerente del Proyecto:** *Ginsberg Yamir Rodríguez Irías* *División Gestión y Desarrollo de Proyectos* *Departamento de Tecnología y Comunicaciones*	**Fecha:** 12/07/2018	**Firma:**
Revisado por:	**Jefe de Proyecto Funcional:** *Leyla Margoth Banegas García* *Sección de Recaudaciones Fiscales* *Departamento Servicios Fiscales*	**Fecha:** 12/07/2018	**Firma:**
	Jefe Sección de Recaudaciones Fiscales: *Carlos Alberto Anariba* *Departamento Servicios Fiscales*	**Fecha:** 12/07/2018	**Firma:**
Aprobado por:	**Jefe Depatamento:** *Raúl Edgardo Sánchez Flores* *Departamento Servicios Fiscales*	**Fecha:** 12/07/2018	**Firma:**

CONTROL DE VERSIONES:

Versión	Causa del Cambio	Responsable del Cambio	Fecha del Cambio
1.0	Versión Inicial	Ginsberg Rodríguez	12/07/2018
1.1	Ajustes por revisión por parte del área del negocio	*Leyla Banegas* *Carlos Anariba*	12/07/2018

RECOPILACIÓN DE REQUISITOS

Como se va a realizar la recopilación de requerimientos y como se planifica la recopilación:

1. Entrevistas a usuarios funcionales del Departamento Servicios Fiscales.
2. Análisis de documentación de referencia (procesos, reglas de negocio, normas y políticas).
3. Elaboración del documento de Especificaciones de Requisitos de Software (ERS), utilizando el formato "DGDP-ERS", el cual se encuentra en la siguiente ubicación: /Documentos/3. Referencias del Proyecto/Plantillas del Proyecto/Formato de Especificación de Requisitos de Software.

PRIORIZACIÓN DE REQUISITOS

Como se va a realizar la priorización de requerimientos:

Para la priorización utilizaremos un listado de todos los requerimientos clasificándolos en una escala del 1 al 10 donde consideraremos el poder (Capacidad de cada interesado en hacer cumplir su requerimiento) y el impacto (Cuanto puede afectar el requerimiento al proyecto), el porcentaje de influencia del poder será de 60% y de

impacto será de 40%. Dicha clasificación será la que determine la priorización de requerimientos.
A continuación, presentamos el formato que se utilizará para la clasificación de los requerimientos:

Ítem	Interesado	Requisito	Poder (Escala del 1 al 10)	Impacto (Escala del 1 al 10)	Clasificación (Escala del 1 al 10)	Observaciones

La escala de priorización de los requisitos es la siguiente:

Prioridad del Requisito	
Alto	8 a 10
Intermedio	5 a 7
Bajo	1 a 4

Trazabilidad

Definición de los atributos de los requerimientos que serán empleados para confirmar su cumplimiento:

Para hacer el seguimiento ordenado a los requerimientos del usuario, utilizaremos una matriz de trazabilidad, donde detallaremos los requerimientos, descripción, prioridad, código EDT, estado actual y fecha, según el siguiente formato:

Requisito	Descripción	Prioridad (Escala del 1 al 10)	Código EDT	Estado Actual	Fecha

Gestión de cambios

Descripción de cómo los requerimientos pueden ser cambiados, incluyendo una evaluación del impacto y el proceso de aceptación:

- Los líderes funcionales podrán solicitar cambios de requerimientos al Jefe de Proyecto Funcional.
- Los requerimientos pasarán en primera instancia por el Jefe de Proyecto Funcional, quien realizará un análisis del impacto, el cual será presentado al Gerente del Proyecto para su visto bueno.
- El Jefe de Proyecto Funcional utilizará el formato "DGDP-FRC", el cual se encuentra en la siguiente ubicación: /Documentos/3. Referencias del Proyecto/Plantillas del Proyecto/Formato de Requerimiento de Cambio.
- El Gerente del Proyecto puede aprobar y/o rechazar la solicitud de cambio.

Verificación de requisitos

Métodos para verificar requerimientos, incluyendo las métricas para su medición:

1. La revisión de cada requerimiento será responsabilidad del propietario del mismo.
2. Número de entregables completados dentro de plazo.
3. Número de entregables completados fuera de plazo.

Anexo 3: Plan de Gestión de Tiempo

PLAN DE GESTIÓN DE TIEMPO

Código: STIRECFIS -PGTI-01
Versión 1.1

Proyecto:	Sistema de Transferencia de Recaudaciones Fiscales	**Siglas:**	STIRECFIS
Entregable:	Plan de Gestión de Comunicaciones (PGCO)	**Total Páginas:**	2
Elaborado por:	**Gerente del Proyecto:** *Ginsberg Yamir Rodríguez Irías* *División Gestión y Desarrollo de Proyectos* *Departamento de Tecnología y Comunicaciones*	**Fecha:** 13/07/2018	**Firma:**
Revisado por:	**Jefe de Proyecto Funcional:** *Leyla Margoth Banegas García* *Sección de Recaudaciones Fiscales* *Departamento Servicios Fiscales*	**Fecha:** 13/07/2018	**Firma:**
	Jefe Sección de Recaudaciones Fiscales: *Carlos Alberto Anariba* *Departamento Servicios Fiscales*	**Fecha:** 13/07/2018	**Firma:**
Aprobado por:	**Jefe Depatamento:** *Raúl Edgardo Sánchez Flores* *Departamento Servicios Fiscales*	**Fecha:** 13/07/2018	**Firma:**

CONTROL DE VERSIONES:

Versión	Causa del Cambio	Responsable del Cambio	Fecha del Cambio
1.0	Versión Inicial	*Ginsberg Yamir Rodríguez Irías*	13/07/2018
1.1	Ajustes por revisión por parte del área del negocio	*Leyla Margoth Banegas García* *Carlos Alberto Anariba*	13/07/2018

CRONOGRAMA DEL PROYECTO:

Ver Cronograma del Proyecto - versión 1.0.

PERSONA(S) AUTORIZADA(S) A SOLICITAR CAMBIO EN CRONOGRAMA:

Nombre	Cargo	Departamento
Leyla Margoth Banegas García	Jefe de Sección	Servicios Fiscales
Ginsberg Rodríguez	Gestor de Proyectos	Tecnología y Comunicaciones

PERSONA(S) QUE APRUEBA(N) REQUERIMIENTO DE CAMBIO DE CRONOGRAMA:

Nombre	Cargo	Departamento
Ginsberg Rodríguez	Gestor de Proyectos	Tecnología y Comunicaciones

RAZONES ACEPTABLES PARA CAMBIOS EN CRONOGRAMA DEL PROYECTO:

- Solicitud de cambio de alcance por parte del Jefe de Proyecto Funcional.
- Atrasos ocasionados por factores externos al proyecto.
- Accidentes de trabajo.
- Mal estimación de la secuencia de actividades.

DESCRIBIR CÓMO CALCULAR Y REPORTAR EL IMPACTO EN EL PROYECTO POR EL CAMBIO EN CRONOGRAMA:

- Para reportar el impacto sobre cambios de requerimiento en el cronograma, se utilizará el formato "DGDP-FRC", el cual se encuentra en la siguiente ubicación: /Documentos/3. Referencias del Proyecto/Plantillas del Proyecto/Formato de Requerimiento de Cambio.
- El informe será entregado al equipo del proyecto para ser analizado en reunión de trabajo con la finalidad de discutir las alternativas y seleccionar la más adecuada para el proyecto.

DESCRIBIR CÓMO LOS CAMBIOS AL CRONOGRAMA SERÁN ADMINISTRADOS:

- El Jefe de Proyecto Funcional, evaluará las necesidades de cambio de requerimiento e informará al Gerente del Proyecto la necesidad de realizar un cambio en el cronograma.
- El Gerente del Proyecto, junto con el equipo de proyecto, evaluará las solicitudes de cambio para determinar la criticidad del mismo.
- En caso de que la solicitud de cambio del cronograma afecte el alcance del proyecto o sobrepase los límites del cronograma establecidos en el plan de gestión del proyecto, estos deberán ser presentados al Comité de Tecnología y Seguridad de la Información (CTSI), para que este último tome la decisión de aprobar o rechazar la propuesta.

Anexo 4: Plan de Gestión de Riesgos

PLAN DE GESTIÓN DE RIESGOS

Código: STIRECFIS-PGRS-01
Versión 1.1

Proyecto:	Sistema de Transferencia de Recaudaciones Fiscales	**Siglas:**	STIRECFIS
Entregable:	Plan de Gestión de Riesgos (PGRS)	**Total Páginas:**	2
Elaborado por:	**Gerente del Proyecto:** *Ginsberg Yamir Rodríguez Irías* *División Gestión y Desarrollo de Proyectos* *Departamento de Tecnología y Comunicaciones*	**Fecha:** 30/07/2018	**Firma:**
Revisado por:	**Jefe de Proyecto Funcional:** *Leyla Margoth Banegas García* *Sección de Recaudaciones Fiscales* *Departamento Servicios Fiscales*	**Fecha:** 30/07/2018	**Firma:**
	Jefe Sección de Recaudaciones Fiscales: *Carlos Alberto Anariba* *Departamento Servicios Fiscales*	**Fecha:** 30/07/2018	**Firma:**
Aprobado por:	**Jefe Depatamento:** *Raúl Edgardo Sánchez Flores* *Departamento Servicios Fiscales*	**Fecha:** 30/07/2018	**Firma:**

CONTROL DE VERSIONES:

Versión	Causa del Cambio	Responsable del Cambio	Fecha del Cambio
1.0	Versión Inicial	*Ginsberg Yamir Rodríguez Irías*	30/07/2018
1.1	Ajustes por revisión por parte del área del negocio	*Leyla Margoth Banegas García* *Carlos Alberto Anariba*	30/07/2018

DESCRIPCIÓN DE LA METODOLOGÍA DE GESTIÓN DEL RIESGO A SER USADA:

Alcances:

- La identificación y priorización de riesgos más críticos será realizado por el equipo del proyecto.
- Las acciones a tomar serán revisadas y aprobadas por el Gerente del Proyecto.
- El seguimiento y el control de los riesgos será realizado por el Gerente del Proyecto.

Herramientas:

- Tormenta de ideas.
- Juicio de expertos.
- Lista de verificación de riesgos potenciales.
- Análisis de los supuestos identificados.

Fuentes de Datos:
• La identificación de los riesgos se realizará por parte del equipo del proyecto, según experiencia y juicio de especialistas. • Se tomará en consideración riesgos considerados en otros proyectos.
Roles y responsabilidades:
• Equipo del Proyecto: Responsable de identificación y priorización los riesgos, proponer acciones para afrontar los riesgos identificados. • Gerente del Proyecto: Responsable dar el seguimiento a los riesgos y aprobar acciones propuestas para mitigar los riesgos.
Acción para el manejo de los Riesgos:
• Identificación de Riesgos. • Evaluación de los Riesgos en el Proyecto. • Plan de Respuesta de Riesgos.

PRESUPUESTO:

• No se ha asignado presupuesto para la gestión de riesgos en el proyecto.

SINCRONIZACIÓN:

• El Gerente del Proyecto, está encargado de gestionar los riesgos del proyecto a lo largo de todo su ciclo de vida, esto implica que su supervisión es continua para detectar nuevos riesgos. • Los puntos a revisar durante la ejecución del proyecto será de forma quincenal, donde se informa el rendimiento del trabajo y la situación de los riesgos actualizados con su respectivo plan de contingencia y soluciones alternativas.

Anexo 5: Plan de Gestión de Calidad

PLAN DE GESTIÓN DE CALIDAD

Código: STIRECFIS-PGCA-01
Versión 1.1

Proyecto:	Sistema de Transferencia de Recaudaciones Fiscales	**Siglas:**	STIRECFIS
Entregable:	Plan de Gestión de Calidad (PGCA)	**Total Páginas:**	3
Elaborado por:	**Gerente del Proyecto:** *Ginsberg Yamir Rodríguez Irías* *División Gestión y Desarrollo de Proyectos* *Departamento de Tecnología y Comunicaciones*	**Fecha:** 17/08/2018	**Firma:**
Revisado por:	**Jefe de Proyecto Funcional:** *Leyla Margoth Banegas García* *Sección de Recaudaciones Fiscales* *Departamento Servicios Fiscales*	**Fecha:** 17/08/2018	**Firma:**
	Jefe Sección de Recaudaciones Fiscales: *Carlos Alberto Anariba* *Departamento Servicios Fiscales*	**Fecha:** 17/08/2018	**Firma:**
Aprobado por:	**Jefe Depatamento:** *Raúl Edgardo Sánchez Flores* *Departamento Servicios Fiscales*	**Fecha:** 17/08/2018	**Firma:**

CONTROL DE VERSIONES:

Versión	Causa del Cambio	Responsable del Cambio	Fecha del Cambio
1.0	Versión Inicial	*Ginsberg Yamir Rodríguez Irías*	17/08/2018
1.1	Ajustes por revisión por parte del área del negocio	*Leyla Margoth Banegas García* *Carlos Alberto Anariba*	17/08/2018

OBJETIVO DE CALIDAD DEL PROYECTO:

La meta del proyecto es crear la mayor cantidad de entregables posibles sin defectos en base a los requerimientos definidos en el proyecto y en fechas establecidas en el cronograma de actividades, con una cobertura mínima del 90%.

IDENTIFICACIÓN DE ESTÁNDARES:

- Estándares Técnicos:
  1. El lenguaje utilizado para este tipo de desarrollo será Visual Basic .NET.
  2. El servidor de aplicación donde será desplegado el sistema son Windows Server.
  3. El servidor de base de datos donde será almacenada la información es Oracle 12c.
  4. La aplicación será ejecutada en Internet Explorer o Google Chrome.
  5. El marco de referencia para la arquitectura del sistema es TOGAF.
  6. Aplicación del proceso de Microsoft Security Development Lifecycle (SDL).

- Estándares de documentación:
  1. La gestión del proyecto se lleva bajo la referencia de la metodología PMI.
  2. La administración del ciclo de vida del desarrollo del sistema se lleva acabo con la Metodología de Desarrollo de Sistemas e Implementación de Soluciones de Terceros del Departamento de Tecnológica y Comunicaciones.
  3. Los cambios en el alcance deberán ser documentados utilizará el formato "DGDP-FRC", el cual se encuentra en la siguiente ubicación: /Documentos/3. Referencias del Proyecto/Plantillas del Proyecto/Formato de Requerimiento de Cambio.

Métricas del ciclo de vida del software:

¿Qué hacer?	• ERS: Especificación de requisitos del Software.
Definición	• Definimos como cumplir los objetivos.
Construcción	• Desarrollamos el código.
Estabilización	• Realizamos pruebas sobre el código desarrollado.
Liberación	• Entrega del sistema al cliente. • Adaptación finales y cierre de proyecto.

Identificación de métricas:

Métrica	Meta	Análisis Razonado	Como se realizará
Atraso en el cronograma de actividades.	<10%	Un atraso mayor implicaría mover y ajustar actividades afectando la ruta crítica del proyecto.	Verificación de las fechas de corte planeadas en el proyecto.
Movimiento de personal del proyecto.	Líder Funcionales o Desarrolladores	La curva de aprendizaje para los nuevos integrantes afectaría la entrega del proyecto.	Observación y conversación. Manejo de conflictos. Habilidades interpersonales. Actividades de trabajo en equipo.
Pruebas Técnicas.	Calificación aprobatoria mínima del 90%	Se requiere realizar en forma periódica la revisión de código.	Se obtiene un reporte de los resultados obtenidos en la revisión.
Pruebas de seguridad.	Calificación aprobatoria mínima del 90%	Se requiere realizar en forma periódica la revisión de código.	Se obtiene un reporte de los resultados obtenidos en la revisión.
Pruebas de usuario.	Solucionar el 100% de las observaciones detectadas por el usuario.	La liberación de entregables con observaciones no resueltas podría ocasionar pérdida de confianza en los usuarios.	Por cada entregable del proyecto se realizarán escenarios de pruebas de usuario con el líder funcional.

Plan de prevención de defectos:

- Se realizarán pruebas técnicas de cada uno de los entregables.
- Se llevarán a cabo pruebas funcionales por cada uno de los entregables.

Anexo 6: Plan de Gestión de Comunicaciones

PLAN DE GESTIÓN DE COMUNICACIONES

Código: STIRECFIS-PGCO-01
Versión 1.0

Proyecto:	Sistema de Transferencia de Recaudaciones Fiscales	**Siglas:**	STIRECFIS
Entregable:	Plan de Gestión de Comunicaciones (PGCO)	**Total Páginas:**	3
Elaborado por:	**Gerente del Proyecto:** *Ginsberg Yamir Rodríguez Irías* *División Gestión y Desarrollo de Proyectos* *Departamento de Tecnología y Comunicaciones*	**Fecha:** 20/08/2018	**Firma:**
Revisado por:	**Jefe de Proyecto Funcional:** *Leyla Margoth Banegas García* *Sección de Recaudaciones Fiscales* *Departamento Servicios Fiscales*	**Fecha:** 20/08/2018	**Firma:**
	Jefe Sección de Recaudaciones Fiscales: *Carlos Alberto Anariba* *Departamento Servicios Fiscales*	**Fecha:** 20/08/2018	**Firma:**
Aprobado por:	**Jefe Depatamento:** *Raúl Edgardo Sánchez Flores* *Departamento Servicios Fiscales*	**Fecha:** 20/08/2018	**Firma:**

CONTROL DE VERSIONES:

Versión	Causa del Cambio	Responsable del Cambio	Fecha del Cambio
1.0	Versión Inicial	*Ginsberg Yamir Rodríguez Irías*	20/08/2018

COMUNICACIONES DEL PROYECTO:

Ver Matriz de Comunicaciones del Proyecto - versión 1.0.

PROCEDIMIENTO PARA ACTUALIZAR EL PLAN DE GESTIÓN DE COMUNICACIONES:

- El Plan de Gestión de las Comunicaciones deberá ser revisado y/o actualizado cada vez que:
  1. Hay una solicitud de cambio aprobada que impacte el plan del proyecto.
  2. Hay una acción correctiva que impacte los requerimientos o necesidades de información de los interesados.
  3. Hay personas que ingresan o salen del proyecto.
  4. Hay cambios en las asignaciones de personas a roles del proyecto.
  5. Hay solicitudes inusuales de informes o reportes adicionales.
  6. Hay quejas, sugerencias, comentarios o evidencias de requerimientos de información no satisfechos.
  7. Hay evidencias de resistencia al cambio.
  8. Hay evidencias de deficiencias de comunicación dentro o fuera del proyecto.

- La actualización del Plan de Gestión de las Comunicaciones deberá seguir los siguientes pasos:
  1. Identificación y clasificación de interesados.
  2. Determinación de requerimientos de información.
  3. Elaboración de la matriz de comunicaciones del proyecto.
  4. Actualización del plan de gestión de las comunicaciones.
  5. Aprobación del plan de gestión de las comunicaciones.
  6. Difusión del nuevo plan de gestión de las comunicaciones.

GUÍAS PARA EVENTOS DE COMUNICACIÓN:

- Guías para Reuniones. - Todas las reuniones deberán seguir las siguientes pautas:
  1. Debe fijarse la agenda con anterioridad.
  2. Debe coordinarse e informarse fecha, hora, y lugar con los participantes.
  3. Se deben fijar los objetivos de la reunión.
  4. Se debe emitir un acta de reunión (ver formato adjunto), la cual se debe repartir a los participantes (previa revisión por parte de ellos).
- Guías para Correo Electrónico. - Todos los correos electrónicos deberán seguir las siguientes pautas:
  1. Los correos electrónicos entre el equipo de proyecto y el Departamento Internacional deberán ser enviado por el Gerente del Proyecto con copia al Departamento de Tecnológica y Comunicaciones, para establecer una sola vía formal de comunicación.

GUÍAS PARA DOCUMENTACIÓN DEL PROYECTO:

- Guías para codificación de documentos. - La codificación de los documentos del proyecto será la siguiente: AAAA-BBB-CCC.DDD.
  Dónde: AAAA = Código del proyecto (STIRECFIS)
  BBB = Abreviatura del tipo de documento (PGAL, PGRE, PGTI, PGRS, etc.).
  CCC = Versión del documento (01 a 99).
  DDD = Formato del archivo (DOC, EXE, PDF, MPP, etc.).
- Guías para almacenamiento de documentos. - El almacenamiento de los documentos del proyecto deberá seguir las siguientes pautas:
  1. Durante la ejecución del proyecto la documentación generada estará a disposición de los interesados en la siguiente dirección: Portal STIRECFIS.
  2. El Gerente del Proyecto consolidará todas las versiones controladas y numeradas de los documentos, en un archivo final del proyecto, el cual será entregado a la biblioteca técnica del Departamento de Tecnología y Comunicaciones.

GUÍAS PARA EL CONTROL DE VERSIONES:

- Todos los documentos de proyecto están sujetos al control de versiones, utilizando el siguiente formato:

Versión	Causa del Cambio	Responsable del Cambio	Fecha del Cambio

- Cada vez que se emite una versión del documento se llena una fila en el registro de cambios, anotando la versión, la causa del cambio, responsable del cambio, y la fecha correspondiente de la versión del documento.
- Debe haber correspondencia entre el código de versión del documento que figura en el registro de cambios y el código de versión del documento que figura en el nombre del archivo (ver Guía para Codificación de Documentos).

GLOSARIO DE TERMINOLOGÍA DEL PROYECTO:

Ver Glosario de Terminología del Proyecto - versión 1.0.

Anexo 7: Matriz de Comunicaciones

MATRIZ DE COMUNICACIONES DEL PROYECTO

Código: STIRECFIS-MCP-01
Versión 1.0

Proyecto:	Sistema de Transferencia de Recaudaciones Fiscales	**Siglas:**	STIRECFIS
Entregable:	Matriz de Comunicaciones del Proyecto (MCP)	**Total Páginas:**	4
Elaborado por:	**Gerente del Proyecto:** *Ginsberg Yamir Rodríguez Irías* *División Gestión y Desarrollo de Proyectos* *Departamento de Tecnología y Comunicaciones*	**Fecha:** 21/08/2018	**Firma:**
Revisado por:	**Jefe de Proyecto Funcional:** *Leyla Margoth Banegas García* *Sección de Recaudaciones Fiscales* *Departamento Servicios Fiscales*	**Fecha:** 21/08/2018	**Firma:**
	Jefe Sección de Recaudaciones Fiscales: *Carlos Alberto Ananiba* *Departamento Servicios Fiscales*	**Fecha:** 21/08/2018	**Firma:**
Aprobado por:	**Jefe Depatamento:** *Raúl Edgardo Sánchez Flores* *Departamento Servicios Fiscales*	**Fecha:** 21/08/2018	**Firma:**

CONTROL DE VERSIONES:

Versión	Causa del Cambio	Responsable del Cambio	Fecha del Cambio
1.0	Versión Inicial	*Ginsberg Yamir Rodríguez Irías*	21/08/2018

MATRIZ DE COMUNICACIONES DEL PROYECTO:

Información	Contenido	Formato	Nivel de Detalle	Responsable de Comunicar	Grupo Receptor	Frecuencia de Comunicación	Código EDT
Planificación del proyecto	Planificación detallada del proyecto: alcance, tiempo, calidad, RRHH, comunicaciones y riesgos	Plan de Gestión del Proyecto	Muy Alto	Gerente del Proyecto	Patrocinador, Equipo del Proyecto	Una sola vez	1.0 Planificación
Notificación de inicio del proyecto	Nota para los agentes cambiarios donde se informa el inicio del proyecto y se solicita indicar los contactos que participaran en la ejecución del proyecto	Circular del BCH	Muy alto	Patrocinador	Agentes Cambiarios	Una sola vez	1.3 Ejecución
Registro de reuniones de trabajo	Detalle de asuntos y acuerdos relevantes del proyecto	Acta de Reunión del Proyecto	Detallado	Gerente del Proyecto	Patrocinador, Equipo del Proyecto, Interesados	A demanda	1.3 Ejecución
Requerimientos de usuario	Definición detallada de los procesos de negocio a automatizar en el sistema	Requerimientos de Usuario	Detallado	Gerente del Proyecto	Patrocinador, Equipo del Proyecto	Una sola vez	2.0 Análisis y Diseño
Requisitos del sistema	Especificaciones detalladas de los requerimientos del sistema	Especificaciones de Requisitos de Software	Detallado	Gerente del Proyecto	Patrocinador, Equipo del Proyecto	Una sola vez	2.0 Análisis y Diseño
Presentación de prototipo del sistema	Diapositivas donde se presenta las funciones propuesta del sistema	Presentación de PowerPoint	Detallado	Desarrolladores	Patrocinador, Equipo del Proyecto	Una sola vez	2.0 Análisis y Diseño
Presentación de modificaciones de la boleta	Diapositivas donde se presenta las modificaciones de la	Presentación de PowerPoint	Detallado	Desarrolladores	Patrocinador, Equipo del Proyecto,	Una sola vez	2.0 Análisis y Diseño

	boleta				Agentes Cambiarios		
Especificaciones de requisitos del sistema	Detalle de los especificaciones de requisitos del sistema	Especificaciones de Requisitos del Sistema	Detallado	Desarrolladores	Patrocinador, Equipo del Proyecto	Una sola vez	2.0 Análisis y Diseño
Notificación de las especificaciones de requisitos del servicio WEB y capturador	Nota para los agentes cambiarios donde se entrega las especificaciones de requisitos del servicio WEB y capturador	Circular del BCH	Detallado	Patrocinador	Patrocinador, Equipo del Proyecto, Agentes Cambiarios	Una sola vez	1.3 Ejecución
Estado del proyecto	Estado Actual, Pronóstico de Tiempo, Problemas y/o Pendientes	Informe de Avance	Alto	Gerente del Proyecto	Patrocinador, Jefe de Proyecto Funcional	Semanal	1.3 Ejecución
Notificación de inicio de prueba piloto	Nota para los agentes cambiarios donde se indica el inicio de la prueba piloto	Circular del BCH	Alto	Patrocinador	Agentes Cambiarios	Una sola vez	1.3 Ejecución
Resultado de la prueba piloto	Detalle del resultado de la prueba piloto	Formatos de Prueba Piloto	Detallado	Desarrolladores	Patrocinador, Equipo del Proyecto, Agentes Cambiarios	Una sola vez	3.0 Construcción
Capacitación de usuario	Capacitación sobre el uso del sistema	Plan de Capacitación	Alto	Desarrolladores	Patrocinador, Equipo del Proyecto	Una sola vez	4.0 Estabilización
Capacitación de agentes cambiarios	Capacitación sobre el uso del servicio WEB y capturador	Plan de Capacitación	Alto	Desarrolladores	Patrocinador, Equipo del Proyecto, Agentes Cambiarios	Una sola vez	4.0 Estabilización
Capacitación de personal de la División de	Capacitación del sistema a nivel técnico	Plan de Capacitación	Alto	Desarrolladores	División de Servicios Tecnológicos	Una sola vez	4.0 Estabilización

Servicios Tecnológicos							
Notificación de inicio de pruebas de usuario	Nota para los agentes cambiarios donde se indica el inicio de las pruebas de usuario	Circular del BCH	Alto	Patrocinador	Agentes Cambiarios	Una sola vez	1.3 Ejecución
Resultado de las pruebas de usuario	Detalle del resultado de las pruebas de usuario	Formatos de Prueba de Usuario	Detallado	Desarrolladores	Patrocinador, Equipo del Proyecto	Una sola vez	4.0 Estabilización
Notificación de inicio del paralelo	Nota para los agentes cambiarios donde se indica el inicio del paralelo	Circular del BCH	Alto	Patrocinador	Agentes Cambiarios	Una sola vez	1.3 Ejecución
Notificación de salida a producción	Nota para los agentes cambiarios donde se indica la salida a producción	Circular del BCH	Alto	Patrocinador	Agentes Cambiarios	Una sola vez	1.3 Ejecución
Productos del proyecto	Documentos y sistema	Entregables del Proyecto	Detallado	Gerente del Proyecto	Patrocinador, Jefe de Proyecto Funcional	Una sola vez	4.0 Estabilización
Cierre del proyecto	Comunicación sobre el cierre del proyecto	Cierre del Proyecto	Medio	Gerente del Proyecto	Patrocinador, Jefe de Proyecto Funcional	Una sola vez	5.0 Liberación

Anexo 8: Glosario de Terminología del Proyecto

GLOSARIO DE TERMINOLOGÍA DEL PROYECTO

Código: STIRECFIS-GTP-01
Versión 1.0

Proyecto:	Sistema de Transferencia de Recaudaciones Fiscales	**Siglas:**	STIRECFIS
Entregable:	Plan de Gestión de Comunicaciones (PGCO)	**Total Páginas:**	5
Elaborado por:	**Gerente del Proyecto:** *Ginsberg Yamir Rodríguez Irías* *División Gestión y Desarrollo de Proyectos* *Departamento de Tecnología y Comunicaciones*	**Fecha:** 22/08/2018	**Firma:**
Revisado por:	**Jefe de Proyecto Funcional:** *Leyla Margoth Banegas García* *Sección de Recaudaciones Fiscales* *Departamento Servicios Fiscales*	**Fecha:** 22/08/2018	**Firma:**
	Jefe Sección de Recaudaciones Fiscales: *Carlos Alberto Anariba* *Departamento Servicios Fiscales*	**Fecha:** 22/08/2018	**Firma:**
Aprobado por:	**Jefe Depatamento:** *Raúl Edgardo Sánchez Flores* *Departamento Servicios Fiscales*	**Fecha:** 22/08/2018	**Firma:**

CONTROL DE VERSIONES:

Versión	Causa del Cambio	Responsable del Cambio	Fecha del Cambio
1.0	Versión Inicial	Ginsberg Rodríguez	22/08/2018

SIGLAS COMUNES:

Sigla	Definición
CRP	Cronograma del proyecto
EDT	Estructura de desglose del trabajo
GTP	Glosario de terminología del proyecto
IRP	Identificación de riesgos del proyecto
MCP	Matriz de comunicaciones del proyecto
ORP	Organigrama del proyecto
PGAL	Plan de gestión del alcance
PGCA	Plan de gestión de calidad
PGCO	Plan de gestión de comunicaciones

PGPE	Plan de gestión de personal
PGPO	Plan de gestión del proyecto
PGRE	Plan de gestión de requisitos
PGRS	Plan de gestión de riesgos
PGTI	Plan de gestión de tiempo
PRRP	Plan de respuesta de los riesgos del proyecto
RAM	Matriz de asignación de responsabilidades
RU	Requerimiento de usuario
RE	Requerimiento del sistema

DEFINICIONES:

Alcance: La suma de productos, servicios y resultados que se proporcionarán como un proyecto. Véase también alcance del proyecto y alcance del producto.

Alcance del Proyecto: El trabajo que debe realizarse para entregar un producto, servicio o resultado con las funciones y características especificadas.

Amenaza: Una condición o situación desfavorable para el proyecto, conjunto de circunstancias negativas, conjunto de eventos negativos, riesgo que si se hace realidad tendrá un impacto negativo en un objetivo del proyecto, o posibilidad de cambios negativos. Compárese con oportunidad.

Calidad: El grado en el que un conjunto de características inherentes satisface los requisitos.

Cambio en el Alcance: Cualquier cambio en el alcance del proyecto. Un cambio en el alcance casi siempre requiere un ajuste en el coste o cronograma del proyecto. También conocido como: Cambio del Alcance.

Categoría de Riesgo: Un grupo de posibles causas de riesgo. Las causas de riesgo pueden agruparse en categorías como técnica, externa, de la organización, ambiental o de dirección de proyectos. Una categoría puede incluir subcategorías como madurez técnica, clima o estimación agresiva. Véase también estructura de desglose del riesgo.

Cerrar Proyecto: El proceso de finalizar todas las actividades en todos los grupos de procesos del proyecto para cerrar formalmente el proyecto o una fase de él. También conocido como: Cerrar el Proyecto o Cierre del Proyecto.

Control de Cambios: Identificar, documentar, aprobar o rechazar y controlar cambios en las líneas base del proyecto.

Control del Cronograma: El proceso de controlar los cambios del cronograma del proyecto.

Criterios de Aceptación: Aquellos criterios, incluidos los requisitos de rendimiento y condiciones esenciales, que deben cumplirse antes de que se acepten los productos entregables del proyecto.

Cronograma del Proyecto: Las fechas planificadas para realizar las actividades del cronograma y las fechas

planificadas para cumplir los hitos del cronograma.

Definición del Alcance: El proceso de desarrollar un enunciado del alcance del proyecto detallada como base para futuras decisiones del proyecto.

Disparadores: Indicadores de qué ha ocurrido o está por ocurrir un riesgo. Los disparadores pueden descubrirse en el proceso de identificación de riesgos y pueden observarse en el proceso de seguimiento y control de riesgos. A veces se les llama síntomas de riesgo o señales de advertencia.

Equipo del Proyecto: Todos los miembros del equipo del proyecto.

Estructura de Desglose del Trabajo (EDT): Una descomposición jerárquica con orientación hacia el producto entregable relativa al trabajo que será ejecutado por el equipo del proyecto para lograr los objetivos del proyecto y crear los productos entregables requeridos. Organiza y define el alcance total del proyecto. Cada nivel descendente representa una definición cada vez más detallada del trabajo del proyecto. La EDT se descompone en paquetes de trabajo. La orientación hacia el producto entregable de la jerarquía incluye los productos entregables internos y externos. Véase también paquete de trabajo, cuenta de control, y estructura de desglose del trabajo del contrato. También conocido como: Desglose de la Estructura del Trabajo; Estructura de Desagregación del Trabajo (EDT); Estructura de Descomposición del Trabajo (EDT); Estructura de la División del Trabajo; Estructura Detallada de Trabajo (EDT); o Estructura Detallada del Trabajo (EDT).

Fase del Proyecto: Un conjunto de actividades del proyecto relacionadas lógicamente, que generalmente culminan con la finalización de un producto entregable principal. Las fases del proyecto (también denominadas simplemente fases) suelen completarse en forma secuencial, pero pueden superponerse en determinadas situaciones de proyectos. Las fases pueden subdividirse en subfases y, a su vez, en componentes; esta jerarquía, si el proyecto o las partes del proyecto se dividen en fases, está contenida en la estructura de desglose del trabajo. Una fase del proyecto es un componente de un ciclo de vida del proyecto. Una fase del proyecto no es un grupo de procesos de dirección de proyectos.

Interesado: Personas y organizaciones como clientes, patrocinadores, organización ejecutante y el público, involucrados activamente con el proyecto, o cuyos intereses pueden verse afectados de manera positiva o negativa por la ejecución o conclusión del proyecto. También pueden influir sobre el proyecto y sus productos entregables. También conocido como: Interesados o Involucrados.

Juicio de Expertos: Un juicio que se brinda sobre la base de la experiencia en un área de aplicación, área de conocimiento, disciplina, industria, etc. según resulte apropiado para la actividad que se está llevando a cabo. Dicha experiencia puede ser proporcionada por cualquier grupo o persona con una educación, conocimiento, habilidad, experiencia o capacitación especializada, y puede obtenerse de numerosas fuentes, incluyendo: otras unidades dentro de la organización ejecutante; consultores; interesados, incluidos clientes; asociaciones profesionales y técnicas; y grupos industriales.

Lecciones Aprendidas: Lo que se aprende en el proceso de realización del proyecto. Las lecciones aprendidas pueden identificarse en cualquier momento. También considerado un registro del proyecto, que se debe incluir en la base de conocimientos de lecciones aprendidas.

Matriz de Asignación de Responsabilidades / Responsibility Assignment Matrix (RAM): Una estructura que relaciona la estructura de desglose de la organización con la estructura de desglose del trabajo para ayudar a garantizar que cada componente del alcance del proyecto se asigne a una persona responsable.

Metodología: Un sistema de prácticas, técnicas, procedimientos y normas utilizado por quienes trabajan en una

disciplina.

Mitigar el riesgo: Una técnica de planificación de la respuesta a los riesgos asociada con amenazas que pretende reducir la probabilidad de ocurrencia o el impacto de un riesgo por debajo de un umbral aceptable. También conocido como: Disminuir el Riesgo o Mitigación del Riesgo.

Patrocinador: La persona o el grupo que ofrece recursos financieros, monetarios o en especie, para el proyecto.

Plan de Gestión de Calidad: El plan de gestión de calidad describe cómo el equipo de dirección del proyecto implementará la política de calidad de la organización ejecutante. El plan de gestión de calidad es un componente o un plan subsidiario al plan de gestión del proyecto. El plan de gestión de calidad puede ser formal o informal, muy detallado o ampliamente esbozado, dependiendo de los requisitos del proyecto. También conocido como: Plan de Administración de Calidad; Plan de Gerencia de Calidad; o Plan de Gerenciamiento de Calidad.

Plan de Gestión de las Comunicaciones: El documento que describe: las necesidades y expectativas de comunicación para el proyecto; cómo y bajo qué formato se comunicará la información; dónde y cuándo se realizará cada comunicación; y quién es el responsable de efectuar cada tipo de comunicación. Dependiendo de las necesidades de los interesados en el proyecto, un plan de gestión de las comunicaciones puede ser formal o informal, muy detallado o ampliamente esbozado. El plan de gestión de las comunicaciones es un plan subsidiario del plan de gestión del proyecto o una parte de él. También conocido como: Plan de Administración de las Comunicaciones; Plan de Gerencia de Comunicaciones; o Plan de Gerenciamiento de las Comunicaciones.

Plan de Gestión de personal: El documento que describe cuándo y cómo se cumplirán los requisitos de recursos humanos. Es un plan subsidiario del plan de gestión del proyecto o una parte de él. Dependiendo de las necesidades del proyecto, el plan de gestión de personal puede ser informal y ampliamente esbozado, o formal y muy detallado. La información del plan de gestión de personal varía según el área de aplicación y el tamaño del proyecto. También conocido como: Plan de Administración de Personal; Plan de Gerencia de Personal; o Plan de Gerenciamiento de Personal.

Plan de Gestión de Riesgos: El documento que describe cómo se estructurará y realizará en el proyecto la gestión de riesgos del proyecto. Es un plan subsidiario del plan de gestión del proyecto o una parte de él. Dependiendo de las necesidades del proyecto, el plan de gestión de riesgos puede ser informal y ampliamente esbozado, o formal y muy detallado. La información del plan de gestión de riesgos varía según el área de aplicación y el tamaño del proyecto. El plan de gestión de riesgos es diferente del registro de riesgos ya que éste contiene la lista de riesgos del proyecto, los resultados del análisis de riesgos y las respuestas a los riesgos. También conocido como: Plan de Administración de Riesgos; Plan de Gerencia de Riesgos; o Plan de Gerenciamiento de Riesgos.

Planificación de Calidad: El proceso de identificar qué estándares de calidad son relevantes para el proyecto y de determinar cómo satisfacerlos. También conocido como: Planeación de Calidad.

Planificación de la Respuesta a los Riesgos: El proceso de desarrollar opciones y acciones para mejorar las oportunidades y reducir las amenazas a los objetivos del proyecto. También conocido como: Planeación de la Respuesta a los Riesgos.

Planificación de las Comunicaciones: El proceso de determinar las necesidades con respecto a la información y las comunicaciones de los interesados en el proyecto: quiénes son, cuál es su nivel de interés e influencia sobre el proyecto, quién necesita qué tipo de información, cuándo la necesita y cómo se le entregará. También

conocido como: Planeación de las Comunicaciones.

Planificación de los Recursos Humanos: El proceso de identificar y documentar los roles dentro del proyecto, las responsabilidades y las relaciones de comunicación, así como de crear el plan de gestión de personal. También conocido como: Planeación de los Recursos Humanos.

Procedimiento: Una serie de pasos que se siguen en un orden regular definitivo con un propósito.

Proceso: El conjunto de medidas y actividades interrelacionadas realizadas para obtener un conjunto específico de productos, resultados o servicios.

Proyecto: Un esfuerzo temporal que se lleva a cabo para crear un producto, servicio o resultado único.

Requisito: Una condición o capacidad que un sistema, producto, servicio, resultado o componente debe satisfacer o poseer para cumplir con un contrato, norma, especificación u otros documentos formalmente impuestos. Los requisitos incluyen las necesidades, deseos y expectativas cuantificadas y documentadas del patrocinador, del cliente y de otros interesados. También conocido como: Requerimiento.

Riesgo: Un evento o condición incierta que, si se produce, tiene un efecto positivo o negativo en los objetivos de un proyecto. Véase también categoría de riesgo y estructura de desglose del riesgo.

Rol: Una función definida que debe realizar un miembro del equipo del proyecto, como evaluar, archivar, inspeccionar o codificar.

Solicitud de Cambio: Solicitudes para ampliar o reducir el alcance de un proyecto, modificar políticas, procesos, planes o procedimientos, modificar costes o presupuestos, o revisar cronogramas. Las solicitudes de cambio pueden hacerse directa o indirectamente, pueden iniciarse en forma externa o interna y pueden tener carácter obligatorio u opcional, ya sea desde el punto de vista legal o contractual. Únicamente se procesan las solicitudes de cambio formalmente documentadas, y sólo se implementan las solicitudes de cambio aprobadas.

Usuario: La persona u organización que usará el producto o servicio del proyecto.

Anexo 9: Plan de Gestión de Personal

PLAN DE GESTIÓN DE PERSONAL

Código: STIRECFIS-PGPE-01
Versión 1.0

Proyecto:	Sistema de Transferencia de Recaudaciones Fiscales	**Siglas:**	STIRECFIS
Entregable:	Plan de Gestión de Personal (PGPE)	**Total Páginas:**	5
Elaborado por:	**Gerente del Proyecto:** *Ginsberg Yamir Rodríguez Irías* *División Gestión y Desarrollo de Proyectos* *Departamento de Tecnología y Comunicaciones*	**Fecha:** 23/08/2018	**Firma:**
Revisado por:	**Jefe de Proyecto Funcional:** *Leyla Margoth Banegas García* *Sección de Recaudaciones Fiscales* *Departamento Servicios Fiscales*	**Fecha:** 23/08/2018	**Firma:**
	Jefe Sección de Recaudaciones Fiscales: *Carlos Alberto Anariba* *Departamento Servicios Fiscales*	**Fecha:** 23/08/2018	**Firma:**
Aprobado por:	**Jefe Depatamento:** *Raúl Edgardo Sánchez Flores* *Departamento Servicios Fiscales*	**Fecha:** 23/08/2018	**Firma:**

CONTROL DE VERSIONES:

Versión	Causa del Cambio	Responsable del Cambio	Fecha del Cambio
1.0	Versión Inicial	*Ginsberg Yamir Rodríguez Irías*	23/08/2018

ORGANIGRAMA DEL PROYECTO:

Ver Organigrama del Proyecto - versión 1.0.

DESCRIPCIÓN DE ROLES:

Nombre del Rol:	Gerente del Proyecto
Objetivos del Rol:	
Es la persona que gestiona y es el principal responsable por el éxito del proyecto, y por tanto es quien asume el liderazgo y la administración de los recursos para lograr los objetivos fijados por el patrocinador.	
Responsabilidades:	
• Elaborar el plan de proyecto. • Elaborar el informe de estado del proyecto.	

• Coordinar actividades previstas en el cronograma. • Realizar reuniones de seguimiento del proyecto. • Dirigir y supervisar la planificación del proyecto. • Firmar la documentación generada en el proyecto. • Elaborar el informe de cierre del proyecto.
Funciones:
• Planificar el proyecto. • Ejecutar el proyecto. • Controlar el proyecto. • Cerrar el proyecto. • Ayudar a gestionar el control de cambios del proyecto. • Gestionar los recursos del proyecto. • Solucionar problemas y superar los obstáculos del proyecto.
Niveles de autoridad:
• Decide sobre la programación detallada de los recursos humanos asignados al proyecto. • Decide sobre modificaciones a las líneas base del proyecto. • Decide sobre planes y programas del proyecto. • Decide sobre la información y los entregables del proyecto.
Reporta a:
• Jefe División Ingreso y Adjudicación y Tenencia de Divisas (Patrocinador del Proyecto). • Jefatura de Tecnología y Comunicaciones.
Supervisa a:
• Jefe de Proyecto Funcional. • Líder Funcional. • Desarrolladores. • Staff de Apoyo.
Incorporación al Proyecto (Renuncia, Incapacidad, Vacaciones o Remplazo):
Inmediata designación de reemplazo por parte del Departamento de Tecnología y Comunicaciones.

Nombre del Rol:	Jefe de Proyecto Funcional
Objetivos del Rol:	
Es la persona que colabora con la gestión del proyecto, es el principal responsable de definir el alcance y requisitos del sistema.	
Responsabilidades:	
• Revisar el plan de proyecto. • Elaborar en conjunto con el Gerente del Proyecto el informe de estado del proyecto. • Coordinar actividades previstas en el cronograma. • Participar en reuniones de seguimiento del proyecto. • Firmar la documentación generada en el proyecto.	

• Aprobar el alcance y requerimientos del proyecto. • Revisar Manual de Usuario del sistema. • Aprobar los entregables del proyecto.
Funciones:
• Planificar el proyecto. • Validar entregables. • Cerrar el proyecto. • Ayudar a gestionar el control de cambios del proyecto. • Gestionar los recursos del proyecto. • Solucionar problemas y superar los obstáculos del proyecto.
Niveles de autoridad:
• Decide sobre planes y programas del proyecto. • Decide sobre la información y los entregables del proyecto.
Reporta a:
• Jefe División Servicios Fiscales (Patrocinador del Proyecto). • Jefe Sección Servicios Fiscales.
Supervisa a:
• Líder funcional.
Incorporación al Proyecto (Renuncia, Incapacidad, Vacaciones o Remplazo):
Inmediata designación de reemplazo por parte del Departamento Internacional.

Nombre del Rol:	Líder Funcional
Objetivos del Rol:	
Es la persona que colabora en la definición del alcance y requisitos del proyecto.	
Responsabilidades:	
• Participar en reuniones de seguimiento del proyecto. • Definir requerimientos del proyecto. • Realizar actividades previstas en el cronograma. • Elaborar Manual de Usuario del sistema. • Probar los entregables del proyecto.	
Funciones:	
• Participar en el proyecto. • Probar entregables.	
Niveles de autoridad:	
• No definido.	
Reporta a:	

• Jefe de Proyecto Funcional.
Supervisa a:
• No aplica
Incorporación al Proyecto (Renuncia, Incapacidad, Vacaciones o Remplazo):
Inmediata designación de reemplazo por parte del Departamento Servicios Fiscales.

Nombre del Rol:	Desarrolladores
Objetivos del Rol:	
Es la persona encargada de construir el sistema en base a los requerimientos definidos por el patrocinador y líderes funcionales.	
Responsabilidades:	
• Participar en la ejecución del plan de proyecto. • Colaborar en la elaboración del informe de estado del proyecto. • Realizar actividades previstas en el cronograma. • Participar en reuniones de seguimiento del proyecto. • Desarrollar los componentes del sistema. • Elaborar la documentación técnica del sistema. • Elaborar planes y casos de prueba de los componentes desarrollados. • Brindar capacitación y entrenamiento a usuarios funcionales del sistema. • Entrenar al personal técnico de la División de Servicios Tecnológicos.	
Funciones:	
• Ejecutar el proyecto. • Desarrollar entregables. • Probar entregables. • Cerrar el proyecto.	
Niveles de autoridad:	
• Decide sobre la metodología de desarrollo del sistema. • Decide sobre la metodología de la trasferencia de conocimiento.	
Reporta a:	
• Gerente del Proyecto.	
Supervisa a:	
• No aplica.	
Incorporación al Proyecto (Renuncia, Incapacidad, Vacaciones o Remplazo):	
Inmediata designación de reemplazo por parte del Departamento de Tecnología y Comunicaciones.	

Nombre del Rol:	Staff de Apoyo

Objetivos del Rol:
Es la persona que ayuda con la exitosa implementación del sistema.
Responsabilidades:
• Participar en la ejecución del plan de proyecto. • Realizar actividades previstas en el cronograma. • Definir la arquitectura del sistema. • Diseñar la base de datos del sistema. • Brindar soporte del sistema en el ambiente de producción. • Administrar la infraestructura del sistema. • Diseñar los procesos de negocio del sistema. • Definir pistas de auditoría en el sistema. • Definir las medidas de seguridad que debe cumplir el sistema. • Controlar la mitigación de riegos del sistema.
Niveles de autoridad:
• No definido.
Reporta a:
• Gerente del Proyecto.
Supervisa a:
• No aplica.
Incorporación al Proyecto (Renuncia, Incapacidad, Vacaciones o Remplazo):
Designación a demanda por parte del proyecto.

Anexo 10: Organigrama del Proyecto

ORGANIGRAMA DEL PROYECTO

Código: STIRECFIS-ORP-02
Versión 2.0

Proyecto:	Sistema de Transferencia de Recaudaciones Fiscales	**Siglas:**	STIRECFIS
Entregable:	Organigrama del Proyecto (ORP)	**Total Paginas:**	2
Elaborado por:	**Gerente del Proyecto:** *Ginsberg Yamir Rodríguez Irías* *División Gestión y Desarrollo de Proyectos* *Departamento de Tecnología y Comunicaciones*	**Fecha:** 24/08/2018	**Firma:**
Revisado por:	**Jefe de Proyecto Funcional:** *Leyla Margoth Banegas García* *Sección de Recaudaciones Fiscales* *Departamento Servicios Fiscales*	**Fecha:** 24/08/2018	**Firma:**
	Jefe Sección de Recaudaciones Fiscales: *Carlos Alberto Anariba* *Departamento Servicios Fiscales*	**Fecha:** 24/08/2018	**Firma:**
Aprobado por:	**Jefe Depatamento:** *Raúl Edgardo Sánchez Flores* *Departamento Servicios Fiscales*	**Fecha:** 24/08/2018	**Firma:**

CONTROL DE VERSIONES:

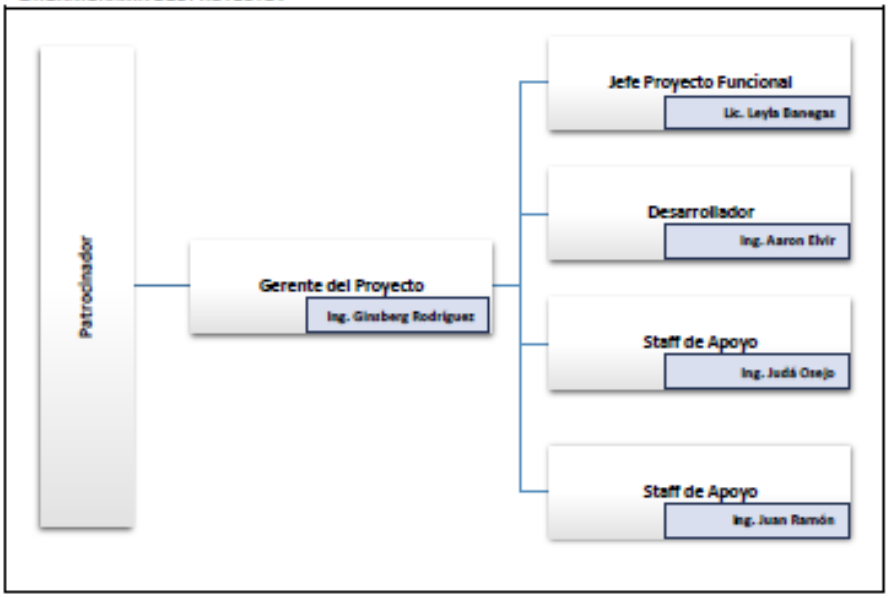
Versión	Causa del Cambio	Responsable del Cambio	Fecha del Cambio
1.0	Versión Inicial	*Ginsberg Yamir Rodríguez Irías*	24/08/2018
2.0	Incorporación de nuevo integrante al equipo del proyecto	*Ginsberg Yamir Rodríguez Irías*	24/08/2018

EQUIPO DEL PROYECTO:

Rol	Nombre	Cargo	Departamento
Patrocinador	Lic. *Raúl Edgardo Sánchez Flores*	Jefe Departamento *Servicios Fiscales*	Servicios Fiscales
	Lic. *Carlos Alberto Anariba*	Jefe Sección de *Servicios Fiscales*	Servicios Fiscales
Interesado	Lic. *Leyla Margoth Banegas García*	Jefe de Proyecto Funcional	Servicios Fiscales
Gerente del Proyecto	Ing. *Ginsberg Yamir Rodríguez Irías*	Gestor de Proyecto	Tecnología y Comunicaciones
Desarrollador	Ing. Aaron Ismael Elvir Rosales	Analista de Informática	Tecnología y Comunicaciones

Rol	Nombre	Cargo	Departamento
Staff de Apoyo	Ing. Judá Edgardo Osejo	Arquitecto de Aplicaciones	Tecnología y Comunicaciones
	Ing. Juan Ramón García	Arquitecto de Datos	Tecnología y Comunicaciones

ORGANIGRAMA DEL PROYECTO:



Anexo 11: Matriz de Asignación de Responsabilidades

MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES

Código: STIRECFIS-RAM-01
Versión 1.2

Proyecto:	Sistema de Transferencia de Recaudaciones Fiscales	**Siglas:**	STIRECFIS
Entregable:	Matriz de Asignación de Responsabilidades (RAM)	**Total Páginas:**	3
Elaborado por:	**Gerente del Proyecto:** *Ginsberg Yamir Rodríguez Irías* *División Gestión y Desarrollo de Proyectos* *Departamento de Tecnología y Comunicaciones*	**Fecha:** 27/08/2018	**Firma:**
Revisado por:	**Jefe de Proyecto Funcional:** *Leyla Margoth Banegas García* *Sección de Recaudaciones Fiscales* *Departamento Servicios Fiscales*	**Fecha:** 27/08/2018	**Firma:**
	Jefe Sección de Recaudaciones Fiscales: *Carlos Alberto Anariba* *Departamento Servicios Fiscales*	**Fecha:** 27/08/2018	**Firma:**
Aprobado por:	**Jefe Depatamento:** *Raúl Edgardo Sánchez Flores* *Departamento Servicios Fiscales*	**Fecha:** 27/08/2018	**Firma:**

CONTROL DE VERSIONES:

Versión	Causa del Cambio	Responsable del Cambio	Fecha del Cambio
1.0	Versión Inicial	*Ginsberg Yamir Rodríguez Irías*	27/08/2018
1.1	Ajuste por revisión por parte del área del negocio	*Leyla Margoth Banegas García* *Carlos Alberto Anariba*	27/08/2018
1.2	Ajuste por revisión por parte del área del negocio	*Raúl Edgardo Sánchez Flores*	27/08/2018

LEYENDAS:

Códigos de Responsabilidades:	Código de Roles:
R= Responsable A=Aprueba P=Participa V=Verifica/Revisa	PR= Patrocinador IN= Interesado GP=Gerente del Proyecto JP=Jefe de Proyecto Funcional LF=Líder Funcional DE= Desarrollador SA=Staff de Apoyo

MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES:

Código EDT	Nombre de Trabajo	Roles						
		PR	IN	GP	JP	LF	DE	SA
1	**Planificación**							
1.1	Envío de la Notificación del Inicio de Proyecto	A	P	P	R	P		
1.2	Plan del Proyecto	A	V	R	V	P	P	P
1.3	**Gestión**							
1.3.1	Actas de Reunión del Proyecto		V	R	V	P	P	P
1.3.2	Informes de Avance del Proyecto		V	R	V			
2	**Definición**							
2.1	**Levantamiento de Requerimientos**							
2.1.1	Requerimientos de Usuario	A	V	V	V	P	R	P
2.1.2	Requerimientos del Sistema	A	V	V	V	P	R	P
2.1.3	Matriz de Priorización de Requisitos		V	R	V	P	P	
2.2	**Diseño del Sistema**							
2.2.1	Especificaciones de los Requisitos del Sistema	A	V	V	V	P	R	P
2.2.2	Arquitectura de Datos			V			P	R
2.2.3	Arquitectura de Aplicación			V			P	R
2.2.4	Envío de Notas con las Especificaciones de Requerimiento del Servicio Web a los Agentes Cambiarios	V	P	P	R	P		
2.2.5	Prototipo del Sistema	A	V	V	V	P	R	P
2.2.6	Preparación del Borrador de Normativa Cambiaria	A	P		P	P		
3	**Construcción**							
3.1	Envío de la Aprobación de la Normativa Cambiara	P	P	P	P	P		
3.2	Configuración del Servidor de Aplicación y Base de Datos						V	R
3.3	Código Fuente del Módulo Administrativo			V			R	
3.4	Código Fuente del Módulo de la Boleta			V			R	
3.5	Código Fuente del Servicio WEB			V			R	
3.6	Configuración de Herramienta de Reportes			V			R	P
3.7	Resultado de Pruebas Interna			V			R	
3.8	Notificación de Prueba Piloto con los Agentes Cambiarios	A	R	P	R	P		
3.9	Resultado de Prueba Piloto		V	V	V	P	R	
3.10	Matriz de Trazabilidad de Requisitos		V	V	V	P	R	
4	**Estabilización**							
4.1	Envío de la notificación del Inicio de las Pruebas con los Agentes Cambiarios	A	P	P	R	P		

4.2	Capacitación a Usuarios		V	P	V	R	R	
4.3	Capacitación a Agentes Cambiarios		V	P	V	R	R	
4.4	Resultado de Pruebas de Usuario		V	V	V	P	R	
4.5	Resultado de Pruebas de Certificación		V	V	V	P	R	
4.6	Envío de la Notificación del Inicio del Paralelo	A	P	P	R	P		
4.7	Migración de datos de ambiente de Pruebas a Producción						P	R
4.8	Envío de la Notificación de la Salida a Producción	A	P	P	R	P		
4.9	Certificación de Salida a Producción		V	V	V	P	R	
5	**Liberación**							
5.1	Manual de Usuario		V	V	V	R	P	
5.2	Documentación Técnica del Sistema			V			R	
5.3	Acta de Entrega del Sistema	A	V	R	V			
5.4	Documento de Lecciones Aprendidas			V			R	P
5.5	Entrega de documentación a la Biblioteca Técnica			R			P	
5.6	Acta de Entrega de Código Fuente			R			P	
5.7	Capacitación Técnica del Sistema			V			R	R
5.8	Acta de Transferencia de Conocimiento			R				

Anexo 12: Lecciones Aprendidas

Registro de lecciones aprendidas proyectos OTP y STI-RECFIS

Elaborado por: Ing. Aaron Elvir y Ginsberg Rodriguez

Nro. De Referencia	Código de Proyecto	Nombre del Proyecto	Área / Categoría	Fecha	Amenaza / Oportunidad	Título	Descripción de la Situación	Descripción del Impacto en los objetivos del proyecto	Acciones Correctivas y Preventivas Implementadas	Lección Aprendida / Recomendaciones
1	OTP	Implementación OTP	Gestión de Requerimientos	30/7/2018	Amenaza	Documento de Diseño con insuficiente detalle.	Por ser un proyecto nuevo dentro del BCH, los escenarios no fueron descritos en detalle, por lo cual se tuvieron que estar realizando ajustes hasta llegar al producto esperado, además, en algunos casos se hizo referencia al comportamiento de un sistema anterior, lo cual dificulto la capacidad para desarrollar los propios requerimientos. Está situación ocasionó interpretaciones inadecuadas del alcance por parte del equipo de desarrollo, por lo se tuvo un retrabajo en ciertos componentes del proyecto.	Se retrasó la fecha de finalización del componente OTP	Como acción correctiva, se realizaron ajustes a los requerimientos. Luego se realizaron desarrollos de la funcionalidad esperada. Como acción preventiva, se revisaron el resto de los documentos de diseño funcional para buscar identificar situaciones similares y tomar los correctivos antes de comenzar a desarrollar esos componentes.	Implementar un control de aprobación de los documentos funcionales. Crear un checklist de aprobación en el cual se describa en detalle los procesos de negocio y comportamiento esperados.
2	OTP	Implementación OTP	Gestión Tecnica	30/7/2018	Oportunidad	Desarrollo de habilidades de investigación e implementación de aplicaciones vb.net	Se conto con el apoyo de la jefatura para poder investigar, desarrollar e implementar el proyecto OTP	Se alcanzo el objetivo final del proyecto.	Ninguna	Se recomienda seguir desarrollando proyecto que ayuden a impulsar las habilidades de desarrollo de los técnicos de la división de desarrollos de sistemas
3	STI-RECFIS	Sistema de Transferencia de Recaudaciones Fiscales	Gestion del Alcance	20/10/2018	Amenaza	Poco claridad del alcance del proyecto	No se tenian claro el alcance del proyecto por parte del usuario, ya que ellos solo querian sistematizar su proceso manual, por lo tanto genero un poco de friccion indicar que se tienen que realizar mantenimientos a las tablas que podran administrar los usuarios	Se tuvo que tener varias reuniones con los funcionales para explicar el alcance del proyecto y asi poder cumplir en tiempo todos los requerimientos.	Reuniones periodicas para implementar cambios y correciones a los desarrollos ya realizados	Se recomienda tener reuniones antes de iniciar los desarrollas para que los productos sean aceptados si necesidad de realizar grandes ajustes

Anexo 13: Hoja de Ruta del Proyecto

Hoja de ruta del producto (Agile Roadmap)

Proyecto: Implementación One Time Password (OTP)

Período: **Agosto de 2018**
Organización: **Banco Central de Honduras**
Cliente: **Tecnología y Comunicaciones**
Dueño del producto (Owner): **TYC**
Scrum Master: **Aaron Elvir**

Banco Central de Honduras	1er. Hito	2do. Hito	3er. Hito	4ta. Hito
Investigación Criptografía	Funcionalidad			
Desarrollo de Modelo Criptográfico		Funcionalidad Desarrollo		
Pruebas y Documentación de los Resultados Obtenidos			Funcionalidad Pruebas	
Implementación STI-RECFIS				Funcionalidad Final

Anexo 14: Pila de producto (Product Backlog)

Desarrollo ágil: Pila de Producto (Product Backlog)

Elaborado por: Ginsberg Rodríguez

Id	Tarea	Tipo	Estado	Responsable	Duración	Comentarios
SPRINT: INVESTIGACIÓN CRIPTOGRAFÍA						
1	Investigar sobre la metodología de encriptación	Investigación	Finalizado	Aaron Elvir	1 Dia	Se investigación sobre la criptografía simétrica y la asimétrica
2	Investigar sobre los métodos de encriptación utilizados en la actualidad	Investigación	Finalizado	Aaron Elvir	1 Dia	Se determino que existen métodos estándar para la encriptación por ejemplo SHA0, SHA1, SHA256, SHA512
SPRINT: DESARROLLO DE MODELO CRIPTOGRAFICO						
3	Implementar librerías Criptográficas	Análisis/Diseño	Finalizado	Aaron Elvir	1 Dia	Se logro implementar las librerías criptográficas por medio de AddOn
4	Desarrollo de clases y librerías para implementar los diferentes métodos de encriptación	Desarrollo	Finalizado	Aaron Elvir	2 Días	Se logro implementar los métodos criptográficos estandarizados por medio de las librerías Microsoft.
SPRINT: PRUEBAS Y DOCUMENTACIÓN DE LOS RESULTADOS OBTENIDOS						
5	Desarrollo de interfaz de usuario para probar los resultados obtenidos	Pruebas	Finalizado	Aaron Elvir	2 Días	N/A
6	Documentación de resultados obtenidos, y documentación de lecciones aprendidas	Documentación	Finalizado	Aaron Elvir	1 Dia	N/A
SPRINT: IMPLEMENTACIÓN STI-RECFIS						
7	Generar dll para incorporar a la solución STI-RECFIS	Desarrollo	Finalizado	Aaron Elvir	1 Dia	N/A
8	Implementar solución al proyecto STI-RECFIS	Desarrollo	Finalizado	Aaron Elvir	1 Dia	N/A

Anexo 15: Formatos de Pruebas

DEPARTAMENTO DE TECNOLOGÍA Y COMUNICACIONES
PROYECTO DE MIGRACIÓN DE BASE DE DATOS
FORMATO DE PRUEBAS

Datos de Prueba			
Elemento o Sistema:	STI-RECFIS		
Fecha:	10 de octubre de 2018		
Hora de Inicio:	02:00 pm	**Hora de finalización:**	04:03 pm
Código de Prueba	**INTERNO-STI-RECFIS_PRUEBAS**		
Objetivos de la prueba:	Comprobar el funcionamiento de mejoras y funcionalidad general del sistema STI-RECFIS		

Instrucciones	
1	Por cada actividad se asignó un representante de TYC que le ayudará en sus consultas.
2	Utilizar usuario y contraseña del directorio activo (ADS).
3	Por cada actividad realizada incluya una captura de pantalla como evidencia.
4	Una vez finalizada las verificaciones realice lo siguiente: 1. Remita vía correo electrónico a aaron.elvir@bch.hn, selim.nazar@bch.hn y estrella.germer@bch.hn copia del documento incluyendo las evidencias. 2. Imprima **solo** la sección de "***Lista de actividades***" y la "***Sección de Firmas***" la cual se encuentra al final del documento. 3. Firme el documento 4. Remita el documento firmado a Aaron Elvir

DEPARTAMENTO DE TECNOLOGÍA Y COMUNICACIONES
PROYECTO DE MIGRACIÓN DE BASE DE DATOS
FORMATO DE PRUEBAS

Detalle de Actividades de la Prueba

Actividad 1: Conexión al **ambiente de pruebas** al sistema STI-RECFIS URL: https://recfispruebas.bch.sp/Recfis/Login.aspx
Ingreso a la pantalla de login.
Observaciones
1. INCLUIR COMENTARIO **ACCESO CORRECTO AL STI-RECFIS.**   

Actividad 2: Realizar consulta y descarga de archivos con diferentes criterios de búsqueda

Visualización de los datos mostrados en pantalla

Observaciones

2. SE CORRIGIO EL PROBLEMA QUE PRESENTABA EN EL MODULO DE DESCARGA, AHORA SE MUESTRA UN MENSAJE DE AVISO.

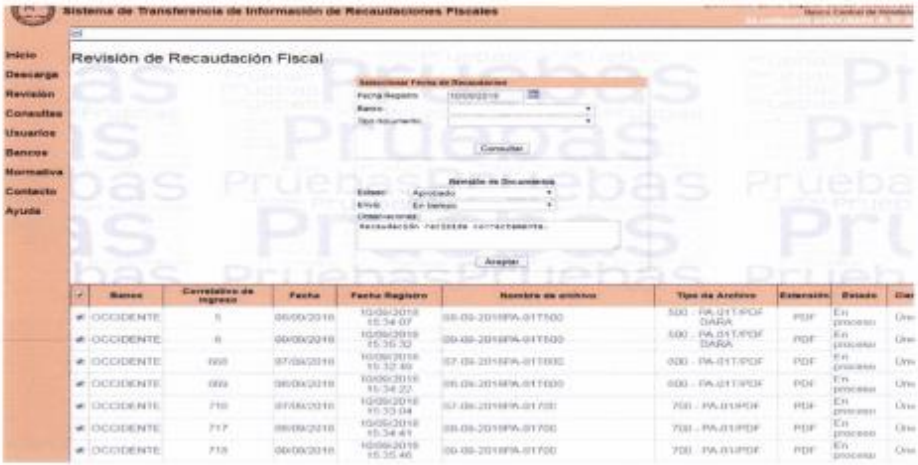
Transacción	Fecha	Nombre de archivo	Tipo de Archivo	Extensión	Estado	Cierre	Envio	Fecha Registro	Banco
4	07/09/2018	07-09-2018PA-01T500	500 - PA-01T/PDF DARA	PDF	Rechazado	Unico	En tiempo	10/09/2018 15:32:33	OCCIDENTI
5	08/09/2018	08-09-2018PA-01T500	500 - PA-01T/PDF				En tiempo	10/09/2018 15:34:07	OCCIDENTI
6	09/09/2018	09-09-2018PA-01T500					En tiempo	10/09/2018 15:35:32	OCCIDENTI
668	07/09/2018	07-09-2018PA-01T600					En tiempo	10/09/2018 15:32:48	OCCIDENTI
669	08/09/2018	08-09-2018PA-01T600					En tiempo	10/09/2018 15:34:22	OCCIDENTI
716	07/09/2018	07-09-2018PA-01700	700 - PA-01/PDF	PDF	En proceso	Unico	En tiempo	10/09/2018 15:33:04	OCCIDENTI
717	08/09/2018	08-09-2018PA-01700	700 - PA-01/PDF	PDF	En proceso	Unico	En tiempo	10/09/2018 15:34:41	OCCIDENTI
718	09/09/2018	09-09-2018PA-01700	700 - PA-01/PDF	PDF	En proceso	Unico	En tiempo	10/09/2018 15:35:46	OCCIDENTI

Actividad 3: Realizar la revisión y rechazo de una PA

AUTORIZACION Y RECHAZO DE ARCHIVOS MASIVOS Y UNITARIOS

Observaciones	

3. AL MOMENTO DE DAR CLICK EN EL BOTON ACEPTAR SE TARDA MUCHO EN CARGAR LA PAGINA COMO QUE SE QUEDA PEGADO EL SISTEMA, SIN EMBARGO, SI SE ENVIAN LOS CORREOS.



Actividad 4: Visualización de correos enviados por parte de los usuarios financieros
VISUALIZACION DE LOS CORREOS ENVIADOS AUTOMATICAMENTE POR EL SISTEMA
Observaciones

4. SE VALIDÓ LA CARGA DE LA INFORMACIÓN POR PARTE DEL USUARIO FINANCIERO, ASI COMO, LOS CORREOS DE CONFIRMACIÓN DE LA INFORMACIÓN.

Sistema de Carga de Información de Recaudación Fiscal
Notificación de Carga de Información

Se le notifica que su información correspondiente al ***11/10/2018***, *ha sido cargada con éxito en el sistema a las* ***15:45:51*** *horas.*
Nombre de archivo: ***07-09-2018PA-01T500_4***
Información cargada por el usuario: Aaron Ismael Elvir Rosales.

Atentamente,

Sección de Recaudación Fiscal.
Departamento de Servicios Fiscales.
Banco Central de Honduras.

Sistema de Carga de Información de Recaudaciones Fiscal
Notificación de Carga de Recibo Electrónico

Se le notifica que se recibieron y cargaron satisfactoriamente las Recaudaciones Fiscales correspondientes al archivo: ***07-09-2018PA-01T500_4*** con fecha ***11/10/2018***
Información revisada por: Yessica Patricia Mendoza.

Atentamente,

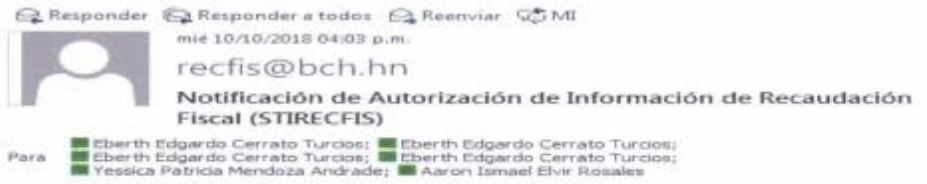
Sección de Recaudación Fiscal.
Departamento de Servicios Fiscales.
Banco Central de Honduras.

Actividad 5: Visualización de correos enviados a los usuarios financieros del estado de los documentos que fueron recibidos por el BCH

VISUALIZACION DE LOS CORREOS ENVIADOS AUTOMATICAMENTE POR EL SISTEMA

Observaciones	

5. SI SE LOGRO VISUALIZAR LOS CORREOS ENVIADOS.


Responder Responder a todos Reenviar MI

mié 10/10/2018 04:03 p.m.

recfis@bch.hn

Notificación de Autorización de Información de Recaudación Fiscal (STIRECFIS)

Para Eberth Edgardo Cerrato Turcios; Eberth Edgardo Cerrato Turcios; Eberth Edgardo Cerrato Turcios; Eberth Edgardo Cerrato Turcios; Yessica Patricia Mendoza Andrade; Aaron Ismael Elvir Rosales

Sistema de Carga de Información de Recaudaciones Fiscal
Notificación de Carga de Recibo Electrónico

Se le notifica que se revisó y aprobó satisfactoriamente las Recaudaciones Fiscales correspondientes al archivo: ***012000201809092018091014582 4.PAT*** con fecha ***10/09/2018*** correspondientes a ***OCCIDENTE***
Información revisada por: Eberth Edgardo Cerrato Turcios.

Atentamente,

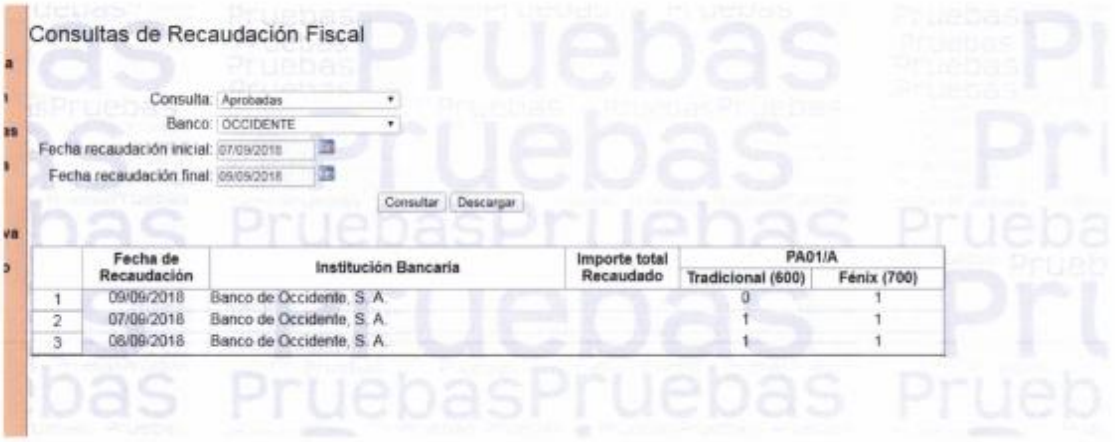
Sección de Recaudación Fiscal.
Departamento de Servicios Fiscales.
Banco Central de Honduras.

Actividad 6: Consulta de recaudaciones fiscales por diferentes bancos, estatus de documentos y fechas de recaudación

VISUALIZACION DE LA INFORMACIÓN EN PANTALLA

Observaciones

6. SI SE LOGRA VISUALIZAR LA INFORMACION EN EL MODULO DE CONSULTA



Consultas de Recaudación Fiscal

Consulta: Aprobadas
Banco: OCCIDENTE
Fecha recaudación inicial: 07/09/2018
Fecha recaudación final: 09/09/2018
Consultar Descargar

	Fecha de Recaudación	Institución Bancaria	Importe total Recaudado	PA01/A	
				Tradicional (600)	Fénix (700)
1	09/09/2018	Banco de Occidente, S. A.		0	1
2	07/09/2018	Banco de Occidente, S. A.		1	1
3	06/09/2018	Banco de Occidente, S. A.		1	1

Actividad 7: Descarga a Excel de los consultas generadas en pantalla

DESCARGA A EXCEL DE LOS DOCUMENTOS GENERADOS

Observaciones

7. SI SE EXPORTAN A EXCEL LOS DOCUMENTOS GENERADOS

Banco Central de Honduras
Departamento de Servicios Fiscales
Sección de Recaudaciones Fiscales

Reporte de PA01 aprobadas
OCCIDENTE
Rango de Fecha
Inicial:07/09/2018 Final:09/09/2018

Fecha de Recaudación	Institución Bancaria	Importe total Recaudado	PA01/A	
			Tradicional (600)	Fénix (700)
09/09/2018	Banco de Occidente, S. A.		0	1
07/09/2018	Banco de Occidente, S. A.		1	1
08/09/2018	Banco de Occidente, S. A.		1	1

Actividad 8: Creación y actualización de nuevos usuarios al sistema

ADMINISTRACION DE USUARIOS

Observaciones

8. SI SE PUEDE VISUALIZAR EL MODULO DE USUARIOS


Mantenimiento de Usuarios

Código:
Banco:
Usuario AD:
Nombre(s):
Teléfono:
Apellido(s):
Correo electrónico:
Estado: Activo / Inactivo
Limpiar | Guardar
Filtro banco:

Modificar	Código	Nombre	Apellido	Usuario AD	Correo	Teléfono	Banco
Modificar	8	Sara	Martinez	sm1606041	eberth.cerrato@bch.hn	1260	Banco Central de Honduras
Modificar	42	Saby Marella	Rivera Lopez	banadesasrivera	eberth.cerrato@bch.hn	2237-5663 Ext 114	Banco Nacional de Desarrollo Ag
Modificar	16	REINA	BAQUIS	CAPM08	eberth.cerrato@bch.hn	2237-5663 EXT. 150	Banco Nacional de Desarrollo Ag
Modificar	3	David Alejandro	Romero Quiroz	dr113068	eberth.cerrato@bch.hn	2710	Banco Nacional de Desarrollo Ag
Modificar	43	Reina	Baquis Cerna	banadesarbaquis	aaron.elvir@bch.hn	2237-5663 Ext 115	Banco Nacional de Desarrollo Ag
Modificar	44	Alex Alfredo	Guzman Canelas	honduraselguzman	eberth.cerrato@bch.hn	2290-2121	Banco de Honduras, S.A
Modificar	56	José Francisco	Funez Martinez	honduraslpfunez	eberth.cerrato@bch.hn	2545-1503	Banco de Honduras, S.A
Modificar	12	JUAN JOSE	CHAVEZ	CAPM01	elvros2000@yahoo.com.mx	2290-2140	Banco de Honduras, S.A
Modificar	45	Juan Jose	Chavez Ordoñez	honduranjchavez	eberth.cerrato@bch.hn	2290-2140	Banco de Honduras, S.A
Modificar	59	Lidia Marisela	Velasquez Alvarado	honduraslvelasquez	eberth.cerrato@bch.hn	2290-2121	Banco de Honduras, S.A

1

Actividad 9: Creación y actualización de nuevos bancos al sistema

ADMINISTRACION DE BANCOS

Observaciones

8. SI SE LOGRA ENTRAR EL MODULO DE BANCOS

Mantenimiento de Bancos

Código: 48
Nombre corto:
Descripción:
Estado: * Activo ○ Inactivo

Limpiar | Guardar

Modificar	Código	Nombre Corto	Descripción	Fecha
Modificar	2	BANADESA	Banco Nacional de Desarrollo Agrícola	05/07/2015
Modificar	3	HONDURAS	Banco de Honduras, S.A.	14/08/2015
Modificar	4	BANCATLAN	Banco Atlántida, S. A.	14/08/2015
Modificar	9	BANTRAB	Banco de los Trabajadores, S.A.	14/08/2015
Modificar	12	OCCIDENTE	Banco de Occidente, S. A.	14/08/2015
Modificar	15	FICENSA	Banco Financiera Centroamericana, S.A.	14/08/2015
Modificar	18	BANHCAFE	Banco Hondureño del Café, S. A.	14/08/2015
Modificar	20	BANPAIS	Banco del País, S. A.	14/08/2015
Modificar	22	LAFISE	Banco Lafise, S. A.	14/08/2015
Modificar	24	CONTINENTAL	Banco Continental, S. A.	14/08/2015
Modificar	30	FICOHSA	Banco Financiera Comercial Hondureña, S.A.	14/08/2015
Modificar	39	DAVIVIENDA	Banco DaVivienda, S.A.	14/08/2015
Modificar	40	BAC	BAC Honduras, S.A.	14/08/2015
Modificar	43	PROMERICA	Banco Promérica, S. A.	14/08/2015
Modificar	46	BANRURAL	Banco de Desarrollo Rural, S. A.	17/04/2017

1

Descripción: STI-RECFIS Pruebas				
Lista de Actividades a comprobar funcionamiento				
Actividad	**Responsable**	**Contraparte TYC**	**Nombre de Actividad**	**¿Funcionó correctamente?**
1.	Eberth Cerrato	Aarón Elvir	Ingreso al sistema	SI ☒ NO ☐
2.	Eberth Cerrato	Aarón Elvir	Consulta y descarga de archivos recibidos	SI ☒ NO ☐
3.	Eberth Cerrato	Aarón Elvir	Autorización y rechazo de PA	SI ☒ NO ☐
4.	Eberth Cerrato	Aarón Elvir	Visualización de correos enviados por el usuario financiero	SI ☒ NO ☐
5.	Eberth Cerrato	Aarón Elvir	Visualización de correos enviados, informando el estatus de los documentos al usuario financiero	SI ☒ NO ☐
6.	Eberth Cerrato	Aarón Elvir	Consulta de recaudaciones fiscales por diferentes parámetros de búsqueda	SI ☒ NO ☐
7.	Eberth Cerrato	Aarón Elvir	Descarga a Excel de los documentos visualizados en la pantalla de consultas	SI ☒ NO ☐
8.	Eberth Cerrato	Aarón Elvir	Creación y actualización de usuarios	SI ☒ NO ☐
9.	Eberth Cerrato	Aarón Elvir	Creación actualización de bancos	SI ☒ NO ☐
10.	Eberth Cerrato	Aarón Elvir	Certificación correcta del uso del sistema	SI ☒ NO ☐

Anexo 16: Informe Técnico de Capacitación

Noviembre

INFORME DE CAPACITACIÓN 2018

Sistema de Transferencia de Información de Recaudación Fiscal (STI-RECFIS)

Transferencia de conocimientos

INFORME DE CAPACITACIÓN

TRANSFERENCIA DE CONOCIMIENTOS
Sistema de Transferencia de Información de Recaudación Fiscal

DEL 05 al 07 DE
NOVIEMBRE DE 2018

INFORME DE CAPACITACIÓN

I. Antecedentes.

El STI-RECFIS tiene como propósito agilizar la transmisión de los archivos electrónicos y documentos soportes que respaldan las recaudaciones fiscales del estado, procesadas por las instituciones bancarias autorizadas.

II. Objetivo de la Capacitación.

Proporcionar a los participantes el conocimiento acerca de la interacción con los distintos elementos de software del STI-RECFIS, herramientas utilizadas y demás elementos que fueron necesarios para el desarrollo del sistema.

III. Duración de la capacitación.

Del 05 al 07 de noviembre del año 2018 en horario de 04:00 p.m. a 05:00 p.m.

IV. Lugar.

Salón de sesiones del Departamento de Tecnología y Comunicaciones, cita en 7mo. Piso del Edificio Principal del BCH.

V. Participantes.

a. Ponentes.

- Ingeniero Aaron Ismael Elvir Rosales – DGDP

b. Asistentes.

Asistieron 2 personas en representación de la DMSC y 1 persona en representación de DOyT:

- Ingeniero Ergar Fransué Vargas Espinal.
- Ingeniero Lester Obedy Sandoval Nuñez
- Ingeniero Edy Javier Milla Reyes

VI. Anexos.

- Anexo I – Temario de capacitación
- Anexo II – Lista de asistencia

Anexo I
Temario.

PROGRAMACIÓN DEL PLAN DE TRANSFERENCIA DE CONOCIMIENTO										
SISTEMA DE TRANSFERENCIA DE INFORMACION DE RECAUDACIÓN FISCAL (STI-RecFis)										
TEMA	INSTRUCTOR	TIEMPO	FECHA	HORARIO	UBICACIÓN	PARTICIPANTES	RESPONSABLE DIRECTO	RESPONSABLE CONTINGENCIA	% AVANCE	OBSERVACIONES
1. Generalidades del Sistema	Aaron Elvir	15 Min	5/11/2018	4:00 p.m.- 5:00 p.m.	Edificio Principal	[illegible]	[illegible]	[illegible]	100.00%	
a. Introducción										
b. Objetivo General										
c. Objetivos Específicos										
2. Uso del STI-RECFIS	Aaron Elvir	15 Min	5/11/2018	4:00 p.m.- 5:00 p.m.	Edificio Principal	[illegible]	[illegible]	[illegible]	100.00%	
3. Desarrollo del Sistema	Aaron Elvir	60 Min	05/11/2018 06/11/2018	4:00 p.m.- 5:00 p.m.	Edificio Principal	[illegible]	[illegible]	[illegible]	100.00%	
a. Tipos de usuarios y accesos del sistema										
b. Arquitectura de aplicación										
c. Arquitectura de negocio										
d. Pantallas del sistema										
e. Seguridad										
f. Esquema de autenticación de usuarios										
f. Herramientas utilizadas en el desarrollo										
4. Información de la base de datos	Aaron Elvir	60 Min	06/11/2018 07/11/2018	4:00 p.m.- 5:00 p.m.	Edificio Principal	[illegible]	[illegible]	[illegible]	100.00%	
a. Modelo de datos										
b. Inventario de objetos en la BD										
5. Implementación del Sistema	Aaron Elvir	30 Min	7/11/2018	4:00 p.m.- 5:00 p.m.	Edificio Principal	[illegible]	[illegible]	[illegible]	100.00%	
a. Requerimientos del equipo										
b. Instalación del sistema										
c. Detalle de los ambientes creados										
TOTAL CAPACITACION		180 Min							100.00%	

Anexo II
Lista de Asistencia

LISTADO DE PARTICIPANTES CAPACITACION					
SISTEMA DE TRANSFERENCIA DE INFORMACION DE RECAUDACION FISCAL STI-RECFIS					
NUMERO	DEPTO	NOMBRE	NO. EMPLEADO	FECHA	FIRMA
1	TyC	[illegible]	[illegible]	[illegible]	[illegible]
2	TyC	[illegible]	[illegible]	[illegible]	[illegible]
3	TyC	[illegible]	[illegible]	[illegible]	[illegible]

Aaron Ismael Enir Rojales

LISTADO DE PARTICIPANTES CAPACITACION					
SISTEMA DE TRANSFERENCIA DE INFORMACION DE RECAUDACION FISCAL STI-RECFIS					
NUMERO	DEPTO	NOMBRE	NO. EMPLEADO	FECHA	FIRMA
1	T.I.C.	[illegible]	[illegible]	5/1/2014	[illegible]
2	T.I.C.	[illegible]	[illegible]	5/1/2014	[illegible]
3	T.I.C.	[illegible]	[illegible]	5/1/2014	[illegible]
4	T.I.C.	[illegible]	[illegible]	5/1/2014	[illegible]

Pavon Ismael Elvin Rosales

LISTADO DE PARTICIPANTES CAPACITACION					
SISTEMA DE TRANSFERENCIA DE INFORMACION DE RECAUDACION FISCAL STI-RECFIS					
NUMERO	DEPTO	NOMBRE	NO. EMPLEADO	FECHA	FIRMA
1	TyC	[illegible]	115039	6/1/2016	[illegible]
2	TyC	[illegible]	[illegible]	6/1/2016	[illegible]
3	TyC	JAVIER SANDOVAL	113083	6/1/2016	[illegible]
4	TyC	Edy [illegible]	103074	6/1/2016	[illegible]

Aaron Ismael Elvir Rosales

BIBLIOGRAFÍA

BCH. (27 de Julio de 2018). *http://www.bch.hn/.* Obtenido de http://www.bch.hn/operativasd.php

Clarín. (26 de Enero de 2014). *https://www.clarin.com/.* Obtenido de https://www.clarin.com/entremujeres/tech/tardaria-hacker-descifrar-contrasena_0_r1PjBAYv7e.html

devjoker. (26 de Julio de 2006). *http://www.devjoker.com/.* Obtenido de http://www.devjoker.com/gru/tutorial-PL-SQL/PLSQ/Tutorial-PL-SQL.aspx

Financiero, E. (19 de Jul de 2017). Resguarde su información sensible con el doble factor de autenticación. *El Financiero; San José, Costa Rica*. Obtenido de https://search.proquest.com/docview/1953331303?accountid=35325

IAIP. (s.f.). *https://portalunico.iaip.gob.hn.* Obtenido de https://portalunico.iaip.gob.hn/archivos/PIMIENTA/Planeacion%20y%20rendicion%20de%20cuentas/Planes/Plan%20Estrategico/2017/PDEM%20UNITEC.pdf

Instituto Hondureño de Turismo. (s.f.). *http://www.iht.hn.* Obtenido de http://www.iht.hn/wp-content/uploads/2015/09/ley_propiedad.pdf

Microsoft. (Octubre de 2016). *https://msdn.microsoft.com/.* Obtenido de https://msdn.microsoft.com/es-es/library/y66ey2hh(v=vs.110).aspx

Microsoft. (Octubre de 2016). *https://msdn.microsoft.com/.* Obtenido de https://msdn.microsoft.com/es-es/library/2dx6wyd4(v=vs.110).aspx

Olmos, A. G. (Abril de 2015). *http://www.oracle.com/.* Obtenido de http://www.oracle.com/technetwork/es/articles/idm/advanced-security-option-oracle-2522472-esa.html

Oracle. (Junio de 2007). *http://www.oracle.com/.* Obtenido de http://www.oracle.com/technetwork/es/database/enterprise-edition/documentation/oracle-advanced-security-11g-426368-esa.pdf

Oracle. (2011). *https://docs.oracle.com.* Obtenido de https://docs.oracle.com/cd/E24693_01/appdev.11203/e23448/d_random.htm

Oracle. (2014). *https://docs.oracle.com.* Obtenido de https://docs.oracle.com/cd/E11882_01/timesten.112/e21645/d_random.htm

oracle-base. (s.f.). *https://oracle-base.com/.* Obtenido de https://oracle-base.com/articles/misc/dbms_random

owasp. (2 de Febrero de 2016). *https://www.owasp.org.* Obtenido de https://www.owasp.org/index.php/Insecure_Randomness

RSA - AMAZON. (26 de Enero de 2007). *https://www.amazon.com.* Obtenido de https://www.amazon.com/RSA-SecurID-SID700-hardware-token/dp/B000MW4228

Sampieri, R. H., & Lucio, C. F. (2003). Metodología de la Investigación. En R. Hernández Sampieri, C. Fernández Collado, & P. Baptista Lucio, *Metodología de la investigación* (Tercera ed., pág. 9). México: Mc Graw Hill. Obtenido de https://investigar1.files.wordpress.com/2010/05/sampieri-hernandez-r-cap3-planteamiento-del-problema.pdf

Sampieri, R. H., & Lucio, C. F. (2003). Metodología de la Investigación. En R. Hernández Sampieri, C. Fernández Collado, & P. Baptista Lucio, *Metodología de la investigación* (Tercera ed., pág. 9). México: Mc Graw Hill. Obtenido de https://investigar1.files.wordpress.com/2010/05/sampieri-hernandez-r-cap3-planteamiento-del-problema.pdf

The Open Group. (2018). *http://pubs.opengroup.org/.* Obtenido de http://pubs.opengroup.org/architecture/togaf9-doc/arch/chap02.html

Scambray, J., & McClure, S. (s.f.). HACKERS EN WINDOWS 2000. Secretos y soluciones para la seguridad en Windows 2000 (Primera). Madrid: McGRAW HILL/INTERAMERICANA DE ESPAÑA, S.A.U.

Dimes, T. (2015). *Conceptos Básicos De Scrum: Desarrollo De Software Agile Y Manejo De Proyectos Agile*. Babelcube Inc.

Menezo, G., & De, J. (2017). Sistema de autenticación de dos factores basado en tarjeta inteligente y tecnologías NFC. Recuperado de https://repositorio.unican.es/xmlui/handle/10902/10509

Mahalakshmi, M., & Sundararajan, D. M. (2013). Traditional SDLC Vs Scrum Methodology – A Comparative Study, *3*(6), 5.

Redacción. (2017, diciembre 21). Las 25 peores contraseñas de 2017 que demuestran que estamos a merced de los hackers (y cómo mejorarlas). *BBC News Mundo*. Recuperado de https://www.bbc.co.uk/mundo/noticias-42427928

Sobh, T. (2008). *Advances in Computer and Information Sciences and Engineering*. Dordrecht, NETHERLANDS: Springer. Recuperado de http://ebookcentral.proquest.com/lib/bvunitecvirtual-ebooks/detail.action?docID=364599

Dimes, T. (2015). *Conceptos Básicos De Scrum: Desarrollo De Software Agile Y Manejo De Proyectos Agile*. Babelcube Inc.

Menezo, G., & De, J. (2017). Sistema de autenticación de dos factores basado en tarjeta inteligente y tecnologías NFC. Recuperado de https://repositorio.unican.es/xmlui/handle/10902/10509

Qué es SCRUM. (2008, agosto 4). Recuperado 25 de agosto de 2018, de https://proyectosagiles.org/que-es-scrum/

Redacción. (2017, diciembre 21). Las 25 peores contraseñas de 2017 que demuestran que estamos a merced de los hackers (y cómo mejorarlas). *BBC News Mundo*. Recuperado de https://www.bbc.co.uk/mundo/noticias-42427928

Sobh, T. (2008). *Advances in Computer and Information Sciences and Engineering*. Dordrecht, NETHERLANDS: Springer. Recuperado de http://ebookcentral.proquest.com/lib/bvunitecvirtual-ebooks/detail.action?docID=364599

Dimes, T. (2015). *Conceptos Básicos De Scrum: Desarrollo De Software Agile Y Manejo De Proyectos Agile*. Babelcube Inc.

s a merced de los hackers (y cómo mejorarlas). *BBC News Mundo*. Recuperado de https://www.bbc.co.uk/mundo/noticias-42427928

Sobh, T. (2008). *Advances in Computer and Information Sciences and Engineering*. Dordrecht, NETHERLANDS: Springer. Recuperado de http://ebookcentral.proquest.com/lib/bvunitecvirtual-ebooks/detail.action?docID=364599

Dimes, T. (2015). Conceptos Básicos De Scrum: Desarrollo De Software Agile Y Manejo De Proyectos Agile. Babelcube Inc.

Fundamentos Para La Direccion de Proyectos (PMBOK) Quinta Edición.pdf. (s. f.). Recuperado 25 de agosto de 2018, de https://drive.google.com/file/d/0BzPixXEpUh1SZEtGNHhzVy1HQjA/view?usp=embed_facebook

Grady, B. (1994). Object Oriented Analysis and Design with Applications. The Benjamin/Cummings Publishing Company.

Schwaber K. (1997) SCRUM Development Process. In: Sutherland J., Casanave C., Miller J., Patel P., Hollowell G. (eds) Business Object Design and Implementation. Springer, London

Holgado, A. G. (2013). Análisis de integración de soluciones basadas en software como servicio para la implantación de ecosistemas tecnológicos corporativos, 76.

DINSMORE, P. C.; SILVEIRA NETO, F. H. (2005) Gerenciamento de Projetos: Como Gerenciar seu Projeto com Qualidade, dentro do Prazo e Custos Previstos. Rio de Janeiro: QualityMark.

PROJECT MANAGEMENT INSTITUTE (2013) A guide to the Project Management of Body of Knowledge (PMBOK). 5. ed. Pennsylvania, PA, USA: Project Management Institute.

Virla, M. Q. (2010). Confiabilidad y coeficiente Alpha de Cronbach, 6.

Celina Oviedo, H., & Campo Arias, A. (2005). Aproximación al uso del coeficiente alfa de Cronbach. Revista Colombiana de Psiquiatría, XXXIV(4). Recuperado de http://www.redalyc.org/resumen.oa?id=80634409

Molero Escobar, G. (2011, septiembre). CLÚSTER DE ALTO RENDIMIENTO EN UN CLOUD: EJEMPLO DE APLICACIÓN EN CRIPTOANÁLISIS DE FUNCIONES HASH. Universidad de Almería.

Franco, J. P., Sarasa Lopez, M. A., & Salazar Riaño, J. L. (2001, septiembre 26). CRIPTOGRAFIA DIGITAL: FUNDAMENTOS Y APLICACIONES (2ª ED.) | VV.AA. | 9788477335580. https://www.casadellibro.com/libro-criptografia-digital-fundamentos-y-aplicaciones-2-ed/9788477335580/798279