



MAESTRÍA EN  
**SEGURIDAD  
INFORMÁTICA**

PORTAFOLIO DE TRABAJOS

MA Ing. Ricardo Alejandro Pérez Rodríguez

Guatemala, mayo de 2024

## INTRODUCCIÓN

Este portafolio representa las oportunidades de diversos proyectos cruciales para desarrollo el profesional y también ayudaron a diversas entidades, a continuación, se encuentra una síntesis de los proyectos que se desarrollaron a lo largo de los cursos, para la clase de emprendimiento empresarial el proyecto se enfocó en un análisis exhaustivo de las tecnologías perimetrales apoyadas por la inteligencia artificial para poder controlar accesos y salidas en zonas residenciales, mejorando la vida de los residentes en cuanto a seguridad.

El siguiente proyecto realizado en la clase de seguridad de aplicaciones, se centró en la evaluación de riesgo y vulnerabilidades sobre CMS para una entidad privada, dentro de este se encontrará lista de activos, vulnerabilidades y riesgos y un resultado de cómo se encuentra dicha entidad. Como tercer proyecto se encuentra el realizado en la clase de planeación de la continuidad el cual aborda los diferentes planes de continuidad que las diferentes empresas deben de poseer para garantizar una debida continuidad de negocios, y dando a entender los procesos críticos, el proyecto fue basado en una entidad bancaria.

Como cuarto proyecto realizado en la clase de gestión de proyectos, dentro de este se encuentra como es la debida documentación que un proyecto real debe de llevar a cabo, esto basado en una empresa llamada Pillofon. Como quinto proyecto realizado en la clase de Diseños de seguridad y CMMI se encuentra la implementación de un modelo de madurez CMMI, enfocada en la organización de Disagro de Guatemala, dentro de este encontrará una planificación y estimación de mejoras en los procesos siguiendo niveles de madurez del CMMI. El sexto proyecto desarrollado en la clase de gobierno, riesgo y cumplimiento, dentro de este encontrará una gestión de riesgos para el sector bancario, y lo fundamental que son las resoluciones de seguridad JM-102-2011 y la JM-104-2021 para garantizar que estas organizaciones se mantengan en funcionamiento.

Finalmente, el último proyecto el cual es un artículo científico, en este encontrará información fundamental y síntesis de como se encuentra la seguridad de una entidad guatemalteca, y sus deficiencias. Todos estos proyectos reflejan una dedicación constante de buenas prácticas y la mejora de en distintos ámbitos informáticos.

## **ÍNDICE**

Emprendimiento empresarial.

Seguridad de aplicaciones.

Plan de continuidad de negocios para servicios bancarios.

Gestión de proyecto para una aplicación móvil gestión y atención de clientes

Diseños de seguridad y CMMI

Gobierno, riesgo y cumplimiento

Proyecto de investigación

**UNIVERSIDAD MARIANO GÁLVEZ DE GUATEMALA**  
**Facultad de Ingeniería en Sistemas de Información**  
**Maestría en Seguridad Informática**  
**Emprendimiento Empresarial**  
**Sección A**



**Proyecto Final**

Ing. Harold Rafael Cancinos Arbizu

Haroldo Rafael  
Cancinos  
Arbizu

Firmado digitalmente  
por Haroldo Rafael  
Cancinos Arbizu  
Fecha: 2022.09.13  
20:32:15 -06'00'

40  
40

Carné	Nombre
1293-17-646	Bryan Orlando Aguirre Sagastume
1293-17-11537	Kevin Oswaldo Loarca Fuentes
1293-17-1255	Ricardo Alejandro Pérez Rodríguez
1293-17-6119	André Alessandro Espinoza Barrientos
1293-07-1719	Cristian Elí del Cid Rodríguez

Guatemala, 4 de septiembre del 2022

# Índice

Introducción .....	3
Resumen .....	4
Antecedentes.....	5
Justificación .....	7
Desarrollo .....	10
Modelo de negocio .....	16
Área financiera.....	17
Área mercadológica.....	20
Análisis de Situación .....	20
Público Objetivo .....	22
Estrategias .....	22
Metas de Mercadeo .....	23
Área legal.....	23
Área informática.....	29
Propuestas de mejora.....	32
Campaña Publicitaria Facebook .....	34
Conclusiones .....	36
Recomendaciones .....	37
Anexo 1 .....	38
Publicación Inicial – Campaña Facebook.....	38
Referencias Bibliográficas .....	39

## **Introducción**

Teniendo en consideración que la seguridad familiar es una de las premisas a tener en consideración al momento de seleccionar un lugar de vivienda, y considerando que en la actualidad una de las mayores problemáticas de la sociedad es poder proveer dicha seguridad debido a los numerosos riesgos provenientes de una amplia variedad de fuentes se concluye que de forma individual o familiar dicha seguridad debe ser afianzada por los medios necesarios. Ante estas circunstancias es imprescindible que las organizaciones y comités residenciales realicen una evaluación de los riesgos asociados y establezca la estrategias y controles necesarios para ofrecer una permanente protección y salvaguarda de la familia y sus integrantes dentro de sus hogares.

El presente trabajo presenta un estudio, análisis y puesta en práctica de las principales tecnologías de seguridad perimetral, para lo cual se evaluaran conceptos y características relacionadas con la seguridad perimetral apoyada por inteligencia artificial que permite un total control de los ingresos y egresos dentro de la zona residencial, teniendo en consideración las principales amenazas, vulnerabilidades y necesidades que proporcionan un entorno dinámico, operable y a la vez satisfacen las necesidades tanto del residente como del visitante.

Se proporcionará el diseño del sistema de seguridad perimetral, considerando tecnologías emergentes eficientes que se ajustan al requerimiento y objetivos de seguridad de cada condominio.

## **Resumen**

La solución se basa en un sitio web para un lugar de vivienda que cuenta con las siguientes opciones y características a su disposición:

Hasta el momento se tienen contemplados cuatro roles, el administrador, residente, tesorero y agente de seguridad; cada uno de estos cuenta con diferentes características disponibles para que puedan desempeñar su trabajo. El agente de seguridad puede ver el registro de visitas realizado por los residentes para tener un historial, pero además el sistema cuenta con conectividad entre las cámaras de vigilancia y la talanquera para que de este modo cuando un residente llegue a la entrada la cámara envíe la imagen de la placa al sistema para compararla con el registro de visitas y si esta se encuentra registrada entre el horario asignado abrirá automáticamente para la visita. En caso de que no esté registrado el agente de seguridad podría dar el visto bueno al visitante en ciertas ocasiones establecidas. Además, si se tiene habilitada la opción el sistema asignará automáticamente un número de parqueo al visitante.

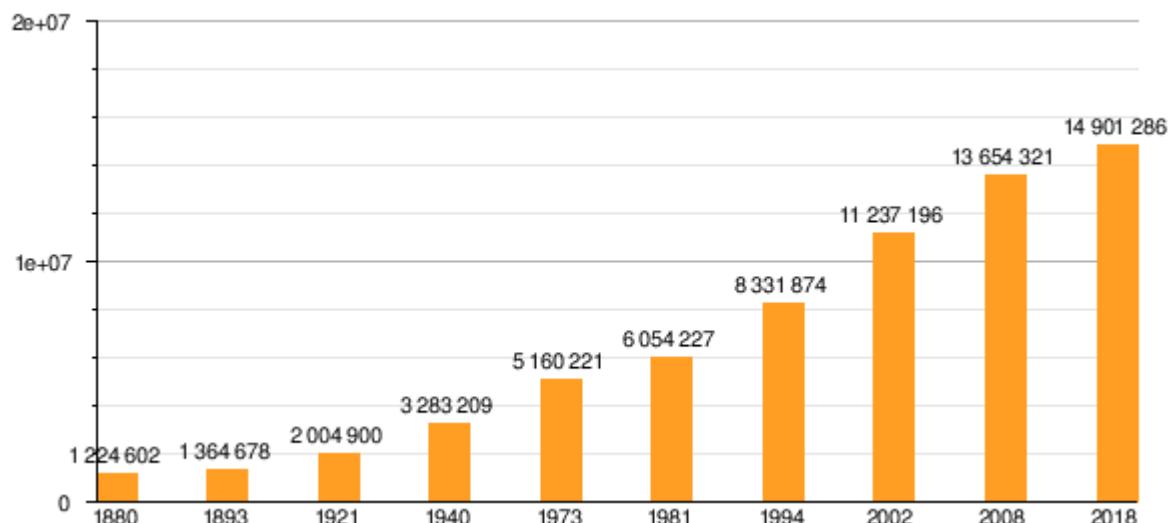
El tesorero tiene la opción de ver el historial de pagos realizados por todos los residentes e imprimir distintos reportes de estos para presentarlos a la Junta Directiva u otro uso parecido. El rol de residente cuenta con la opción de registrar las visitas, proveyendo información acerca de la misma como el nombre, apellido, DPI, horario estimado de entrada y las placas para que el sistema lo pueda ingresar automáticamente y solicitar permisos de ingreso a las áreas recreativas que lo necesiten. También cuenta con la opción de ver el apartado de anuncios que se publican para poder estar enterado de ellos y tiene la posibilidad de crear un nuevo anuncio que deseé transmitir a los demás residentes. Además, cuenta la opción de visualizar el historial de pagos y sus pagos pendientes.

Por último, el administrador es el super usuario que gestiona el sistema, este tiene mantenimiento de pagos, la gestión de la parte de anuncios, mantenimiento de las áreas recreativas que necesiten la solicitud de un permiso para el ingreso, administración de permisos de los distintos roles, la configuración general del sistema para que este se pueda ajustar y sea lo más personal para cada lugar de vivienda, visualizar y generar todos los reportes disponibles y la gestión de todos los usuarios.

## Antecedentes

El crecimiento poblacional en Guatemala y en todo el mundo se ve de manera exponencial por lo que la creación de nuevas viviendas es fundamental hoy en día, esto se comprueba la figura 1 que se encuentra más adelante en donde se puede observar claramente el aumento de la población que vive actualmente en Guatemala con respecto a años anteriores, y con esto se puede plantear el aumento de las diferentes construcciones de estructuras grandes habitacionales, es decir condominios, residenciales, edificios residenciales y toda aquella estructura en la que cuyo objetivo es proveer una vivienda a las personas y con beneficios para los mismos, debido a la alza de la necesidad de viviendas en Guatemala.

**Figura 1. Evolución Demográfica**



*Ilustración 1 - Elaboración Propia*

Con el aumento de la población también han aumentado el número de actos delictivos, de acuerdo con la siguiente cita de un artículo de prensa libre (Solorzano, 2022) “De acuerdo con las estadísticas del Cien las extorsiones registran un incremento desde noviembre del año pasado y se mantiene una tendencia al alza.” Dentro de este artículo menciona que en base a las estadísticas de la entidad Cien han demostrado que las extorsiones han aumentado, y que apenas solo un tercio son denunciadas, por lo que se espera que aumenten más las denuncias y el número de afectados sea aún mayor, además dentro del mismo artículo se especifica que no solo las extorsiones han aumentado, también homicidios, lesionados, violaciones, secuestros, extorsiones, robo de vehículos y asaltos en viviendas.

Otro claro ejemplo del aumento de actos delictivos se encuentra en la siguiente cita de la sección internacional de la sociedad de Suiza (SWI, 2022) “Las extorsiones en Guatemala aumentaron un 22 % en enero de 2022 en comparación con el último mes de 2021, según informó este miércoles una organización no gubernamental”. Claramente se ve un aumento de actos delictivos en Guatemala a pesar que aumente dependiendo de las temporadas del año pero estos actos son persistentes año con año dentro del territorio guatemalteco, por lo tanto muchas personas que tienen la oportunidad de vivir en un lugar que se encuentre con muro perimetral o que posee algún medio más de seguridad para vivir tranquilamente lo hará, con la finalidad de resguardarse de estos actos delictivos, proteger a su familia y salir enfrente de su caso sin miedo a que suceda algún hecho delictivo.

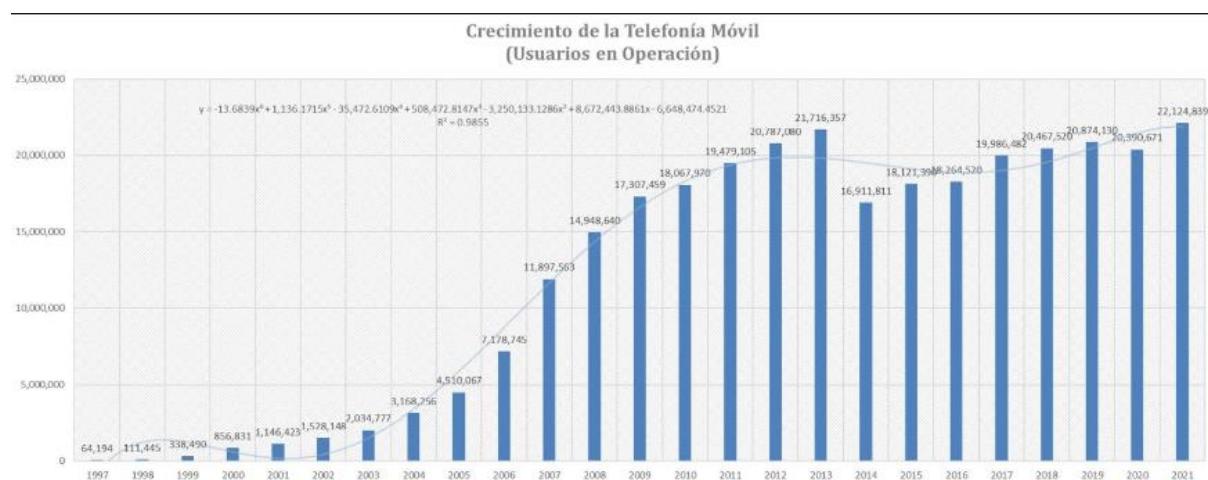
De acuerdo a lo anterior, en donde plantea el crecimiento de la población y el crecimiento de los actos delictivos en diferentes zonas de Guatemala han llevado a los guatemaltecos en busca de dichas viviendas protegidas por muros perimetrales, servicios de seguridad, garitas, controles avanzados para gestiones de ingresos y muchas cosas más, sin embargo no toda persona puede darse la oportunidad de vivir en residenciales de alta calidad con seguridad avanzada dentro de este tipo de estructuras residenciales por lo tanto una buena parte vive en residenciales con mínima seguridad, e incluso se ha dado lugar a la organización de vecinos en donde cierran calles, entradas vehiculares y peatonales, tratando de crear un espacio seguro en donde puedan vivir, por lo tanto este tipo de estructuras residenciales no tienen la capacidad de implementar tecnología sofisticada en seguridad y solo se quedan con garita y algunos guardias que rodean la zona protegida.

## Justificación

La tecnología cada día avanza más, se desarrolla con mucha más facilidad proporcionando a toda la humanidad lo suficiente para poder estar interconectado mediante el internet, a pesar de esto no se logra obtener un buen provecho de estas oportunidades y únicamente se utilizan como medios de entretenimiento y comunicación en la mayoría de los casos.

En la siguiente figura 2, se visualiza el crecimiento del uso de la telefonía móvil, desde el año 1997 al 2021, de esta grafica se puede dar a entender el uso y el crecimiento de los nuevos teléfonos celulares de hoy en día dentro del territorio guatemalteco, y ahora debido a la pandemia se puede entender que todas estas personas que cuentan con un teléfono celular inteligente tienen acceso al internet.

**Figura 2. Crecimiento de la Telefonía Móvil**



*Ilustración 2 - Mesa Editorial 12 abril 2022 (Dinero.hn)*

En la siguiente figura 3, se visualiza desde el año 2012 hasta el 2022 el crecimiento del número de los usuarios nuevos en internet y el porcentaje que ha aumentado año con año, de esta manera confirmamos que con el aumento de los celulares también ha aumentado los usuarios en internet dentro del territorio guatemalteco, y más ahora que pasamos por una dura temporada de una pandemia con más razón los guatemaltecos han tenido acceso a internet.

**Figura 3. Número de usuarios de internet**

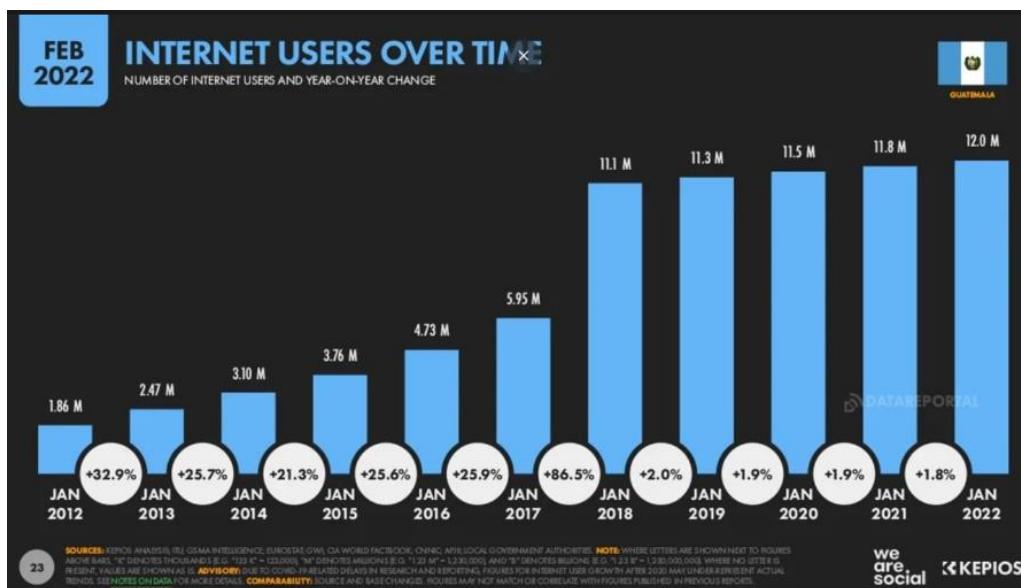


Ilustración 3 - Yi Min Shum 17 abril 2022 (Situación digital, Internet y redes sociales Guatemala 2022)

En la siguiente figura 4, están porcentajes de los diferentes dispositivos que acceden al internet dentro del territorio guatemalteco, se aprecia que el dispositivo más predominante es el teléfono móvil, seguido por las computadoras, tabletas y consolas, se puede entender que el mayor flujo de acceso al internet proviene de los celulares y claro la mayoría de las personas que poseen un celular de seguro acceden con él al internet a consultar sus redes sociales.

**Figura 4. Porcentaje de dispositivos que consumen internet**

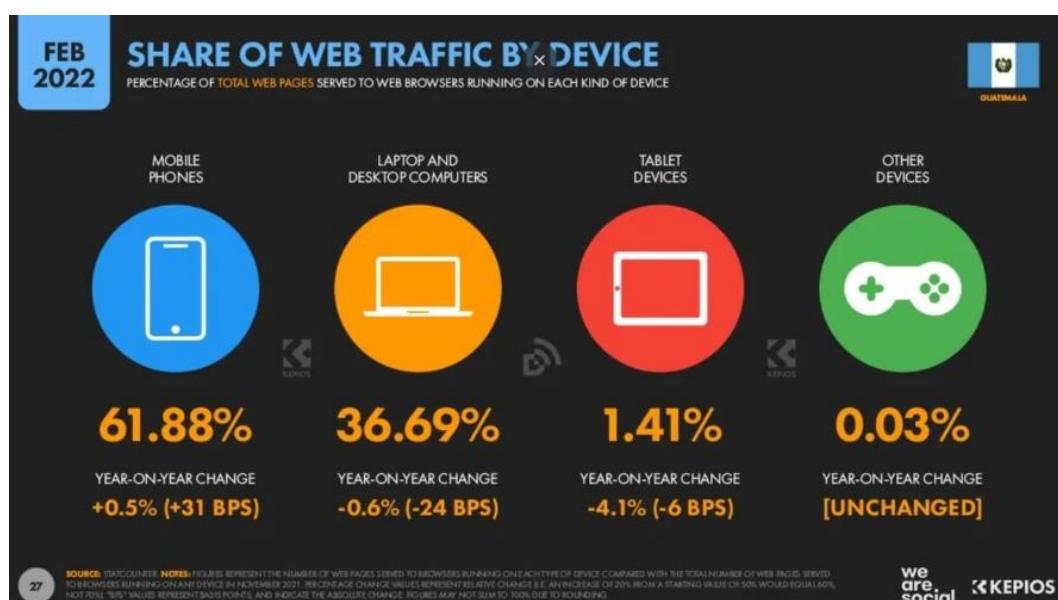


Ilustración 4 - Yi Min Shum 17 abril 2022 (Situación digital, Internet y redes sociales Guatemala 2022)

Basado en el figura 1 y en las citas citadas en antecedentes podemos concluir que el crecimiento de la población guatemalteca es inevitable por lo que se crean más viviendas, debido a esto también la delincuencia ha crecido, habiendo aumentos de actos delictivos como robo, extorsiones, violaciones, otros, dando mucho temor hacia los ciudadanos guatemaltecos, dando la oportunidad al negocio inmobiliario de poder crear estructuras residenciales ya sea verticales o horizontales e inclusive en otros casos la creación de espacios seguros por asociaciones de vecinos, todo esto para poder solventar esa falta de sensación de seguridad que muchos guatemaltecos buscan hoy en día.

A pesar del crecimiento de estas estructuras la mayoría de las familias no logran alcanzar a vivir en residenciales que contengan una muy buena seguridad, que gocen de tecnología de punta para poder cuidarse de los delincuentes y que sean de una gran utilidad, si no que deben de conformarse con el típico sistema de seguridad de cámaras y guardias de seguridad, que únicamente se encuentran en la garita y otros dando rondas dentro del área que protegen, por lo tanto no existe alguna otra herramienta que ayude a estos sistemas.

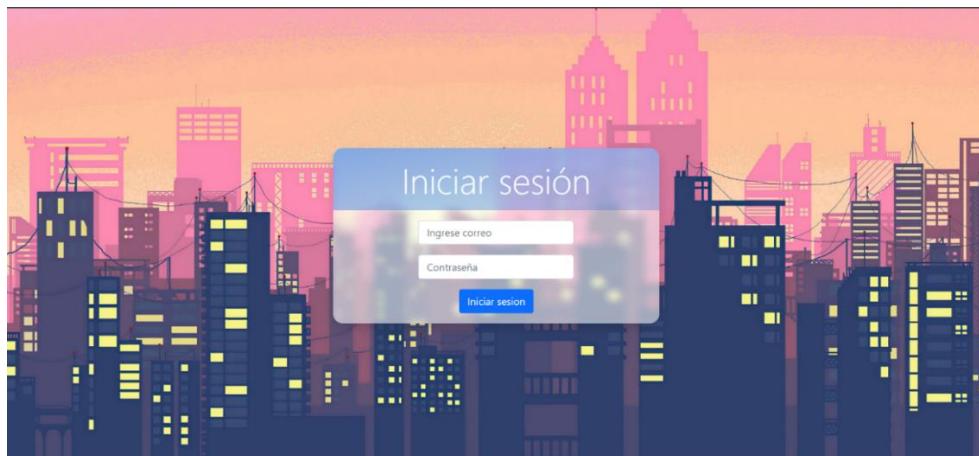
Basados en la figura 2 a la 4, y lo antes descrito se puede plantear que la mayoría de las personas tienen un teléfono móvil o alguna computadora, estos mismo con acceso a internet y lo pueden utilizar todo el día, por lo tanto, si existiera alguna aplicación que sea de utilidad como complemento de estos sistemas de seguridad comunes, puede resultar una gran ventaja para proveer de protección hacia sus residentes, proveyendo de múltiples servicios y funciones, de esta manera se podrá mantener estricto control en las garitas y tener más beneficios, tales como: control de visitas, registros automático de visitas, control de pagos, creación de citas para áreas verdes, balance de gastos del residencial, área de noticias, alertas de pagos, alertas de incidentes dentro del residencial y varias cosas más, esto basado en la idea que existe una aplicación web al alcance de todos, que sea de fácil uso y que tenga un versión móvil para que todo el mundo la pueda utilizar desde el alcance de su mano, de esta manera este sistema común de seguridad puede tener una gran mejora y tener un control más estricto y con mayor capacidad de respuesta hacia incidentes dentro del residencial

## Desarrollo

Por parte del desarrollo en este caso se visualizarán algunas de las pantallas más importantes del sistema en cual se podrá observar los diferentes datos que muestra, los diferentes visualizaciones o usuarios que existen y los informes que se pueden generar en el sistema, este sistema podrá modificarse dependiendo también de las necesidades de los diferentes clientes que necesiten el sistema añadiendo que este posee compatibilidad con operativos móviles.

se puede visualizar la pantalla del prototipo de cómo se integra el inicio de sesión, en donde el usuario con su correo y contraseña puede acceder al aplicativo, es la única página pública para todos los usuarios entre ellos residentes, tesorero y guardia.

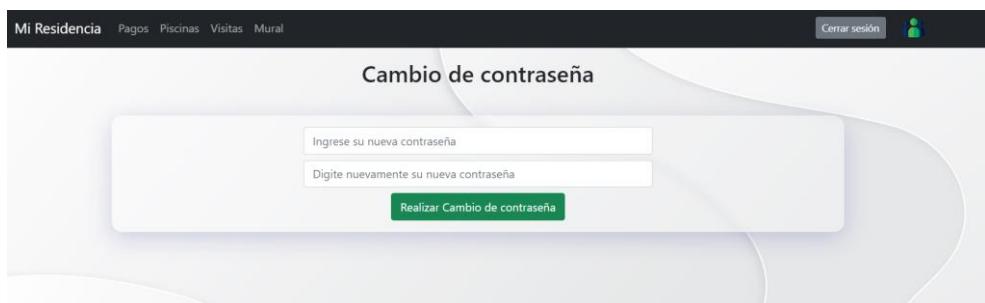
**Figura 5. Inicio de sesión**



*Ilustración 5 - Elaboración Propia*

Cada uno de los usuarios tiene la opción de poder cambiar su contraseña ya que al inicio del usuario se le proporciona una temporal.

**Figura 6. Cambio de contraseña**



*Ilustración 6 - Elaboración Propia*

**Figura 6. Cambio de contraseña (Elaboración propia).**

En la siguiente imagen se puede visualizar la vista de los residentes en ella puede observar el estado de pago que se encuentra si falta de pago o se encuentra solvente, los meses de pago y el historial de pagos que ha realizado el residente.

**Figura 7. Historial de pagos de cuota de mantenimiento**

The screenshot shows a user interface for managing maintenance payments. At the top, there is a navigation bar with links: Mi Residencia, Pagos, Piscinas, Visitas, Mural, Cerrar sesión (Logout), and a user icon. Below the navigation, two large boxes display the current status: "Estado: Falta pago" (Status: Outstanding payment) and "Meses: 7" (Months: 7). A central section titled "Historial de pagos" (Payment History) contains a table with the following data:

Fecha de pago	Mes pagado
13/01/2022	2/2022
13/01/2022	1/2022
13/01/2022	12/2021
13/01/2022	11/2021
10/11/2021	10/2021

At the bottom of the history table is a blue button labeled "Ver más..." (View more...).

*Ilustración 7 - Elaboración Propia*

Además, en dado caso la empresa o residencia lo solicite se puede habilitar el apartado de reservación de áreas recreativas las cuales indicaran el día que desean reservar el área para poder apartarlo.

**Figura 8. Reservación de áreas**

The screenshot shows a user interface for managing area reservations. At the top, there is a navigation bar with links: Mi Residencia, Pagos, Piscinas, Visitas, Mural, Cerrar sesión (Logout), and a user icon. Below the navigation, a section titled "Reservación en área de piscina" (Reservation in pool area) includes a date input field set to "03/09/2022" and a "Reservar" (Reserve) button. A message below the input field states: "Por favor no elimine el registro el mismo día de la reservacion, estaría perdiendo su reservación" (Please do not delete the registration on the same day of the reservation, you would be losing your reservation). A table lists five reservation entries:

#	Fecha	Estado	Eliminar
1	2022-09-04	Activo	X
2	2022-09-03	Activo	X
3	2022-08-28	Activo	X
4	2022-01-15	Activo	X
5	2022-01-14	Activo	X

*Ilustración 8 - Elaboración Propia*

Frecuentes es de acceso rápido es decir se guarda dentro de select.

**Figura 9. Registro de visita**

Mi Residencia Pagos Piscinas Visitas Mural Cerrar sesión

Visitas

Visitas frecuentes

Nueva visita

Historial de visitas

*Ilustración 9 - Elaboración Propia*

En la siguiente imagen se puede visualizar la vista del lado del guardia de seguridad el cual el podrá visualizar los tickets de visitas del día en cual nos muestra información del nombre del visitante, tipo de entrada y posible hora de ingreso.

**Figura 10. Visualización de visitas en el día**

Mi Residencia Visitantes Historial de visitas Cerrar sesión

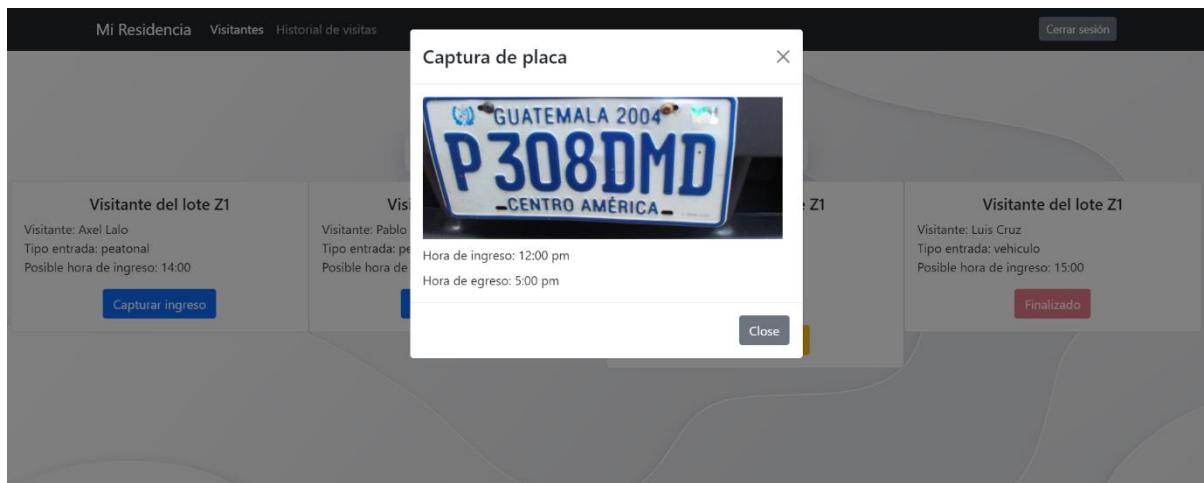
Visitantes del dia

Digite lote a buscar

*Ilustración 10 - Elaboración Propia*

Al momento que el visitante ingrese de manera vehicular este gracias a las cámaras que se implementan este tomara captura de la placa del vehículo el cual ingreso y este se almacenara en el sistema con él información de la placa.

**Figura 11. Registro de ingreso**



*Ilustración 11 - Elaboración Propia*

Además, del registro y el monitorio de las entradas de las visitas el usuario de guarda podrá tener el historial de visitas y podrá realizarlo en dos opciones mostrar las visitas del día o por un rango el cual el usuario tendrá que colocarlo.

**Figura 12. Historial de visitas**

#	Lote	Visitante	Fecha	Tipo de ingreso
1	A1	Ricardo Perez	2022-08-28	vehiculo
2	A1	Miguel	2022-08-28	vehiculo
3	A1	Miguel	2022-08-28	vehiculo
4	A1	Ricardo Perez	2022-08-28	vehiculo
5	A1	Miguel	2022-08-28	vehiculo
6	A1	Ricardo Perez	2022-08-28	vehiculo
7	A1	Wallter	2022-08-29	vehiculo
8	A1	Wallter	2022-08-29	vehiculo

*Ilustración 12 - Elaboración Propia*

El usuario guarda puede descargar un reporte de visitas descargado, el botón se encuentra al final el cual descargará un Excel en el cual se podrá visualizar el listado de información que está en la base de datos.

**Figura 13. Exportación de datos**

Lote	Visitante	Fecha	Tipo de ingreso
1 A1	Ricardo Perez	28/8/2022	vehículo
2 A1	Miguel	28/8/2022	vehículo
3 A1	Miguel	28/8/2022	vehículo
4 A1	Ricardo Perez	28/8/2022	vehículo
5 A1	Miguel	28/8/2022	vehículo
6 A1	Ricardo Perez	28/8/2022	vehículo
7 A1	Walter	29/8/2022	vehículo
8 A1	Walter	29/8/2022	vehículo
9 Z1	Campero	29/8/2022	vehículo
10 Z1	macdonalds	29/8/2022	vehículo
11 Z1	pizza hut	29/8/2022	vehículo
12 Z1	Luis Cruz	31/8/2022	vehículo
13 Z1	Pablo Ruiz	31/8/2022	peatonal
14 Z1	Axel Lalo	31/8/2022	peatonal
15 Z1	Kevin Paz	31/8/2022	peatonal

*Ilustración 13 - Elaboración Propia*

En la parte de vista de Tesorero este posee más opciones para poder visualizar entre ellos generar los pagos del día o en rango, visualizar por manzana o sector (Dependerá de la solicitud de la residencial) y el lote en específico.

**Figura 14. Control de cobros y gastos**

#	Fecha de pago	Lote	Mes Pagado	Accion
1	2022-08-29	A3	2021-05-20	pago
2	2022-08-29	A3	2021-10-20	pago
3	2022-08-29	A3	2022-02-20	pago
4	2022-08-29	A3	2021-03-20	pago
5	2022-08-29	A3	2022-05-20	pago
6	2022-08-29	A3	2021-07-20	pago
7	2022-08-29	A3	2021-11-20	pago
8	2022-08-29	A3	2021-04-20	pago
9	2022-08-29	A3	2022-03-20	pago
10	2022-08-29	A3	2022-07-20	pago

*Ilustración 14 - Elaboración Propia*

En el apartado de estado general se puede visualizar las diferentes manzanas o sectores y los lotes con sus respectivos pagos si el lote aún debe este aparecerá en la visualización.

**Figura 15. Estado de pagos de mantenimiento**

A	B	C	D	E	F	G	H	I	J	K	L
A1 Debe: 7		C42 Debe: 19									
A2 Al dia											
A3 Debe: 1											
A4 Debe: 21											
A5 Debe: 20											
A6 Debe: 21											
A7 Debe: 21											
A8 Debe: 21											
A9 Debe: 21		C43 Debe: 21									

*Ilustración 15 - Elaboración Propia*

En el aparato de manzana podemos buscar el historial específicamente por manzana el sistema solo le solicitará la fecha en específico o si en dado caso selecciona el rango tendrá que colocar los rangos para la búsqueda y colocar la manzana la cual desean visualizar el historial.

**Figura 16. Visualización de pagos**

#	Fecha de pago	Lote	Mes Pagado	Acción
1	2022-08-28	A2	2022-07-20	pago
2	2022-08-28	A2	2022-02-20	pago
3	2022-08-28	A2	2022-05-20	pago
4	2022-08-28	A2	2022-04-20	pago
5	2022-08-28	A2	2022-06-20	pago
6	2022-08-28	A2	2022-08-20	pago
7	2022-08-28	A2	2022-09-20	pago
8	2022-08-28	A2	2022-03-20	pago
9	2022-08-29	A3	2021-05-20	pago

*Ilustración 16 - Elaboración Propia*

Por último, la opción de realizar reportes también lo puede realizar el usuario tesorero de igual manera que el usuario guarda que lo descargara en formato Excel.

**Figura 17. Exportación de datos**

#	Fecha de pago	Lote	Mes Pagado	Acción
1	28/8/2022	A2	20/7/2022	pago
2	28/8/2022	A2	20/2/2022	pago
3	28/8/2022	A2	20/5/2022	pago
4	28/8/2022	A2	20/4/2022	pago
5	28/8/2022	A2	20/6/2022	pago
6	28/8/2022	A2	20/8/2022	pago
7	28/8/2022	A2	20/9/2022	pago
8	28/8/2022	A2	20/3/2022	pago
9	29/8/2022	A3	20/5/2021	pago
10	29/8/2022	A3	20/10/2021	pago
11	29/8/2022	A3	20/1/2022	pago
12	29/8/2022	A3	20/3/2021	pago
13	29/8/2022	A3	20/5/2022	pago
14	29/8/2022	A3	20/7/2021	pago
15	29/8/2022	A3	20/11/2021	pago
16	29/8/2022	A3	20/4/2021	pago
17	29/8/2022	A3	20/3/2022	pago
18	29/8/2022	A3	20/7/2022	pago
19	29/8/2022	A3	20/2/2021	pago
20	29/8/2022	A3	20/9/2021	pago
21	29/8/2022	A3	20/12/2021	pago
22	29/8/2022	A3	20/8/2021	pago
23	29/8/2022	A3	20/1/2022	pago
24	29/8/2022	A3	20/6/2022	pago
25	29/8/2022	A3	20/6/2021	pago
26	29/8/2022	A3	20/4/2022	pago
27	29/8/2022	A3		

*Ilustración 17 - Elaboración Propia*

Finalmente cabe aclarar que todas las páginas mostradas tienen versión móvil, es decir que es responsive dependiendo del dispositivo y en ese documento únicamente se detallaron las más importantes.

### Modelo de negocio

Para poder alcanzar una mejor comprensión de lo que el modelo de negocio es, se procederá con una definición formal. Se puede describir el término “Modelo” como la representación de un objeto con una descripción simple, la cual puede utilizarse para efectuar cálculos; por otra parte “Negocio” es la actividad de compra y venta de bienes y/o servicios que permite la generación de ingresos. Como resultado de la combinación de estos conceptos puede definirse que el modelo de negocio es la representación de como una organización compra y/o vende bienes y/o servicios y gana dinero por ello. (Osterwalder, 2004)

Teniendo una definición más clara del concepto de modelo de negocio. Se puede inferir que el modelo de negocio es de cebo y anzuelo. El cebo de este modelo y para este emprendimiento se refiere a ofrecer una parte del producto a bajo coste con el fin de poder promover los servicios modulares de la aplicación y lograr una rentabilidad mayor de los beneficios adicionales del servicio.

**Figura 18. Modelo de negocio**



Ilustración 18 - Elaboración Propia

### Área financiera

Para la parte financiera la realización de los costos se planteó los diferentes gastos que se realizaran en la elaboración del sistema en cual permita el ingreso de los diferentes datos para el ingreso de visitas en las empresas que lo solicitan, para ellos nos enfocamos en los costos de programación el cual este depende del nivel de complejidad en este caso se realizado para una página web hecha con React, JavaScript, Bootstrap y Firebase con una base de datos noSQL anexando a eso está incluido las horas hombre las cuales el equipo de desarrollo está integrado por 1 Administrador de proyecto y varios Desarrolladores el cual se detallan en la tabla de presupuesto.

Además del costo de programación agregamos a los costos el proceso de integración a la empresa, esto quiere decir en dado caso la empresa que solicite el

sistema ya posee un sistema dentro se realizará la migración de los datos que posee en su empresa a nuestro sistema así poder integrar toda la información que contenga dicha empresa, este costo dependerá de varios aspectos, la magnitud de los datos que poseen, el orden en el cual estás los datos y la migración hacia nuestra nueva base.

Sobre la base de datos este está agregado en el costo general de la base el cual se está utilizando Firebase y el costo dependerá ya que Firebase posee productos estandarizados y además productos para poder modificar de acuerdo a la necesidad que se desea en este caso este dependerá la empresa la cual se implementará el sistema el cual en el alojamiento de la base de datos estará la autenticación, cloud firestone, cloud functions y el hosting el cual este puede rondar entre los trescientos dólares hasta los dos mil dólares.

Con respecto a los demás apartados los cuales son Análisis & diseño, pruebas y capacitaciones dependerá las necesidades de la empresa ya que en dado caso las empresas necesitan realizar modificaciones o ampliaciones de información este llevará un proceso de análisis y diseño para que el sistema que se esté entregando sea de alta calidad y realice correctamente el trabajo solicitado para ellos también estará involucrado el apartado de pruebas y capacitación ya que cada usuario el cual manejará el sistema tendrá una capacitación para poder realizar el buen uso del sistema.

Como pudimos ver anteriormente el sistema cuenta con el registro de las placas vehiculares por medio de cámaras inteligentes las cuales tendrán un costo dependiente de la cantidad de cámaras que desea el cliente, añadiendo el costo de la talanquera o plumilla la cual están sincronizada con el ingreso de la información en el sistema como del monitoreo de las cámaras que estarán en los puntos estratégicos de los clientes.

Todo esto mencionado anteriormente está estipulado en una tabla el cual se encuentran los costos sobre la realización del sistema y el costo del mantenimiento de nuestra empresa tomando en cuenta los diferentes salarios y el mobiliario que se estaría utilizando:

**Tabla 1. Presupuesto**

#EDT	# Activ.	Concepto	Cantidad	Unidad	Precio unit.	Total	
1	Desarrollo de Software	DBA-backend	480	Horas Hombre	Q 55.00	Q 26,400.00	
		Diseñador UI	336	Horas Hombre	Q 50.00	Q 16,800.00	
		Frontend developer	704	Horas Hombre	Q 55.00	Q 38,720.00	
		Frontend developer	704	Horas Hombre	Q 55.00	Q 38,720.00	
		Tester	950	Horas Hombre	Q 40.00	Q 38,000.00	
		Encargada de publicidad	950	Horas Hombre	Q 35.00	Q 33,250.00	
						<i>Subtotal/</i> Q 191,890.00	
2	Compras Mobiliario y Equipo	Computadora para administracion	3	Recursos Tecnologí	Q 3,000.00	Q 9,000.00	
		Computadora para desarrollo	5	Recursos Tecnologí	Q 4,000.00	Q 20,000.00	
		Monitores	12	Recursos Tecnologí	Q 2,000.00	Q 24,000.00	
		Hub multiport	8	Recursos Tecnologí	Q 150.00	Q 1,200.00	
		Licencias de software(Windows, antivirus y office)	8	Recursos Tecnologí	Q 100.00	Q 800.00	
		Monitores	4	Recursos Tecnologí	Q 500.00	Q 2,000.00	
		Material de oficina	5	Recursos de oficina	Q 100.00	Q 500.00	
						<i>Subtotal/</i> Q 57,500.00	
4	Servicios	Internet		Meses de servicio	Q 400.00	Q -	
		Luz	5	Meses de servicio	Q 300.00	Q 1,500.00	
		Pago de alquiler de oficina amueblada	5	Meses de servicio	Q 3,000.00	Q 15,000.00	
		Pago servicios publicos (agua, limpieza, etc)	5	Meses de servicio	Q 200.00	Q 1,000.00	
						<i>Subtotal/</i> Q 17,500.00	
						<i>Subtotal/</i> Q 266,890.00	
		N/A	Reserva para contingencias	0.1		Q 1,750.00	
		N/A	Costos indirectos	0.05		Q 875.00	
						<b>TOTAL</b> Q 269,515.00	

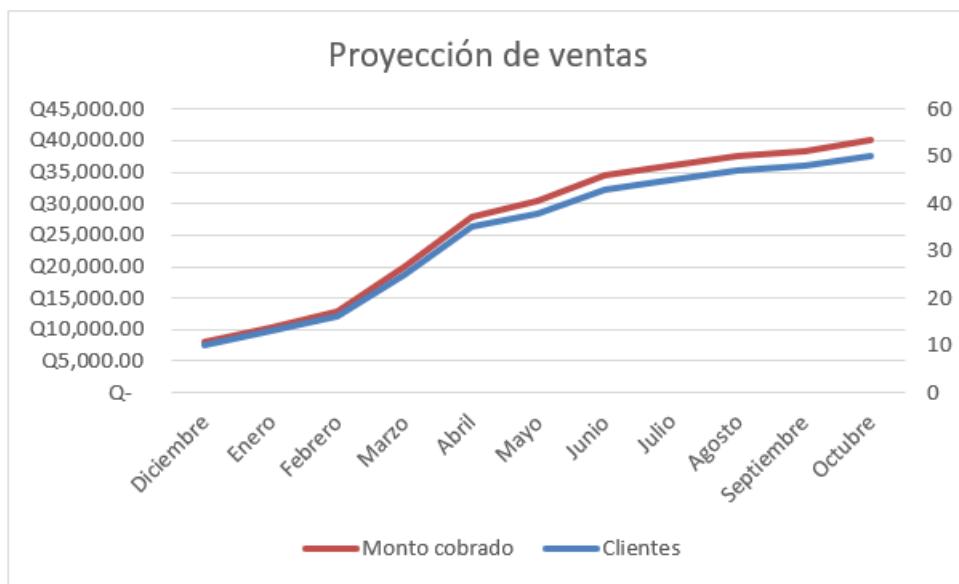
*Tabla 1 - Elaboración Propia*

Como nos podemos dar cuenta en la tabla superior nos indica los diferentes costos estos añadiendo las horas hombre de implementación e integración del sistema logrando así poseer ingresos el cual pueden costear los gastos y poseer ganancias dependiendo las necesidades de las empresas está planeado poseer ganancias de 50% al 75% del producto.

Además de ello se posee contemplado un porcentaje de reserva por contingencia en dado caso suceda un riesgo dentro de la empresa poseemos ese porcentaje el cual se realizó un estudio para evaluar dicho porcentaje y también se posee un porcentaje de los costos indirectos que puede tener la empresa, raspberry pi y talanquera, eso es un costo adicional que la empresa debe de pagar dependiendo de sus activos, pues ya pueden poseer de estos dispositivos en sus garitas, sin embargo los costos aproximadamente son: mil quetzales de la raspberry pi y 600 de la cámara, con el servicio de la talanquera deberá de ser contratada por otra empresa.

De acuerdo con el precio de venta establecido de un costo de 800 quetzales, se prevé las siguientes ventas en la figura 19, siendo la línea roja la cantidad de dinero a recibir por mes y la línea azul la cantidad de clientes que se proyectan tener.

**Figura 19. Proyección de ventas**



*Ilustración 19 – proyección de ventas*

De acuerdo con esta proyección se espera lograr obtener la inversión hasta octubre del otro año, sumando un total de Q. 296,000.00 que es más de lo invertido para la creación de dicho software.

Finalmente se debe de recalcar que el precio de venta es de 800 quetzales mensuales, gracias a la base de datos utilizada de los proveedores de Firebase, se tiene buen margen de uso gratuito, si este se llegará a pasar de estos datos gratuitos pues queda a cargo del cliente pagar ese costo extra que es lo que ellos estarían utilizando demás de estos límites que impone Firebase.

## Área mercadológica

### Análisis de Situación

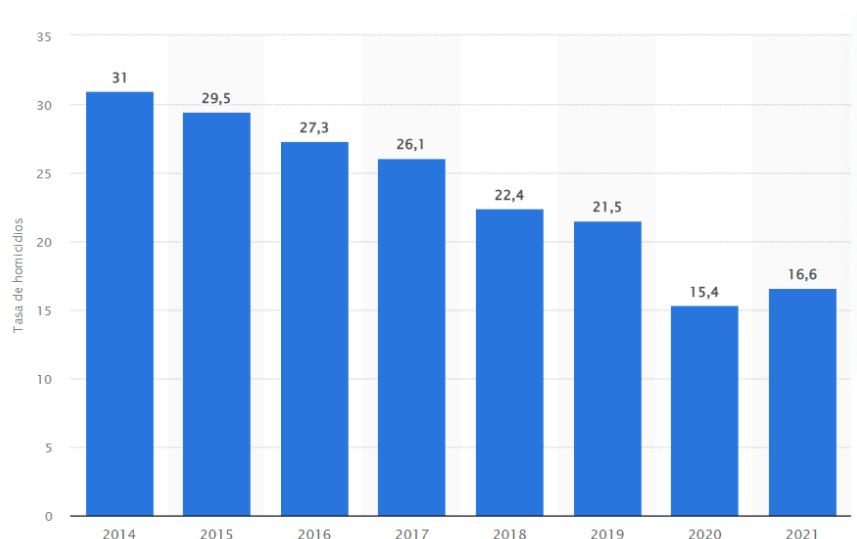
El estado actual del crecimiento exponencial de habitantes en zonas geográficas que tienen un valor estratégico independientemente de su índole atrae y justifica la inversión que muchos terceros toman en crear complejos o localidades residenciales para la venta de viviendas. Uno de los atractivos de este tipo de sitios es la seguridad, normalmente los domicilios se encuentran ubicados en una zona cercada que cuenta

un sistema de entrada y salida por garita que regula y controla el acceso de individuos al lugar.

Esto en un país como lo es Guatemala, donde la delincuencia y actos delictivos son el pan de cada día, junta las necesidades de vivienda y seguridad y hace más apetecible la idea de una inversión así de parte de cualquier persona. Como justificación a esto encontramos que el Instituto Nacional de Estadística de Guatemala en el año 2020, solo en el departamento de Guatemala, registró una cantidad de 43.2 robos y hurtos al día, si incluimos la tasa de homicidios anual, en el año 2021 se obtuvo una media de 16.6 asesinatos por cada 100,000 habitantes, cifras preocupantes para cualquier ciudadano.

Número de homicidios por cada 100,000 habitantes por año

**Figura 20. Número de homicidios**



*Ilustración 20 - Instituto Nacional de Estadística (Indicadores de Hechos Delictivos)*

Teniendo en cuenta esta necesidad y el desarrollo de varias residenciales ya no solo en la ciudad capital, sino en sitios en crecimiento, se llega a la conclusión de que estos sitios necesitan herramientas que optimizan y mejoran el control y la misma seguridad de sus residentes, por lo que se desarrolla una solución/herramienta que pueda cumplir con las necesidades requeridas por la administración de lugares con estos conceptos.

## **Público Objetivo**

La segmentación del público objetivo es fácil de comprender, todos los lugares residenciales o condominios que buscan maneras de ofrecer la mayor seguridad a sus habitantes y que facilite la administración y control del lugar. La herramienta que se ofrece se orienta a la facilitación de diferentes aspectos que pueden contar o no los condominios, además que ofrece un plus a los residentes del lugar que pueden encontrar atractivo este tipo de servicios que son en su beneficio.

Puede que por lo mismo de contar con público objetivo tan específico sea fácil pensar en que no es tan rentable el ofrecer este tipo de producto, pero como fue explicado en el análisis, este tipo de lugares seguirán apareciendo con el tiempo, convirtiéndose en posibles clientes y se cuenta con la ventaja de que las residenciales son lugares pensando para toda una o varias vidas, en cuestión de tiempo, por lo que un solo cliente sería el equivalente a ingresos fijos por un lapso de tiempo prolongado en un caso donde no ocurra nada fuera de lo normal, apostando así, más que por la cantidad de clientes, el tiempo que estos requerirán y usaran el producto.

## **Estrategias**

Se cuenta con dos estrategias principales a la hora de demostrar a los clientes porqué la solución presentada es para ella. La primera es que la herramienta misma se puede ajustar a las necesidades de las residenciales, trabajando por ‘módulos’ que no son más que diferentes opciones que se pueden habilitar y deshabilitar en los diferentes lugares donde esta sea aplicada. Esto funciona como una prueba de que se comprende lo que el cliente quiere y necesita y que no va a tener que pagar por algo de lo cual no va a hacer uso, llegando así a un precio justo. Además, el implementar una solicitud de un cliente en específico funciona como una manera de crear una nueva opción que puede ser demostrada a otros clientes, ya sean potenciales o existentes.

Y la segunda es como se ofrece el producto, es decir, para obtener la herramienta desarrollada, no es necesario que un cliente desembolse una gran cantidad en un solo pago, sino que se ofrecen diferentes tiempos donde se da una licencia para que puedan usar el producto. Esto nos da dos grandes ventajas a la hora de vender.

- El cliente puede optar por adquirir la licencia de menor costo que se ajuste a sus requerimientos, esto sirve como un periodo de tiempo donde la

herramienta será usada como una ‘prueba’ según el cliente, es la entrada principal para que el cliente despeje sus dudas y no sienta que arriesga mucho al implementar una solución de este tipo. El objetivo principal es ‘engancharlo’ para que se quede.

- Se apuesta por pagos que al cliente le pueden parecer pequeños a comparación de lo que costaría comprar una herramienta así, pero sientan estos pagos por varios plazos de tiempo, que al final se van acumulando y formando una gran cantidad, así que en realidad la ganancia está en varios lugares pagando una cantidad razonable, pero por mucho tiempo.

### **Metas de Mercadeo**

Cada una de las metas a mencionar, fue analizada y creada con el fin bilateral de satisfacer a los clientes y lograr obtener beneficios para la empresa y el crecimiento del producto.

- Ganar la confianza de los clientes.
- Obtener retroalimentación constante para mejorar el desarrollo del sistema.
- Conseguir buenas referencias para adquirir más clientes.
- Ofrecer soluciones novedosas que resulten atractivas para los consumidores.
- Crear alianzas con constructoras para ser la primera y única opción.
- Demostrar los beneficios de las implementaciones realizadas para ser más atractivos en el mercado.

Estas metas establecidas a largo plazo tienen como finalidad aumentar la rentabilidad de la empresa y no quedarse estancado, sino encaminarse a la mejora continua del producto.

### **Área legal**

Debido a que debemos de guardar información personal de los residentes se toma en cuenta lo siguiente acerca de la privacidad de esta:

Se puede establecer que la “privacidad de datos” hace referencia a la reserva o confidencialidad que se debe tener a todos aquellos datos que constituyen características, particularidades y circunstancias propias de un individuo y que facilitan y permiten su individualización o identificación dentro de un grupo. Es a estos datos que se les denomina o conoce como “datos personales”. La Corte de

Constitucionalidad ha definido los “datos personales” como todos aquellos datos que permiten identificar a una persona y posibilitan la determinación de una identidad, tales como un número de identificación o elementos específicos característicos de su identidad física, fisiológica, psíquica, económica, cultural, social, etcétera.

La protección de los datos personales de la intromisión arbitraria de terceros se reconoce y protege hoy en día como un derecho fundamental, el “derecho a la protección de datos” o también como el “derecho a la autodeterminación informativa”. El reconocimiento de este derecho surgió como una necesidad de otorgar una protección jurídica a aquellos datos personales que, debido a la tecnología y a la transmisión de información a través de plataformas de comunicación masivas, son susceptibles de un uso inapropiado por parte de terceros, lo cual podría causar graves daños al titular de estos.

La protección de los datos personales, por tanto, supone no solo la protección indirecta del derecho a la privacidad, a la intimidad y al honor de las personas, sino también a la protección del derecho al reconocimiento de la dignidad humana, el cual constituye el origen y fundamento último de la protección y reconocimiento de todos los derechos humanos.

La Corte de Constitucionalidad ha establecido que en Guatemala el derecho al reconocimiento de la dignidad humana se encuentra reconocido y protegido en los primeros cinco artículos de la Constitución Política de la República:

- Artículo 1: Protección a la persona.
- Artículo 2: Deberes del Estado.
- Artículo 3: Derecho a la vida.
- Artículo 4: Libertad de igualdad.
- Artículo 5: Libertad de acción.

Respecto al reconocimiento y protección de los derechos a la intimidad y a la privacidad, la Corte ha señalado que estos se encuentran contenidos en los siguientes artículos constitucionales:

- Artículo 23: Inviolabilidad de la vivienda.
- Artículo 24: Inviolabilidad de correspondencia, documentos y libros.
- Artículo 25: Registro de personas y vehículos.

## **Contenido del derecho a la autodeterminación Informativa o derecho de protección de datos**

El ejercicio del derecho de protección de datos posibilita al individuo el control sobre sus datos personales y, por tanto, le permite comprobar, en todo momento, no solo que sus datos estén correctos y actualizados (en cualquier base de datos pública o privada), sino, además, que su utilización sea conforme a las autorizaciones que otorgó y para la finalidad previamente acordada.

Según lo considerado por la Corte de Constitucionalidad<sup>6</sup>, la plena eficacia del derecho a la autodeterminación informativa o protección de datos permite al individuo gozar, a su vez, de los siguientes derechos:

- Derecho a actualizar sus datos
- Derecho a rectificar sus datos por información errónea, incompleta o inexacta
- Derecho a reservar (confidencialidad) cierta información que sobre ella se obtenga, y que aun cuando ésta pueda ser legalmente requerida, se mantenga en grado de confidencialidad para terceras personas ajenas a la situación que motivó el requerimiento
- Derecho a excluir de circulación informativa, abierta o restringida, información que pueda considerarse en extremo sensible para el interesado o que sea producto de noticias o datos que sólo a este último conciernan (para ser admitida se deben tomar en cuenta los parámetros de trascendencia o interés sociales legítimo respecto a dichos datos).

En ese orden de ideas, en toda comercialización de datos personales se debe garantizar a la persona titular de los mismos los derechos de actualización, rectificación, confidencialidad y exclusión como una forma de resguardar, no solamente su derecho de autodeterminación informativa, sino, indirectamente, los derechos fundamentales a su intimidad personal, privacidad y honor.

## **¿Existen límites al derecho a la autodeterminación informativa o derecho de protección de datos?**

La Corte de Constitucionalidad estableció en su jurisprudencia que, como todo derecho, el derecho a la autodeterminación informativa no es absoluto. Este derecho deberá ceder ante las acciones que persigan garantizar los valores y fines supremos

del Estado (la vida, la libertad, la justicia, la seguridad, la paz y el desarrollo integral de la persona) en el entendido que estos valores constituyen un interés colectivo o general, cuyo cumplimiento o realización supera la relevancia que tiene para la sociedad mantener ciertos datos personales en reserva (el caso de una investigación delictiva, por ejemplo). En estos casos, son las siguientes autoridades estatales las que pueden requerir datos personales sin vulnerar el derecho a la autodeterminación informativa:

- Ministerio Público
- Autoridades policiales
- Autoridades judiciales
- Tribunal Supremo Electoral
- Superintendencia de Administración Tributaria

Es importante establecer que, para que el requerimiento de datos personales sea legítimo y justificado, debe realizarse solamente por autoridades de carácter estatal y los datos personales que éstas recaben deben ser utilizados únicamente para el ejercicio de las funciones propias de cada órgano público que se trate. El Registro Nacional de las Personas (RENAP) es la institución del Estado encargada de determinar qué instituciones pueden necesitar obtener este tipo de datos en cada caso concreto.

### **Datos personales que no se encuentran protegidos por el derecho a la autodeterminación informativa o derecho de protección de datos**

Los siguientes datos personales no se consideran protegidos por el derecho de protección de datos porque se consideran información pública en virtud de lo dispuesto en el artículo 6 literal j de la Ley del Registro Nacional de las Personas:

- El nombre y los apellidos de la persona
- El número de identificación
- Las fechas de nacimiento
- La fecha de defunción
- Sexo
- Vecindad

- Ocupación
- Profesión u oficio
- Nacionalidad
- Estado civil.

Respecto a la exclusión de estos datos personales del derecho a la protección de datos, la Corte de Constitucionalidad ha establecido que los mismos constituyen información que cualquier persona utiliza para identificarse públicamente en sus relaciones sociales, laborales, profesionales y de otra índole. Y que, incluso, figuran en el Documento Personal de Identificación, ya que son los datos que comúnmente permiten la identificación de la persona para el desarrollo de los actos civiles, administrativos, legales y para todos aquellos actos en los que es requisito identificarse. En ese sentido, estos datos personales no constituyen información que pueda atentar contra la intimidad o el honor del individuo, por ser datos que se utilizan comúnmente para efectos de identificación y conocimiento público. Por tanto, facilitar estos datos a personas extrañas al titular de estos, sin su conocimiento ni consentimiento, no entraña vulneración a sus derechos.

Con relación a la dirección de residencia y el número telefónico, la Corte ha considerado que sí se trata de datos personales y los mismos sí se encuentran protegidos por el derecho de protección de datos, lo cual supone, necesariamente, que su divulgación sin autorización del titular se considera una vulneración a este derecho.

### **La inexistencia de una Ley de protección de datos en Guatemala**

Hasta la fecha, no existe dentro del ordenamiento jurídico guatemalteco un cuerpo normativo que regule el tema de protección de datos personales. La Ley de Acceso a la Información Pública, Decreto número 57-2008 del Congreso de la República, contiene y establece ciertos parámetros importantes relacionados con el tema (datos personales, habeas data, información confidencial, el tratamiento y acceso a los datos personales, entre otros) pero lo hace, esencialmente, desde la perspectiva del manejo de datos personales por parte de registros públicos o estatales (registros controlados por entidades que manejan recursos o bienes del Estado o

llevan a cabo funciones públicas). Esto supone la existencia de un “vacío legal” en Guatemala en cuanto a regulación sobre el manejo de datos personales por parte de sujetos privados y, por tanto, en cuanto al derecho de protección de datos o derecho a la autodeterminación informativa en todas sus facetas, manifestaciones y alcances.

Sin embargo, es importante advertir que la Corte de Constitucionalidad ha establecido que mientras persista esta ausencia normativa, toda comercialización de datos personales que se lleve a cabo en el país, deberá cumplir con los siguientes requisitos para ser válida y legítima según los parámetros de protección de derechos fundamentales:

- En la obtención de los datos:
  - Conforme una finalidad plenamente definida.
  - De forma legítima.
  - De manera voluntaria por parte de aquél cuyos datos vayan a ser objeto de comercialización.
- En la utilización de los datos:
  - Con consentimiento de la persona interesada.
  - Con un propósito compatible con aquel para el que se obtuvieron.
- En el registro de los datos:
  - Implementación de controles adecuados que permitan la determinación de la veracidad y actualización de estos.
  - Derecho a rectificación en caso de una errónea o indebida actualización.
  - Derecho a exclusión de la información o datos que el titular considere sensibles o cuya divulgación pueda derivar en daños a su intimidad, honor o privacidad.

## **Multas**

Debido a que la solución informática planea manejar las multas consideradas por el establecimiento se debe de tomar en cuenta lo siguiente:

Estas son válidas solo si están establecidas en el Reglamento de Copropiedad de la comunidad. De esta forma, si esas multas no se encuentran establecidas en esta normativa, no sería posible aplicarlas, y si se aplican, constituyen una acción ilegal y arbitraria, razón por la cual cualquier afectado puede recurrir al Juzgado de Policía Local y reclamar la nulidad de la aplicación de la multa.

Esto, en vista de que el Reglamento de Copropiedad es el único instrumento válido para establecer las sanciones que se deben aplicar a los copropietarios, según lo establece el artículo 21 de la Ley de Copropiedad Inmobiliaria, en donde expresa: “El comité de administración podrá también dictar normas que faciliten el buen orden y administración del condominio, como asimismo imponer las multas que estuvieren contempladas en el reglamento de copropiedad”.

Además de esto el lugar de vivienda debe de dar a conocer a sus residentes el reglamento que deben de cumplir y las multas que se tendrán en caso de que no se cumplan y tener el documento de prueba de recibido.

### **¿Cómo se deben cobrar las multas?**

Así como la multa debe estar registrada en el Reglamento de Copropiedad, también es necesario que haya pruebas del hecho ocurrido. Estas pruebas pueden ser fotográficas o en video, y si hay testigos, también aportan. Luego, se debe enviar la notificación de la multa al habitante o al copropietario correspondiente, con el detalle de la situación y el monto del pago.

El pago de las multas se sumará al fondo común de reserva de la comunidad, según lo establece el artículo 7º de la Ley. En caso de que el vecino o copropietario se niegue al pago de la multa se debe presentar el caso al Juzgado de Policía Local correspondiente.

### **Área informática**

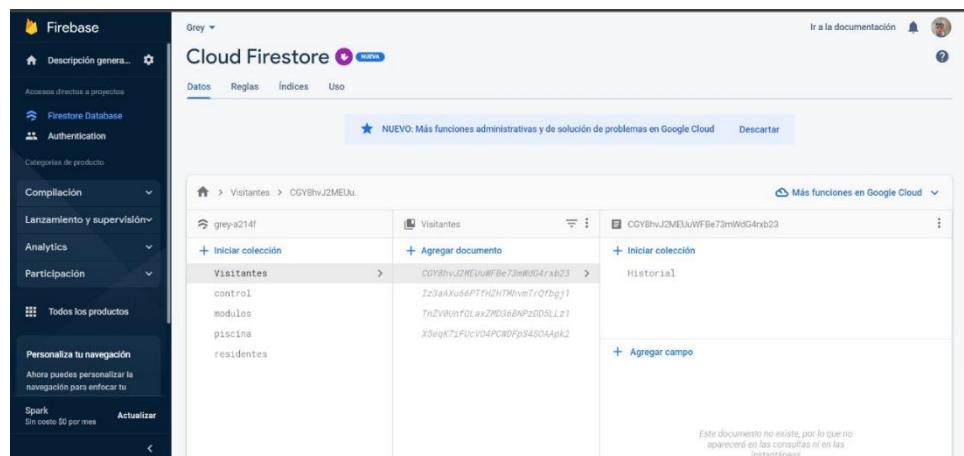
En la planeación de la herramienta se realizó un análisis de las diferentes tecnologías que se podían usar para el desarrollo e implementación de esta, los factores determinantes para la elección fueron la sostenibilidad del sistema y la evolución que este tendrá con el tiempo, así que entré las propuestas destacaron Firebase como base de datos no relacional, ReactJS para el desarrollo y Bootstrap para la maquetación. Estas tres tecnologías cuentan con una amplia documentación en internet y al ser recientes cuentan con muchos años de soporte a futuro en su merced.

#### **Firebase**

Como base de datos, se optó por una no relacional, ya que esta es más amigable al momento de realizar cambios que puedan ser significativos, esta flexibilidad es

ofrecida por firebase, que trabaja con ‘documentos’ que tienen la cantidad de propiedades como sean necesarias. Además de esto Firebase como suite ofrece mucho control sobre más aspectos importantes en cualquier aplicativo. Además de ofrecer control sobre reglas de nuestra db, se puede administrar diferentes tipos de autenticación que se pueden implementar en el sistema, y de la misma manera integrarlo con las reglas de la base de datos, mejorando así la seguridad del sistema, un factor sumamente importante para cualquier aplicación.

**Figura 21. Consola de firebase**



*Ilustración 21 - Elaboración Propia*

## ReactJS

Esta librería basada en JavaScript cuenta con la ventaja de por diseñar aplicaciones en base a componentes independientes y reutilizables, esto con la finalidad de crear interfaces más completas para el usuario. Con todas las bondades de JavaScript, React ofrece un desarrollo rápido y sostenible, que facilita el mantenimiento de una aplicación al momento de estar en producción y tener que realizar modificaciones y mejoras, ofreciendo también un excelente rendimiento. La comunidad de desarrollo que tiene a sus espaldas React, es bastante amplia, siendo desarrollada por Facebook este framework cuenta con bastante soporte, ganando así mucha popularidad recientemente.

**Figura 22. Código de la aplicación web**

```

1 import React, { Fragment, useState, useEffect } from "react";
2 import { auth } from "../fb";
3 import { withRouter } from 'react-router-dom';
4 import { Row, Col, Container, Form, Button, Alert, Spinner } from 'react-bootstrap';
5 const Inicio=(props)=>{
6   const [user, setUser] = useState('');
7   const [contra, setContra] = useState('');
8   const [contra2, setContra2] = useState('');
9   const [fallo, setFallo] = useState('');
10  const [exito, setExito]= useState(false)
11  const [procesando, setProcesando]= useState(false)
12  const borrar= ()=>{
13    setContra('')
14    setContra2('')
15  }
16  const cambioContra= ()=>{
17    setProcesando(true)
18    if (contra.trim()!=""&& contra2.trim()!="") {
19      handleShow('Ingrese los datos requeridos')
20      return;
21    }
22    if (contra==contra2) {
23      user.updatePassword(contra).then((r) => {
24        handleShow2(r)
25      })
26    }
27  }
28}
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
479
480
481
482
483
484
485
486
487
488
489
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
509
510
511
512
513
514
515
516
517
518
519
519
520
521
522
523
524
525
526
527
528
529
529
530
531
532
533
534
535
536
537
538
539
539
540
541
542
543
544
545
546
547
548
549
549
550
551
552
553
554
555
556
557
558
559
559
560
561
562
563
564
565
566
567
568
569
569
570
571
572
573
574
575
576
577
578
579
579
580
581
582
583
584
585
586
587
588
589
589
590
591
592
593
594
595
596
597
598
599
599
600
601
602
603
604
605
606
607
608
609
609
610
611
612
613
614
615
616
617
618
619
619
620
621
622
623
624
625
626
627
628
629
629
630
631
632
633
634
635
636
637
638
639
639
640
641
642
643
644
645
646
647
648
649
649
650
651
652
653
654
655
656
657
658
659
659
660
661
662
663
664
665
666
667
668
669
669
670
671
672
673
674
675
676
677
678
679
679
680
681
682
683
684
685
686
687
687
688
689
689
690
691
692
693
694
695
696
697
697
698
699
699
700
701
702
703
704
705
706
707
708
709
709
710
711
712
713
714
715
716
717
717
718
719
719
720
721
722
723
724
725
726
727
728
729
729
730
731
732
733
734
735
736
737
738
739
739
740
741
742
743
744
745
746
747
748
749
749
750
751
752
753
754
755
756
757
758
759
759
760
761
762
763
764
765
766
767
768
769
769
770
771
772
773
774
775
776
777
778
779
779
780
781
782
783
784
785
786
787
787
788
789
789
790
791
792
793
794
795
796
797
797
798
799
799
800
801
802
803
804
805
806
807
808
809
809
810
811
812
813
814
815
816
817
817
818
819
819
820
821
822
823
824
825
826
827
827
828
829
829
830
831
832
833
834
835
836
837
838
838
839
839
840
841
842
843
844
845
846
847
847
848
849
849
850
851
852
853
854
855
856
857
858
858
859
859
860
861
862
863
864
865
866
867
867
868
869
869
870
871
872
873
874
875
876
876
877
878
878
879
879
880
881
882
883
884
885
886
886
887
887
888
888
889
889
890
891
892
893
894
894
895
895
896
896
897
897
898
898
899
899
900
901
902
903
903
904
904
905
905
906
906
907
907
908
908
909
909
910
910
911
911
912
912
913
913
914
914
915
915
916
916
917
917
918
918
919
919
920
920
921
921
922
922
923
923
924
924
925
925
926
926
927
927
928
928
929
929
930
930
931
931
932
932
933
933
934
934
935
935
936
936
937
937
938
938
939
939
940
940
941
941
942
942
943
943
944
944
945
945
946
946
947
947
948
948
949
949
950
950
951
951
952
952
953
953
954
954
955
955
956
956
957
957
958
958
959
959
960
960
961
961
962
962
963
963
964
964
965
965
966
966
967
967
968
968
969
969
970
970
971
971
972
972
973
973
974
974
975
975
976
976
977
977
978
978
979
979
980
980
981
981
982
982
983
983
984
984
985
985
986
986
987
987
988
988
989
989
990
990
991
991
992
992
993
993
994
994
995
995
996
996
997
997
998
998
999
999
1000
1000
1001
1001
1002
1002
1003
1003
1004
1004
1005
1005
1006
1006
1007
1007
1008
1008
1009
1009
1010
1010
1011
1011
1012
1012
1013
1013
1014
1014
1015
1015
1016
1016
1017
1017
1018
1018
1019
1019
1020
1020
1021
1021
1022
1022
1023
1023
1024
1024
1025
1025
1026
1026
1027
1027
1028
1028
1029
1029
1030
1030
1031
1031
1032
1032
1033
1033
1034
1034
1035
1035
1036
1036
1037
1037
1038
1038
1039
1039
1040
1040
1041
1041
1042
1042
1043
1043
1044
1044
1045
1045
1046
1046
1047
1047
1048
1048
1049
1049
1050
1050
1051
1051
1052
1052
1053
1053
1054
1054
1055
1055
1056
1056
1057
1057
1058
1058
1059
1059
1060
1060
1061
1061
1062
1062
1063
1063
1064
1064
1065
1065
1066
1066
1067
1067
1068
1068
1069
1069
1070
1070
1071
1071
1072
1072
1073
1073
1074
1074
1075
1075
1076
1076
1077
1077
1078
1078
1079
1079
1080
1080
1081
1081
1082
1082
1083
1083
1084
1084
1085
1085
1086
1086
1087
1087
1088
1088
1089
1089
1090
1090
1091
1091
1092
1092
1093
1093
1094
1094
1095
1095
1096
1096
1097
1097
1098
1098
1099
1099
1100
1100
1101
1101
1102
1102
1103
1103
1104
1104
1105
1105
1106
1106
1107
1107
1108
1108
1109
1109
1110
1110
1111
1111
1112
1112
1113
1113
1114
1114
1115
1115
1116
1116
1117
1117
1118
1118
1119
1119
1120
1120
1121
1121
1122
1122
1123
1123
1124
1124
1125
1125
1126
1126
1127
1127
1128
1128
1129
1129
1130
1130
1131
1131
1132
1132
1133
1133
1134
1134
1135
1135
1136
1136
1137
1137
1138
1138
1139
1139
1140
1140
1141
1141
1142
1142
1143
1143
1144
1144
1145
1145
1146
1146
1147
1147
1148
1148
1149
1149
1150
1150
1151
1151
1152
1152
1153
1153
1154
1154
1155
1155
1156
1156
1157
1157
1158
1158
1159
1159
1160
1160
1161
1161
1162
1162
1163
1163
1164
1164
1165
1165
1166
1166
1167
1167
1168
1168
1169
1169
1170
1170
1171
1171
1172
1172
1173
1173
1174
1174
1175
1175
1176
1176
1177
1177
1178
1178
1179
1179
1180
1180
1181
1181
1182
1182
1183
1183
1184
1184
1185
1185
1186
1186
1187
1187
1188
1188
1189
1189
1190
1190
1191
1191
1192
1192
1193
1193
1194
1194
1195
1195
1196
1196
1197
1197
1198
1198
1199
1199
1200
1200
1201
1201
1202
1202
1203
1203
1204
1204
1205
1205
1206
1206
1207
1207
1208
1208
1209
1209
1210
1210
1211
1211
1212
1212
1213
1213
1214
1214
1215
1215
1216
1216
1217
1217
1218
1218
1219
1219
1220
1220
1221
1221
1222
1222
1223
1223
1224
1224
1225
1225
1226
1226
1227
1227
1228
1228
1229
1229
1230
1230
1231
1231
1232
1232
1233
1233
1234
1234
1235
1235
1236
1236
1237
1237
1238
1238
1239
1239
1240
1240
1241
1241
1242
1242
1243
1243
1244
1244
1245
1245
1246
1246
1247
1247
1248
1248
1249
1249
1250
1250
1251
1251
1252
1252
1253
1253
1254
1254
1255
1255
1256
1256
1257
1257
1258
1258
1259
1259
1260
1260
1261
1261
1262
1262
1263
1263
1264
1264
1265
1265
1266
1266
1267
1267
1268
1268
1269
1269
1270
1270
1271
1271
1272
1272
1273
1273
1274
1274
1275
1275
1276
1276
1277
1277
1278
1278
1279
1279
1280
1280
1281
1281
1282
1282
1283
1283
1284
1284
1285
1285
1286
1286
1287
1287
1288
1288
1289
1289
1290
1290
1291
1291
1292
1292
1293
1293
1294
1294
1295
1295
1296
1296
1297
1297
1298
1298
1299
1299
1300
1300
1301
1301
1302
1302
1303
1303
1304
1304
1305
1305
1306
1306
1307
1307
1308
1308
1309
1309
1310
1310
1311
1311
1312
1312
1313
1313
1314
1314
1315
1315
1316
1316
1317
1317
1318
1318
1319
1319
1320
1320
1321
1321
1322
1322
1323
1323
1324
1324
1325
1325
1326
1326
1327
1327
1328
1328
1329
1329
1330
1330
1331
1331
1332
1332
1333
1333
1334
1334
1335
1335
1336
1336
1337
1337
1338
1338
1339
1339
1340
1340
1341
1341
1342
1342
1343
1343
1344
1344
1345
1345
1346
1346
1347
1347
1348
1348
1349
1349
1350
1350
1351
1351
1352
1352
1353
1353
1354
1354
1355
1355
1356
1356
1357
1357
1358
1358
1359
1359
1360
1360
1361
1361
1362
1362
1363
1363
1364
1364
1365
1365
1366
1366
1367
1367
1368
1368
1369
1369
1370
1370
1371
1371
1372
1372
1373
1373
1374
1374
1375
1375
1376
1376
1377
1377
1378
1378
1379
1379
1380
1380
1381
1381
1382
1382
1383
1383
1384
1384
1385
1385
1386
1386
1387
1387
1388
1388
1389
1389
1390
1390
1391
1391
1392
1392
1393
1393
1394
1394
1395
1395
1396
1396
1397
1397
1398
1398
1399
1399
1400
1400
1401
1401
1402
1402
1403
1403
1404
1404
1405
1405
1406
1406
1407
1407
1408
1408
1409
1409
1410
1410
1411
1411
1412
1412
1413
1413
1414
1414
1415
1415
1416
1416
1417
1417
1418
1418
1419
1419
1420
1420
1421
1421
1422
1422
1423
1423
1424
1424
1425
1425
1426
1426
1427
1427
1428
1428
1429
1429
1430
1430
1431
1431
1432
1432
1433
1433
1434
1434
1435
1435
1436
1436
1437
1437
1438
1438
1439
1439
1440
1440
1441
1441
1442
1442
1443
1443
1444
1444
1445
1445
1446
1446
1447
1447
1448
1448
1449
1449
1450
1450
1451
1451
1452
1452
1453
1453
1454
1454
1455
1455
1456
1456
1457
1457
1458
1458
1459
1459
1460
1460
1461
1461
1462
1462
1463
1463
1464
1464
1465
1465
1466
1466
1467
1467
1468
1468
1469
1469
1470
1470
1471
1471
1472
1472
1473
1473
1474
1474
1475
1475
1476
1476
1477
1477
1478
1478
1479
1479
1480
1480
1481
1481
1482
1482
1483
1483
1484
1484
1485
1485
1486
1486
1487
1487
1488
1488
1489
1489
1490
1490
1491
1491
1492
1492
1493
1493
1494
1494
1495
1495
1496
1496
1497
1497
1498
1498
1499
1499
1500
1500
1501
1501
1502
1502
1503
1503
1504
1504
1505
1505
1506
1506
1507
1507
1508
1508
1509
1509
1510
1510
1511
1511
1512
1512
1513
1513
1514
1514
1515
1515
1516
1516
1517
1517
1518
1518
1519
1519
1520
1520
1521
1521
1522
1522
1523
1523
1524
1524
1525
1525
1526
1526
1527
1527
1528
1528
1529
1529
1530
1530
1531
1531
1532
1532
1533
1533
1534
1534
1535
1535
1536
1536
1537
1537
1538
1538
1539
1539
1540
1540
1541
1541
1542
1542
1543
1543
1544
1544
1545
1545
1546
1546
1547
1547
1548
1548
1549
1549
1550
1550
1551
1551
1552
1552
1553
1553
1554
1554
1555
1555
1556
1556
1557
1557
1558
1558
1559
1559
1560
1560
1561
1561
1562
1562
1563
1563
1564
1564
1565
1565
1566
1566
1567
1567
1568
1568
1569
1569
1570
1570
1571
1571
1572
1572
1573
1573
1574
1574
1575
1575
1576
1576
1577
1577
1578
1578
1579
1579
1580
1580
1581
1581
1582
1582
1583
1583
1584
1584
1585
1585
1586
1586
1587
1587
1588
1588
1589
1589
1590
1590
1591
1591
1592
1592
1593
1593
1594
1594
1595
1595
1596
1596
1597
1597
1598
1598
1599
1599
1600
1600
1601
1601
1602
1602
1603
1603
1604
1604
1605
1605
1606
1606
1607
1607
1608
1608
1609
1609
1610
1610
1611
1611
1612
1612
1613
1613
1614
1614
1615
1615
1616
1616
1617
1617
1618
1618
1619
1619
1620
1620
1621
1621
1622
1622
1623
1623
1624
1624
1625
1625
1626
1626
1627
1627
1628
1628
162
```

## **Propuestas de mejora**

La solución informática ya cuenta con una buena cantidad de funcionalidades para que el lugar de vivienda saque provecho de estas, pero ya se tienen ciertas características nuevas que se planean tener a disposición a los clientes para su implementación, tales como las siguientes:

- Aplicación para móviles y tabletas: Actualmente la solución está pensada para funcionar de manera web por lo que no hay problema a acceder a ella desde cualquier sistema operativo existente, pero en el futuro próximo se planea realizar una aplicación móvil que funcione en sistemas Android y iOS ya que son los dispositivos más utilizados actualmente y será de más fácil acceso para los usuarios.
- Anuncios y notificaciones por correo electrónico: Se desea implementar una función para que los anuncios y notificaciones por ejemplo de multas lleguen directamente al correo electrónico registrado del residente además de la bandeja de la aplicación para tener una notificación inmediata de las mismas.
- Informes y reportes: Actualmente ya se cuenta con ciertos informes y reportes tanto para los diferentes roles de administración como para los residentes, pero en el futuro se desea tener un mayor número de estos de modo que los usuarios puedan estar al tanto de la información de manera más sencilla y unificada.
- Solicitud de cambios arquitectónicos: Se encontró que en ciertos lugares de vivienda se debe de solicitar un permiso para realizar ciertos cambios arquitectónicos de la misma, es por esto por lo que se incluirá una función para que los residentes puedan llenar, enviar una solicitud a la junta directiva y llevar el seguimiento de esta.
- Registro de alertas de seguridad: En caso de que algún incidente suceda y se necesite de ayuda de los agentes de seguridad se tendrá un módulo sencillo para que de manera rápida lleguen alertas a seguridad para que puedan ser atendidas en el momento y de esta manera apoyar.
- Calendario de eventos: Se implementará un calendario de eventos en donde aparecerán todas las actividades que se tengan programadas por la administración.

- Votaciones electrónicas: Se encontró que en la mayoría de los lugares de vivienda se tiene una elección para la junta directiva, es por esto por lo que se incluirá una función para poder realizar las votaciones de manera electrónica cuando se necesite, esto llevará los conteos, resultados y mostrará la elección a los residentes.
- Reunión virtual para asambleas: Se encontró que las reuniones virtuales son de mucha ayuda para las personas se incluirá una opción para que cuando se necesite realizar una reunión o asamblea se pueda realizar de manera virtual, a los residentes les llegará la invitación y podrán participar en ella.

## Campaña Publicitaria Facebook

Con el fin de poder completar una campaña publicitaria fue necesario inicialmente crear una página de Facebook de la organización, tras lo cual se completó un análisis para lograr una adecuada segmentación de mercado, teniendo en consideración que de manera regular las personas que buscan realizar modificaciones dentro del condominio pueden ser tanto los comités vecinales o los administradores del residencial se buscó un público objetivo dentro de las edades de 40 a 60 años en géneros tanto masculino como femenino con ubicaciones tanto en la ciudad de Guatemala como en las Zonas aledañas, siendo estas Santa Catarina Pinula, San Jose Pinula, Carretera al Salvador y Mixco. La finalidad de la campaña es alcanzar a la mayoría de los clientes potenciales dentro de las zonas en las que la organización tiene alcance (siendo este un alcance inicial) con un presupuesto de ciento cuarenta quetzales (Q140.00) diarios con una duración de 1 mes calendario.

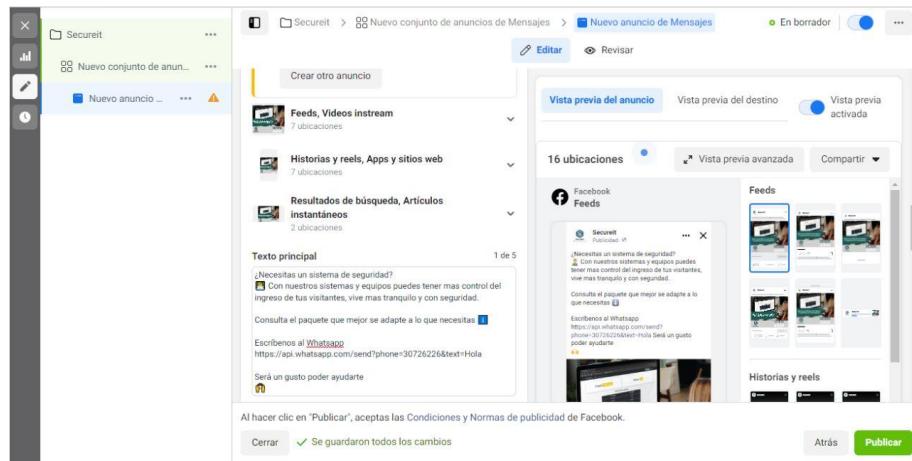
A continuación, se muestra la publicación inicial e imágenes relacionadas a Meta Business la cual permite tanto el lanzamiento de las imágenes publicitarias como el seguimiento de estas.

**Figura 24. Publicación Inicial**



*Ilustración 24 - Elaboración Propia (anexo 1 imagen con mayor escala)*

**Figura 25. Proceso de Creación Publicitaria**



*Ilustración 25 - Elaboración Propia*

**Figura 26. Presupuesto y Calendario**

**Presupuesto y calendario**

**Presupuesto** ⓘ  
Presupuesto diario Q140,00 GTQ  
Gastarás un máximo de Q175,00 algunos días y un importe menor otros. Gastarás un promedio de Q140,00 por día y no más de Q980,00 por semana natural. [Más información](#)

**Calendario** ⓘ  
**Fecha de inicio**  
5/9/2022 11:57 Hora de Guatemala  
**Finalización - Opcional**  
 Definir una fecha de finalización  
4/10/2022 00:00 Hora de Guatemala

*Ilustración 216 - Elaboración Propia*

**Figura 26. Resultados Estimados**



*Ilustración 226 - Elaboración Propia*

## **Conclusiones**

- Para lograr una definición optima del modelo de negocio debe establecerse de forma clara no solo el proceso de creación del producto, sino también, con base en el modelo Canvas, debe planteares los componentes adicionales (fuentes de ingreso, propuesta de valor, recursos clave, etc.) con el fin de lograr una planificación estratégica adecuada y orientada al desarrollo de software como servicio que permita un modelo sostenible en el tiempo.
- Existe una importante acogida de SaaS a nivel mundial con un crecimiento económico significativo de inversión que se acerca al 18% anual (CIO, 2014), lo que indica que la tendencia mundial para pequeñas y medianas empresas se orienta al uso de software con este tipo de distribución.
- El crecimiento exponencial de la población de forma generalizada y el aumento de la criminalidad no solo en el área capitalina guatemalteca sino a lo largo de todo el país da una puerta de entrada a proyectos que ayuden en el proceso de aseguramiento residencial.
- El aumento de acceso a la información y dispositivos informáticos, aumentado gracias a las problemáticas salubres actuales da pie a que soluciones que permitan un menor contacto físico interpersonal sean aplicadas de forma exponencial y a la vez abre una brecha para el crecimiento informático del país.

## **Recomendaciones**

- La realización de un buen proyecto de modelo de negocios se necesita evaluar diferentes aspectos los cuales están la necesidad del humano con respecto al producto que se va a vender, conocer el mercado objetivo entre otros pasos a evaluar para así poder tener un modelo de negocios estructurado de manera correcta.
- Poseer sistemas el cual ayuden a minimizar la carga de labores para los ciudadanos y/o empleados ayuda a automatizar los procedimientos, así como un mejor control, estadística y mejoras de la información que se maneja en las diferentes empresas.
- Implementar seguridad en los sistemas es de suma importancia para la información que se esté manejando en cualquier tipo de sistema informático, la implementación de firewall, segmentaciones entre otros aspectos ayudara al sistema a tener una seguridad para que no suceda el robo de información.
- Implantar exactamente lo cual su comercio ofrecer para darse a conocer que son mejores que los competidores, es el principio de una profundo iniciativa de costo. Cuando se haya determinado varias, se vincula todas ellas a un sistema de entrega de servicios o productos para decidir cómo seguirá siendopreciado para sus consumidores en todo el tiempo.

## Anexo 1

### Publicación Inicial – Campaña Facebook



## **Referencias Bibliográficas**

INE (2018) Resultados del Censo 2018. INE <https://www.censopoblacion.gt>

Wikipedia (20 de junio del 2002). Wikipedia <https://es.wikipedia.org/>

Solorzano (2 de julio del 2022). Aumento de las denuncias por extorsión en ocho meses, según cifras oficiales. Prensalibre <https://www.prensalibre.com/>

Swissinfo.ch (23 de febrero del 2022) Las extorsiones en Guatemala aumentan un 22 % en enero de 2022. Swissinfo <https://www.swissinfo.ch>

Mesa (12 de abril del 2022). Telefonía móvil en Guatemala creció 8,5 % el 2021 y Tigo y claro dominan el mercado. Dinero <https://dinero.hn>

Yi Min Shum (17 de abril del 2022). Situación digital, internet y redes sociales Guatemala 2022. Yiminshum <https://yiminshum.com>

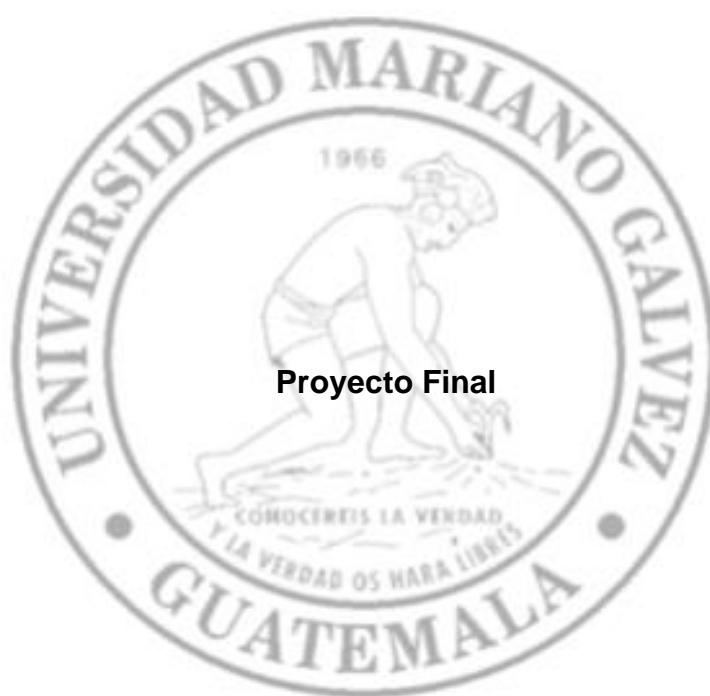
Mata (sin fecha). La privacidad de datos en Guatemala y los derechos fundamentales que se derivan de la misma según la jurisprudencia de la corte de constitucionalidad. Consortiumlegal <https://consortiumlegal.com/>

Resolución 68/167 (abril del 2014). El derecho de la privacidad en la era digital

Recinos (sin fecha). Guatemala: la importancia de los reglamentos en los regímenes de propiedad horizontal. Consortium legal <https://consortiumlegal.com/>

INE (2022) Indicadores de Hechos delictivos, Indicadores de homicidios Policía Nacional Civil. <https://www.ine.gob.gt/ine/estadisticas/bases-de-datos/hechos-delictivos/>

Universidad Mariano Gálvez de Guatemala  
Facultad de Ingeniería de Sistemas de Información  
Maestría de Seguridad de Sistemas de Información  
Seguridad en Aplicaciones  
Ing. Devora Emperatris Meza Orellana



87 Ochenta y siete

DEVORA  
EMPERATRIS  
MEZA ORELLANA

Firmado digitalmente por  
DEVORA EMPERATRIS  
MEZA ORELLANA  
Fecha: 2022.12.15 12:00:52  
-06'00"

1293-10-593	Josue Eduardo Pérez Véliz
1293-13-3807	Valeriano de Jesús Chete Guzmán
1293-17-646	Bryan Orlando Aguirre Sagastume
1293-17-1255	Ricardo Alejandro Pérez Rodriguez
1293-07-1719	Cristian Elí del Cid Rodríguez

Plan Diario Vespertino Sección "D"

## índice

Introducción .....	1
Que es WordPress .....	2
Quienes usan WordPress .....	3
Seguridad en WordPress.....	3
Justificación de la aplicación.....	4
Identificación de activos.....	5
Resultados del análisis por capas .....	1
Tratamiento de los riesgos.....	3
Ciber Defensa.....	8
Pruebas de Penetración: Caja Negra .....	8
Ausencia de fichas (Tokens) Anti-CSRF.....	10
Content Security Policy (CSP) Header Not Set .....	11
Pruebas de Seguridad basado en los riesgos: Caja Gris – Caja Blanca .....	12
Conclusiones .....	46
Recomendaciones .....	47

## Introducción

En la actualidad todas las empresas competitivas en el mercado cuentan con un sitio web institucional, el cual está dedicado a ofrecer información acerca de la empresa, los formatos pueden llegar a ser muy variados dependiendo del giro del negocio de la empresa.

Para hacer que los usuarios puedan compartir información de forma rápida y eficiente se han creado diversos CMS, los cuales han permitido a los usuarios crear sitios web en poco tiempo, pero tanta velocidad ha dejado la brecha de seguridad lo suficientemente amplia para que cualquier persona con conocimientos básicos pueda tomar control de los sitios.

Dichas acciones son preocupantes cuando los CMS comienzan a integrar el servicio de compras en línea, puesto que ya no solamente se comparte información pública, sino que también se manejan datos de pago de los clientes de los sitios.

Es por tal razón en el presente documento se hace un análisis de riesgos por capas, identificación de activos, entre otros elementos más, basados en un CMS popular llamado Wordpress el cual está siendo utilizado en una empresa para compartir información general y hacer compras en línea.

## Que es WordPress

Para entender que es WordPress primero se debe explicar que es un CMS, por sus siglas en inglés un “Content Management System” es un sistema de administración de contenido, el cual permite a los usuarios compartir información de una forma amigable. No es necesario tener amplios conocimientos técnicos en programación para poder usarlos. Es allí donde radica el éxito de muchos CMS.

En el mercado existen muchos CMS algunos son pagados y otros son gratuitos, WordPress es un CMS gratuito el cual fue desarrollado utilizando PHP un lenguaje de programación lo suficientemente ligero para ser utilizado en cualquier servicio de hosting.

Y su popularidad radica justamente en ello, que es un sistema fácil de instalar, puede correr en cualquier hosting y para los usuarios es fácil y rápido de utilizar, también permite el uso de plugins. Dichos Plugins son componentes externos desarrollados por programadores o empresas independientes, que ayudan a agregarle más funcionalidades al sistema.

Como era de esperar, los plugins pueden existir gratuitos o de código abierto y de pago. En un inicio los plugins eran programas auxiliares como se ha mencionado anteriormente agregaban funcionalidades mínimas, por ejemplo, un control de usuarios, control de contraseñas, estilos gráficos, entre otras funcionalidades más.

Sin embargo, al paso del tiempo, los plugins fueron evolucionando a tal grado que algunos se han convertido en subsistemas, dentro de wordpress, tal

es el caso de WooCommerce, este es un plugin gratuito el cual permite a los usuarios tener una tienda en línea.

WooCommerce es un plugin gratuito, una vez instalado permite desde un panel de control amigable, añadir, editar y eliminar productos, procesar compras, tener pasarelas de pago con tarjetas de crédito o débito, según sea el servicio contratado con los bancos. También permite la integración con diversos sistemas de factura electrónica, tal plugin se ha convertido en uno de los favoritos por las empresas y emprendedores para ofrecer sus productos.

## **Quienes usan WordPress**

WordPress es utilizado por usuarios que no cuentan con conocimientos técnicos en programación, que necesitan un sitio web elegante y a la vez fácil de administrar, con un panel de control amigable para que cualquier usuario con conocimientos básicos en el uso de sistemas pueda agregar o quitar información.

Actualmente el 30% de las páginas en el mundo utilizan WordPress, y como se ha dicho anteriormente su mayor uso es para compartir información y hacer comercio en línea.

## **Seguridad en WordPress**

Al ser uno de los CMS más populares en el mercado, ha sido uno de los sistemas más atacados, sin embargo, eso no significa que no sea seguro, existen diversos factores que pueden ayudar a que WordPress quede vulnerable ante un ataque.

Sin embargo, diversos artículos han concluido que la mayoría de las vulnerabilidades encontradas en el CMS se deben a las malas prácticas que han seguidos los usuarios al momento de implementar la herramienta, así como la falta de mantenimiento de esta.

Un ejemplo de ello es el uso de versiones desactualizadas, versiones de plugins abandonados o desactualizados, el uso de contraseñas por defecto. además, que no se mencionan las vulnerabilidades generadas por las configuraciones de seguridad para dominio, certificado SSL entre otras más referentes al perímetro de la aplicación.

Lo cual ha dado como resultado que un estudio realizado en el 2017 por Sucuri, una empresa de seguridad multiplataforma determinó que WordPress es el sitio web más infectado en el que han trabajado estableciendo un 83% de infecciones respecto a sus competidores.

Algunas de las vulnerabilidades encontradas son:

1. Puertas traseras
2. Pharma Hacks
3. Intentos de inicio de sesión por fuerza bruta
4. Redireccionamientos maliciosos
5. Cross-Site Scripting (XSS)
6. Denegación de servicio.

## **Justificación de la aplicación**

Como objeto de investigación se ha elegido a la empresa ManosGT, pues la empresa es un emprendimiento el cual está enfocado en ofrecer una plataforma de comercio en línea a los emprendedores que ofrecen productos

pero que carecen del conocimiento, tiempo y presupuesto para montar su propio sitio de e-commerce. Para lograr que la plataforma funcione alineada con la visión de ManosGT, se ha implementado una instancia de WordPress utilizando la versión 6.1, siendo la versión más actualizada a la fecha en que se realiza la presente investigación.

La aplicación al estar orientada a e-Commerce utiliza el plugin de WooCommerce, por último, cuenta con una base de datos MySQL y un servidor Apache.

El párrafo anterior establece las tecnologías que se están utilizando en la actualidad posteriormente se realizará a profundidad como se utilizan. Sin embargo, la información proporcionada es suficiente para realizar un ataque informático contra los datos de los clientes de la plataforma.

## **Identificación de activos**

La identificación de activos es de importancia debido a que sobre estos mismo será llevado a cabo el análisis de riesgos y también el análisis de las amenazas de estos, por lo que se identificaron los siguientes activos los cuales son correspondientes al objetivo de este proyecto:

No	Proceso	Nombre activo	Descripción	Tipo	Ubicación	Clasificación	Justificación	Criticidad	Propietario	Custodio	Usuarios
1	Registro y consulta de información	Base de datos	Base de datos del aplicativo en donde se almacenan toda la información de los clientes, productos, compras, otros. Esta se encuentra en la nube.	Información	Nube	Confidencial	El aplicativo queda inutilizable	Alta	MangosGT	DBA	Todo publico
2	Envío y recepción de información	Correo electrónicos administrativos	Estos correos son los que administran las cuentas dentro de los dominios que se utilizan para la aplicación y la organización	Información	Nube	Confidencial	Se pierde el control de los servicios contratados	Alta	MangosGT	Administración	Administración
3	Respuesta y uso del aplicativo	Server-Steadfast	El servicio de la nube proveído por Server Steadfast el cual provee hosting, base de datos y unidades lógicas	Servicio	Nube	Confidencial	El aplicativo queda inutilizable	Alta	MangosGT	Jefe de desarrollo	Jefe de desarrollo
4	Almacenaje de información	Copias de seguridad por Steadfast	Activo que se encuentra en el proveedor del servidor web, este es una copia de la base de datos que se realiza de manera automatizada dentro de Steadfast	Servicio	Nube	Confidencial	Se pierde la seguridad de los datos	Media	MangosGT	Jefe de desarrollo	Jefe de desarrollo
5	Dar servicio del aplicativo	Dominio por Steadfast	Servicio de dominio contratado para el host del sitio	Servicio	Nube	Confidencial	El aplicativo queda inutilizable	Alta	MangosGT	Jefe de desarrollo	Todo publico
6	Proveer de conexiones con clientes	Servidor apache	Web server de la aplicación que provee Steadfast	Servicio	Nube	Disponibilidad	El aplicativo queda inutilizable	Alta	MangosGT	Jefe de desarrollo	Todo publico
7	Respuesta y uso del aplicativo	Aplicativo web	El software que se encuentra en funcionamiento en Steadfast	Software	Nube	Disponibilidad	El aplicativo queda inutilizable	Alta	MangosGT	Jefe de desarrollo	Todo publico
8	Uso de programas externos a la institución	Licencia Tableu	Licencia contratada para realizar análisis de datos	Software	Nube	Integridad	Se pierde la oportunidad de analizar los datos	Baja	MangosGT	Analista de datos	Analista de datos y administración
9	Uso de programas externos a la institución	Licencia de MySQL	Licencia adquirida para la incorporarla en la aplicación	Software	Nube	Confidencial	El aplicativo queda inutilizable	Alta	MangosGT	Jefe de desarrollo	DBA, administración y analista de datos
10	Uso de programas externos a la institución	Licencia WordPress	Licencia de WordPress la que permite hacer uso de este para la gestión del aplicativo web	Software	Nube	Confidencial	El aplicativo queda inutilizable	Alta	MangosGT	Jefe de desarrollo	Jefe de desarrollo
11	Uso de programas externos a la institución	Licencia GitHub	Licencia de GitHub para gestionar, almacenar el código del aplicativo	Software	Nube	Disponibilidad	Se pierde la gestión del software por lo que complicaría su desarrollo	Media	MangosGT	Jefe de desarrollo	Administración y desarrolladores
12	Uso de programas externos a la institución	Licencia Jira	Licencia de jira para mantener control del proceso de desarrollo de la aplicación	Software	Nube	Disponibilidad	Perdida del control de gestión del software	Media	MangosGT	Administración	Administración y desarrolladores
13	Uso de programas externos a la institución	Licencias de Plugin	Las licencias adquiridas por unos plugin instalados en WordPress	Software	Nube	Disponibilidad	El aplicativo queda inutilizable	Alta	MangosGT	Jefe de desarrollo	Administración y desarrolladores
14	Uso de programas externos a la institución	Licencia Windows	Licencia para las computadoras que se utilizará de la gestión del aplicativo web	Software	Digital localmente	Disponibilidad	Comunicación de las herramientas de Windows	Baja	MangosGT	Administración	Administración y desarrolladores
15	Uso de programas externos a la institución	Licencia de antivirus Este nod 32	Licencia para las computadoras que se utilizará de la gestión del aplicativo web	Software	Digital localmente	Disponibilidad	Se eleva la amenaza de virus en las computadoras o ataques hacia estas	Media	MangosGT	Administración	Administración y desarrolladores
16	Registro y consulta de información	Discos duros	Discos duros físicos que son respaldos de la base de datos y del aplicativo web	Hardware	Físico localmente	Confidencial	Perdida de todo respaldo y la posibilidad de la reconstrucción del aplicativo	Media	MangosGT	Jefe de seguridad	Administración y DBA
17	Proveer las herramientas necesarias para los trabajadores	Computadoras de la empresa	Computadoras adquiridas para la gestión del aplicativo web	Hardware	Físico localmente	Disponibilidad	Perdida de gestión de los demás activos	Media	MangosGT	Jefe de seguridad	Todo trabajador
18	Uso de programas externos a la institución	sonarQube	Aplicativo para el control de vulnerabilidades de la aplicación	Software	Digital localmente	Confidencial	Aumenta la probabilidad de tener vulnerabilidades	Media	MangosGT	Jefe de desarrollo	Desarrolladores
19	Proveer mantenimiento a la aplicación	Personal de la empresa	Es el personal encargado de desarrollar y gestionar en todo ámbito el aplicativo web	Servicio	Físico localmente	Disponibilidad	Perdida de gestión de los demás activos	Alta	MangosGT	Administración	Todo trabajador

Tabla 1. Activos (elaboración propia, 2022).

## Resultados del análisis por capas

Se ha realizado una lista con 50 vulnerabilidades las cuales se han clasificado por amenaza, vulnerabilidad, seguridad por profundidad y que brecha basada en los pilares es la que resultaría con daños si se sufre un ataque.

ID	AMENAZA	VULNERABILIDAD	SEGURIDAD POR PROFUNDIDAD	BRECHA
1	Robo de Información	Cross-site scripting	APLICACIÓN	CONFIDENCIALIDAD
2	Acceso no Autorizado	Control de acceso Roto	APLICACIÓN	INTEGRIDAD
3	Robo de Información	Fallos de Criptografía	DATOS	CONFIDENCIALIDAD
4	Robo de Información	Inyección SQL	APLICACIÓN	CONFIDENCIALIDAD
5	Inestabilidad Falla en los servicios	Diseño inseguro	PERIMETRO	DISPONIBILIDAD
6	Inestabilidad Falla en los servicios	Configuración incorrecta de Seguridad	POLÍTICAS Y CONTROLES	CONFIDENCIALIDAD
7	Errores en el Software	Componentes vulnerables y obsoletos	APLICACIÓN	INTEGRIDAD
8	Inestabilidad Falla en los servicios	Fallos de identificación y autenticación	APLICACIÓN	CONFIDENCIALIDAD
9	Errores en el Software	Fallos de Integridad de datos y software	DATOS	INTEGRIDAD
11	Acceso no Autorizado	(SSRF) Falsificación de solicitud del lado del servidor	HOST	INTEGRIDAD
12	Exposición de Información	Fallas en cifrado Https	PERIMETRO	CONFIDENCIALIDAD
13	Exposición de Información	Implementación incorrecta en la Nube.	HOST	DISPONIBILIDAD
14	Mecanismos de Control	Fallos en implementación de contraseñas por Default	DATOS	CONFIDENCIALIDAD
15	Acceso no Autorizado	Fallos en Cookies	DATOS	CONFIDENCIALIDAD
16	Acceso no Autorizado	Secuestro de Sesión	APLICACIÓN	CONFIDENCIALIDAD
17	Acceso no Autorizado	Inyección HTTP	RED	CONFIDENCIALIDAD
18	Robo de Información	Clickjacking	PERIMETRO	INTEGRIDAD
19	Acceso no Autorizado	Ejecución Remota de Código	HOST	DISPONIBILIDAD
20	Mecanismos de Control	Falta de doble factor de autenticación	POLÍTICAS Y CONTROLES	DISPONIBILIDAD
21	Exposición de Información	Falta de WAF(Web application Firewall)	POLÍTICAS Y CONTROLES	INTEGRIDAD
22	Acceso no Autorizado	Inyección SSL	HOST	CONFIDENCIALIDAD
23	Mecanismos de Control	Falta de límites para el uso de una función	APLICACIÓN	INTEGRIDAD
24	Complejidad de Uso	Falta de controles para el manejo de información sensible.	POLÍTICAS Y CONTROLES	CONFIDENCIALIDAD
25	Acceso no Autorizado	PHP code injection	APLICACIÓN	INTEGRIDAD
26	Mecanismos de Control	Software no documentado	POLÍTICAS Y CONTROLES	INTEGRIDAD
27	Acceso no Autorizado	No parametrización de privilegios	POLÍTICAS Y CONTROLES	CONFIDENCIALIDAD
28	Acceso no Autorizado	Cross-site request Forgery	DATOS	INTEGRIDAD
29	Acceso no Autorizado	Ataques de encabezados HTTP	DATOS	INTEGRIDAD
30	Robo de Información	Hombre en el medio	RED	CONFIDENCIALIDAD
31	Exposición de Información	Mala gestión a protección de contraseñas.	DATOS	INTEGRIDAD
32	Mecanismos de Control	Manejo inadecuado de errores	APLICACIÓN	CONFIDENCIALIDAD
33	Errores de los usuarios	permitir el ingreso de caracteres especiales	APLICACIÓN	INTEGRIDAD
34	Errores de los usuarios	Permitir a los usuarios el ingreso de cadenas de caracteres muy largas al dato establecido	APLICACIÓN	INTEGRIDAD
35	Errores de motorización	Falta de logs de acciones de los usuarios registrados dentro de la aplicación	APLICACIÓN	INTEGRIDAD
36	Errores de configuración	Dejar disponibles los archivos de configuración de wordpress	APLICACIÓN	CONFIDENCIALIDAD
37	Difusión de software dañino	Permitir a los usuarios subir documentos sin analizarlos por medio de algún antivirus	APLICACIÓN	INTEGRIDAD
38	Errores de secuencia	La aplicación no aplica transacciones al almacenar los datos	APLICACIÓN	INTEGRIDAD
39	Errores de secuencia	la aplicación no aplica rollbacks cuando se ha producido un error en alguna transacción	APLICACIÓN	INTEGRIDAD
40	Alteración accidental de la información	la aplicación permite hacer modificaciones a los pedidos ya cerrados y entregados a los clientes	APLICACIÓN	INTEGRIDAD
41	Destrucción de información	Permitir a los usuarios eliminar datos de transacciones exitosas y procesadas	APLICACIÓN	INTEGRIDAD
42	Errores de mantenimiento	Permitir a los administradores de base de datos hacer modificaciones directamente a la base de datos	DATOS	INTEGRIDAD
43	Errores de mantenimiento	Realizar actualizaciones al software en horarios de mayor tráfico	POLÍTICAS Y CONTROLES	DISPONIBILIDAD
44	Caida del sistema por agotamiento de recursos	Mala selección de las dimensiones en el servicio contratado en la nube	PERIMETRO	DISPONIBILIDAD
45	Suplantación de identidad de los usuarios	No existe una implementación de doble factor de autenticación de los usuarios	APLICACIÓN	CONFIDENCIALIDAD
46	Denegación de servicio	No tener un servicio que ayude a relajar la detección de peticiones maliciosas	HOST	DISPONIBILIDAD
47	Escapes de la información	Falta de controles sobre la información que pueden extraer los usuarios administradores del sitio	APLICACIÓN	CONFIDENCIALIDAD
48	Acceso no Autorizado	Falta de control de accesos de personal al data center	APLICACIÓN	CONFIDENCIALIDAD
49	Errores en el Software	Falta de conocimiento de personal encargado de mantenimiento del sistema	APLICACIÓN	DISPONIBILIDAD
50	Errores de configuración	Mala documentación por parte del personal encargado del sistema	APLICACIÓN	DISPONIBILIDAD

Tabla 2. Análisis por capas (elaboración propia, 2022).

Con base en el análisis de profundidad se procede con un análisis de los riesgos según el modelo DREAD con el fin de poder ofrecer un mnemónico más entendible de los niveles de amenaza y su posible impacto dentro de la organización, debe tenerse en consideración que el modelo DREAD divide en cinco diferentes categorías el proceso de evaluación, las cuales son:

- **Damage (Daño)**, que mide el impacto resultado de la explotación de la vulnerabilidad.
- **Reproducibility (Reproducción)**, midiendo la facilidad de repetición del incidente.
- **Explotability (Explotación)**, complejidad o coste de la explotación
- **Affected Users (Usuarios afectados)**, nivel de afección del incidente, cuantos usuarios y/o recursos se ven afectados y su nivel de importancia.
- **Discoverability (Descubrimiento)**, facilidad con que la vulnerabilidad es descubierta.

Tipos de Ataque	DREAD risk						
	Daño Potencial	Reproducibilidad	Explotabilidad	Usuarios Afectados	Visibilidad	Columna2	Riesgo (Max = 3)
Ataque de Lectura							
Intercepción	3	3	2	2	2		2.4
Acceso a Agentes	2	2	2	3	2		2.2
Procedencia	1	1	1	2	2		1.4
Sondeo							
Ataques de Antología	1	2	2	1	1		1.4
Sondeo Activo	2	2	1	1	1		1.4
Alteraciones							
Modificaciones de Interaccion	3	2	2	2	2		2.2
Modificaciones de Registros de Agentes	3	2	2	1	2		2
Inyección							
Inyección de Mensajes	1	2	1	1	1		1.2
Inyección de Contenido	2	2	2	1	1		1.6
Inundación							
Inundacion de Vinculo	2	2	1	3	2		2
Inundacion de Agentes	2	3	2	2	2		2.2
Denegacion de Servicios (DoS)							
Denegacion de Servicios Logica (LDoS)							
Repudio	2	2	2	2	2		2
Fraude							
Agente Falso	1	3	2	1	1		1.6
Servicio Falso	3	3	2	2	2		2.4
Ataque de Reputación	2	3	3	3	3		2.8
3: Riesgo Alto, 2: Riesgo Medio, 1: Riesgo Bajo							

Tabla 3. Obtención de riesgos DREAD (elaboración propia, 2022).

De los 50 ataques, se ha realizado una evaluación basados en el impacto y la probabilidad que en que ocurra el ataque, por lo tanto, se calcula la criticidad de la vulnerabilidad. En la siguiente imagen se puede observar que de muchas de las vulnerabilidades no representan una criticidad alta, sin embargo, esto no significa que la aplicación al sufrir un ataque no tenga un impacto alto, al contrario, el impacto de varias de las vulnerabilidades es de nivel crítico.

ID	AMENAZA	VULNERABILIDAD	SEGURIDAD POR PROFUNDIDAD	BRECHA	EVASIÓN		
					PROBABILIDAD	IMPACTO	CRITICIDAD
1	Robo de Información	Cross-site scripting	APLICACIÓN	CONFIDENCIALIDAD	POSIBLE	CATASTRÓFICO	MEDIO
2	Acceso no Autorizado	Control de acceso Roto	APLICACIÓN	INTEGRIDAD	IMPROBABLE	CATASTRÓFICO	BAJO
3	Robo de Información	Fallas de Criptografía	DATOS	CONFIDENCIALIDAD	PROBABLE	MODERADO	MEDIO
4	Robo de Información	Inyección SQL	APLICACIÓN	CONFIDENCIALIDAD	IMPROBABLE	CATASTRÓFICO	BAJO
5	Inestabilidad Falla en los servicios	Diseño inseguro	PERIMETRO	DISPONIBILIDAD	POSIBLE	MODERADO	BAJO
6	Inestabilidad Falla en los servicios	Configuración incorrecta de Seguridad	POLÍTICAS Y CONTROLES	CONFIDENCIALIDAD	POSIBLE	MAYOR	MEDIO
7	Errores en el Software	Componentes vulnerables y obsoletos	APLICACIÓN	INTEGRIDAD	POSIBLE	MODERADO	BAJO
8	Inestabilidad Falla en los servicios	Fallas de identificación y autenticación	APLICACIÓN	CONFIDENCIALIDAD	IMPROBABLE	CATASTRÓFICO	BAJO
9	Errores en el Software	Fallas de Integridad de datos y software	DATOS	INTEGRIDAD	IMPROBABLE	CATASTRÓFICO	BAJO
11	Acceso no Autorizado	(SSRF) Falsificación de solicitud del lado del servidor	HOST	INTEGRIDAD	RARO	MENOR	MUY BAJO
12	Exposición de Información	Fallas en cifrado Https	PERIMETRO	CONFIDENCIALIDAD	PROBABLE	MENOR	BAJO
13	Exposición de Información	Implementación incorrecta en la Nube.	HOST	DISPONIBILIDAD	POSIBLE	MAYOR	MEDIO
14	Mecanismos de Control	Fallas en implementación de contraseñas por Default	DATOS	CONFIDENCIALIDAD	POSIBLE	CATASTRÓFICO	MEDIO
15	Acceso no Autorizado	Fallas en Cookies	DATOS	CONFIDENCIALIDAD	RARO	MENOR	MUY BAJO
16	Acceso no Autorizado	Secuestro de Sesión	APLICACIÓN	CONFIDENCIALIDAD	IMPROBABLE	MODERADO	BAJO
17	Acceso no Autorizado	Inyección HTTP	RED	CONFIDENCIALIDAD	RARO	MENOR	MUY BAJO
18	Robo de Información	Clickjacking	PERIMETRO	INTEGRIDAD	IMPROBABLE	MODERADO	BAJO
19	Acceso no Autorizado	Ejecución Remota de Codigo	HOST	DISPONIBILIDAD	IMPROBABLE	CATASTRÓFICO	BAJO
20	Mecanismos de Control	Falta de doble factor de autenticación	POLÍTICAS Y CONTROLES	DISPONIBILIDAD	CASI SEGURO	MODERADO	MEDIO
21	Exposición de Información	Falta de WAF(Web application Firewall)	POLÍTICAS Y CONTROLES	INTEGRIDAD	PROBABLE	MAYOR	ALTO
22	Acceso no Autorizado	Inyección SSL	HOST	CONFIDENCIALIDAD	RARO	MODERADO	MUY BAJO
23	Mecanismos de Control	Falta de límites para el uso de una función	APLICACIÓN	INTEGRIDAD	POSIBLE	MODERADO	BAJO
24	Complejidad de Uso	Falta de controles para el manejo de información sensible.	POLÍTICAS Y CONTROLES	CONFIDENCIALIDAD	POSIBLE	MAYOR	MEDIO
25	Acceso no Autorizado	PHP code Inyection	APLICACIÓN	INTEGRIDAD	RARO	MODERADO	MUY BAJO
26	Mecanismos de Control	Software no documentado	POLÍTICAS Y CONTROLES	INTEGRIDAD	POSIBLE	INSIGNIFICANTE	MUY BAJO
27	Acceso no Autorizado	No parametrización de privilegios	POLÍTICAS Y CONTROLES	CONFIDENCIALIDAD	POSIBLE	MAYOR	MEDIO
28	Acceso no Autorizado	Cross-site request Forgery	DATOS	INTEGRIDAD	IMPROBABLE	CATASTRÓFICO	BAJO
29	Acceso no Autorizado	Ataques de encabezados HTTP	DATOS	INTEGRIDAD	RARO	CATASTRÓFICO	MUY BAJO
30	Robo de Información	Hombre en el medio	RED	CONFIDENCIALIDAD	POSIBLE	CATASTRÓFICO	MEDIO
31	Exposición de Información	Mala gestión a protección de contraseñas.	DATOS	INTEGRIDAD	RARO	CATASTRÓFICO	MUY BAJO
32	Mecanismos de Control	Manejó inadecuado de errores	APLICACIÓN	CONFIDENCIALIDAD	CASI SEGURO	MAYOR	ALTO
33	Errores de los usuarios	permitir el ingreso de caracteres especiales	APLICACIÓN	INTEGRIDAD	POSIBLE	MAYOR	MEDIO
34	Errores de los usuarios	Permitir a los usuarios el ingreso de cadenas de caracteres muy largas al dato establecido	APLICACIÓN	INTEGRIDAD	PROBABLE	MODERADO	BAJO
35	Errores de motorización	Falta de logs de acciones de los usuarios registrados dentro de la aplicación	APLICACIÓN	INTEGRIDAD	PROBABLE	MENOR	BAJO
36	Errores de configuración	Dejar disponibles los archivos de configuración de wordpress	APLICACIÓN	CONFIDENCIALIDAD	IMPROBABLE	CATASTRÓFICO	BAJO
37	Difusión de software dañino	Permitir a los usuarios subir documentos sin analizarlos por medio de algún antivirus	APLICACIÓN	INTEGRIDAD	CASI SEGURO	MENOR	BAJO
38	Errores de secuencia	La aplicación no aplica transacciones al almacenar los datos	APLICACIÓN	INTEGRIDAD	PROBABLE	MODERADO	MEDIO
39	Errores de secuencia	la aplicación no aplica rollbacks cuando se ha producido un error en alguna transacción	APLICACIÓN	INTEGRIDAD	PROBABLE	MAYOR	ALTO
40	Alteración accidental de la información	la aplicación permite hacer modificaciones a los pedidos ya cerrados y entregados a los clientes	APLICACIÓN	INTEGRIDAD	POSIBLE	MAYOR	MEDIO
41	Destrucción de información	Permitir a los usuarios eliminar datos de transacciones exitosas y procesadas	APLICACIÓN	INTEGRIDAD	CASI SEGURO	MODERADO	MEDIO
42	Errores de mantenimiento	Permitir a los administradores de base de datos hacer modificaciones directamente a la base de datos	DATOS	INTEGRIDAD	IMPROBABLE	CATASTRÓFICO	BAJO
43	Errores de mantenimiento	Realizar actualizaciones al software en horarios de mayor tráfico	POLÍTICAS Y CONTROLES	DISPONIBILIDAD	IMPROBABLE	MAYOR	BAJO
44	Caida del sistema por agotamiento de recursos	Mala selección de las dimensiones en el servicio contratado en la nube	PERIMETRO	DISPONIBILIDAD	PROBABLE	CATASTRÓFICO	ALTO
45	Suplantación de identidad de los usuarios	No existe una implementación de doble factor de autenticación de los usuarios	APLICACIÓN	CONFIDENCIALIDAD	CASI SEGURO	MODERADO	MEDIO
46	Denegación de servicio	No tener un servicio que ayude a relizar detección de peticiones maliciosas	HOST	DISPONIBILIDAD	PROBABLE	MAYOR	ALTO
47	Escapes de la información	Falta de controles sobre la información que pueden extraer los usuarios administradores del sitio	APLICACIÓN	CONFIDENCIALIDAD	POSIBLE	MODERADO	BAJO
48	Acceso no Autorizado	Falla de control de accesos de personal al data center	APLICACIÓN	CONFIDENCIALIDAD	POSIBLE	MAYOR	MEDIO
49	Errores en el Software	Falta de conocimiento de personal encargado de mantenimiento del sistema	APLICACIÓN	DISPONIBILIDAD	IMPROBABLE	CATASTRÓFICO	BAJO
50	Errores de configuración	Mala documentación por parte del personal encargado del sistema	APLICACIÓN	DISPONIBILIDAD	PROBABLE	MAYOR	ALTO

Tabla 4. Impacto (elaboración propia, 2022).

Ya que se ha realizado una evaluación del impacto probabilidad y criticidad, se tiene como segunda parte el efecto del impacto, esto hace referencia si el efecto del ataque afectaría a la reputación del sitio respecto al cliente, si incumple en multas o penalidades, si es una afectación en la productividad, entre otras clasificaciones más, por lo tanto, para esta evaluación, el efecto de impacto se ha desarrollado como se muestra en la siguiente tabla:

ID	AMENAZA	VULNERABILIDAD	EFECTO DEL IMPACTO	
1	Robo de Información	Cross-site scripting	REPUTACIÓN / CONFIANZA DEL CLIENTE	CATASTRÓFICO
2	Acceso no Autorizado	Control de acceso Roto	REPUTACIÓN / CONFIANZA DEL CLIENTE	CATASTRÓFICO
3	Robo de Información	Fallos de Criptografía	FINANCIERO / TECNOLOGÍA	MODERADO
4	Robo de Información	Inyección SQL	FINANCIERO / TECNOLOGÍA	MAYOR
5	Inestabilidad Falla en los servicios	Diseño inseguro	PRODUCTIVIDAD / OPERACIONAL / ESTRATÉGICO	MENOR
6	Inestabilidad Falla en los servicios	Configuración incorrecta de Seguridad	FINANCIERO / TECNOLOGÍA	MAYOR
7	Errores en el Software	Componentes vulnerables y obsoletos	FINANCIERO / TECNOLOGÍA	MODERADO
8	Inestabilidad Falla en los servicios	Fallos de identificación y autenticación	REPUTACIÓN / CONFIANZA DEL CLIENTE	CATASTRÓFICO
9	Errores en el Software	Fallos de Integridad de datos y software	REPUTACIÓN / CONFIANZA DEL CLIENTE	CATASTRÓFICO
11	Acceso no Autorizado	(SSRF) Falsificación de solicitud del lado del servidor	FINANCIERO / TECNOLOGÍA	MENOR
12	Exposición de Información	Fallas en cifrado Https	FINANCIERO / TECNOLOGÍA	MENOR
13	Exposición de Información	Implementación incorrecta en la Nube.	FINANCIERO / TECNOLOGÍA	MAYOR
14	Mecanismos de Control	Fallos en implementación de contraseñas por Default	FINANCIERO / TECNOLOGÍA	MAYOR
15	Acceso no Autorizado	Fallos en Cookies	FINANCIERO / TECNOLOGÍA	MENOR
16	Acceso no Autorizado	Secuestro de Sesión	FINANCIERO / TECNOLOGÍA	MODERADO
17	Acceso no Autorizado	Inyección HTTP	FINANCIERO / TECNOLOGÍA	MENOR
18	Robo de Información	Clickjacking	FINANCIERO / TECNOLOGÍA	MODERADO
19	Acceso no Autorizado	Ejecución Remota de Código	REPUTACIÓN / CONFIANZA DEL CLIENTE	CATASTRÓFICO
20	Mecanismos de Control	Falta de doble factor de autenticación	FINANCIERO / TECNOLOGÍA	MODERADO
21	Exposición de Información	Falta de WAF(Web application Firewall)	PRODUCTIVIDAD / OPERACIONAL / ESTRATÉGICO	MODERADO
22	Acceso no Autorizado	Inyección SSL	FINANCIERO / TECNOLOGÍA	MODERADO
23	Mecanismos de Control	Falta de límites para el uso de una función	PRODUCTIVIDAD / OPERACIONAL / ESTRATÉGICO	MENOR
24	Complejidad de Uso	Falta de controles para el manejo de información sensible.	PRODUCTIVIDAD / OPERACIONAL / ESTRATÉGICO	MODERADO
25	Acceso no Autorizado	PHP code Inyection	FINANCIERO / TECNOLOGÍA	MODERADO
26	Mecanismos de Control	Software no documentado	MULTAS / PENAS LEGALES / CUMPLIMIENTO	IN SIGNIFICANTE
27	Acceso no Autorizado	No parametrización de privilegios	PRODUCTIVIDAD / OPERACIONAL / ESTRATÉGICO	MODERADO
28	Acceso no Autorizado	Cross-site request Forgery	FINANCIERO / TECNOLOGÍA	MAYOR
29	Acceso no Autorizado	Ataques de encabezados HTTP	FINANCIERO / TECNOLOGÍA	MAYOR
30	Robo de Información	Hombre en el medio	FINANCIERO / TECNOLOGÍA	MAYOR
31	Exposición de Información	Mala gestión a protección de contraseñas.	MULTAS / PENAS LEGALES / CUMPLIMIENTO	IN SIGNIFICANTE
32	Mecanismos de Control	Manejo inadecuado de errores	REPUTACIÓN / CONFIANZA DEL CLIENTE	MAYOR
33	Errores de los usuarios	permitir el ingreso de caracteres especiales	FINANCIERO / TECNOLOGÍA	MAYOR
34	Errores de los usuarios	Permitir a los usuarios el ingreso de cadenas de caracteres muy largas al dato establecido	PRODUCTIVIDAD / OPERACIONAL / ESTRATÉGICO	MENOR
35	Errores de motorización	Falta de logs de acciones de los usuarios registrados dentro de la aplicación	MULTAS / PENAS LEGALES / CUMPLIMIENTO	IN SIGNIFICANTE
36	Errores de configuración	Dejar disponibles los archivos de configuración de wordpress	REPUTACIÓN / CONFIANZA DEL CLIENTE	CATASTRÓFICO
37	Difusión de software dañino	Permitir a los usuarios subir documentos sin analizarlos por medio de algún antivirus	PRODUCTIVIDAD / OPERACIONAL / ESTRATÉGICO	MENOR
38	Errores de secuencia	La aplicación no aplica transacciones al almacenar los datos	PRODUCTIVIDAD / OPERACIONAL / ESTRATÉGICO	MENOR
39	Errores de secuencia	la aplicación no aplica rollbacks cuando se ha producido un error en alguna transacción	PRODUCTIVIDAD / OPERACIONAL / ESTRATÉGICO	MODERADO
40	Alteración accidental de la información	la aplicación permite hacer modificaciones a los pedidos ya cerrados y entregados a los clientes	FINANCIERO / TECNOLOGÍA	MAYOR
41	Destrucción de información	Permitir a los usuarios eliminar datos de transacciones exitosas y procesadas	REPUTACIÓN / CONFIANZA DEL CLIENTE	MODERADO
42	Errores de mantenimiento	Permitir a los administradores de base de datos hacer modificaciones directamente a la base de datos	REPUTACIÓN / CONFIANZA DEL CLIENTE	CATASTRÓFICO
43	Errores de mantenimiento	Realizar actualizaciones al software en horarios de mayor tráfico	REPUTACIÓN / CONFIANZA DEL CLIENTE	MAYOR
44	Caida del sistema por agotamiento de recursos	Mala selección de las dimensiones en el servicio contratado en la nube	REPUTACIÓN / CONFIANZA DEL CLIENTE	CATASTRÓFICO
45	Suplantación de identidad de los usuarios	No existe una implementación de doble factor de autenticación de los usuarios	MULTAS / PENAS LEGALES / CUMPLIMIENTO	IN SIGNIFICANTE
46	Denegación de servicio	No tener un servicio que ayude a relizar detección de peticiones maliciosas	PRODUCTIVIDAD / OPERACIONAL / ESTRATÉGICO	MODERADO
47	Escapes de la información	Falta de controles sobre la información que pueden extraer los usuarios administradores del sitio	FINANCIERO / TECNOLOGÍA	MODERADO
48	Acceso no Autorizado	Falta de control de accesos de personal al data center	FINANCIERO / TECNOLOGÍA	MAYOR
49	Errores en el Software	Falta de conocimiento de personal encargado de mantenimiento del sistema	PRODUCTIVIDAD / OPERACIONAL / ESTRATÉGICO	MODERADO
50	Errores de configuración	Mala documentación por parte del personal encargado del sistema	REPUTACIÓN / CONFIANZA DEL CLIENTE	MAYOR

Tabla 5. Efecto del impacto (elaboración propia, 2022).

Para comprender aún mejor los resultados se ha diseñado una matriz de calor la cual se ha definido con la siguiente estructura:

		GRAVEDAD GENERAL DEL RIESGO				
IMPACTO EN LOS PROCESOS	CATASTRÓFICO	Paraliza todas las operaciones de la entidad.				
	MAYOR	Interrumpe la prestación de servicios críticos que se brinda a los clientes, debido a la caída significativa de las operaciones. Pérdida potencial de clientes.				
	MODERADO	Operativamente es sostenible, pero dificulta o retrasa las operaciones. Interrumpe parcialmente algunos servicios importantes que se brindan a los clientes.				
	MENOR	Afecta parcialmente las operaciones. Interrumpe servicios pero que no tienen incidencia directa en la relación con los clientes.				
	IN SIGNIFICANTE	Tiene un efecto nulo o muy pequeño en las operaciones.				
		BAJO	MEDIO	ALTO	MUY ALTO	MUY ALTO
		BAJO	BAJO	MEDIO	ALTO	MUY ALTO
		MUY BAJO	BAJO	MEDIO	MEDIO	ALTO
		MUY BAJO	BAJO	BAJO	BAJO	MEDIO
		MUY BAJO	MUY BAJO	MUY BAJO	BAJO	BAJO
		No se registra en los últimos 5 años.	Se podría presentar una vez cada 5 años.	Se podría presentar una vez al año.	Se podría presentar una vez cada mes.	Se podría presentar varias veces en el mes.
		RARO	IMPROBABLE	POSIBLE	PROBABLE	CASI SEGURO
PROBABILIDAD DE OCURRENCIA						

Tabla 6. Gravedad de riesgos (elaboración propia, 2022)

Donde los riesgos que se encuentren en el cuadrante de impacto catastrófico con una probabilidad casi segura, deben ser las vulnerabilidades a las que la empresa debe tomar acciones inmediatas.

Sin embargo, para los resultados obtenidos la matriz de calor refleja solamente dos vulnerabilidades a las cuales se les debe prestar la atención prioritaria, tal y como se muestra en los resultados de la matriz de calor, a continuación:

		GRAVEDAD GENERAL DEL RIESGO				
IMPACTO EN LOS PROCESOS	CATASTRÓFICO	Paraliza todas las operaciones de la entidad.				
	MAYOR	Interrumpe la prestación de servicios críticos que se brinda a los clientes, debido a la caída significativa de las operaciones. Pérdida potencial de clientes.				
	MODERADO	Operativamente es sostenible, pero dificulta o retrasa las operaciones. Interrumpe parcialmente algunos servicios importantes que se brindan a los clientes.				
	MENOR	Afecta parcialmente las operaciones. Interrumpe servicios pero que no tienen incidencia directa en la relación con los clientes.				
	IN SIGNIFICANTE	Tiene un efecto nulo o muy pequeño en las operaciones.				
		2	9	3	1	0
		0	1	7	4	1
		2	2	5	2	3
		3	0	0	2	1
		0	0	1	0	0
		No se registra en los últimos 5 años.	Se podría presentar una vez cada 5 años.	Se podría presentar una vez al año.	Se podría presentar una vez cada mes.	Se podría presentar varias veces en el mes.
		RARO	IMPROBABLE	POSIBLE	PROBABLE	CASI SEGURO
PROBABILIDAD DE OCURRENCIA						

Tabla 7. Resultado de análisis de riesgos (elaboración propia, 2022).

Al mismo tiempo la matriz de calor refleja que la mayoría de las vulnerabilidades pueden llegar a ser tratadas con planificación de acción por parte de la empresa.

Adicionalmente a los resultados obtenidos por la matriz de calor, se han realizado la siguiente serie de graficas para comprender cuales son los elementos donde el impacto puede ser mayor.

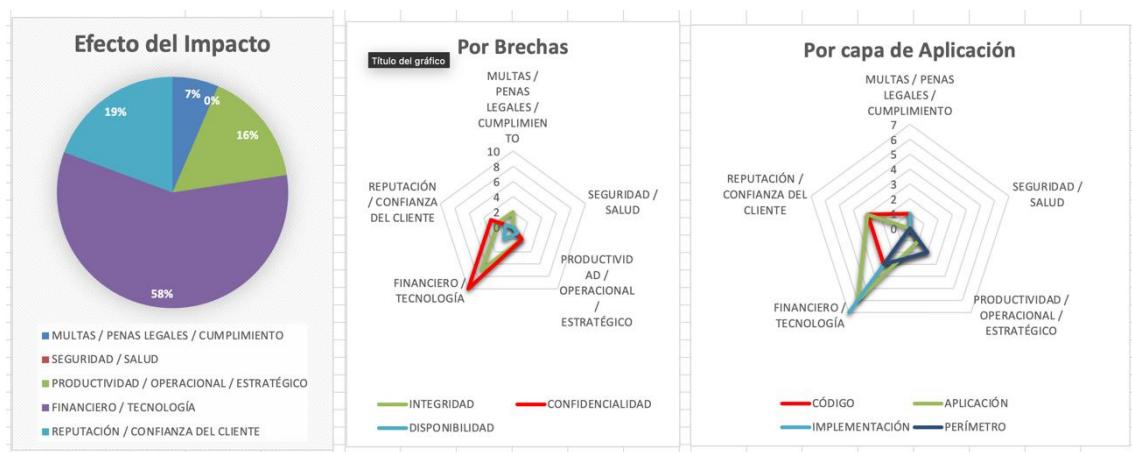


Figura 1. Efecto del Impacto (elaboración propia, 2022)

La grafica de pie, muestra como el impacto de las vulnerabilidades es mayor en el la parte financiero y tecnología, lo que quiere decir que si un ataque llegara a ocurrir es más probable que este afecte directamente a las finanzas de la empresa y la tecnología que se está utilizando.

En la segunda grafica se muestra que la brecha que puede causar mayores perdidas económicas es la confidencialidad y la integridad de los datos, puesto que, al ser una tienda en línea, la mayoría de la información es sensible y no es de carácter público.

Por último, la tercera grafica permite ver que la mayor parte de vulnerabilidades se encuentran en la aplicación tanto en el uso como en el

manejo de los datos y la implementación realizada al momento de hacer pública la aplicación.

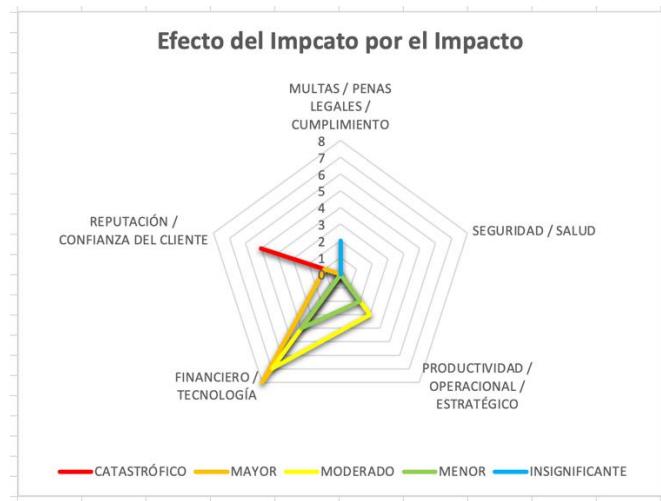


Figura 2. Impacto de vulnerabilidades (elaboración propia, 2022).

En la gráfica anterior se puede ver como el impacto mayor, así como moderado y menor recae sobre las finanzas y tecnología de la empresa, pero si se ve en detalle el impacto catastrófico que puede llevar a la empresa una situación difícil en el mercado está ligada a la reputación y a la confianza con los clientes.

Siendo dichas vulnerabilidades las que se deben priorizar al momento de realizar las mitigaciones correspondientes.

Tomando encuentro la criticidad de las vulnerabilidades encontradas, se puede ver que el dictámos global de la evolución del riesgo es **alto** por lo que importante tomar acciones inmediatas,

## Tratamiento de los riesgos

De los riesgos encontrados dentro de la evaluación como equipo externo se le han recomendado realizar las siguientes acciones de forma general.

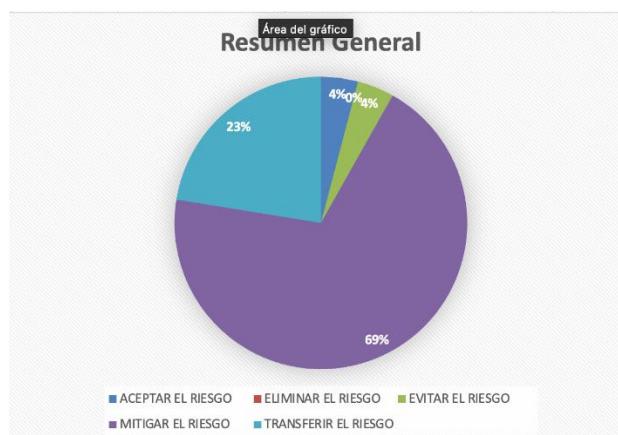


Figura 3. Resumen general (elaboración propia, 2022).

Para el 69% de los casos, se recomienda mitigar el riesgo lo cual quiere decir que con base a la naturaleza de las vulnerabilidades encontradas el equipo de informática de la empresa deberá realizar acciones, las cuales se detallan más adelante, con la finalidad de mitigar el riesgo.

Mientras que el 23% de las vulnerabilidades se recomienda transferir el riesgo, lo que significa que el riesgo existe, pero no es posible solventarlo por el mismo equipo de informática de la empresa, por lo tanto, se buscará a un tercero quien será el encargado de realizar las acciones correspondientes para que el riesgo no ocurra.

En la siguiente grafica se puede observar que la mayoría de las vulnerabilidades que serán mitigadas se centran en la brecha de confidencialidad y la brecha de integridad. Lo cual quiere decir que la empresa tiene un buen equipo para mantener la continuidad de la página, pero muchas sospechas sobre el manejo de los datos.

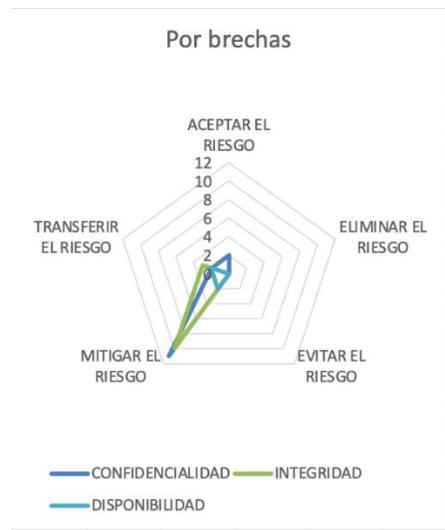


Figura 4. Riesgos por brechas (elaboración propia, 2022).

Por otra parte, se ha encontrado que las vulnerabilidades en gran medida están ligadas a la aplicación, esto quiere decir al manejo de formularios, pantallas, opciones de usuarios, que pueden llegar a solventarse, y casi de forma similar el código, donde se requieren hacer validaciones por parte de los programadores para que la aplicación pueda seguir funcionando de forma segura respecto a los datos de los usuarios.



Figura 5. Riesgos por capas (elaboración propia, 2022)

Por lo tanto, una vez que se conocen las acciones generales a realizar es se deben conocer las acciones específicas respecto a las vulnerabilidades mencionadas al inicio de la evaluación.

VULNERABILIDAD	TRATAMIENTO DEL RIESGO	SOLUCIONES
Cross-site scripting	MITIGAR EL RIESGO	Se debe validar dentro del código de la aplicación que todos los inputs no permitan el ingreso de caracteres especiales, así mismo limitar el tamaño de los campos al tamaño esperado de la información a ingresar.
Control de acceso Roto	MITIGAR EL RIESGO	Se recomienda utilizar un doble factor de autenticación basado en correo electrónico de los usuarios siempre y cuando esté verificado, al mismo tiempo se recomienda implementar controles de uso lo cual ayudara a determinar si ha existido actividad fuera de los horarios mas comunes
Fallos de Criptografía	MITIGAR EL RIESGO	Se le recomienda implementar cifrado sincrono basado en llaves SHA 256 la cual ayudara a la aplicación a mantener un cifrado continuo en la transmisión de información dentro del sistema.
Inyección SQL	MITIGAR EL RIESGO	Se recomienda no utilizar directamente los valores ingresados por los usuarios a las consultas SQL, al mismo tiempo se recomienda utilizar librerías que ayuden a mantener las cadenas de texto limpias de caracteres especiales y a encontrar patrones de SQL.
Diseño inseguro	TRANSFERIR EL RIESGO	Se recomienda transferir el riesgo a una empresa dedicada al desarrollo de software basados en estandares de seguridad como ISO 27001 o similares
Configuración incorrecta de Seguridad	MITIGAR EL RIESGO	Se recomienda utilizar las buenas prácticas que establece el fabricante respecto al uso de wodpress, así mismo se recomienda realizar pruebas por cada cambio realizado dentro del flujo de la aplicación
Componentes vulnerables y obsoletos	MITIGAR EL RIESGO	Se recomienda mantener la versión de wordpress y WooCommerce actualizada a las últimas versiones lanzadas, al mismo tiempo se recomienda actualizar todas las dependencias, tanto de la aplicación como las del lenguaje de programación
Fallos de identificación y autenticación	MITIGAR EL RIESGO	Se debe agregar un factor de autenticación basado en dispositivos móviles, con la finalidad que los usuarios administradores puedan acceder a la información más sensible y para los usuarios finales se debe establecer mecanismos de seguridad basados en tokens ya sea en web o en app móvil.
Fallos de Integridad de datos y software	MITIGAR EL RIESGO	Se recomienda utilizar logs y monitoreo de los al momento que ocurre un error, el cual deberá accionar al momento que ocurre un error en las transacciones, específicamente en las transacciones monetarias
(SSRF) Falsificación de solicitud del lado del servidor	MITIGAR EL RIESGO	se debe aplicar controles basados en código que ayuden a la aplicación a determinar si la información está viajando de lugares reconocidos como seguros o en su defecto que sea del mismo servidor donde se ha hecho la petición
Fallas en cifrado Https	MITIGAR EL RIESGO	Se debe aplicar una herramienta que ayude a los administradores de sistemas a automatizar las renovaciones de certificados SSL, así como realizar validaciones para que el sitio no permita realizar operaciones si el certificado no es válido.
Implementación incorrecta en la Nube.	MITIGAR EL RIESGO	Se deben aplicar políticas que ayuden a los técnicos en sistemas a realizar mejoras implementaciones y configuraciones independientemente de que nube se esté utilizando.
Fallos en implementación de contraseñas por Default	MITIGAR EL RIESGO	Se debe aplicar una política que ayude a los administradores en sistemas a endurecer las contraseñas que se utilizarán dentro del sitio, así mismo dentro de la aplicación se debe aplicar una solución para que el usuario pueda cambiar su contraseña usando métodos seguros
Fallos en Cookies	ACEPTAR EL RIESGO	Validar la autenticidad de las Cookies y no ser utilizadas para almacenar información relevante que luego puede ser utilizado en contra de los propios usuarios.
Secuestro de Sesión	MITIGAR EL RIESGO	Validar la cantidad e sesiones que puede tener abierta un usuario, en diferentes equipos, dicha validaciones se debe realizar desde la aplicación
Inyección HTTP	ACEPTAR EL RIESGO	Validar dentro de la aplicación si la información ha viajado desde una dirección segura utilizando https o implementar una solución en la nube.
Clickjacking	MITIGAR EL RIESGO	detectar desde la aplicación utilizando Javascript el uso de extensiones de navegador que puedan estar modificando el código original de la página
Ejecución Remota de Código	MITIGAR EL RIESGO	Dejar habilitados únicamente los puertos seguros como 443 para las peticiones por https, por otra parte se deben validar los campos y variables por URL dentro de la aplicación y validar que los plugins instalados en el sitio sean seguros y no tengan brechas de seguridad que puedan poner en peligro toda la aplicación.
Falta de doble factor de autenticación	TRANSFERIR EL RIESGO	Aplicar doble factor de seguridad en diferentes niveles de la aplicación, con diferentes proveedores, para todos los tipos de usuarios.
Falta de WAF(Web application Firewall)	TRANSFERIR EL RIESGO	Se debe elegir un proveedor que ayude a configurar un WAF en la nube y al mismo tiempo que ayude a realizar las configuraciones seguras específicas para el sitio web

Tabla 8. Tratamiento de riesgos (elaboración propia, 2022).

Inyección SSL	TRANSFERIR EL RIESGO	Contratar a una empresa que ayude a fortalecer las configuraciones de servidor y sitio web para que este tipo de vulnerabilidad no ocurran
Falta de limites para el uso de una función	MITIGAR EL RIESGO	A nivel de código se deben validar que las funciones terminen o tengan métodos (condiciones de salida) para terminar así mismo en base de datos, con la finalidad que las funciones no reserven recursos que no serán utilizados más
Falta de controles para el manejo de información sensible.	MITIGAR EL RIESGO	Se deben establecer políticas para los desarrolladores que ayuden a mantener el flujo de la información segura, así como el uso de métodos criptográficos
PHP code Inyección	MITIGAR EL RIESGO	Se recomienda a los programadores establecer un patrón de diseño donde el frontend se separe del backend en la gran medida que WordPress lo permita con la finalidad de no poder ejecutar código PHP fuera de la aplicación y así mismo no almacenar cadenas grandes en la base de datos que puedan ser utilizadas para inyectar código en general
Software no documentado	TRANSFERIR EL RIESGO	Se debe contratar una empresa que ayude a documentar el software a nivel de código como a nivel de implementación con la finalidad que al informar no se escape junto con los empleados
No parametrización de privilegios	MITIGAR EL RIESGO	La aplicación debe ser capaz de identificar los roles de los usuarios basados en una estructura de módulos, con la finalidad de parametrizar de forma granular los permisos que los usuarios podrán tener sin importar si son usuarios administradores o usuarios finales
Cross-site request Forgery	MITIGAR EL RIESGO	Todas las peticiones que se realicen dentro de la aplicación deben estar validadas y ser entregadas a los destinatarios correspondientes, para ello existen librerías que ayudan a identificar la procedencia y el destino de cada petición
Ataques de encabezados HTTP	TRANSFERIR EL RIESGO	El riesgo se deberá transferir a los proveedores de nube y los proveedores de dominio así mismo utilizar servicios como Cloudflare que ayudaran a mantener el riesgo mitigado
Hombre en el medio	TRANSFERIR EL RIESGO	Al tener una aplicación en la nube es importante que existan protocolos de encriptación en la aplicación para evitar caer en ataques de hombre en medio
Mala gestión a protección de contraseñas.	MITIGAR EL RIESGO	Aplicar políticas de contraseñas seguras y comparar entre hash y no texto plano sin encriptar a nivel de código
Manejo inadecuado de errores	MITIGAR EL RIESGO	Todos los errores que la aplicación se a capaz de generar deberán ser manejados de forma que no se muestre al usuario un detalle o similar y al mismo tiempo estos deben ser almacenados en logs que los administradores puedan leer a posteriori
permitir el ingreso de caracteres especiales	MITIGAR EL RIESGO	Validar el ingreso de caracteres especiales en todos los inputs de la aplicación con la finalidad de evitar un ingreso de código o similar que pueda ser ejecutado posteriormente
Permitir a los usuarios el ingreso de cadenas de caracteres muy largas al dato establecido	MITIGAR EL RIESGO	LIMITAR la cantidad de caracteres dentro del código de la aplicación con la finalidad que no puedan ingresar código elaborado
Falta de logs de acciones de los usuarios registrados dentro de la aplicación	MITIGAR EL RIESGO	Se debe monitorear todas las acciones de los usuarios dentro de la aplicación con la finalidad de auditar el comportamiento de los usuarios y evitar comportamiento sospechoso en transacciones monetarias
Dejar disponibles los archivos de configuración de WordPress	MITIGAR EL RIESGO	Se debe validar que no existan configuraciones erróneas en el servidor que permitan a los usuarios poder acceder a los archivos de configuración de WordPress y obtener claves de base de datos, entre otros más
Permitir a los usuarios subir documentos sin analizarlos por medio de algún antivirus	MITIGAR EL RIESGO	Todos los documentos que se suban al servidor deberán estar almacenados en una carpeta con los permisos de escritura pero no de ejecución así mismo deben ser analizados por un antivirus antes de ser almacenados permanentemente
La aplicación no aplica transacciones al almacenar los datos	MITIGAR EL RIESGO	La aplicación a nivel de código deberá aplicar transacciones que permitan hacer un rollback de las modificaciones realizadas con anterioridad
La aplicación no aplica rollbacks cuando se ha producido un error en alguna transacción	MITIGAR EL RIESGO	Si se ha producido un fallo a nivel de base de datos estos deberán ser revertidos de forma fácil y rápida utilizando transacciones
La aplicación permite hacer modificaciones a los pedidos ya cerrados y entregados a los clientes	MITIGAR EL RIESGO	Se debe validar que un pedido realizado desde la aplicación y finalizado de forma correcta no podrá ser actualizado desde la aplicación ni siendo un usuario administrador
Permitir a los usuarios eliminar datos de transacciones exitosas y procesadas	MITIGAR EL RIESGO	Los administradores y usuarios no podrán hacer eliminaciones de datos siempre y cuando las transacciones estén finalizadas correctamente desde la aplicación.
Permitir a los administradores de base de datos hacer modificaciones directamente a la base de datos	MITIGAR EL RIESGO	Implementar políticas que ayuden a mantener la integridad de los datos y limitar a los usuarios administradores a no realizar modificaciones directamente en la base de datos a menos que exista un permiso previo por las áreas involucradas
Realizar actualizaciones al software en horarios de mayor tráfico	EVITAR EL RIESGO	Implementar políticas para no permitir las actualizaciones en horarios de mayor tráfico, con la finalidad de evitar que se pierda información o se deje sin disponibilidad el servicio

Tabla 9. Tratamiento de riesgos 2 (elaboración propia, 2022)

Mala selección de las dimensiones en el servicio contratado en la nube	TRANSFERIR EL RIESGO	Los administradores de sistemas deberan tener una constante actualizacion a los servicios contratados en la nube sengun la necesidad de crecimiento de la aplicación
No existe una implementación de doble factor de autenticación de los usuarios	TRANSFERIR EL RIESGO	implementar dobel factor de autenticacion basada endiferentes proveedores
No tener un servicio que ayude a relajar detección de peticiones maliciosas	MITIGAR EL RIESGO	Implementar soluciones de firewall o similar que ayude a detectar cuando es una peticion maliciosa o no
Falta de controles sobre la información que pueden enxtraer los usuarios administradores del sitio	MITIGAR EL RIESGO	Dentro de la aplicación se debe limitar el nivel de extracción de datos permitido para los usuarios finales
Falta de control de accesos de personal al data center	EVITAR EL RIESGO	Si bien el servicio es en la nube se debe tener controlado el acceso fisico a las oficinas de sistemas para que no cualquier persona pueda obtener acceso a los codigos fuentes utilizados
Falta de conocimiento de personal encargado de mantenimiento del sistema	TRANSFERIR EL RIESGO	Se deben aplicar capacitaciones constantes a los usuarios y administradores del sitio sobre wodpress para mantener el sitio en las mejores condicioneas y evitar el robo de datos entre otros riesgos mas
Mala documentacion por parte del personal encargado del sistema	TRANSFERIR EL RIESGO	Debe existir una politica que oblique a los usuarios administradores de sistemas a documentar la aplicación y que sea una actualizacion constante

Tabla 10. Tratamiento de riesgos 3 (elaboración propia, 2022)

## Ciber Defensa

### Pruebas de Penetración: Caja Negra

Para las pruebas de penetración o caja negra se utilizó el software de ZAP OWASP el cual es un escáner de seguridad web de código abierto. Luego de realizar un ataque automatizado al sitio de ManosGT se obtuvieron los siguientes resultados:

Esta es la matriz obtenida por tipo de alerta de acuerdo con el nivel de riesgo y confianza. Notamos que no se cuenta con ningún riesgo de nivel alto. De los que se debería de poner más atención están los riesgos de nivel medio de los cuales se cuenta con un total de 5, sin embargo, de esos solo uno es de nivel alto y los demás están en un nivel más bajo.

Riesgo	Alto	0	0	0	0
	Medio	1	2	2	5
	Bajo	1	6	1	8
	Informativo	0	3	5	8
	Total	2	11	8	21
	Alto	Medio	Bajo	Total	Confianza

Tabla 11. Matriz de alerta (elaboración propia, 2022)

A continuación, se detallan el nombre, cantidad y riesgo por tipo de alerta mencionada en la tabla anterior.

Tipo de Alerta	Riesgo	Cantidad
Ausencia de fichas (tokens) Anti-CSRF	Medio	3588
Content Security Policy (CSP) Header Not Set	Medio	461
Hidden File Found	Medio	1
Missing Anti-clickjacking Header	Medio	451
Vulnerable JS Library	Medio	1
Cookie No HttpOnly Flag	Bajo	194
Cookie Without Secure Flag	Bajo	194
Cookie without SameSite Attribute	Bajo	201
Cross-Domain JavaScript Source File Inclusion	Bajo	2
Divulgación de la marca de hora - Unix	Bajo	1043
El servidor divulga información mediante un campo(s) de encabezado de respuesta HTTP ""X-Powered-By""	Bajo	595
Strict-Transport-Security Header Not Set	Bajo	909
X-Content-Type-Options Header Missing	Bajo	854
Content-Type Header Missing	Informativo	4
Cookie Poisoning	Informativo	7
Divulgación de información - Comentarios sospechosos	Informativo	986
Incompatibilidad de caracteres	Informativo	8
Modern Web Application	Informativo	477

Re-examine Cache-control Directives	Informativo	446
User Agent Fuzzer	Informativo	36
User Controllable HTML Element Attribute (Potential XSS)	Informativo	2065

Tabla 12. Resultados de la tabla de alerta (elaboración propia, 2022)

En este caso notamos que el tipo de alerta más común y representativo por mucho es la Ausencia de fichas (Tokens) Anti-CSRF y lo sigue Content Security Policy (CSP) Header Not Set, los dos con un nivel de riesgo Medio. A continuación, se describirán estos.

### **Ausencia de fichas (Tokens) Anti-CSRF**

La ausencia de estas puede llegar a ocasionar la falsificación de solicitudes entre sitios. Una falsificación de solicitudes entre sitios es un ataque que implica obligar a una víctima a enviar una solicitud HTTP a un destino sin su conocimiento o intención para realizar una acción como víctima. Esto sucede cuando un servidor web está diseñado para recibir una solicitud de un cliente sin ningún mecanismo para verificar que se envió intencionalmente, entonces podría ser posible que un atacante engañe a un cliente para que realice una solicitud involuntaria al servidor web que se tratará como una solicitud auténtica. Esto se puede hacer a través de una URL, carga de imágenes, XMLHttpRequest, etc. Y puede resultar en la exposición de datos o la ejecución de código no deseado. La causa subyacente es la funcionalidad de la aplicación que utiliza acciones predecibles de URL/formulario de forma repetible. La naturaleza del ataque es que CSRF explota la confianza que un sitio web tiene para un usuario. Por el contrario, cross-site scripting (XSS) explota la confianza que un usuario tiene para un sitio web. Al igual que XSS, los ataques CSRF no son necesariamente entre sitios, pero pueden serlo. La falsificación de solicitudes entre sitios también se conoce como CSRF, XSRF, ataque de un solo clic, conducción de sesión, adjunto confundido y navegación marítima.

Los ataques CSRF son efectivos en una serie de situaciones, que incluyen:

- La víctima tiene una sesión activa en el sitio objetivo.
- La víctima se autentica a través de la autenticación HTTP en el sitio de destino.
- La víctima está en la misma red local que el sitio objetivo.

CSRF se ha utilizado principalmente para realizar una acción contra un sitio objetivo utilizando los privilegios de la víctima, pero se han descubierto técnicas recientes para divulgar información al obtener acceso a la respuesta. El riesgo de divulgación de información aumenta drásticamente cuando el sitio de destino es vulnerable a XSS, porque XSS se puede usar como plataforma para CSRF, lo que permite que el ataque opere dentro de los límites de la política del mismo origen.

Las consecuencias variarán dependiendo de la naturaleza de la funcionalidad que es vulnerable al CSRF. Un atacante podría realizar efectivamente cualquier operación como víctima. Si la víctima es un administrador o usuario privilegiado, las consecuencias pueden incluir obtener un control completo sobre la aplicación web: eliminar o robar datos, desinstalar el producto o usarlo para lanzar otros ataques contra todos los usuarios del producto. Debido a que el atacante tiene la identidad de la víctima, el alcance de CSRF está limitado solo por los privilegios de la víctima.

### **Content Security Policy (CSP) Header Not Set**

CSP es una capa adicional de seguridad que ayuda a detectar y mitigar ciertos tipos de ataques, incluyendo Cross-Site Scripting (XSS) y ataques de inyección de datos.

Un objetivo principal de CSP es mitigar e informar de los ataques XSS. Los ataques XSS explotan la confianza del navegador en el contenido recibido del servidor. Los scripts maliciosos son ejecutados por el navegador de la víctima porque el navegador confía en la fuente del contenido, incluso cuando no proviene de donde parece provenir.

CSP permite a los administradores del servidor reducir o eliminar los vectores por los cuales XSS puede ocurrir especificando los dominios que el navegador debe considerar como fuentes válidas de scripts ejecutables. Un navegador compatible con CSP solo ejecutará scripts cargados en archivos de origen recibidos de esos dominios permitidos, ignorando todos los demás scripts (incluidos los scripts en línea y los atributos HTML de control de eventos).

Además de restringir los dominios desde los que se puede cargar el contenido, el servidor puede especificar qué protocolos se pueden utilizar; por ejemplo (e idealmente, desde el punto de vista de la seguridad), un servidor puede especificar que todo el contenido debe cargarse mediante HTTPS.

La configuración de la directiva de seguridad de contenido implica agregar el encabezado HTTP Content-Security-Policy a una página web y asignarle valores para controlar qué recursos puede cargar el agente de usuario para esa página.

### **Pruebas de Seguridad basado en los riesgos: Caja Gris – Caja Blanca**

Para las pruebas de seguridad se realizaron análisis del código por medio de SonarQube y Snyk. Estos son softwares que evalúan el código fuente utilizando diversas herramientas de análisis de código estático de código fuente para detectar errores. Para obtener una mejor perspectiva de lo que wordpress conlleva se realizó el análisis completo al código que está en el repositorio de wordpress, al plugin de WooComerce que es el más utilizado en puntos de ventas y por último al código del proyecto de ManosGT y se encontró lo siguiente:

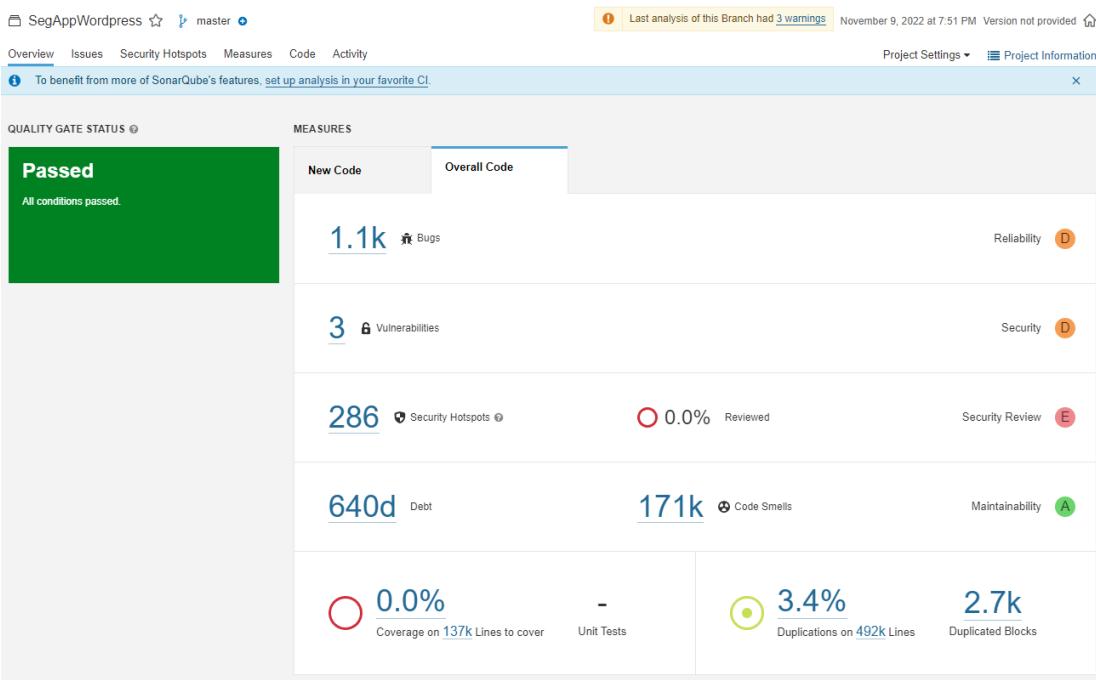


Figura 6. Pruebas de seguridad (elaboración propia, 2022)

Se puede observar que se encontraron 1.1k de bugs, 3 vulnerabilidades, 286 bloques de código que deben de ser revisados con respecto a la seguridad de la aplicación, además de 171 mil code smells que son características del código que pueden llegar a representar un problema.

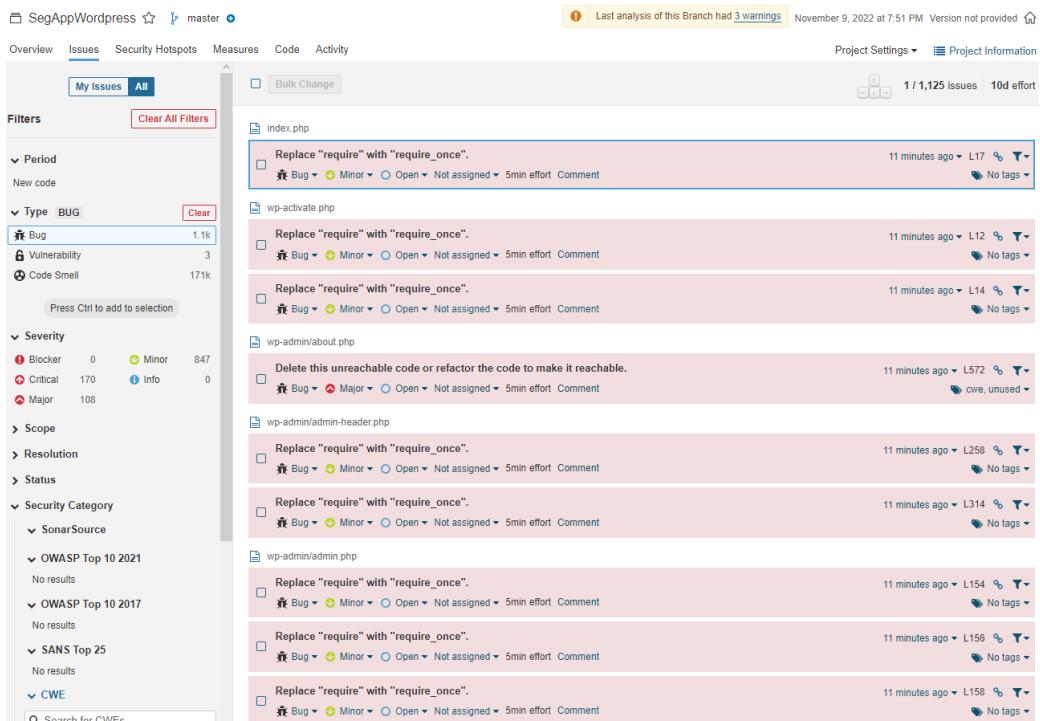


Figura 7. Resultado de pruebas de seguridad (elaboración propia, 2022).

Entre los bugs encontrados se detallan algunos y también se puede observar que del análisis realizado se cuenta con diferente severidad entre las cuales hay 170 en estado crítico que deberían de ser atendidos a la brevedad.

The screenshot shows a security analysis interface for a WordPress application. The main navigation bar includes 'Overview', 'Issues' (selected), 'Security Hotspots', 'Measures', 'Code', and 'Activity'. A message at the top right indicates 'Last analysis of this Branch had 3 warnings' on November 9, 2022, at 7:51 PM. The 'Issues' tab is active, showing a list of vulnerabilities. On the left, there are filters for 'Period', 'Type' (selected 'VULNERABILITY'), 'Severity', and 'Scope'. The 'VULNERABILITY' section shows three items:

- Enable server hostname verification on this SSL/TLS connection. (Critical, 11 minutes ago, L152)
- Enable server certificate validation on this SSL/TLS connection. (Critical, 11 minutes ago, L153)
- Enable server hostname verification on this SSL/TLS connection. (Critical, 11 minutes ago, L161)

Each item has a 'Comment' link and a 'cwe, owasp-a3, owasp-a6, owasp-m3, ...' link. The bottom right of the interface shows '1 / 3 issues' and '15min effort'.

Figura 8. Resultado de pruebas de seguridad 2 (elaboración propia, 2022).

Acá se detallan las 3 vulnerabilidades encontradas que se refiere al certificado SSL/TLS con el cual no cuenta por el momento.

The screenshot shows a security analysis interface for a WordPress application. The main navigation bar includes 'Overview', 'Issues' (selected), 'Security Hotspots' (selected), 'Measures', 'Code', and 'Activity'. A message at the top right indicates 'Last analysis of this Branch had 3 warnings' on November 9, 2022, at 7:51 PM. The 'Security Hotspots' tab is active, showing a list of 286 hotspots. On the left, there are filters for 'Assigned to me' (selected 'All'), 'Status' (selected 'To review'), and 'Overall code'. The status summary shows 'Security Hotspots Reviewed' at 0.0%.

The main area displays a list of security hotspots categorized by priority:

- HIGH:**
  - Authentication (4)
  - SQL Injection (2)
- MEDIUM:**
  - Permission (6)
  - Weak Cryptography (27)
- LOW:**
  - Encryption of Sensitive Data (65)
  - Insecure Configuration (23)
  - Log Injection (13)
  - Others (146)

One specific hotspot is highlighted in the code editor for wp-admin/includes/class-ftp.php:

```

137     $this->_can_restore(FALSE);
138     $this->_code=0;
139     $this->_message="";
140     $this->_ftp_buff_size=4096;
141     $this->_curtype=NULL;
142     $this->_SetMask(0022);
143     $this->_SetType(FTP_AUTOASCII);
144     $this->_SetTimeout(30);
145     $this->_Passive(!$this->_port_available);
146     $this->_Login("anonymous");
147     $this->_password="anon@ftp.com";
148
149     $this->_features=array();
150     $this->_OS_local=FTP_OS_UNIX;
151     $this->_OS_remote=FTP_OS_UNIX;
152     $this->_features=array();
153     if(strtoupper(substr(PHP_OS, 0, 3)) == 'WIN') $this->_OS_local=FTP_OS_WINDOWS;
154     elseif(strtoupper(substr(PHP_OS, 0, 3)) == 'MAC') $this->_OS_local=FTP_OS_MAC;
155
156     function ftp_base($port_mode=FALSE) {
157         $this->__construct($port_mode);
158     }

```

A comment box highlights the line '\$this->\_password="anon@ftp.com";' with the message: "'password' detected in this variable name, review this potentially hardcoded credential." The 'Comment' button is visible below the code editor.

Figura 9. Resultado de pruebas de seguridad 3 (elaboración propia, 2022).

De los bloques de seguridad que necesitan una revisión encontramos que entre los más altos están que estos se pueden ser problemas con relación a la autenticación y al SQL Injection.

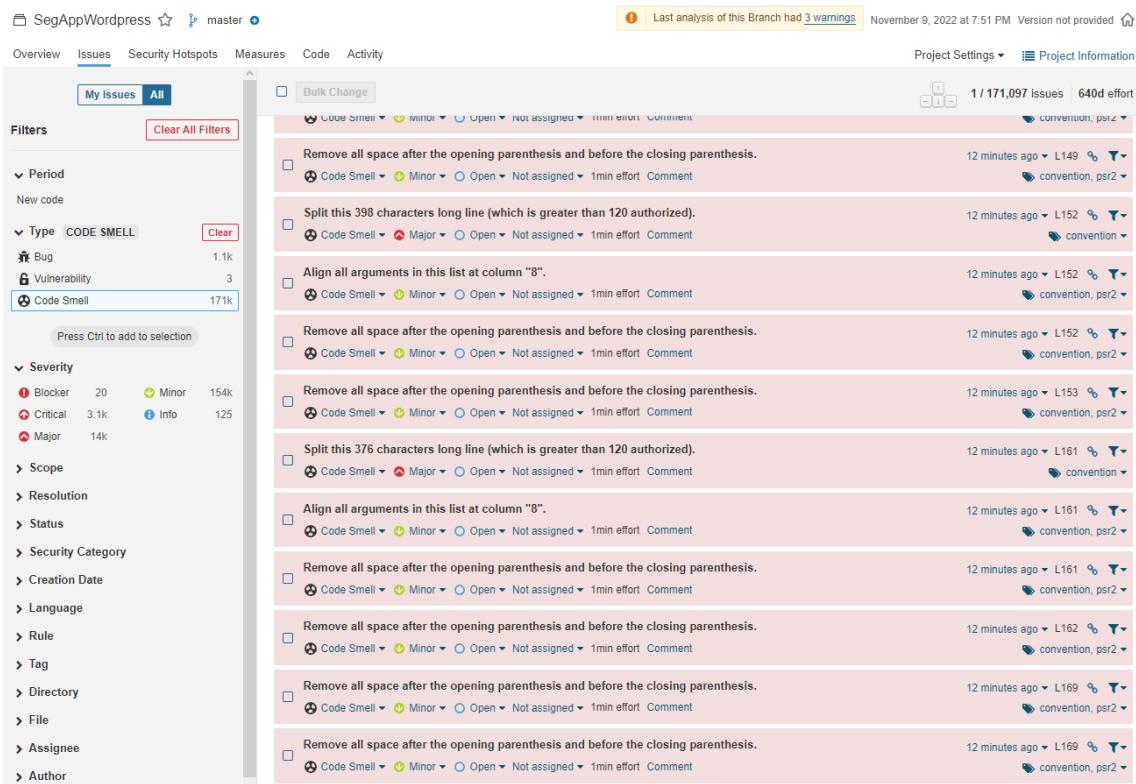


Figura 10. Resultado de pruebas de seguridad 4 (elaboración propia, 2022).

En esta parte se detallan algunos code smells que la mayoría tienen una severidad mínima pero que de igual manera se pueden resolver para que exista una mejor calidad en el código en general.

Con Snyk se realizó el mismo análisis al repositorio de Wordpress y se obtuvieron los siguientes resultados:

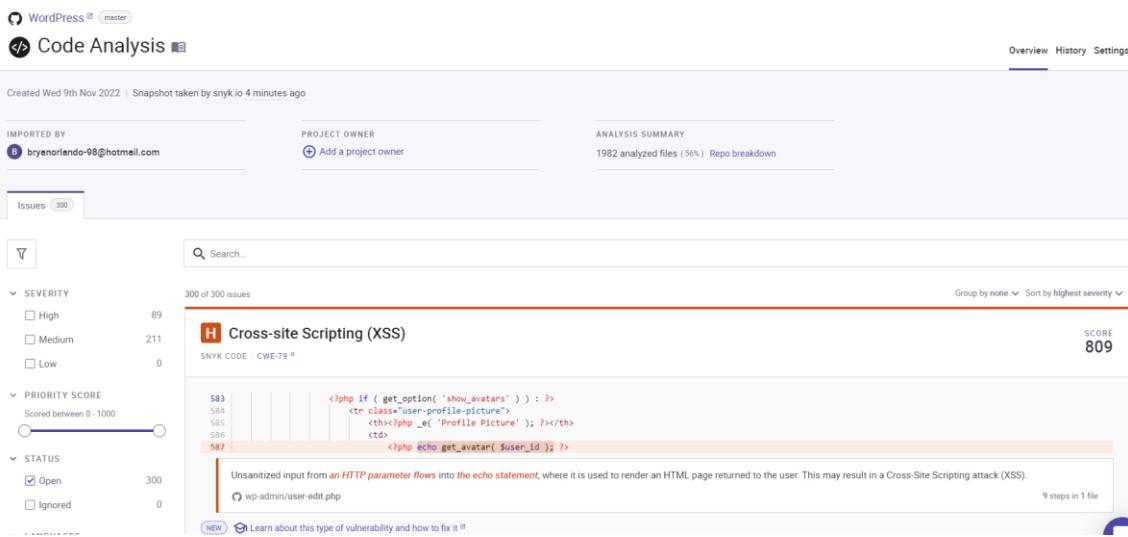


Figura 11. Code análisis. (elaboración propia, 2022).

De los resultados nos muestra el conteo de vulnerabilidades que encuentra de acuerdo con la severidad de estas, encontramos que hay 89 altas y 211 medianas que son las que más impacto tienen.

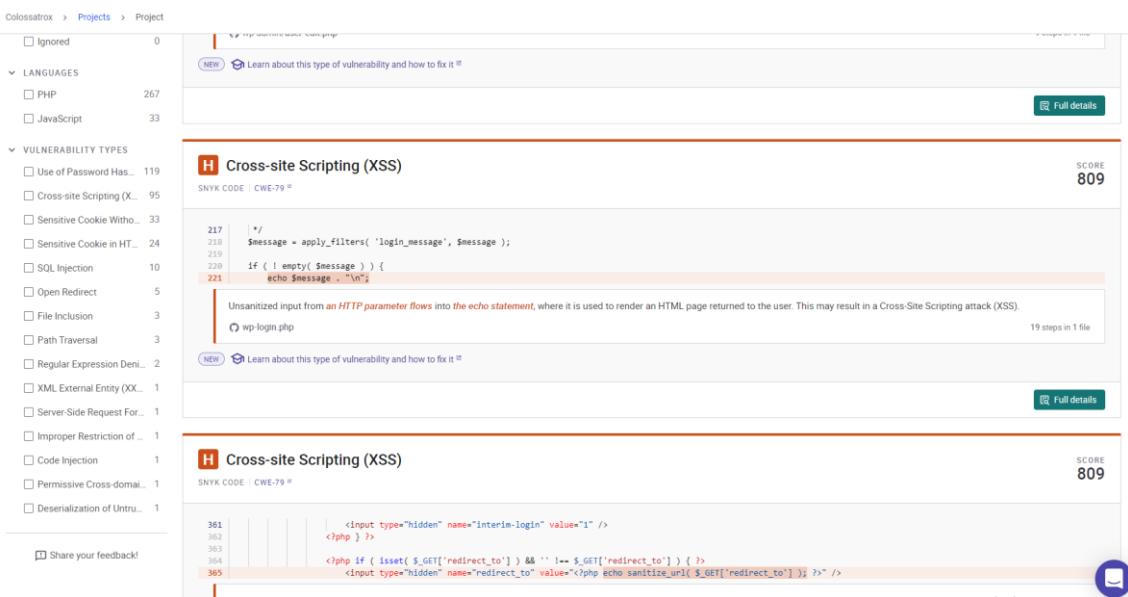


Figura 12. Code análisis 2. (elaboración propia, 2022).

Con base a lo anterior notamos que el tipo de vulnerabilidad más común tiene relación con problemas de autenticación con 199 y siguiendo está el Cross-site Scripting con 95 que son vulnerabilidades que se deben de tener en mente porque los atacantes pueden sacar provecho de estas.

Al analizar el plugin de WooCommerce nos presenta los siguientes resultados:

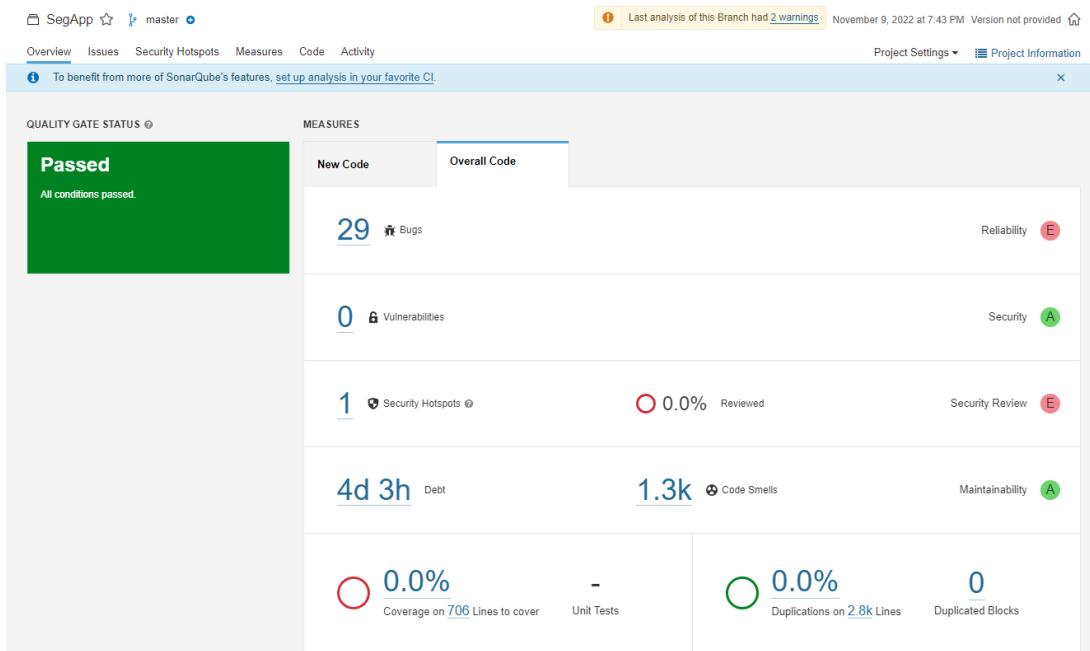


Figura 13. Plugin de WordPress (elaboración propia, 2022).

Se puede notar que en este caso el plugin individualmente no tiene mayores vulnerabilidades que pueden ser aprovechadas.

Y por último se realizó el análisis al código de ManosGT para obtener el reporte de este sitio web individualmente.

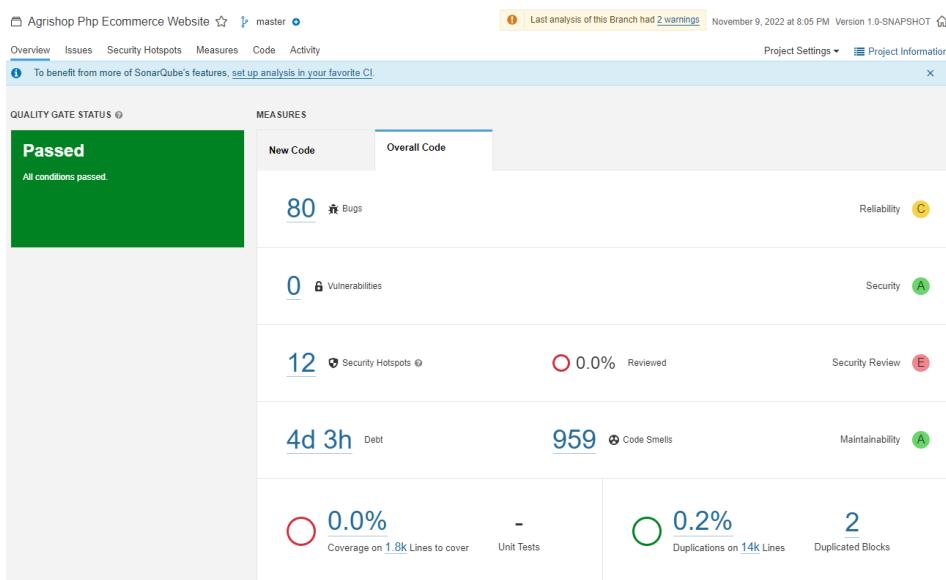


Figura 14. Plugin de WordPress 2 (elaboración propia, 2022).

En este reporte notamos que también no se cuenta con vulnerabilidades, sin embargo, tenemos 12 fragmentos de código que podrían llegar a representar un problema sino se revisa. Entre esas se detallan las siguientes:

The screenshot shows a software interface for code review. At the top, it displays the project name "Agrishop Php Ecommerce Website" and the branch "master". It indicates that the last analysis had 2 warnings and was performed on November 9, 2022, at 8:05 PM. The version is listed as "Version 1.0-SNAPSHOT". Below this, there are tabs for Overview, Issues, Security Hotspots, Measures, Code, and Activity. The "Filters" section shows "Assigned to me" selected. The "Status" dropdown is set to "To review". The "Overall code" dropdown is also visible. On the right, there's a progress bar for "Security Hotspots Reviewed" at 0.0%.

In the main content area, a message says "Make sure that using this pseudorandom number generator is safe here." It notes that using pseudorandom number generators (PRNGs) is security-sensitive (php S2245). The status is set to "TO REVIEW". The code snippet shown is:

```

92     $error_message = 'Some input is wrong, please try again.';
93
94 }
95
96 }
97
98 }
99
100 } else {
101
102     $random = mt_rand(0,999999999);
103
104     Session::add('add_product_rand', $random);
105     $template_variables['rand'] = $random;
106 }
107
108 require_once MODELS_DIR . '/Area.php';
109 require_once MODELS_DIR . '/Category.php';
110 $template_variables['areas'] = (new Area())->getAreas();
111 $template_variables['categories'] = (new Category())->getCategories();
112 $template_variables['need_activation'] = !$active;

```

A callout box highlights the line "Make sure that using this pseudorandom number generator is safe here." with a comment button.

Figura 15. Vulnerabilidades de plugins (elaboración propia, 2022).

Entre estas se tienen 3 de severidad Mediana, pero al analizar a lo que el riesgo se refiere notamos que no es un riesgo como tal, por lo que se concluye que el código y las prácticas implementadas dentro de ManosGT es de buena calidad.

En formato Gherkin se detallan algunas pruebas de diferentes casos de uso probados.

**Feature:** Registrar venta

As a empleado

Quiero registrar una venta de un cliente

**Scenario:** Registrar en el sistema venta de un cliente

**Given** Que he accedido al sistema como administrador

**When** Presiono la opción de ventas en el sidebar del lado izquierdo

**And** Presiono la opción de ventas

**And** Presiono el botón verde de Agregar en la parte superior.

**And** Presiono el desplegable de Tienda.

**And** Presiono la opción de ventas

**And** Selecciono la opción de Capital

**And** Presiono el botón de Agregar Artículos

**And** Presiono el botón de + color naranja en la columna de opciones del producto de chocolates hershey

**And** Presiono el botón de + color naranja en la columna de opciones del producto de chocolates hershey

**And** Presiono el botón de Ok o x para cerrar el mensaje

**And** Presiono el botón de cerrar del modal de productos

**And** Ingreso “**1000000**” en el campo de cantidad

**And** Presiono el botón de Ok o x para cerrar el mensaje

**And** Presiono el desplegable de Moneda

**And** Selecciono la opción de Quetzal

**And** Presiono el desplegable de Forma de Pago

And Seleccióno la opción de Tarjeta de Crédito

And Presiono el botón de Guardar

And Presiono el botón de Ok o x para cerrar el mensaje

Then Debería de haber cerrado el mensaje de Venta

Registrada

And La tabla de ventas se actualiza con la nueva compra registrada

And La cantidad del inventario de chocolates hershey disminuyó en la tienda de la capital

**Feature:** Desactivar artículo

As a empleado

Quiero desactivar un artículo

**Scenario:** Desactivar artículo para no poder realizar ventas

**Given** Que he accedido al sistema como administrador

**When** Presiono la opción de almacén en el sidebar del lado izquierdo

**And** Presiono la opción de Artículos de las opciones que desplegó

**And** Presiono el botón rojo con la x de los chocolates hershey con el toolbar que dice Inactivar

**And** Presiono Ok en el mensaje de pregunta que se muestra.

**Then** Debería de haber cerrado el mensaje de Artículo desactivado

**And** El botón que tenía la x de inactivar debería de haber cambiado a azul con un cheque y el toolbar a Activar

**And** La columna de estado de ese producto se debe mostrar en rojo y dice Desactivado

**And** El producto no debería de aparecer en el listado para compras de los clientes

**Feature:** Reporte de inventario de una tienda

As a empleado

Quiero tener el pdf del reporte del inventario de una tienda

**Scenario:** Reporte en PDF del inventario de la tienda de la capital

**Given** Que he accedido al sistema como administrador

**When** Presiono la opción de almacén en el sidebar del lado izquierdo

**And** Presiono la opción de Inventario de las opciones que desplegó

**And** Presiono el desplegable de Tienda

**And** Seleccióno la opción de Capital

**And** Presiono el botón de PDF

**Then** Debería de cambiar la información de la tabla que muestra por el inventario actual de la tienda de la capital

**And** Debería de generar un archivo PDF con la información que muestra la tabla.

**Feature:** Modificar la información de la empresa.

As a administrados

Quiero modificar información de la empresa para que se muestre en la página

**Scenario:** Modificar el logo de la empresa por el más reciente.

**Given** Que he accedido al sistema como administrador

**When** Presiono la opción de Configuración en el sidebar del lado izquierdo

**And** Presiono el botón amarillo con el lápiz de la columna de Opciones

**And** Presiono el botón de Seleccionar archivo en el campo de Logo

**And** Seleccióno la imagen del nuevo logo en mis recursos

**And** Presiono el botón de Guardar

**And** Presiono Ok o x en el mensaje que desplegó

**Then** Debería de haber cerrado el mensaje

**And** Debería de actualizar el registro con la imagen del nuevo logo

**And** En la página que visualizan los clientes se debería de visualizar el nuevo logo

**Feature:** Buscar un producto

As a cliente

Quiero buscar en la página un producto que necesito

**Scenario:** Buscar producto en el portal de clientes.

**Given** Que he accedido a la página de clientes

**When** Presiono sobre el campo de Buscar en la esquina superior izquierda

**And** Ingreso “Chocolate” en el campo de búsqueda

**And** Presiono Enter

**Then** Debería de cargar todos los productos que contengan Chocolate en el nombre, categoría o descripción

Estas mismas pruebas y otras realizadas se detallan en otro formato final que se utilizó.

<b>Test Case ID</b>	1		
<b>Priority</b>	Baja		
<b>Description</b>	Iniciar sesión en el sistema		
<b>Module</b>	Punto de Venta – Inicio de sesión		
<b>Prepared By</b>	Bryan Aguirre	<b>Date Prepared</b>	15/11/2022
<b>Reviewed / Updated</b>	Bryan Aguirre	<b>Date Reviewed</b>	15/11/2022
<b>Tested By</b>	Bryan Aguirre	<b>Date Tested</b>	15/11/2022
<b>Test Activities</b>			
Sl. No.	<b>Step Description</b>	<b>Expected Results</b>	<b>Actual Results</b>
1	Iniciar WampServer64	WampServer64 funcionando correctamente con todos los servicios levantados.	Resultado Esperado
2	Ingresar a la página local de prueba.	Despliega login para iniciar sesión en el punto de ventas	Resultado Esperado
3	Ingresar el valor de Usuario en el campo de Usuario y el de Password en el campo de Password.	Ingreso correcto al sistema, opciones de Almacén, compras, Ventas, Pagos, Recursos Humanos, Acceso, Configuración y Cerrar Sesión habilitadas, además en la esquina superior derecha debe de salir el nombre del usuario que en este caso es “Admin”.	Resultado Esperado
<b>Test Data Sets</b>			
<b>Data Type</b>	<b>Data Set 1</b>	<b>Data Set 2</b>	<b>Data Set 3</b>
String	Usuario=admin	Password=admin	
<b>Test Case Result</b>		APROBADO	

<b>Test Case ID</b>	2		
<b>Priority</b>	Baja		
<b>Description</b>	Agregar Compra		
<b>Module</b>	Punto de Venta – Compras		
<b>Prepared By</b>	Bryan Aguirre	<b>Date Prepared</b>	15/11/2022
<b>Reviewed / Updated</b>	Bryan Aguirre	<b>Date Reviewed</b>	15/11/2022
<b>Tested By</b>	Bryan Aguirre	<b>Date Tested</b>	15/11/2022
<b>Test Activities</b>			
Sl. No.	<b>Step Description</b>	<b>Expected Results</b>	<b>Actual Results</b>
1	Acceder al sistema como administrador (Test Case ID 1)	Ingreso correcto al sistema y todas las opciones habilitadas.	Resultado Esperado
2	Presionar la opción de compras en el sidebar del lado izquierdo.	Despliega las opciones de Ingresos y Proveedores	Resultado Esperado
3	Presionar la opción de ingresos	Despliega la pantalla de Compras con el listado de compras que se tiene en la base de datos.	Resultado Esperado
4	Presionar el botón verde de Agregar en la parte superior.	<ul style="list-style-type: none"> <li>* Despliega los campos de Proveedor, Tienda, Fecha, Usuario, Impuestos, Moneda y botones de Limpiar, Cancelar y Agregar Artículos.</li> <li>* Proveedor y Tienda son campos desplegables los cuales deberían de tener opciones cargadas.</li> <li>* El campo de Fecha debe de tener el valor de la fecha actual.</li> <li>* Botón de Agregar Artículos bloqueado</li> <li>* Campo de Usuario bloqueado y con valor de "Admin".</li> <li>* Botón de Guardar oculto</li> </ul>	Resultado Esperado
5	Presionar el desplegable de Proveedor	Despliega los proveedores disponibles	Resultado Esperado
6	Seleccionar el proveedor de Coca Cola	<ul style="list-style-type: none"> <li>* Campo de proveedor muestra Coca Cola</li> <li>* Bloquea desplegable de proveedor</li> </ul>	Resultado Esperado
7	Presionar el desplegable de Tienda	Despliega las tiendas disponibles	Resultado Esperado
8	Seleccionar la tienda de la Capital	<ul style="list-style-type: none"> <li>* Campo de tienda muestra Capital</li> <li>* Bloquea desplegable de Tienda</li> </ul>	Resultado Esperado

		* Desbloquea botón de Agregar Artículos	
9	Presionar botón de agregar Artículos	Despliega modal con productos disponibles a adquirir.	Resultado Esperado
10	Presionar el botón de "+" Color naranja en la columna de opciones del producto de chocolates hershey	* En la tabla de artículos se agregó 1 unidad de chocolates hershey * Muestra el botón de Guardar	Resultado Esperado
11	Presionar el botón de "+" Color naranja en la columna de opciones del producto de chocolates hershey	Muestra un mensaje de alerta que dice "Este producto ya está agregado".	Resultado Esperado
12	Presionar botón de OK o x	Mensaje de alerta se cierra	Resultado Esperado
13	Presionar botón de cerrar del modal de productos	Cierra modal de productos	Resultado Esperado
14	Cambiar la cantidad escribiendo un número o bien presionando las flechas de arriba y abajo del campo de cantidad	* Cantidad debe de cambiar * Columna de subtotal debe de cambiar por el resultado de la multiplicación de cantidad por precio de compra * Total debe de cambiar por el resultado de la suma de subtotales.	Resultado Esperado
15	Ingresar el valor de Impuesto en el campo de Impuesto	Muestra el valor ingresado en el campo de impuesto	Resultado Esperado
16	Presionar el desplegable de Moneda	Despliega las monedas disponibles	Resultado Esperado
17	Seleccionar la moneda de Quetzal	Campo de moneda muestra Quetzal	Resultado Esperado
18	Presionar botón de Guardar	* Muestra mensaje de "Compra registrada" * Proveedor recibe correo con el listado de la compra para su distribución.	No se recibió correo
19	Presionar botón de OK o x	* Mensaje de registro se cierra * Tabla de compras se actualiza con la nueva compra registrada. * La cantidad del inventario de chocolates hershey aumentó en la tienda de la capital	Resultado Esperado

**Test Data Sets**

Data Type	Data Set 1	Data Set 2	Data Set 3
Double	Impuesto=0.18		
<b>Test Case Result</b>		NO APROBADO	

<b>Test Case ID</b>	3		
<b>Priority</b>	Baja		
<b>Description</b>	Registrar venta		
<b>Module</b>	Punto de Venta – Ventas		
<b>Prepared By</b>	Bryan Aguirre	<b>Date Prepared</b>	15/11/2022
<b>Reviewed / Updated</b>	Bryan Aguirre	<b>Date Reviewed</b>	15/11/2022
<b>Tested By</b>	Bryan Aguirre	<b>Date Tested</b>	15/11/2022
<b>Test Activities</b>			
Sl. No.	<b>Step Description</b>	<b>Expected Results</b>	<b>Actual Results</b>
1	Acceder al sistema como administrador (Test Case ID 1)	Ingreso correcto al sistema y todas las opciones habilitadas.	Resultado Esperado
2	Presionar la opción de ventas en el sidebar del lado izquierdo.	Despliega las opciones de Ventas, Clientes, Tienda y Seguimiento de Venta	Resultado Esperado
3	Presionar la opción de ventas	Despliega la pantalla de Ventas con el listado de ventas que se tiene en la base de datos.	Resultado Esperado
4	Presionar el botón verde de Agregar en la parte superior.	<ul style="list-style-type: none"> <li>* Despliega los campos de Tienda, Usuario, Fecha, C/F, NIT, Cliente, Moneda, Forma de Pago y botones de Limpiar, Cancelar y Agregar Artículos.</li> <li>* Cliente, Moneda, Forma de Pago y Tienda son campos desplegables los cuales deberían de tener opciones cargadas.</li> <li>* El campo de Fecha debe de tener el valor de la fecha actual.</li> <li>* Botón de Agregar Artículos bloqueado</li> <li>* Campo de Usuario bloqueado y con valor de "Admin".</li> <li>* Botón de Guardar oculto</li> </ul>	Resultado Esperado
5	Presionar el desplegable de Tienda	Despliega las tiendas disponibles	Resultado Esperado
6	Seleccionar la tienda de la Capital	<ul style="list-style-type: none"> <li>* Campo de tienda muestra Capital</li> <li>* Bloquea desplegable de Tienda</li> <li>* Desbloquea botón de Agregar Artículos</li> </ul>	Resultado Esperado
7	Presionar botón de agregar Artículos	Despliega modal con productos disponibles en el inventario de la tienda seleccionada.	Resultado Esperado

8	Presionar el botón de “+” Color naranja en la columna de opciones del producto de chocolates hershey	* En la tabla de artículos se agregó 1 unidad de chocolates hershey * Muestra el botón de Guardar	Resultado Esperado
9	Presionar el botón de “+” Color naranja en la columna de opciones del producto de chocolates hershey	Muestra un mensaje de alerta que dice “Este producto ya está agregado”.	Resultado Esperado
10	Presionar botón de OK o x	Mensaje de alerta se cierra	Resultado Esperado
11	Presionar botón de cerrar del modal de productos	Cierra modal de productos	Resultado Esperado
12	Cambiar la cantidad escribiendo el valor de Cantidad en el campo de cantidad.	* Cantidad debe de cambiar * Muestra mensaje de que la cantidad no puede ser mayor a la de stock, se pondrá el valor máximo. * Cantidad cambia a la cantidad máxima disponible en stock * IVA muestra el resultado de la multiplicación del precio del producto por la cantidad por el 12%. * Subtotal muestra el resultado de la multiplicación de precio por cantidad * Fila de totales muestra el total de sumar todos los IVA y en la otra todos los subtotales.	Resultado Esperado
13	Presionar botón de OK o x	Mensaje se cierra	Resultado Esperado
14	Marcar casilla de C/F	* Se muestra un cheque y en color azul la casilla de CF. * Bloquea el campo de NIT * Bloquea el desplegable de cliente	Resultado Esperado
15	Presionar el desplegable de Moneda	Despliega las monedas disponibles	Resultado Esperado
16	Seleccionar la moneda de Quetzal	Campo de moneda muestra Quetzal	Resultado Esperado
17	Presionar el desplegable de Forma de Pago	Despliega las formas de pago disponibles	Resultado Esperado
18	Seleccionar la forma de pago de tarjeta de crédito	Campo de forma de pago muestra tarjeta de crédito	Resultado Esperado
17	Presionar botón de Guardar	Muestra mensaje de “Venta registrada”	Resultado Esperado
19	Presionar botón de OK o x	* Mensaje de registro se cierra * Tabla de ventas se actualiza con la nueva compra registrada. * La cantidad del inventario de chocolates hershey disminuyó en la tienda de la capital	Resultado Esperado

<b>Test Data Sets</b>			
<b>Data Type</b>	<b>Data Set 1</b>	<b>Data Set 2</b>	<b>Data Set 3</b>
Int	Cantidad=10000000000		
<b>Test Case Result</b>	APROBADO		

<b>Test Case ID</b>	4		
<b>Priority</b>	Baja		
<b>Description</b>	Mover artículos de bodega a tienda		
<b>Module</b>	Punto de Venta – Mover productos		
<b>Prepared By</b>	Bryan Aguirre	<b>Date Prepared</b>	15/11/2022
<b>Reviewed / Updated</b>	Bryan Aguirre	<b>Date Reviewed</b>	15/11/2022
<b>Tested By</b>	Bryan Aguirre	<b>Date Tested</b>	15/11/2022
<b>Test Activities</b>			
SI. No.	<b>Step Description</b>	<b>Expected Results</b>	<b>Actual Results</b>
1	Acceder al sistema como administrador (Test Case ID 1)	Ingreso correcto al sistema y todas las opciones habilitadas.	Resultado Esperado
2	Presionar la opción de Almacén en el sidebar del lado izquierdo.	Despliega las opciones de Artículos, Categorías, Promoción, Inventarios, Bodegas y Artículos de Bodega a Tienda	Resultado Esperado
3	Presionar la opción de Artículos de Bodega a Tienda	<ul style="list-style-type: none"> <li>* Despliega la pantalla de Artículos de Bodega a Tienda</li> <li>* Despliega los campos de Bodega, Tienda y botones de Limpiar, Cancelar y Agregar Artículos.</li> <li>* Bodega y Tienda son campos desplegables los cuales deberían de tener opciones cargadas.</li> <li>* Botón de Agregar Artículos bloqueado</li> <li>* Botón de Mover oculto</li> </ul>	Resultado Esperado
4	Presionar el desplegable de Bodega	Despliega las bodegas disponibles	Resultado Esperado
5	Seleccionar la bodega de Bodega Central	<ul style="list-style-type: none"> <li>* Campo de Bodega muestra Bodega Central</li> <li>* Bloquea desplegable de Bodega</li> </ul>	Resultado Esperado
6	Presionar el desplegable de Tienda	Despliega las tiendas disponibles	Resultado Esperado
7	Seleccionar la tienda de la Capital	<ul style="list-style-type: none"> <li>* Campo de tienda muestra Capital</li> <li>* Bloquea desplegable de Tienda</li> <li>* Desbloquea botón de Agregar Artículos</li> </ul>	Resultado Esperado
8	Presionar botón de agregar Artículos	Despliega modal con productos disponibles en el inventario de la bodega seleccionada.	Resultado Esperado

8	Presionar el botón de “+” Color naranja en la columna de opciones del producto de chocolates hershey	* En la tabla de artículos se agregó 1 unidad de chocolates hershey * Muestra el botón de Mover	Resultado Esperado
9	Presionar el botón de “+” Color naranja en la columna de opciones del producto de chocolates hershey	Muestra un mensaje de alerta que dice “Este producto ya está agregado”.	Resultado Esperado
10	Presionar botón de OK o x	Mensaje de alerta se cierra	Resultado Esperado
11	Presionar botón de cerrar del modal de productos	Cierra modal de productos	Resultado Esperado
12	Cambiar la cantidad escribiendo el valor de Cantidad en el campo de cantidad.	* Cantidad debe de cambiar * Muestra mensaje de que la cantidad no puede ser mayor a la de stock, se pondrá el valor máximo. * Cantidad cambia a la cantidad máxima disponible en el stock de la bodega * Fila de total muestra el total de sumar todas las cantidades.	Resultado Esperado
13	Presionar botón de OK o x	Mensaje se cierra	Resultado Esperado
14	Presionar botón de Mover	Muestra mensaje de ¿Estás seguro de mover los productos de la Bodega a la tienda elegida?	Resultado Esperado
15	Presionar botón de Ok	Muestra mensaje de Productos movidos	Resultado Esperado
16	Presionar botón de OK o x	* Mensaje se cierra * Datos de la pantalla se limpian	Resultado Esperado
17	Presionar la opción de Inventario	* Despliega la pantalla de Inventarios * Despliega el campo de Tienda y una tabla con los productos del inventario * Tienda es campo desplegable el cual debería de tener opciones cargadas.	Resultado Esperado
18	Presionar el desplegable de Tienda	Despliega las tiendas disponibles	Resultado Esperado
19	Seleccionar la tienda de la Capital	En la tabla de productos, en la fila de chocolate hershey debe de tener la cantidad que se agregó anteriormente. Si esta tienda ya tenía de este producto la cantidad que muestra debe de ser la anterior más la cantidad que se agregó anteriormente.	Resultado Esperado

**Test Data Sets**

Data Type	Data Set 1	Data Set 2	Data Set 3
Int	Cantidad=10000000000		

<b>Test Case Result</b>		APROBADO	

<b>Test Case ID</b>	5		
<b>Priority</b>	Baja		
<b>Description</b>	Agregar Trabajador		
<b>Module</b>	Punto de Venta – Trabajadores		
<b>Prepared By</b>	Bryan Aguirre	<b>Date Prepared</b>	15/11/2022
<b>Reviewed / Updated</b>	Bryan Aguirre	<b>Date Reviewed</b>	15/11/2022
<b>Tested By</b>	Bryan Aguirre	<b>Date Tested</b>	15/11/2022
<b>Test Activities</b>			
Sl. No.	<b>Step Description</b>	<b>Expected Results</b>	<b>Actual Results</b>
1	Acceder al sistema como administrador (Test Case ID 1)	Ingreso correcto al sistema y todas las opciones habilitadas.	Resultado Esperado
2	Presionar la opción de Recursos Humanos en el sidebar del lado izquierdo.	Despliega la opción de Trabajadores	Resultado Esperado
3	Presionar la opción de trabajadores	Despliega la pantalla de Trabajadores con el listado de trabajadores que se tiene en la base de datos.	Resultado Esperado
4	Presionar el botón verde de Agregar en la parte superior.	Despliega los campos de Nombre, Apellido, Fecha de Nacimiento, Fecha de Ingreso, correo, Teléfono, Dirección y botones de Cancelar y Guardar	Resultado Esperado
5	Ingresar el valor de Nombre en el campo de Nombre	Campo de Nombre muestra lo ingresado	Resultado Esperado
6	Ingresar el valor de Apellido en el campo de Apellido	Campo de Apellido muestra lo ingresado	Resultado Esperado
7	Presionar el campo de Fecha de nacimiento	Despliega un selector de fechas	Resultado Esperado
8	Seleccionar la fecha 02 de mayo de 1998	Campo de fecha de nacimiento muestra 02/05/1998	Resultado Esperado
9	Presionar el campo de Fecha de Ingreso	Despliega un selector de fechas	Resultado Esperado
10	Seleccionar la fecha 02 de mayo de 2020	Campo de fecha de ingreso muestra 02/05/2020	Resultado Esperado
11	Ingresar el valor de Correo en el campo de Correo	Campo de Correo muestra lo ingresado	Resultado Esperado

12	Ingresar el valor de Teléfono en el campo de Teléfono	Campo de Teléfono muestra lo ingresado	Resultado Esperado
13	Ingresar el valor de Dirección en el campo de Dirección	Campo de Dirección muestra lo ingresado	Resultado Esperado
12	Presionar botón de OK o x	Mensaje de alerta se cierra	Resultado Esperado
11	Presionar botón de cerrar del modal de productos	Cierra modal de productos	Resultado Esperado
17	Presionar botón de Guardar	Muestra mensaje de "Trabajador registrado"	Resultado Esperado
19	Presionar botón de OK o x	* Mensaje de registro se cierra * Tabla de trabajadores se actualiza con la nueva compra registrada.	Resultado Esperado

**Test Data Sets**

Data Type	Data Set 1	Data Set 2	Data Set 3
String	Nombre=Bryan	Apellido=Aguirre	Correo=bryanor-98@hotmail.com
String	Dirección=Mi casa		
Int	teléfono=12345678		
<b>Test Case Result</b>	APROBADO		

Por medio de Selenium IDE se realizaron algunas pruebas que se detallan a continuación:

## Agregar Compra

The screenshot shows the Selenium IDE interface with the following details:

- Project:** Calidad de Software
- Test Case:** Agregar Compra
- URL:** http://localhost:8090/PuntoDeVentaSeminario/vistas/login.php
- Test Steps:**
  - 18. ✓ click (target: css=form-group:nth-child(6) .filter-option)
  - 19. ✓ click (target: css=form-group:nth-child(6) li:nth-child(2) .text)
  - 20. ✓ select (target: id=itmMormeda, value: Quetzal)
  - 21. ✓ click (target: id=itmAgregaArt)
  - 22. ✓ mouse over (target: id=itmAgregaArt)
  - 23. ✓ mouse out (target: id=itmAgregaArt)
  - 24. ✓ click (target: id=itmAgregaArt)
  - 25. ✓ click (target: css=odd:nth-child(1) .fa-plus)
  - 26. ✓ click (target: xpath=/button[@onclick='agregarDetalle(3,\'Lapices Mongol Triangulares\',25,207)'])
  - 27. ✓ type (target: id=cantidad0, value: 2)
  - 28. ✓ click (target: id=cantidad0)
  - 29. ✓ click (target: id=itmGuardaR)
  - 30. ✓ assert text (target: css=.modal-footer > .btn-primary, value: OK)
- Log:**
  - 22. mouseOver on id=itmAgregaArt OK
  - 23. mouseOut on id=itmAgregaArt OK
  - 24. click on css=odd:nth-child(1) .fa-plus OK
  - 25. click on /button[@onclick='agregarDetalle(3,\'Lapices Mongol Triangulares\',25,207)'] OK
  - 26. click on css=close OK
  - 27. type on id=cantidad0 with value 2 OK
  - 28. click on id=cantidad0 OK
  - 29. click on id=itmGuardaR OK
  - 30. assertText on css=.modal-footer > .btn-primary with value OK OK
- Message:** 'Agregar Compra' completed successfully.

Figura 16. Prueba con Selenium (elaboración propia, 2022).

## Agregar Trabajador

The screenshot shows the Selenium IDE interface with the following details:

- Project:** Calidad de Software
- Test Case:** Agregar Trabajador
- URL:** http://localhost:8090/PuntoDeVentaSeminario/vistas/login.php
- Test Steps:**
  - 11. ✓ type (target: id=nombre, value: Bryan)
  - 12. ✓ type (target: id=apellidos, value: Aguirre)
  - 13. ✓ click (target: id=fechaNac)
  - 14. ✓ type (target: id=fechaNac, value: 1990-05-02)
  - 15. ✓ click (target: id=fechaNac)
  - 16. ✓ type (target: id=correo, value: bagupires@miung.edu.gt)
  - 17. ✓ click (target: id=correo)
  - 18. ✓ type (target: id=telefono, value: 33550978)
  - 19. ✓ click (target: id=direccion)
  - 20. ✓ click (target: id=direccion)
  - 21. ✓ type (target: id=direccion, value: Copacabana)
  - 22. ✓ click (target: id=itmGuardaR)
  - 23. ✓ assert text (target: css=.modal-footer > .btn-primary, value: OK)
- Log:**
  - 15. click on id=fechaNac OK
  - 16. type on id=fechaNac with value 2021-09-02 OK
  - 17. click on id=correo OK
  - 18. type on id=correo with value bagupires@miung.edu.gt OK
  - 19. type on id=telefono with value 33550978 OK
  - 20. click on id=direccion OK
  - 21. type on id=direccion with value Copacabana OK
  - 22. click on id=itmGuardaR OK
  - 23. Trying to find css=.modal-footer > .btn-primary OK
- Message:** 'Agregar Trabajador' completed successfully.

Figura 17. Prueba con Selenium 2(elaboración propia, 2022).

## Mover artículos de Bodega a tienda

The screenshot shows the Selenium IDE interface with a test case titled 'Mover artículos de Bodega a tienda'. The test steps are as follows:

- ✓ Agregar Compra
- ✓ Agregar Trabajador
- ✓ Mover artículos de Bodega a tienda

Test Step Details:

Command	Target	Value
✓ click	css=odd:nth-child(3).fa	
✓ mouse over	css=odd:nth-child(3).fa	
✓ mouse out	css=odd:nth-child(3).fa	
✓ click	css=modal-footer > .btn	
✓ type	id=cantidad1	2
✓ click	id=cantidad1	
✓ type	id=cantidad1	3
✓ click	id=cantidad1	
✓ click	id=btnGuardar	
✓ mouse over	id=btnGuardar	
✓ mouse out	id=btnGuardar	
✓ click	css= modal-footer > .btn-primary	
✓ assert text	css= modal-footer > .btn-primary	

Log:

24. type on id=cantidad1 with value 2 OK.
25. click on id=cantidad1 OK.
26. type on id=cantidad1 with value 3 OK.
27. click on id=cantidad1 OK.
28. click on id=btnGuardar OK.
29. mouseOver on id=btnGuardar OK.
30. mouseOut on id=btnGuardar OK.
31. click on css= modal-footer > .btn-primary OK.
32. Trying to find css= modal-footer > .btn-primary... OK.

'Mover artículos de Bodega a tienda' completed successfully.

Figura 18. Prueba con Selenium 4 (elaboración propia, 2022).

## Desactivar Venta

The screenshot shows the Selenium IDE interface with a test case titled 'Desactivar Venta'. The test steps are as follows:

- ✓ Desactivar Venta
- Eliminar Proveedor

Test Step Details:

Command	Target	Value
✓ open	http://localhost:8990/PuntoDeVentaSeminaro/vistas/login.php	
✓ set window size	801x824	
✓ click	id=usuario	
✓ type	id=usuario	admin
✓ type	id=clave	admin
✓ click	css=treeview:nth-child(4) > a	
✓ click	css=menu-open > li:nth-child(1) > a	
✓ click	css=btn-danger nth-child(2)	
✓ click	css=btn-primary nth-child(2)	
✓ assert text	css= modal-footer > .btn-primary	
✓ click	css= modal-footer > .btn-primary	
✓ click	css= content-wrapper	

Log:

5. type on id=clave with value admin OK.
6. click on css= btn OK.
7. click on css= treeview:nth-child(4) > a OK.
8. Trying to find css= menu-open > li:nth-child(1) > a... OK.
9. click on css= btn-danger nth-child(2) OK.
10. click on css= btn-primary nth-child(2) OK.
11. assertText on css= modal-footer > .btn-primary with value OK OK.
12. click on css= modal-footer > .btn-primary OK.
13. click on css= content-wrapper OK.

'Desactivar Venta' completed successfully.

Figura 19. Prueba con Selenium 5 (elaboración propia, 2022).

## Eliminar Proveedor

The screenshot shows the Selenium IDE interface with a test case titled "Eliminar Proveedor". The test steps are as follows:

Command	Target	Value
✓ click	id=usuario	
✓ type	id=usuario	admin
✓ type	id=clave	admin
✓ click	css=btn	
✓ click	linkText=Compras	
✓ click	linkText=Proveedores	
✓ click	css=fa-pencil	
✓ click	css= form-group > btn-danger	
✓ click	css= sorting_1 > btn-danger	
✓ click	css= btn-primary nth-child(2)	
✓ assert text	css= modal-footer > btn	OK
✓ click	css= modal-footer > btn	
✓ click	css= content-wrapper	

Below the table, there are input fields for "Command", "Target", "Value", and "Description". The "Log" section at the bottom contains the following entries:

- 1. click on linkText=Compras OK 10:56:13
- 2. Trying to find linkText=Proveedores... OK 10:56:14
- 3. click on css=fa-pencil OK 10:56:14
- 4. click on css= form-group > btn-danger OK 10:56:14
- 5. click on css= sorting\_1 > btn-danger OK 10:56:15
- 6. click on css= btm-primary nth-child(2) OK 10:56:15
- 7. Trying to find css= modal-footer > btn... OK 10:56:15
- 8. click on css= modal-footer > btn OK 10:56:15
- 9. click on css= content-wrapper OK 10:56:15

"'Eliminar Proveedor' completed successfully" is also listed.

Figura 20. Prueba con Selenium 6 (elaboración propia, 2022).

### 5. Casos de abuso

Un caso de abuso es un modelo de especificaciones y requisitos de seguridad utilizado de forma general o estandarizada en los procesos de desarrollo de software y es de forma directa una adaptación del modelo de Caso de Uso, el término “Caso de Abuso” fue introducido por primera vez a finales de los 90’s por John McDermott y Chris Fox, mientras trabajaban en el departamento de informática de la universidad de Virginia.

Es utilizado para definir el abuso de una aplicación con un enfoque en las interacciones entre un actor y el sistema correspondiente que generalmente es el que recibe el daño causado en asociación a uno de los actores.

Con el fin de poder realizar una evaluación de casos de abuso se procede con el análisis de los posibles escenarios básicos en el cual una actor externo o interno al proceso puede llegar a vulnerar de alguna forma el mismo iniciando con los escenarios más básicos.

Requisito de Seguridad Caso de Abuso 001	
Titulo	Como agente de amenazas externo se intenta ingresar caracteres especiales en los inputs de la aplicación.
¿Quién?	Agente de amenaza con la capacidad de ingresar al servicio e ingresar datos en las casillas disponibles dentro del sistema
¿Cuándo?	Durante el proceso de ingreso de datos
¿Dónde?	<a href="http://www.tienda.manosgt.com">http://www.tienda.manosgt.com</a>
Objetivo Inmediato	Conseguir introducir caracteres especiales para obtener información del sistema
Objetivo Final	Producir un ataque de robo de información. Por ejemplo: Ataque de tipo inyección SQL que permita leer los datos dentro de las bases de datos.
Contexto/Pro- condiciones	Se presume que el agente de amenaza se encuentra dentro de la página web, en el punto en el que se requiere ingresar datos a la misma.
Respuesta/Post- condiciones	La entrada de datos es validada en cuanto a forma y formato. Se impide dado la validación de forma el ingreso de caracteres especiales dentro del input del sistema

Tabla 13. Casos de abuso 1 (elaboración propia, 2022)

Resultado Esperado	Mensaje de error describiendo el campo invalido. valoración de la actividad dentro del registro de seguridad en casos determinados
Comentarios	Criminal Computacional. - obtención no autorizada de los datos -Acto Fraudulento
Elementos Relacionados	Amenaza #1 - Robo de información- Cross-site scripting
Cumple Resultado Esperados	Si[ ]. - No[ ]

Tabla 14. Casos de abuso 2 (elaboración propia, 2022)

Requisito de Seguridad Caso de Abuso 002	
Titulo	Como agente de amenazas externo se logra ingreso a la aplicación tras fallos de control de acceso
¿Quién?	Agente de amenaza con la capacidad de ingresar al servicio sin requerimientos de control de acceso (usuario y contraseña).
¿Cuándo?	Durante el proceso de ingreso a la aplicación
¿Dónde?	<a href="http://www.tienda.manosgt.com">http://www.tienda.manosgt.com</a>
Objetivo Inmediato	Ingresar al sistema de forma no autorizada con el fin de obtener información privilegiada

Objetivo Final	Producir un ataque de robo de información. Por ejemplo. Acceder a la información de clientes tras un acceso no regulado por usuario y contraseña
Contexto/Pro- condiciones	Se presume que el agente de amenaza se encuentra dentro del sistema y que cuenta con acceso a la información por lo que el sistema se encuentra comprometida al punto en que el intruso cuenta con acceso a los datos de usuarios
Respuesta/Post- condiciones	Es requerido el acceso con doble factor de autenticación con base en el correo electrónico de los usuarios registrados.
Resultado Esperado	Solicitud de código de autenticación secundario recibido por correo electrónico. Mensaje de error en caso de no contar con el código de autenticación secundario
Comentarios	Criminal computacional. - obtención no autorizada de los datos -Acto Fraudulento
Elementos Relacionados	Amenaza #2 - Acceso no Autorizado - Control de Acceso Roto
Cumple Resultado Esperado	Si[ ]. - No[ ]

Tabla 15. Casos de abuso 3 (elaboración propia, 2022)

Requisito de Seguridad <b>Caso de Abuso 003</b>	
Título	Como agente de amenazas externo se logra ingresar datos dentro de URL del servicio
¿Quién?	Agente de amenaza con la capacidad de alcanzar la URL del servicio
¿Cuándo?	Durante el proceso de carga del servicio web
¿Dónde?	<a href="http://www.tienda.manosgt.com">http://www.tienda.manosgt.com</a>
Objetivo Inmediato	Ingresar al sistema código HTTP con el fin de obtener información privilegiada
Objetivo Final	Producir un ataque de robo de información. Por ejemplo. Acceder a la información de clientes tras un acceso no regulado por usuario y contraseña
Contexto/Pro-condiciones	Se presume que el agente de amenaza tiene acceso al servicio des de un endpoint vía web
Respuesta/Post-condiciones	Se valida que dentro del servicio la información viaje de forma correcta desde una dirección segura bajo el uso de https
Resultado Esperado	Mensaje de error describiendo el problema dentro del servicio web. Se valora la actividad dentro del registro de seguridad en todos los casos.
Comentarios	Criminal computacional. - obtención no autorizada de los datos -Acto Fraudulento

Elementos Relacionados	Amenaza #17 - Acceso no autorizado - Inyección de HTTP
Cumple Resultado Esperado	Si[ ]. - No[ ]

Tabla 16. Casos de abuso 4 (elaboración propia, 2022)

Requisito de Seguridad Caso de Abuso 004	
Titulo	Como agente de amenazas externo intenta acceder a la aplicación con el uso de clickjacking
¿Quién?	Agente de amenaza con la capacidad de ingresar al servicio con modificaciones al código original de la página
¿Cuándo?	Durante el proceso de ingreso de datos de un real usuario determinado
¿Dónde?	<a href="http://www.tienda.manosgt.com">http://www.tienda.manosgt.com</a>
Objetivo Inmediato	Conseguir obtener la información de usuarios incluyendo sus credenciales o datos personales
Objetivo Final	Producir un ataque de robo de información. Por ejemplo: Adquirir el usuario y contraseña de un usuario para posteriormente modificar o hacer uso de sus credenciales
Contexto/Pro-condiciones	Se presume que el agente de amenaza ha comprometido el sistema al grado de poder sustituir el envío de información de parte de este

Respuesta/Post-condiciones	Detectar desde la aplicación con el uso de JavaScript el uso de extensiones de navegadores que puedan modificar el código original del sistema
Resultado Esperado	Mensaje de error de certificado de privacidad indicando el complemento comprometido. Se valorala actividad dentro del registro de seguridad en todas las oportunidades
Comentarios	Criminal Computacional. - obtención no autorizada de los datos -Acto Fraudulento
Elementos Relacionados	Amenaza #18 - Robo de información- Clicjacking
Cumple Resultado Esperado	Si[ ]. - No[ ]

Tabla 17. Casos de abuso 5 (elaboración propia, 2022)

Requisito de Seguridad Caso de Abuso 005	
Titulo	Como agente de amenazas externo se logra inyectar Código PHP al servicio web
¿Quién?	Agente de amenaza con la capacidad de ingresar al servicio
¿Cuándo?	Durante el proceso de carga del servicio web
¿Dónde?	<a href="http://www.tienda.manosgt.com">http://www.tienda.manosgt.com</a>

Objetivo Inmediato	Ingresar al sistema código PHP con el fin de obtener información privilegiada
Objetivo Final	Producir un ataque de robo de información. Por ejemplo. Un ataque de tipo inyección PHP que le permita leer los datos de la base de datos del entorno de producción
Contexto/Pro -condiciones	Se presume que el agente de amenaza tiene acceso al servicio des de un endpoint vía web y tiene acceso al ingresar datos del sistema (en este caso en particular en el control de autenticación)
Respuesta/P ost-condiciones	Se establecen en la medida de lo posible un patrón de diseño donde el front end se encuentra separado del backend con la finalidad de no poder ejecutar comandos PHP fuera de la aplicación.
Resultado Esperado	Mensaje de error describiendo el problema dentro del servicio web. Se valora la actividad dentro del registro de seguridad en todos los casos.
Comentarios	Criminal Computacional. - obtención no autorizada de los datos -Acto Fraudulento
Elementos Relacionados	Amenaza #25 - Acceso no autorizado - PHP code Inyection
Cumple Resultado Esperado	Si[ ]. - No[ ]

Tabla 18. Casos de abuso 6 (elaboración propia, 2022)

## Conclusiones

Al finalizar la evaluación de los riesgos de la empresa ManosGT se puede concluir en que los resultados reflejaron que existe una gran cantidad de riesgos que la empresa deberá solucionar en el menor tiempo posible.

Al ser una empresa dedicada al e-commerce, la empresa deberá mantener un constante control respecto a la seguridad de sus clientes, puesto que, al realizar transacciones económicas en el sitio, representa un atractivo para los ciber delincuentes.

Si bien no es posible tener una seguridad al 100% en todos los aspectos, la empresa ManosGT ha demostrado tener el interés de mitigar la mayoría de los riesgos que no representan un costo que no esté contemplado. Para los riesgos que necesitan hacer contrataciones de servicios, comprar algún producto digital o demás, se estarán evaluando en el presupuesto del 2023.

## Recomendaciones

Se le ha recomendado a la empresa ManosGT que la seguridad de sus activos debe ser una prioridad, puesto que, al mantener los datos seguros de sus usuarios, podrán generar confianza hacia los clientes.

También se les ha hecho la recomendación que, por cada cambio realizado en la infraestructura del sitio, o en el sitio se deberá realizar nuevamente una evaluación de los riesgos, con la finalidad de mantener siempre protegidos los sistemas.

Al mismo tiempo se les ha recomendado segmentar los roles de los empleados de IT con el fin de que cada empleado sea responsable de la seguridad de ciertos activos, así pues, el trabajo se distribuirá y no recaerá sobre una sola persona o sobre un grupo reducido de personas.

Universidad Mariano Gálvez de Guatemala

Facultad de Ingeniería de Sistemas de Información

Maestría en Seguridad Informática

Planeación de la continuidad del negocio basado en TIC

Ing. Cristian Waldemar Rosales Meléndez

*Cristian Rosales*

Nota  
40/40  
100/100

CRISTIAN WALDEMAR Firmado digitalmente por CRISTIAN  
ROSALES MELÉNDEZ WALDEMAR ROSALES MELÉNDEZ  
Fecha: 2023.03.29 16:28:37 -06'00'

### **Plan de Continuidad de negocios para servicios bancarios**



1293-17-646 Bryan Orlando Aguirre Sagastume

1293-17-1255 Ricardo Alejandro Pérez Rodríguez

1293-16-13892 Dora Lucrecia Ordoñez Pérez

1293-16-14277 Ana Kristina Cifuentes Castañeda

1293-15-10369 Jonathan Renato del Cid Juárez

1293-16-16201 Juan José Jolón Granados

Guatemala 23 de marzo del 2023

## Índice

Introducción.....	1
Diagrama Jerárquico de la Organización .....	2
Diagramas de procesos críticos .....	3
Actualización diaria de tipo de cambio .....	3
Solicitud y generación de tokens para banca en línea .....	5
Alta disponibilidad de banca en línea .....	7
Validación de cuentas ACH y propias .....	9
BIA.....	11
Plan DRP.....	14
Propósito.....	14
Objetivo.....	14
Ámbito de la aplicación .....	14
Políticas del Plan .....	16
Autorización y Divulgación del Plan: .....	17
Autorización:.....	17
Divulgación: .....	17
Evaluaciones del Plan: .....	18
Reporte de resultados de evaluación del Plan:.....	19

Políticas Específicas.....	19
Declaración de Desastre: .....	20
Estructura para la administración y operación del plan .....	21
Administración .....	21
Junta Directiva .....	21
Comité de riesgos y continuidad del negocio.....	23
Gerencia Informática .....	25
Líder de evaluación .....	28
Líder de Restauración .....	29
Líder de Seguridad de la Información .....	31
Mapa de Interdependencia .....	32
Estrategias de recuperación de desastres .....	42
Procesos operativos de recuperación de desastres .....	44
Proceso de diagnóstico y activación .....	44
Fase de restauración.....	45
Lista de contactos claves .....	46
Actualizaciones.....	46
Detalles del equipo .....	46
Términos y definiciones .....	47

Proveedores críticos.....	50
Documentos Relacionados .....	50
Mapa de distribución Eléctrica y Enfriamiento de Datos .....	51
Mapa de red de centro de datos .....	52
Mapa de Red Banca Electrónica .....	53
Recuperación Banca Electrónica.....	56
Equipo de respuesta .....	56
Procedimientos de detección y notificación .....	56
Procedimientos de recuperación .....	56
Procedimientos de comunicación con los usuarios .....	57
Procedimientos de entrenamiento y simulación.....	57
Actualización y revisión del plan de recuperación .....	58
Instructivo de recuperación aplicación/base de datos banca electrónica	59
Análisis de Riesgo .....	63
Evaluación del riesgo.....	67
Matriz de Riesgo .....	71
Plan de tratamiento.....	77
¿Qué estándar del sistema de Gestión de Continuidad del Negocio implementaría? .....	83

Comprensión del contexto de la organización .....	83
Liderazgo y compromiso .....	83
Planificación.....	84
Implementación .....	84
Evaluación de la capacidad de respuesta .....	84
Mejora continua .....	85
Ciclo de vida .....	86
Planificar .....	86
Hacer .....	87
Verificar .....	87
Actuar.....	87
Administración de la continuidad de negocio .....	88
¿Cuáles Estrategias implementaría para? .....	94
Negocio:.....	94
Tecnología: .....	95
Acuerdos con Proveedores.....	97
Conclusiones.....	102
Referencias bibliográficas .....	103

## Índice de Tablas

Tabla 1. Escala de impacto.....	11
Tabla 2. Tipo de cambio bancario .....	12
Tabla 3. Generación de token de seguridad .....	12
Tabla 4. validación de cuentas ACH y cuentas propias .....	13
Tabla 5. Alta disponibilidad para la banca en línea. ....	13
Tabla 6. Procesos y sus componentes involucrados.....	15
Tabla 7. Tipo de cambio bancario .....	33
Tabla 8. Generación de token de seguridad .....	34
Tabla 9. Validación de cuentas ACH y cuentas propias .....	35
Tabla 10. Alta disponibilidad para la banca en línea .....	37
Tabla 11. Estrategias de recuperación de desastres .....	42
Tabla 12. Listado de contactos.....	46
Tabla 13. Actualizaciones del DRP .....	46
Tabla 14. Detalles de los equipos utilizados por la empresa .....	46
Tabla 15. Servicios de proveedores críticos .....	50
Tabla 16. Documentos relacionados con el DRP .....	50
Tabla 17. Escenarios de fallos.....	58
Tabla 18. Inventario de servidores de centros de datos.....	60
Tabla 19. Información de red de servidores de centros de datos .....	62
Tabla 20. Tabla de riesgos .....	64
Tabla 21. Procesos bancarios de mayor riesgo.....	68
Tabla 22. Cálculo de probabilidad .....	69

Tabla 23. Cálculo de impacto .....	69
Tabla 24. Matriz de riesgo de activos.....	72
Tabla 25. Plan de tratamiento.....	77
Tabla 26. Modelo de capacitación.....	91
Tabla 27. Cronograma de ejecución .....	93
Tabla 28. Tabla indicadora de incumplimiento del servicio .....	98

### **Índice de figuras**

Figura 1. Diagrama jerárquico .....	2
Figura 2. Actualización diaria de tipo de cambio .....	3
Figura 3. Proceso de envío y validación de token.....	5
Figura 4. Alta disponibilidad de banca en línea .....	7
Figura 5. Validación de cuentas ACH y propias .....	9
Figura 6. Estructura organizacional del plan de desastres .....	21
Figura 7. Mapa de Interdependencia tipo de Cambio Bancario .....	38
Figura 8. Mapa de Interdependencia Generación de Token de Seguridad .	39
Figura 9. Mapa de Interdependencia Validación de Cuentas ACH y Cuentas Propias .....	40
Figura 10. Mapa de Interdependencia Alta disponibilidad para la banca en línea .....	41
Figura 11. Proceso de diagnóstico y activación .....	44
Figura 12. Proceso de restauración .....	45
Figura 13. Mapa de distribución eléctrica y enfriamiento de datos .....	51
Figura 14. Enfriamiento de datos .....	52

Figura 15. Mapa de red general .....	52
Figura 16. Mapa de red específica .....	53
Figura 17. IP'S usadas en el sistema .....	54
Figura 18. Mapa de conexión a servidores.....	55
Figura 19. Mapa de equipos (Racks) en Centro de Datos .....	55
Figura 20. Ciclo de vida del estándar 22301 .....	86
Figura 21. Plan de concientización de usuarios .....	88
Figura 22. Fases del plan de concientización .....	89

## Introducción

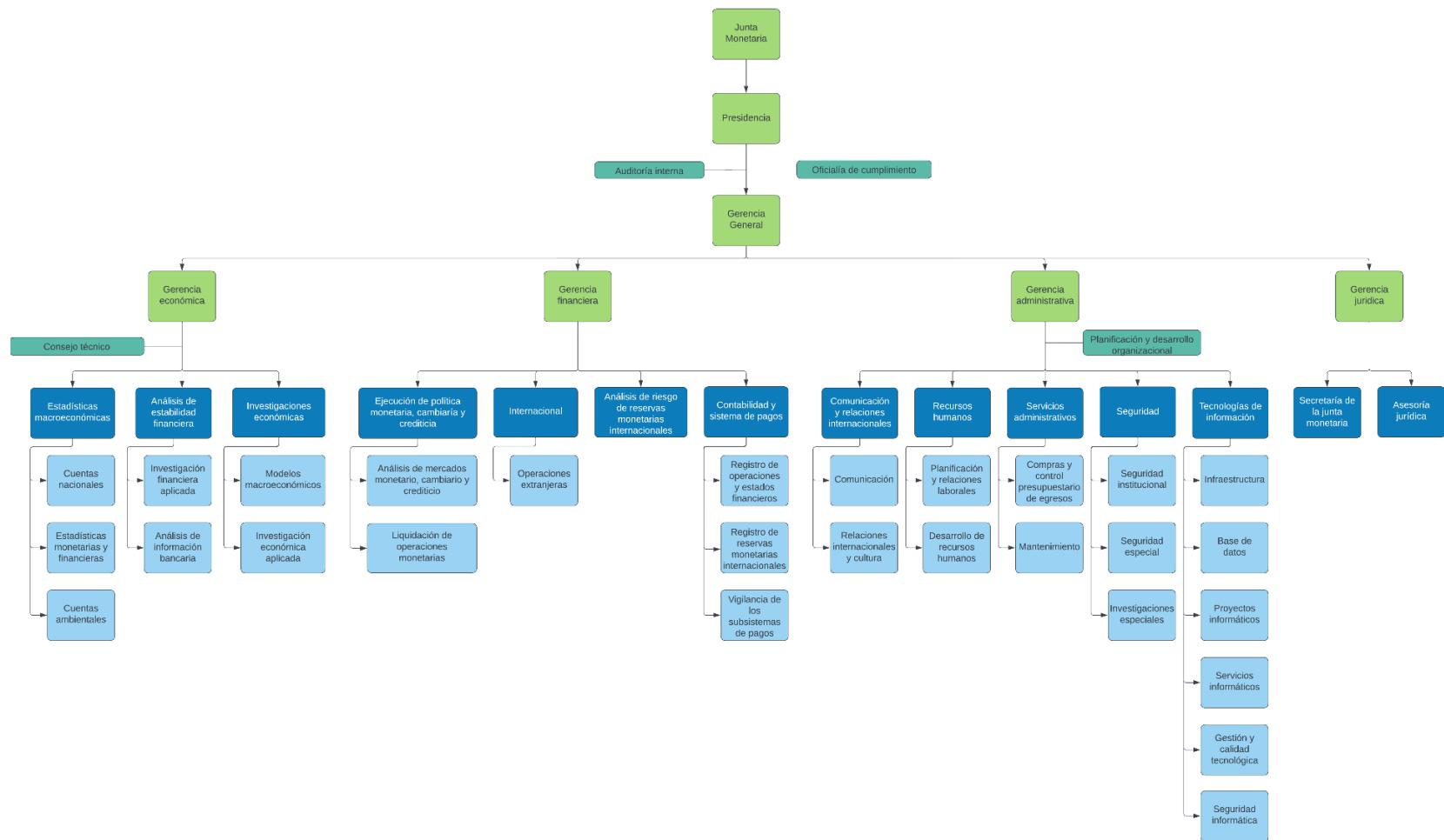
En la actualidad en todas las empresas es necesario contar con planes de continuidad del negocio esto porque deben de estar preparadas para cualquier situación en la cual ponga en riesgo la actividad económica de la misma, ya sean estas situaciones tales como: pandemias, robo de información, ataques cibernéticos o desastres naturales. También se considera que es importante contar con estos planes a causa de la creciente competitividad que hay entre las organizaciones y a las demandas de los clientes que son cada vez más exigentes.

El sector bancario de Guatemala no es la excepción para contar con estos planes de continuidad del negocio, debido a la importancia que tienen en la economía guatemalteca y a lo expuesto que están deben de estar preparados para cualquier situación que les pueda ocurrir, por lo tanto deben de tener de una forma clara todos los riesgos, amenazas, vulnerabilidades con los cuales se pueden enfrentar y sobre estos incidentes que se podrían presentar deberán de contar con un plan de trabajo para la recuperación y restauración de los sistemas.

Por lo cual se lograron detectar cuatro procesos que se consideraron como críticos para una entidad bancaria, sobre estos procesos se detectaron las posibles situaciones en las cuales pueda ocurrir un incidente y que causen grandes pérdidas económicas y al mismo tiempo se realizó el plan de continuidad del negocio para que a pesar de cualquier inconveniente en estos procesos, el negocio pueda seguir funcionando y siendo un buen competente ante la industria.

## Diagrama Jerárquico de la Organización

**Figura 1.** Diagrama jerárquico

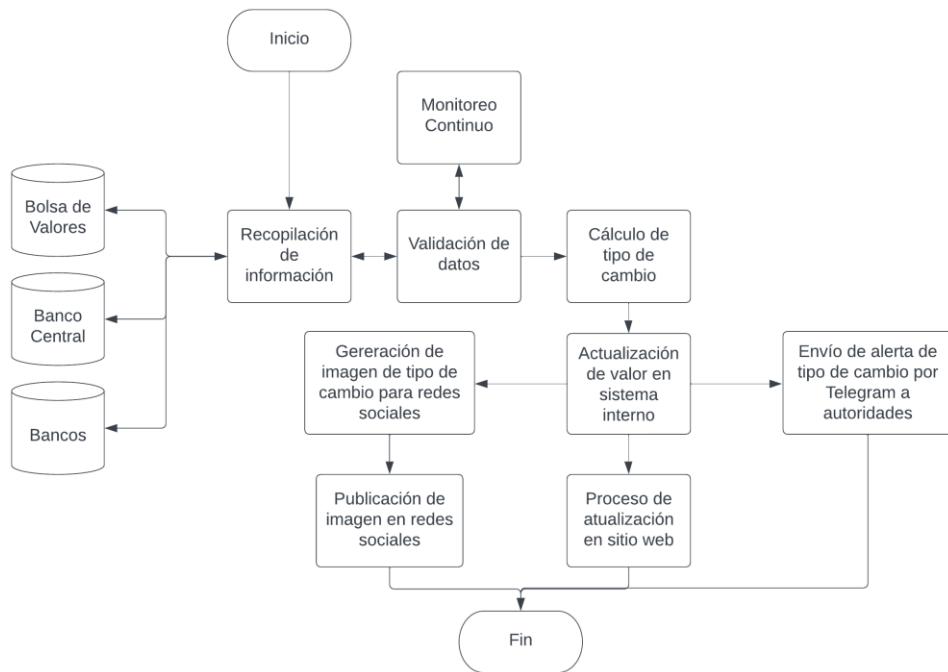


Nota. Diagrama de la organización jerárquica de la empresa. Fuente: elaboración propia.

## Diagramas de procesos críticos

### Actualización diaria de tipo de cambio

**Figura 2.** Actualización diaria de tipo de cambio



Nota. Diagrama que comprende cómo se encuentran los procesos críticos del banco. Fuente: elaboración propia.

Diariamente el banco es responsable de establecer el tipo de cambio del dólar. Como primer paso el banco recopila información del tipo de cambio del dólar de varias fuentes, como la Bolsa de Valores de Guatemala, bancos centrales y otras instituciones financieras, luego, se valida la información recopilada para asegurarse de que sea precisa y actualizada, después, se utiliza una fórmula para calcular el tipo de cambio del dólar basado en la información recopilada. Una vez que se ha calculado el tipo de cambio, se actualiza en el sistema interno del banco. Luego, El

banco publica el tipo de cambio del dólar en su sitio web, en sus sucursales y en otros canales de comunicación, como las redes sociales y la prensa.

El banco monitorea continuamente el tipo de cambio del dólar y realiza actualizaciones según sea necesario para mantener a los clientes informados y actualizados sobre las fluctuaciones en el mercado de divisas.

Las dependencias involucradas en este proceso son las siguientes:

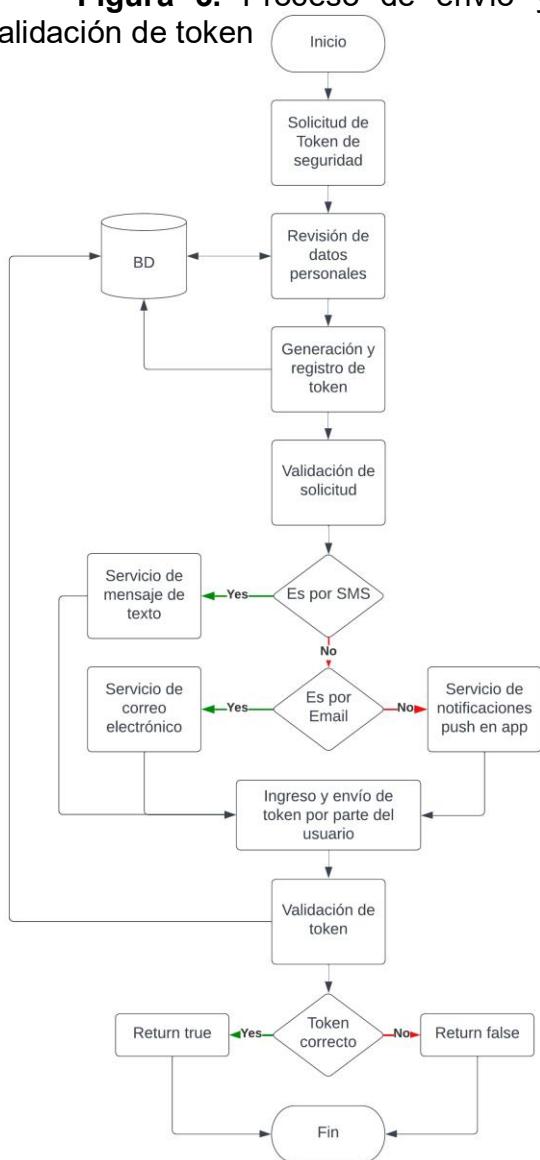
- Operaciones extranjeras
- Cuentas nacionales
- Registro de reservas monetarias internacionales
- Vigilancia de los subsistemas de pagos
- Comunicación
- Infraestructura
- Base de datos
- Seguridad Informática

## Solicitud y generación de tokens para banca en línea

El proceso de generación, revisión y uso de tokens para banca en línea es crucial para garantizar la seguridad de las transacciones financieras realizadas a través de internet. A continuación, se describe este proceso:

La institución financiera genera un token para cada cliente que desea utilizar banca en línea. El token puede ser por medio de SMS, Email o notificaciones push

**Figura 3.** Proceso de envío y validación de token



La institución financiera a la aplicación. Luego, se entrega el token al cliente y se proporciona instrucciones claras sobre cómo utilizarlo para acceder a la banca en línea. El cliente registra el token en la plataforma. Para hacerlo, debe proporcionar información personal y verificar su identidad.

La institución financiera valida que el token registrado por el cliente sea correcto y le notifica en la aplicación, además, se revisa regularmente el funcionamiento del token para garantizar su integridad y seguridad. Si se detecta algún problema, se toman medidas para solucionarlo.

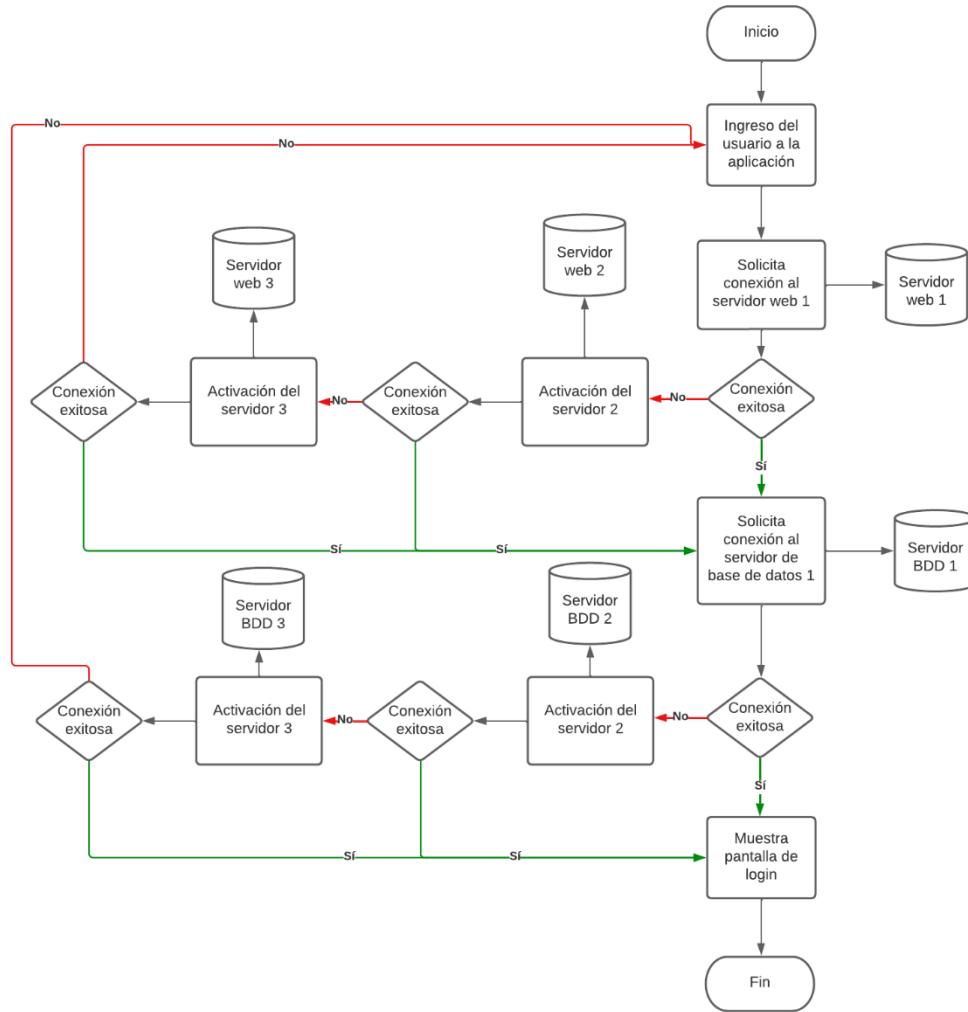
Nota. Diagrama que comprende cómo se encuentran los procesos críticos del banco.

Las dependencias involucradas en este proceso son las siguientes:

- Infraestructura
- Base de datos
- Seguridad Informática
- Proyectos informáticos
- Gestión y calidad tecnológica

## Alta disponibilidad de banca en línea

**Figura 4.** Alta disponibilidad de banca en línea



Nota. Diagrama que comprende cómo se encuentran los procesos críticos del banco. Fuente: elaboración propia.

Mantener la disponibilidad es importante ya que garantiza a los usuarios que podrán utilizar la banca en línea en cualquier momento que sea necesario, incluso en casos de ataques, desperfecto de algún equipo interno o interrupciones. El banco utiliza servidores web y de base de datos redundantes.

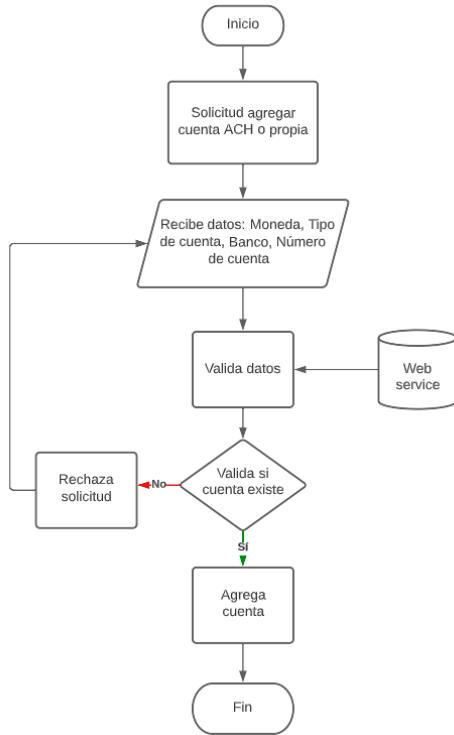
El proceso inicia cuando el usuario ingresa a la aplicación y levanta una solicitud para conectarse al servidor web 1, si la conexión no es exitosa, de forma automática se activará el servidor web 2, si la conexión no es exitosa, de forma automática se activará el servidor web 3 y si la conexión aún no fuere exitosa, regresará a la pantalla de inicio, en cualquiera de los tres casos si la conexión si es exitosa el proceso levanta una solicitud de conexión al servidor de base de datos 1, si la conexión no es exitosa, de forma automática se activará el servidor de BDD 2, si la conexión no es exitosa, de forma automática se activará el servidor de BDD 3 y si la conexión aún no fuere exitosa, regresará a la pantalla de inicio.

Las dependencias involucradas en este proceso son las siguientes:

- Infraestructura
- Base de datos
- Seguridad Informática
- Proyectos informáticos
- Gestión y calidad tecnológica

## Validación de cuentas ACH y propias

**Figura 5.** Validación de cuentas ACH y propias



Nota. Diagrama que comprende cómo se encuentran los procesos críticos del banco. Fuente: elaboración propia

El proceso de validar si una cuenta de otro banco o del mismo banco está ingresada correctamente para agregarla al perfil de un cliente únicamente se realiza cuando el cliente lo solicite a través de la banca en línea, ya sea por la página web o por la aplicación. El primer paso es generar la solicitud, luego ingresar los datos que generalmente se solicitan como moneda, tipo de cuenta, banco y número de cuenta para que el sistema pueda ir a consultar al web service del banco colocado y validar si realmente la cuenta ingresada sí existe en la base de datos, si el sistema logra encontrar la cuenta en la base la agrega al perfil del cliente, si la validación no

es exitosa rechaza la solicitud y regresa al panel inicial donde solicita ingresar los datos.

Las dependencias involucradas en este proceso son las siguientes:

- Infraestructura
- Base de datos
- Seguridad Informática
- Proyectos informáticos
- Gestión y calidad tecnológica
- Relaciones interbancarias

## BIA

Para el análisis de impacto del negocio se ha realizado sobre los cuatro procesos bancarios que se consideraron como críticos, los cuales son: Proceso de tipo de cambio, generación de token de seguridad para banca en línea, alta disponibilidad de banca en línea y validación de cuentas ACH y cuentas propias.

Se ha definido en una escala del 1 al 5 el impacto que tendrá cada actividad si no se logra solucionar en el tiempo esperado, la escala es la siguiente:

**Tabla 1.** Escala de impacto

Escala	Descripción
1	Muy Bajo
2	Bajo
3	Moderado
4	Alto
5	Muy Alto

Nota. Proporciona la escala considerada de impacto para los siguientes cálculos. Fuente: elaboración propia.

Siendo 3 el valor moderado sobre el cual se definirá el RTO de la actividad/proceso.

**Tabla 2.** Tipo de cambio bancario

Servicio: Tipo de cambio bancario									
Actividad	Tipo	< 6 hrs	< 12 hrs	< 24 hrs	< 2 días	RTO	RPO	MTD	Activos afectados
Disponibilidad de información	Legal	0	0	0	0	12 hrs	10 hrs	10 hrs	Agencias bancarias
	Financiero	1	1	2	3				
	Reputacional	1	2	2	3				
	Disponibilidad	2	3	4	5				
Actualización diaria	Legal	0	0	0	0	24 hrs	18 hrs	18 hrs	Clientes, agentes bancarios
	Financiero	1	1	2	3				
	Reputacional	1	1	1	1				
	Disponibilidad	1	2	3	3				
Consumo webservice	Legal	0	0	0	0	24 hrs	18 hrs	18 hrs	Clientes, agentes bancarios, agencia bancaria
	Financiero	1	1	1	1				
	Reputacional	1	1	1	1				
	Disponibilidad	1	2	3	3				
Monitoreo	Legal	0	0	0	0	2 días	1 día	18 hrs	Agencias bancarias
	Financiero	0	0	0	0				
	Reputacional	1	2	2	3				
	Disponibilidad	1	1	1	2				

Nota. Descripción acerca sobre el tipo de cambio bancario en horas y días.

Fuente: elaboración propia.

**Tabla 3.** Generación de token de seguridad

Servicio: Generación de token de seguridad para la banca en línea									
Actividad	Tipo	< 6 horas	< 12 horas	< 24 horas	< 2 días	RTO	RPO	MTD	Activos afectados
Disponibilidad de token	Legal	1	1	1	2	6 hrs	5 hrs	3 hrs	Clientes
	Financiero	2	3	3	5				
	Reputacional	3	3	4	5				
	Disponibilidad	3	4	5	5				
Ingreso aplicación	Legal	1	2	2	2	6 hrs	5 hrs	2 hrs	Clientes
	Financiero	2	3	3	5				
	Reputacional	3	3	4	5				
	Disponibilidad	3	4	5	5				
Transferencia móvil	Legal	1	1	1	2	6 hrs	4 hrs	4 hrs	Clientes
	Financiero	3	4	5	5				
	Reputacional	2	3	3	4				
	Disponibilidad	3	4	5	5				
Adición de cuentas ACH	Legal	0	0	0	0	24 hrs	18 hrs	12 hrs	Clientes
	Financiero	1	1	2	2				
	Reputacional	1	2	2	3				
	Disponibilidad	2	2	3	3				
Creación de cuentas nueva	Legal	0	0	0	0	24 hrs	20 hrs	15 hrs	Clientes
	Financiero	1	1	2	3				
	Reputacional	1	2	2	3				
	Disponibilidad	1	2	3	3				
Pagos	Legal	1	2	3	4	6 hrs	4 hrs	3 hrs	Clientes, gerencias, proveedores
	Financiero	3	4	5	5				
	Reputacional	2	2	3	4				
	Disponibilidad	2	3	4	4				

Nota. Descripción acerca sobre el tipo de cambio bancario en horas y días.

Fuente: elaboración propia.

**Tabla 4. validación de cuentas ACH y cuentas propias.**

Servicio: Validación de cuentas ACH y cuentas propias de banco									
Actividad	Tipo	< 6 horas	< 12 horas	< 24 horas	< 2 días	RTO	RPO	MTD	Activos afectados
Disponibilidad de validación	Legal	1	1	2	3	6 hrs	5 hrs	3 hrs	Aplicación móvil y web.
	Financiero	3	4	5	5				
	Reputacional	3	3	4	4				
	Disponibilidad	2	3	3	4				
Consumo webservice	Legal	0	0	0	0	6 hrs	4 hrs	3 hrs	Aplicación móvil y web.
	Financiero	3	3	4	5				
	Reputacional	2	2	3	4				
	Disponibilidad	3	3	5	5				
Transferencia bancaria	Legal	1	1	2	3	6 hrs	4 hrs	2 hrs	Clientes.
	Financiero	3	4	5	5				
	Reputacional	2	2	3	3				
	Disponibilidad	2	3	4	4				
Adición de cuentas ACH	Legal	0	0	0	0	12 hrs	10 hrs	8 hrs	Clientes, finanzas.
	Financiero	2	4	5	5				
	Reputacional	2	3	4	4				
	Disponibilidad	2	2	3	3				
Servicio de proveedor	Legal	0	0	0	0	12 hrs	8 hrs	6 hrs	Interfaces, servidores
	Financiero	2	3	3	4				
	Reputacional	1	2	2	3				
	Disponibilidad	2	2	3	3				

Nota. Describe el servicio de la validación de cuentas. Fuente: elaboración propia.

**Tabla 5. Alta disponibilidad para la banca en línea.**

Servicio: Alta disponibilidad para la banca en línea									
Actividad	Tipo	< 6 horas	< 12 horas	< 24 horas	< 2 días	RTO	RPO	MTD	Activos afectados
Disponibilidad de aplicación	Legal	1	2	2	3	6 hrs	5 hrs	4 hrs	Clientes, finanzas
	Financiero	3	4	5	5				
	Reputacional	2	3	4	4				
	Disponibilidad	3	3	4	5				
Ingreso aplicación	Legal	0	0	0	0	6 hrs	4 hrs	3 hrs	Clientes
	Financiero	3	3	4	5				
	Reputacional	2	2	3	4				
	Disponibilidad	3	3	4	4				
Monitoreo	Legal	0	0	0	0	2 días	32 hrs	18 hrs	Servidores
	Financiero	1	1	2	3				
	Reputacional	1	1	1	2				
	Disponibilidad	0	0	0	0				
Funcionamiento de servidores web redundantes	Legal	0	0	0	0	12 hrs	8 hrs	6 hrs	Servidores
	Financiero	2	3	3	5				
	Reputacional	1	2	3	3				
	Disponibilidad	2	2	3	3				
Funcionamiento de servidores base de datos redundantes	Legal	0	0	0	0	12 hrs	8 hrs	6 hrs	Servidores
	Financiero	2	3	3	5				
	Reputacional	1	2	3	3				
	Disponibilidad	2	2	3	3				
Servicio de proveedor	Legal	0	0	0	0	12 hrs	7 hrs	5 hrs	Interfaces, servidores
	Financiero	1	2	2	3				
	Reputacional	1	1	2	3				
	Disponibilidad	2	3	4	4				

Nota. Describe el servicio de la alta disponibilidad para la banca en línea y sus componentes. Fuente: elaboración propia.

## Plan DRP

### Propósito

El plan DRP es elaborado con el propósito de que, en caso ocurra un problema el cual provoque que las operaciones de los procesos críticos se detengan, exista una guía donde los empleados conozcan cómo actuar para minimizar el estrés de tomar una decisión apresurada, reducir las pérdidas por inactividad, reducir la probabilidad de que se pierda información y disminuir el tiempo de respuesta ante cualquier eventualidad con el fin de lograr continuar con las operaciones lo más pronto posible.

### Objetivo

Establecer una guía para que la organización pueda reanudar rápidamente las funciones de los sistemas afectados que estén involucrados en procesos críticos para que puedan seguir trabajando después del incidente.

### Ámbito de la aplicación

Se consideran críticos los procesos descritos para el sistema bancario anteriormente por lo que este plan DRP se plantea en el caso de una interrupción de los mismos, considerando los sistemas en los que estos se involucren, por ejemplo: servidores, base de datos, servicios con terceros, seguridad informática, entre otros.

Este plan se encuentra enfocado en la identificación de cada etapa de los procesos descritos y todas las partes interesadas que se involucren en estas, con la finalidad de poder crear planes de recuperación eficaces involucrando tanto los sistemas, departamentos, terceros, entre otros. Además, debe de encontrarse alineado con el plan de continuidad de la empresa.

Como objetivos específicos del plan se plantean los siguientes:

- Crear los planes pertinentes para la restauración de los servicios en el mínimo tiempo posible.
- Identificar los servicios que se involucren en los procesos identificados, personas o servicios terceros y otros departamentos que se involucren con dichos procesos.
- En conjunto con el plan de continuidad, minimizar el impacto de cualquier adversidad que conlleven los procesos planteados.

El presente DRP tratará de abarcar cualquier desastre proveyendo de lo siguiente:

- Identificación de amenazas y riesgo que interrumpan los procesos.
- Planteamiento de estrategias en conjunto con directrices para la identificación de algún suceso que esté sucediendo y todo lo respectivo con alertar y activar algún plan de recuperación.
- Plan de recuperación ante los riesgos y amenazas encontradas.
- Proceso de evaluación después de la interrupción y de recuperación.

**Tabla 6.** Procesos y sus componentes involucrados

Proceso	Involucrados en el proceso
Proceso de envío y validación de token	<ul style="list-style-type: none"> <li>• Infraestructura de red</li> <li>• Base de datos</li> <li>• Seguridad Informática</li> </ul>
Actualización diaria de tipo de cambio	<ul style="list-style-type: none"> <li>• Infraestructura de red</li> <li>• Base de datos</li> <li>• Seguridad Informática</li> </ul>

Validación de cuentas ACH y propias	<ul style="list-style-type: none"> <li>• Infraestructura de red</li> <li>• Base de datos</li> <li>• Seguridad Informática</li> </ul>
Alta disponibilidad de banca en línea	<ul style="list-style-type: none"> <li>• Infraestructura de red</li> <li>• Base de datos</li> <li>• Seguridad Informática</li> </ul>

Nota. Se detalla los componentes que se involucran en los procesos críticos identificados. Fuente: elaboración propia.

### **Políticas del Plan**

#### **Políticas Generales**

#### **Administración del Plan:**

El personal asignado como responsable debe de mantener actualizado el presente plan. Tanto el encargado como el plan definido deben de poder asegurar el cumplimiento de:

- Identificar cambios realizados y poderlos plasmar en dicho plan.
- Contar con una autorización previa a la actualización del documento para poder contar con la firma de autorización y el plan actualizado.
- Contar con la autorización para compartir el plan con las actualizaciones respectivas al área y personal involucrado.

#### **Actualización y Mantenimiento del Plan:**

Se recomienda que el plan pueda ser revisado y actualizado al menos 2 veces al año de manera programada, puede existir la excepción de poder realizar

la actualización al plan de manera no programada según sea la necesidad y la criticidad de este.

Existen causas establecidas por las cuales el plan puede ser actualizado, entre ellas se encuentran establecidas:

- Implementación de mejoras y correcciones a diferentes procesos establecidos anteriormente dentro del plan.
- Actualización del alcance establecido previamente
- Actualización de equipos, procesos u otros.

Se tiene en consideración que pueden darse nuevos casos por los cuales se realizará una actualización al plan, dichos casos pueden ser conocidos o desconocidos. Estos deben de poder identificarse y tomarse en consideración para actualizar el plan y a su vez para futuras actualizaciones. Si se requiere la actualización no programada, deberá de realizarse para tener un mejor control y seguimiento del plan.

### **Autorización y Divulgación del Plan:**

#### **Autorización:**

El plan de Recuperación de Desastres debe de pasar por un proceso de autorización, este DRP debe de ser evaluado y si cumple con las expectativas deseadas será autorizado por un Comité de Control de Riesgos. La autorización de este debe de quedar documentada a través de actas o registros, según se requiera.

#### **Divulgación:**

La persona encargada de realizar la Divulgación de este es el Gerente de informática, él debe de tener el control y realizar la divulgación respectiva únicamente al personan involucrado, se debe de tener un documento con las

personas autorizadas a divulgar dicho plan. El plan debe de entregarse impreso a los involucrados.

La divulgación se debe de realizar cada vez que el plan sufra una nueva actualización, debido a que los involucrados deben de tener la versión actualizada.

### **Evaluaciones del Plan:**

El plan definido debe de evaluarse aproximadamente cada 4 meses, las evaluaciones pueden realizarse de manera controlada. Estas evaluaciones deben de realizarse por el comité de Control de Riesgos permitiendo identificar amenazas, debilidades y mejoras a realizar según sea el caso. Al momento de realizar las pruebas se debe de tomar en cuenta lo siguiente:

- Datos del solicitante de la evaluación: (Nombre, puesto, fecha y justificación de la solicitud de la evaluación).
- Datos de la simulación: (Fecha, hora inicio de simulación, hora final de simulación, tipo de evaluación, posibles escenarios de simulación y el alcance de la evaluación).
- Objetivos y justificación
- Definición de actividades
- Definición de los resultados obtenidos
- Involucrados

El comité de Control y Riesgos es el encargado de elaborar los escenarios de evaluación y a su vez es el encargado de establecer si se notificará la prueba a realizar o la prueba se manejará de manera discreta.

**Reporte de resultados de evaluación del Plan:**

Los resultados de las pruebas realizadas deben plasmarse a través de un documento el cual debe de contener la siguiente estructura:

- Hoja de presentación
- Justificación de las evaluaciones realizadas
- Resultados de la simulación identificando sus fortalezas y debilidades
- Análisis de causa/efecto
- Acciones correctivas y acciones preventivas
  - Acción
  - Responsable
  - Fecha de resolución
- Conclusiones

Los resultados obtenidos se discutirán con el Gerente de informática y el Comité de control de Riegos.

**Políticas Específicas***Activación y Desactivación del Plan:*

**Activación:** La activación del plan podrá realizarse por el Comité de Control de Riesgos junto con el Gerente de Informática. Se tiene definido que el Comité de Control de Riesgos autorizará la activación y el Gerente de Informática tendrá la responsabilidad de definir el personal apropiado para la realización de las actividades de restauración, soporte y recuperación de las operaciones.

**Desactivación:** El Gerente General será el encargado de comunicar a comité de Control de Riesgos si se ha finalizado la declaración del desastre y se

haya restaurado y regresado a la normalidad. Posterior a ello el Comité toma la decisión de Desactivación del plan.

**Declaración de Desastre:**

Se declara desastre 30 minutos después de la primera interrupción de operaciones que se efectúan normalmente, posterior a ello el Gerente de informática debe de comunicar al Comité lo siguiente:

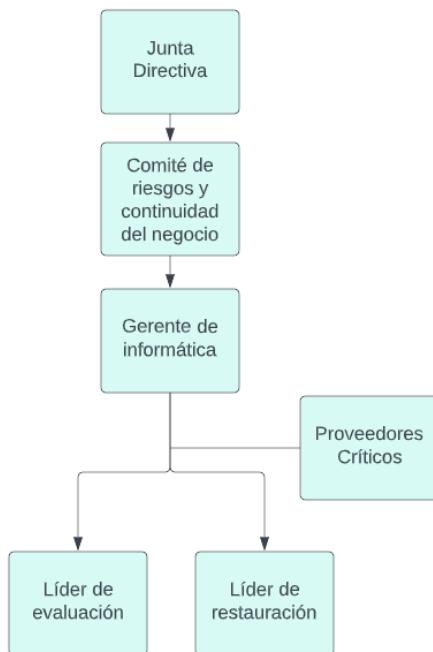
- La Criticidad establecida según la evaluación.
- Las Estrategias definidas para la restauración de los sistemas afectados
- Tiempo estimado de restauración
- Información adicional considerada como relevante

## Estructura para la administración y operación del plan

### Administración

Para la Administración de presente Plan de Recuperación de Desastres se define la siguiente estructura:

**Figura 6.** Estructura organizacional del plan de desastres



Nota. En la imagen se detalla de forma jerárquica la estructura de la administración del plan de desastres. Fuente: elaboración propia.

### *Junta Directiva*

#### Antes de la Emergencia

- Asegurar que los objetivos del presente plan estén alineados con los objetivos estratégicos de la empresa, los cuales deben de incluir como mínimo el cumplimiento de los tiempos objetivos de recuperación (RTO), puntos objetivos de restauración (RPO), tiempos máximos de interrupción (MTPD) y niveles de

disponibilidad de servicios y componentes tecnológicos críticos del centro de distribución y los almacenes de punto de venta

- Asegurar los recursos financieros, tecnológicos, operativos, entre otros, para la sostenibilidad, mejora del presente plan y para afrontar un desastre tecnológico
- Autorizar y Asegurar la realización de simulaciones de DRP y que las mismas incluyan componentes de mejora continua y mayor cobertura protección y redundancia tecnológica
- Revisar de forma mensual el nivel de cumplimiento de los niveles de servicios del centro de datos principal y sus proveedores críticos
- Velar por el fortalecimiento tecnológico aumentando el nivel de cobertura de cada plataforma crítica hasta llegar a contar con un sitio tecnológico alterno (propio o subcontratado)
- Aprobar los tiempos objetivos de recuperación, puntos objetivos de restauración y tiempos máximos de interrupción por plataforma crítica para la continuidad del negocio

#### Durante la Emergencia

- Analizar los riesgos e impactos del evento a afrontar
- Autorizar la declaración de desastre tecnológico
- Autorizar la ejecución de recursos necesarios para la mitigación del evento
- Notificar a las partes interesadas del evento a afrontar

Después de la Emergencia
<ul style="list-style-type: none"> <li>• Autorizar el retorno al sitio principal y desactivación del sitio alterno</li> <li>• Autorizar la finalización de la declaración de desastre tecnológico</li> <li>• Evaluar los resultados finales del desastre afrontado</li> <li>• Revisar y autorizar los ajustes necesarios a los presupuestos y reservas para afrontar emergencias tecnológicas</li> <li>• Revisar y autorizar los cambios / ajustes necesarios al contrato del Proveedor de Tecnología</li> </ul>

### ***Comité de riesgos y continuidad del negocio***

Antes de la Emergencia
<ul style="list-style-type: none"> <li>• Brindar asistencia técnica a la Junta Directiva en la activación del DRP <ul style="list-style-type: none"> <li>• Ser el ente de mayor conocimiento en detalle del DRP, riesgos a mitigar y nivel de afectación en la continuidad del negocio</li> <li>• Asegurar la realización de pruebas de escritorio y simulaciones de DRP</li> <li>• Identificar el nivel de madures del DRP en la Gerencia de Informática</li> <li>• Verificar y validar la efectividad, actualización y cumplimiento de objetivos de los planes relacionados con el DRP</li> </ul> </li> </ul>

- Verificar y validar la capacidad y competencia la Gerencia de Informática en la implementación del DRP
- Definir estrategias de evaluación de daños y reanudación de operaciones

### Durante la Emergencia

- Notificar a la Junta Directiva la necesidad de la activación del DRP, tomando en cuenta los riesgos y continuidad del negocio
- Coordinar con el Gerente de Informática la ejecución operativa del presente DRP
- Apoyar al Gerente de Informática en el cumplimiento del RTO y RPO de los servicios tecnológicos del alcance del presente DRP

### Después de la Emergencia

- Dar seguimiento al cumplimiento del Plan de Recuperación de Desastres Tecnológicos (DRP)
- Dar seguimiento al Gerente de Informática en:
  - Informe de resultados y documentos soporte de pruebas de escritorio
  - Informe de resultados y documentos soporte de simulaciones
  - Informe de resultados y documentos soporte de eventos reales

- Análisis de causas, acciones correctivas, acciones preventivas, evidencia de mejoras, entre otros documentos relacionados a la gestión del DRP
- Dar seguimiento a la restauración de daños tecnológicos

### ***Gerencia Informática***

#### **Antes de la Emergencia**

- Ser el Coordinador del DRP dirigiendo a los equipos operativos en la implementación del presente plan
  - Asegurar que los objetivos del presente plan estén alineados con los objetivos estratégicos de la empresa, los cuales deben de incluir como mínimo el cumplimiento de los tiempos objetivos de recuperación (RTO), puntos objetivos de restauración (RPO), tiempos máximos de interrupción (MTPD) y niveles de disponibilidad de servicios y componentes tecnológicos críticos del centro de distribución y los almacenes de punto de venta
  - Asegurar la sostenibilidad en el cumplimiento de los tiempos RTO, RPO, MTPD y niveles de disponibilidad de componentes tecnológicos
    - Contar con toda la documentación (energía eléctrica, enfriamiento, comunicaciones, equipos, aplicaciones, bases de datos, entre otros) de los Sitio Principal / Sitio Alterno y que la misma se encuentre actualizada como mínimo 1 vez al año
    - Asegurar la disponibilidad del personal operativo en el sitio principal para la realización del presente plan

- Asegurar el nivel de redundancia tecnológica y operativa mediante la realización de las pruebas de simulación o bien según sea necesario
  - Reportar de forma mensual el cumplimiento de los niveles de servicios
  - Asegurar la realización de simulaciones de DRP y que las mismas incluyan componentes de mejora continua y mayor cobertura de protección
  - Medir a los proveedores los cuales brinden productos y/o servicios que afecten la continuidad del negocio, tales como proveedores de comunicaciones, equipos, aplicativos, otros.
  - Velar por la existencia, vigencia y cumplimiento de los niveles de servicio contratos con los proveedores del Sitio Principal y en los puntos de venta
  - Verificar y validar que los miembros y el personal relacionado con el DRP estén familiarizados y entendidos del rol, responsabilidad y autoridad en el manejo del DRP
  - Identificar necesidades de actualización / ajuste al DRP
  - Asegurar que la empresa cuente con la información documentada de toda la infraestructura de los centros de datos principal, alterno y procesos de recuperación de los servicios tecnológicos

### Durante la Emergencia

- Evaluar la criticidad del evento y determinar plan de acciones a seguir, analizando los riesgos e impactos del evento basado en la información recopilada durante el proceso de activación de sitio alterno

- Gestionar la activación del plan de recuperación de desastres y las distintas alternativas para poder afrontar el evento
  - Autorizar la ejecución de recursos necesarios para la mitigación del evento
  - Reportar las acciones realizadas y el estado de mitigación del evento durante la emergencia
  - Dirigir al Equipo de Restauración en la implementación de los procedimientos de recuperación

### Después de la Emergencia

- Documentar el evento afrontado, en donde se identifiquen las causas que originaron el evento, plan de acción (acciones correctivas y/o acciones preventivas), nivel de impacto técnico, análisis de riesgo, entre otros.
- Elaborar un plan de restauración del Sitio Principal el cual incluya la estimación financiera e información técnica para la habilitación del sitio afectado
  - Coordinar la restauración del Sitio Principal asegurando que cumpla con las especificaciones técnicas
  - Gestionar la finalización de la declaración de desastre tecnológico
  - Documentar, evaluar y presentar los resultados finales del desastre afrontado
  - Proponer y someter a aprobación los cambios / ajustes necesarios al Plan de Desastre Tecnológico y todos los documentos relacionados que así lo requieran

**Líder de evaluación**

Antes de la Emergencia
<ul style="list-style-type: none"><li>• Documentar, evaluar, identificar y mitigar los riesgos de la infraestructura tecnológica del Sitio Principal</li><li>• Reportar al Gerente de Informática y Comité de Riesgos y Continuidad del Negocio los riesgos identificados, calificación del riesgo inherente, mecanismos de mitigación y calificación de riesgos residuales</li><li>• Sugerir y apoyar al Gerente de Informática en la realización de pruebas de simulación de desastres tecnológicos</li><li>• Revisar y asegurar la calidad de la información documentada y entregada al Banco (energía eléctrica, enfriamiento, comunicaciones, equipos, aplicaciones, bases de datos, entre otros)</li><li>• Asegurar el registro y notificación de la totalidad de incidentes dentro del Sitio Principal y Sitio Alterno, los cuales pueden comprometer la prestación de los productos y/o servicios</li><li>• Asegurar el cumplimiento del RTO, RPO, MTPD y niveles de disponibilidad de cada una de las plataformas críticas</li><li>• Asegurar que todos los proveedores de tecnología cuenten y cumplan con niveles de servicios contratados</li><li>• Implementar mecanismos de registro, evaluación y mitigación de incidentes tecnológicos</li></ul>

### Durante la Emergencia

- Coordinar y dirigir al equipo de evaluación en la ejecución del proceso de activación del presente plan
- Analizar los riesgos e impactos del evento a afrontar basado en la información recopilada durante el proceso de recuperación
- Apoyar al Gerente de Informática en la evaluación y decisión técnica de activar el DRP

### Después de la Emergencia

- Documentar el evento afrontado, en donde se identifiquen las causas que originaron el evento, plan de acción (acciones correctivas y/o acciones preventivas), nivel de impacto técnico, entre otros.
- Proponer y someter a aprobación los cambios / ajustes necesarios al Plan de Desastre Tecnológico y todos los documentos relacionados que así lo requieran
- Socializar al equipo de evaluación los ajustes realizados al presente plan y sus documentos relacionados

### ***Líder de Restauración***

#### Antes de la Emergencia

- Documentar, evaluar, identificar y mitigar los riesgos de la infraestructura tecnológica del Sitio Principal, esto con el fin de poder restaurar los servicios tecnológicos del centro de datos después de afrontar un evento

- Sugerir y apoyar al Gerente General del Proveedor de Tecnología en la realización de pruebas de simulación de desastres tecnológicos
  - Revisar y asegurar la calidad de la información documentada del presente DRP
    - Asegurar que el equipo de restauración cuente con la información actualizada, personal capacitado y las metodologías de certificación de componentes para la restauración del Sitio Principal
    - Implementar buenas prácticas operativas / administrativas y mecanismos de medición para el personal interno que estén relacionados con la mitigación de riesgos y eventos de desastre tecnológico

### Durante la Emergencia

- El equipo de restauración no realiza actividades durante una emergencia

### Después de la Emergencia

- Coordinar y dirigir al equipo de restauración en la ejecución del proceso de restaurar el Sitio Principal del presente plan
  - Evaluar el nivel de impacto del evento afrontado en el Sitio Principal
  - Cuantificar y documentar el plan de acción para la restauración del Sitio Principal
  - Coordinar con los proveedores la implementación de las actividades de restauración

### **Líder de Seguridad de la Información**

<b>Antes de la Emergencia</b>
<ul style="list-style-type: none"> <li>• Velar por el cumplimiento de las buenas prácticas de la seguridad de la información aplicadas en el Sitio Principal             <ul style="list-style-type: none"> <li>• Realizar pruebas de vulnerabilidad a los componentes tecnológicos y penetración de plataformas en el Sitio Principal</li> <li>• Revisar las mediciones y acciones realizadas para la mitigación de riesgos y eventos de desastre tecnológico</li> <li>• Validar el cumplimiento de los planes de acción y efectividad de los controles de las acciones realizadas para la mitigación de incidentes tecnológicos</li> <li>• Reportar los hallazgos encontrados durante las revisiones de seguridad</li> </ul> </li> </ul>

<b>Durante la Emergencia</b>
<ul style="list-style-type: none"> <li>• Auditar la realización del DRP</li> <li>• Certificar cada plataforma restaurada cuente con los niveles de acceso aptos para su funcionamiento</li> </ul>

<b>Después de la Emergencia</b>
<ul style="list-style-type: none"> <li>• Identificar y documentar los hallazgos de seguridad afrontados durante el evento, en donde se identifiquen las causas que originaron dichos hallazgos, nivel de impacto y plan de acción (acciones correctivas y/o acciones preventivas) para la mitigación de dichos hallazgos</li> </ul>

- Participar en la presentación de los resultados finales del desastre afrontado al Comité de Riesgo y Continuidad del Negocio
  - Verificar el proceso de restauración tecnológica
  - Recomendar cambios / ajustes necesarios al contrato del Proveedor de Tecnología, al Plan de Desastre Tecnológico y todos los documentos relacionados que así lo requieran

### **Mapa de Interdependencia**

Los sistemas y aplicaciones de Tecnología de la Información (TI) son fundamentales para el funcionamiento de una organización bancaria moderna. Cada día, miles de transacciones financieras son procesadas a través de sistemas automatizados, y la continuidad de estos procesos críticos es vital para el éxito de la organización. Sin embargo, los desastres naturales, fallas de hardware y software, ataques cibernéticos y otros eventos imprevistos pueden interrumpir el funcionamiento normal de los sistemas de TI y afectar gravemente la capacidad de una organización bancaria para servir a sus clientes y mantener su reputación en el mercado.

Para minimizar los riesgos y asegurar la continuidad del negocio, las organizaciones bancarias necesitan desarrollar y mantener un Plan de Recuperación de Desastres (DRP) robusto. Un componente crítico del DRP es el mapa de interdependencia bancario. Este mapa es una representación visual de cómo los diferentes sistemas y aplicaciones de TI están interconectados y cómo se relacionan con los procesos de negocio de la organización bancaria.

A continuación, exploraremos en detalle qué es un mapa de interdependencia bancario en un DRP, por qué es importante y cómo se utiliza para ayudar a las organizaciones bancarias a mantener la continuidad del negocio en caso de un desastre.

El proceso de tipo de cambio bancario es un elemento crítico para la operación diaria de una organización bancaria. Este proceso implica el cálculo y registro de los tipos de cambio de las diferentes monedas y divisas utilizadas en las transacciones financieras. La rapidez y precisión en la ejecución de este proceso es vital para mantener la satisfacción de los clientes y garantizar la continuidad del negocio.

**Tabla 7.** Tipo de cambio bancario

Mapa de Interdependencia: Tipo de Cambio Bancario				
Proceso	Recurso de TI	Tiempo	RPO	Comentario
<b>Registro de transacciones</b>	Sistema de registro bancario	En tiempo real	0 horas	El sistema registra las transacciones en tiempo real y actualiza los saldos de las cuentas correspondientes.
<b>Determinación del tipo de cambio</b>	Software de tipo de cambio	En tiempo real	0 horas	El software determina el tipo de cambio en función de los datos actuales del mercado.
<b>Comunicación con el mercado internacional de divisas</b>	Sistema de comunicación de divisas	En tiempo real	0 horas	El sistema establece la comunicación con el mercado internacional de divisas para obtener información y realizar transacciones.
<b>Gestión del riesgo cambiario</b>	Software de gestión de riesgos	Diario	24 horas	Los analistas utilizan el software para evaluar el riesgo cambiario y tomar medidas para minimizarlo.

<b>Reporte de operaciones cambiarias</b>	Sistema de reporte bancario	Semanal	4 horas	El sistema genera reportes de las operaciones cambiarias realizadas durante la semana para fines contables y regulatorios.
<b>Mantenimiento de infraestructura de TI</b>	Equipo de soporte de TI	Como sea necesario	N/A	El equipo de soporte de TI mantiene y actualiza la infraestructura de TI para garantizar la operación continua del proceso.

Nota. La tabla describe los recursos, tiempo y el RPO establecidos por la administración para el proceso de tipo de cambio bancario. Fuente: elaboración propia.

La generación de tokens de seguridad es un proceso crítico para la seguridad de la información en una organización bancaria. Este proceso implica la creación y distribución de los tokens de seguridad utilizados para autenticar a los usuarios y garantizar que solo los usuarios autorizados tengan acceso a los datos sensibles.

**Tabla 8.** Generación de token de seguridad

Mapa de Interdependencia: Generación de Token de Seguridad					
Proceso	Recurso de TI	Tiempo	RPO	Comentario	
<b>Generación de token de seguridad</b>	Generador de token de seguridad	En tiempo real	0 horas	El generador de token de seguridad genera un código de seguridad único que se utiliza para autenticar al usuario.	
<b>Validación del token</b>	Software validación token	En tiempo real	0 horas	El software de validación de token verifica que el código de seguridad sea válido y correspondiente a un usuario autorizado.	
<b>Comunicación con el servidor de autenticación</b>	Servidor de autenticación	En tiempo real	0 horas	El servidor de autenticación verifica la identidad del usuario y autoriza el acceso.	

<b>Almacenamiento seguro de tokens</b>	Base de datos de tokens	N/A	N/A	Los tokens se almacenan de forma segura en una base de datos para su uso futuro y para mantener un registro de su uso.
<b>Mantenimiento del generador de token</b>	Equipo de soporte de TI	Como necesario sea	N/A	El equipo de soporte de TI mantiene y actualiza el generador de token para garantizar su operación continua y su compatibilidad con otros sistemas.

Nota. La tabla describe los recursos, tiempo y el RPO establecidos por la administración para el proceso de generación de token de seguridad. Fuente: elaboración propia.

El proceso de validación de cuentas ACH es un elemento fundamental para la operación diaria de una organización bancaria que maneja transacciones electrónicas. Este proceso implica la verificación de la información bancaria de los clientes y la validación de la autorización de la transacción antes de que se procese.

La precisión y rapidez en la ejecución de este proceso es vital para mantener la satisfacción de los clientes y garantizar la continuidad del negocio. En este contexto, el uso de un mapa de interdependencia es una herramienta valiosa para garantizar la eficacia del proceso de validación de cuentas ACH y mantener la continuidad del negocio en caso de un desastre.

**Tabla 9.** Validación de cuentas ACH y cuentas propias

Mapa de Interdependencia: Validación de Cuentas ACH y Cuentas propias				
Proceso	Recurso de TI	Tiempo	RPO	Comentario
<b>Validación de cuenta ACH</b>	Base de datos de cuentas ACH	En tiempo real	0 horas	La base de datos de cuentas ACH se utiliza para validar la cuenta ACH del destinatario y garantizar que sea una cuenta válida y activa.

<b>Validación de cuenta propia</b>	Base de datos de cuentas propias	En tiempo real	0 horas	La base de datos de cuentas propias se utiliza para validar la cuenta del remitente y garantizar que sea una cuenta válida y activa.
<b>Verificación de fondos suficientes</b>	Sistema de verificación de fondos	En tiempo real	0 horas	El sistema de verificación de fondos se utiliza para verificar que el remitente tenga fondos suficientes para realizar la transacción.
<b>Comunicación con la red de ACH</b>	Sistema de comunicación de ACH	En tiempo real	0 horas	El sistema de comunicación de ACH se utiliza para transmitir la transacción a la red de ACH para su procesamiento.
<b>Procesamiento de transacciones ACH</b>	Sistema de procesamiento de ACH	Diario	24 horas	El sistema de procesamiento de ACH se utiliza para procesar las transacciones ACH y realizar los depósitos correspondientes en las cuentas de destino.
<b>Mantenimiento de la infraestructura de TI</b>	Equipo de soporte de TI	Como sea necesario	N/A	El equipo de soporte de TI mantiene y actualiza la infraestructura de TI para garantizar la operación continua del proceso.

Nota. La tabla describe los recursos, tiempo y el RPO establecidos por la administración para el proceso validación de cuentas. Fuente: elaboración propia.

En este contexto, un mapa de interdependencia es una herramienta invaluable para comprender la complejidad del proceso de alta disponibilidad y garantizar que todas las interdependencias entre los recursos de Tecnología de la Información (TI) y los procesos de negocio estén debidamente documentadas. Este mapa ayuda a identificar los puntos críticos del proceso, las interrupciones que pueden surgir y cómo se pueden resolver de manera efectiva.

**Tabla 10.** Alta disponibilidad para la banca en línea

Mapa de Interdependencia: Alta disponibilidad para la banca en línea				
Proceso	Recurso de TI	Tiempo	RPO	Comentario
<b>Detección de fallas</b>	Monitoreo de servidor	En tiempo real	0 horas	El monitoreo de servidor se utiliza para detectar y alertar al equipo de soporte de TI sobre cualquier falla en el sistema.
<b>Implementación de redundancia</b>	Servidores duplicados, balanceador de carga	En tiempo real	0 horas	Los servidores duplicados y el balanceador de carga se utilizan para proporcionar redundancia y garantizar la continuidad del servicio en caso de una falla.
<b>Implementación de respaldo de datos</b>	Almacenamiento de datos duplicado	Diario	24 horas	El almacenamiento de datos duplicado se utiliza para proporcionar respaldo de datos y garantizar la recuperación de datos en caso de una falla del sistema.
<b>Implementación de sistemas de recuperación ante desastres</b>	Infraestructura de recuperación ante desastres	Horas o días	Variado	La infraestructura de recuperación ante desastres se utiliza para garantizar la recuperación del sistema y de los datos en caso de un desastre natural u otra emergencia.
<b>Mantenimiento y actualización de la infraestructura de TI</b>	Equipo de soporte de TI	Como sea necesario	N/A	El equipo de soporte de TI mantiene y actualiza la infraestructura de TI para garantizar la operación continua y la alta disponibilidad del servicio de banca en línea.

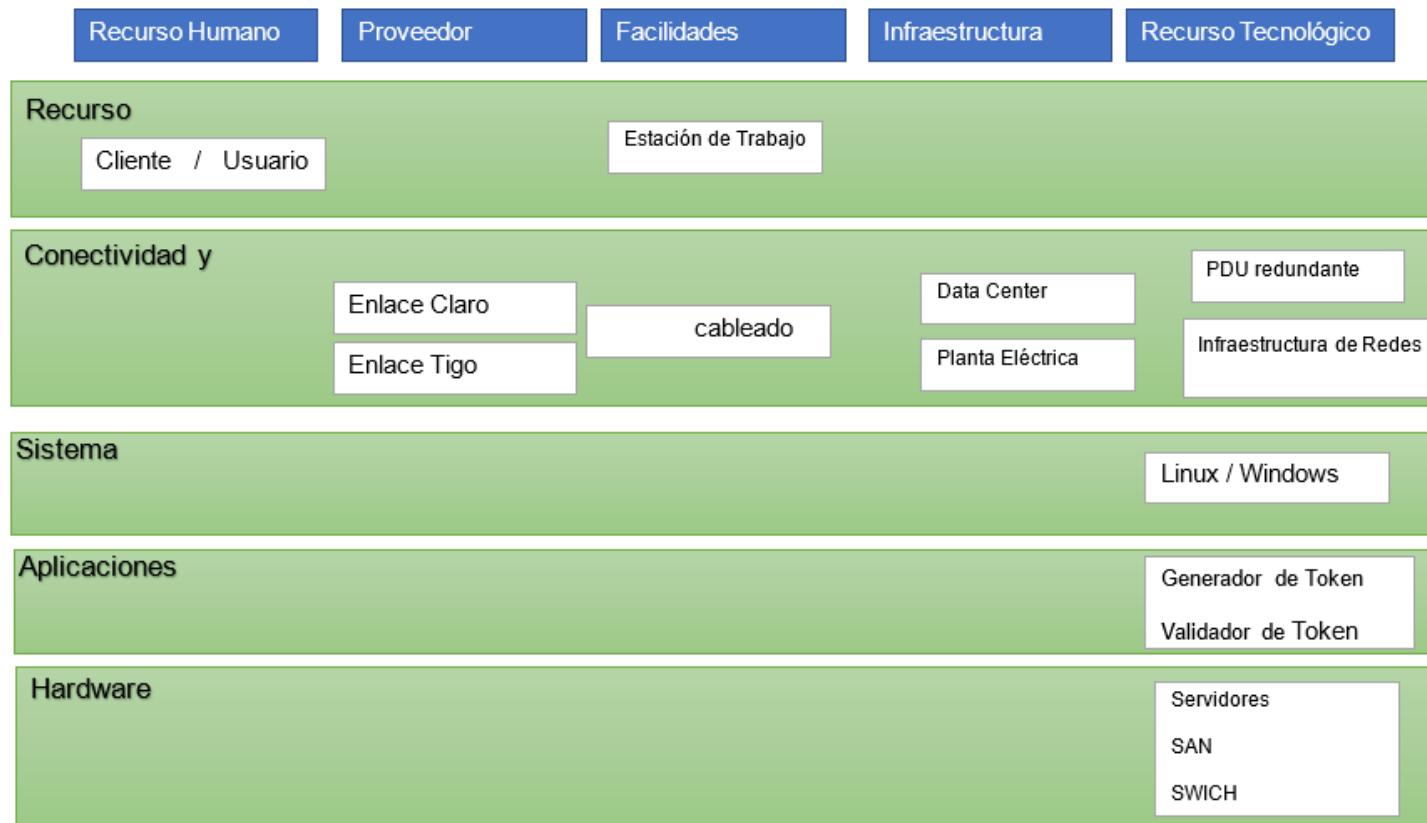
Nota. La tabla describe los recursos, tiempo y el RPO establecidos por la administración para el proceso de alta disponibilidad para la banca en línea. Fuente: elaboración propia.

**Figura 7.** Mapa de Interdependencia tipo de Cambio Bancario



Nota. Se detalla a continuación el mapa de interdependencia para el proceso de cambio bancario. Fuente: elaboración propia.

**Figura 8. Mapa de Interdependencia Generación de Token de Seguridad**



Nota. Se detalla a continuación el mapa de interdependencia para el proceso de generación de token de seguridad. Fuente: elaboración propia.

**Figura 9.** Mapa de Interdependencia Validación de Cuentas ACH y Cuentas Propias



Nota. Se detalla a continuación el mapa de interdependencia para el proceso de validación de cuentas ACH.

Fuente: elaboración propia.

**Figura 10.** Mapa de Interdependencia Alta disponibilidad para la banca en línea



Nota. Se detalla a continuación el mapa de interdependencia para el proceso de alta disponibilidad de banca en línea. Fuente: elaboración propia.

## Estrategias de recuperación de desastres

**Tabla 11.** Estrategias de recuperación de desastres

Tipo de falla	Ubicación	Estrategia de mitigación	Estrategia de recuperación	Documento relacionado
<b>Caída del proveedor principal de internet.</b>	Datacenter	Enlace redundante al proveedor secundario de internet.	Activación de enlace secundario al proveedor de internet.	Procedimiento de reconexión de internet.
<b>Caída del servidor web.</b>	Datacenter	Configuración del servidor web redundante.	Activación de servidor web redundante.	Procedimiento de redundancia en servidores.
<b>Caída del servidor de base de datos</b>	Datacenter	Configuración del servidor de base de datos redundante.	Activación del servidor redundante de BDD.	Procedimiento de redundancia en servidores.
<b>Interrupción del suministro de energía eléctrica.</b>	Datacenter	Tener UPS para cada dispositivo.  Planta propia de generación de energía.	Activación automática de UPS de cada dispositivo.  Activación automática de planta propia de energía eléctrica.	Procedimiento de activación de UPS.  Procedimiento de activación automática de planta de energía eléctrica.

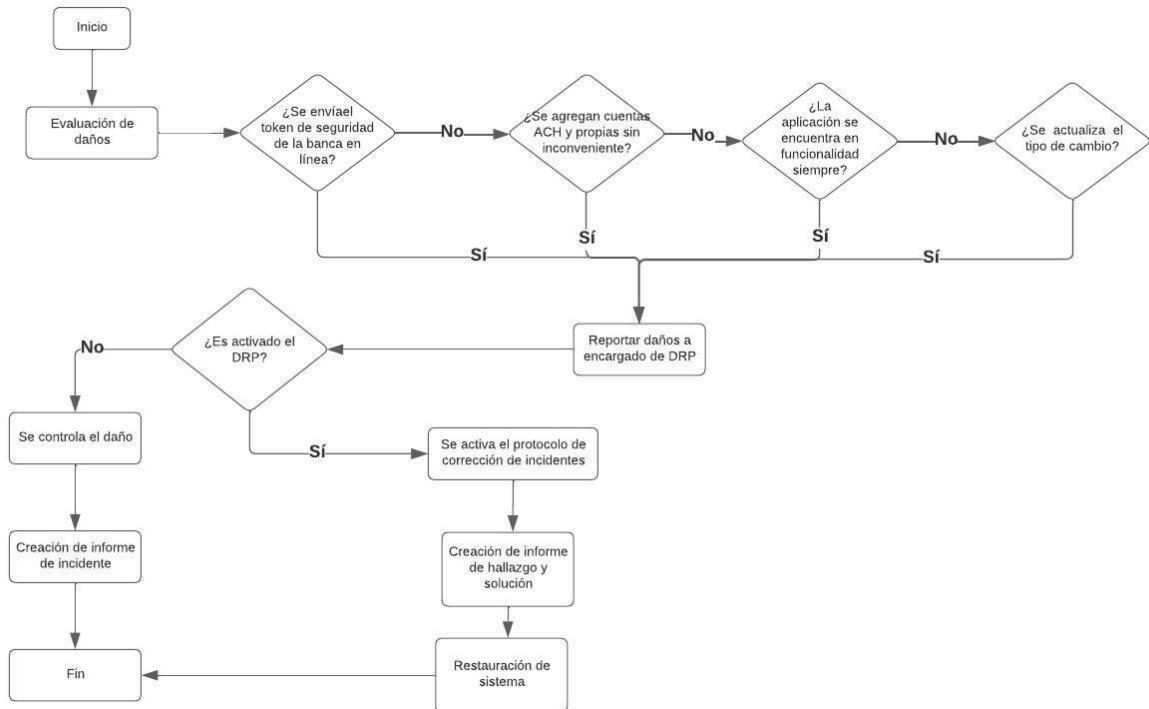
<b>Falta de la conexión del webservice que provee la tasa de cambio.</b>	Web service	Personal de mantenimiento y soporte 24/7.  Canal de comunicación de emergencia con proveedores.	Ejecución de evaluación del webservice y corrección por parte del personal de soporte 24/7.  Activación del canal de comunicación de canal de emergencia.	Procedimiento de validación del webservice.  Procedimiento del canal de comunicación de canal de emergencia.
--	-------------	---	---	--

Nota. Tabla que describe cada estrategia para evitar cierto tipo de falla. Fuente: elaboración propia.

## Procesos operativos de recuperación de desastres

### Proceso de diagnóstico y activación

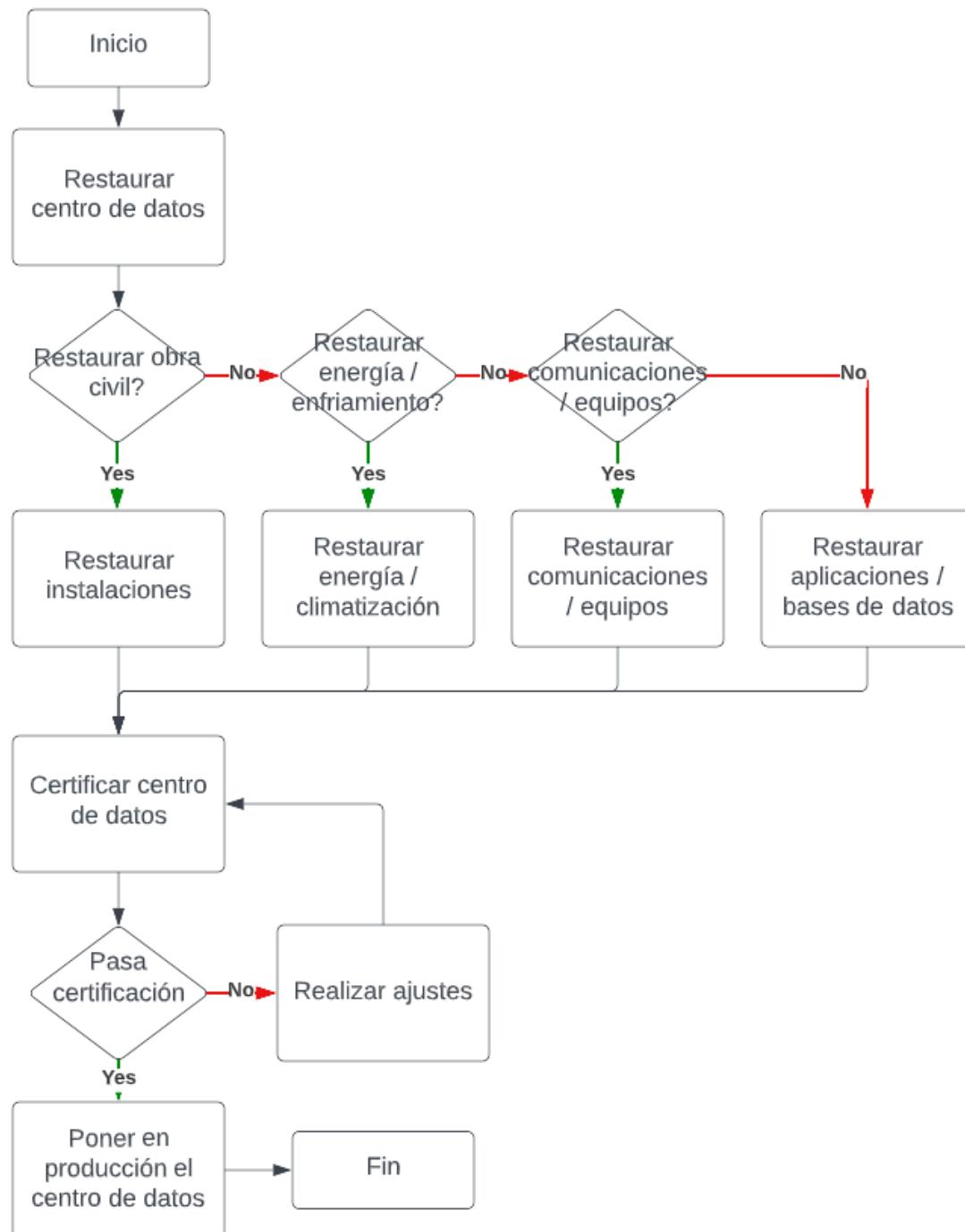
**Figura 11.** Proceso de diagnóstico y activación



Nota. Diagrama que representa el proceso de diagnóstico y activación de los desastres ocurridos. Fuente: elaboración propia.

### Fase de restauración

**Figura 12.** Proceso de restauración



Nota. Diagrama que describe los pasos para el proceso de recuperación. Fuente: elaboración propia.

## **Lista de contactos claves**

**Tabla 12.** Listado de contactos

Nombre y apellido	Puesto	Contacto
Luis Ovalle	Coordinador de banca en línea	<a href="mailto:lovalle@gmail.com">lovalle@gmail.com</a>
Renata Quiñonez	Coordinador de desarrollo	<a href="mailto:rquinonez@gmail.com">rquinonez@gmail.com</a>
Rigoberto Pérez	Desarrollador banca digital	<a href="mailto:rperez@gmail.com">rperez@gmail.com</a>
Luis Urizar	Desarrollador banca digital	<a href="mailto:lurizar@gmail.com">lurizar@gmail.com</a>
Proveedor de servicio web.		
Proveedor de servidores web y de base de datos.		
Proveedor de valores de tasa de cambio		

Nota. Tabla con el listado de los contactos importantes para el banco. Fuente: elaboración propia.

## **Actualizaciones**

**Tabla 13.** Actualizaciones del DRP

Nombre	Fecha	Descripción	Versión	Aprobado por

Nota. Tabla con las actualizaciones que el DRP ha tenido. Fuente: elaboración propia.

## **Detalles del equipo**

**Tabla 14.** Detalles de los equipos utilizados por la empresa

Servicio	Activo	Grupo	Disponibilidad
Servidores	Servidor Web banca en línea	Servidores de aplicación	1
Servidores	Servidor redundante web	Servidores de aplicación	2
Base de datos	Servidor redundante de base de datos	Servidores de base de datos	2
Base de datos	Servidor Base de datos	Servidores de base de datos	1
Red	Cableado	Red	2
Red	Enlace internet Tigo	Red	1
Red	Enlace internet Claro	Red	1

Información	Webservice tasa de cambio	Información	2
Información	Webservice validación de cuentas	Información	2
Información	Token banca en línea	Información	
Seguridad	Firewall	Seguridad	3
Seguridad	Protocolos de seguridad	Seguridad	2
Seguridad	Certificados SSL	Seguridad	3
Seguridad	Cuarto de servidores	Seguridad	3
Electricidad	PDU	Electricidad	3
Electricidad	UPS	Electricidad	3
Hardware	Computadoras	Hardware	2
Hardware	Routers	Hardware	2
Hardware	Switches	Hardware	2

Nota. Tabla que posee los componentes de hardware para el correcto funcionamiento de los procesos planteados en el DRP. Fuente: elaboración propia.

### Términos y definiciones

**ACH** - Por sus siglas en inglés significa Automated Clearing House network, que en español es Cámara de Compensación Automatizada, es un sistema de compensación automatizado que permite realizar de forma segura operaciones como transferencias o pagos entre bancos del sistema.

**Aplicación WEB** - Programa de software que se ejecuta en un servidor web al cual únicamente se puede acceder a través de un navegador que se encuentre conectado a internet.

**Base de datos** - Es la agrupación de datos de forma estructurada y organizada que se almacena de forma digital en un sistema con la capacidad de gestionar datos.

**BIA** - Por sus siglas en inglés significa Business Impact Analysis, que en español es Análisis de Impacto del Negocio. Es un análisis que permite identificar y evaluar el nivel de impacto con relación a la gestión del negocio.

**Datacenter** – Es un centro de procesamiento de datos es un gran espacio encargado específicamente de resguardar los equipos electrónicos como servidores, ventiladores, conexiones y otros elementos que conforman una red.

**DRP** - Por sus siglas en inglés significa Disaster Recovery Plan, que en español es Plan de Recuperación de Desastres, es un plan donde se establecen las medidas que se tomarán para respaldar la información perdida ante un desastre.

**Firewall** - En español significa cortafuegos, que es un programa informático que controla el acceso de una computadora a la red de la computadora.

**Infraestructura** - Conjunto de servicios, instalaciones y dispositivos necesarios para el desarrollo de una actividad o acoplar para que un lugar pueda ser utilizado.

**ISP** - Por sus siglas en inglés significa Internet Service Provider, que en español es Proveedor de Servicios de Internet, es la empresa encargada de brindar al acceso a internet.

**Normas ISO** - Grupo de pautas con reconocimiento internacional que surgieron con la necesidad de ayudar a las empresas a instituir niveles de homogeneidad en relación con la gestión y prestación de servicios.

**Notificaciones push** - Mensajes que llegan a nuestros smartphones, tablets y smartwatches, pero sólo a través de alguna aplicación que tengamos instalada.

**RPO** - Por sus siglas en inglés significa Recovery Point Objective, que en español es objetivo de punto de recuperación, y consiste en la cantidad de información que se puede perder dentro del período más relevante para una empresa.

**RTO** - Por sus siglas en inglés significa Recovery Time Objective, que en español es objetivo de tiempo de recuperación, que es la cantidad de tiempo en que un sistema o aplicación puede estar inactivo sin causar pérdidas significativas a la empresa.

**SMS** - Por sus siglas en inglés significa Short Message Service, que en español es servicio de mensajes cortos, y son mensajes cortos de texto que se pueden enviar entre teléfonos celulares.

**SQL** - Por sus siglas en inglés significa Structured Query Language, que en español es lenguaje de consulta estructurado, que es un lenguaje de computación para trabajar con bases de datos y relaciones entre tablas.

**Token** - En el contexto bancario en informática, es un identificador utilizado para comprobar y asegurar la seguridad de una operación.

**UPS** - Por sus siglas en inglés significa Uninterruptible power supply, que en español es fuente de alimentación de energía ininterrumpida, es un dispositivo que cuenta con baterías de alto poder para suministrar gran capacidad de corriente en caso de emergencia.

**VPN** - Por sus siglas en inglés significa Virtual Private Network, que en español es Red Privada Virtual, que es una conexión protegida a una red privada.

**WAF** - Por sus siglas en inglés significa Web Application Firewall, que en español es el Cortafuegos de una Aplicación Web, es un software que se encarga de proteger la capa de aplicación y analizar cada petición en dicha capa.

**WS** - Por sus siglas en inglés significa Web Service, que en español es Servicio web, es una tecnología que utiliza un conjunto de protocolos para facilitar el intercambio de información entre aplicaciones o sistemas.

## Proveedores críticos

**Tabla 15.** Servicios de proveedores críticos

Servicio	Empresa	Nombre	Correo	Telefono	Telefono móvil
Proveedor de routers	Tigo	Ansoni Velasquez	avelasquez@tigo.com.gt	22703000	56958865
Proveedor de Switch	Tigo	Ansoni Velasquez	avelasquez@tigo.com.gt	22703000	56958865
Internet	Tigo	Ansoni Velasquez	avelasquez@tigo.com.gt	22703000	56958865
Internet	Claro	Iris Alvarez	iris_alvarez@claro.com.gt	24569555	52132648
Servidores web	AWS	Regina Paiz	reginaP@aws.com.gt		42156578
Servidores de base de datos	AWS	Regina Paiz	reginaP@aws.com.gt		42156578
Valores de tasa de cambio	Banco de Guatemala	Freddy del Cid	freddy_DE@bancoguatemala.com.gt	22569400	48798562
Computadoras	Dell	Kimberly Zacarías	kmzacarias4@dell.com.gt	25364444	49635265
Firewall	Tigo	Lucrecia Bonilla	lu_bonilla@tigo.com.gt	22987700	35659524

Nota. Tabla con el número de contacto de los proveedores críticos del banco.

Fuente: elaboración propia.

## Documentos Relacionados

**Tabla 16.** Documentos relacionados con el DRP

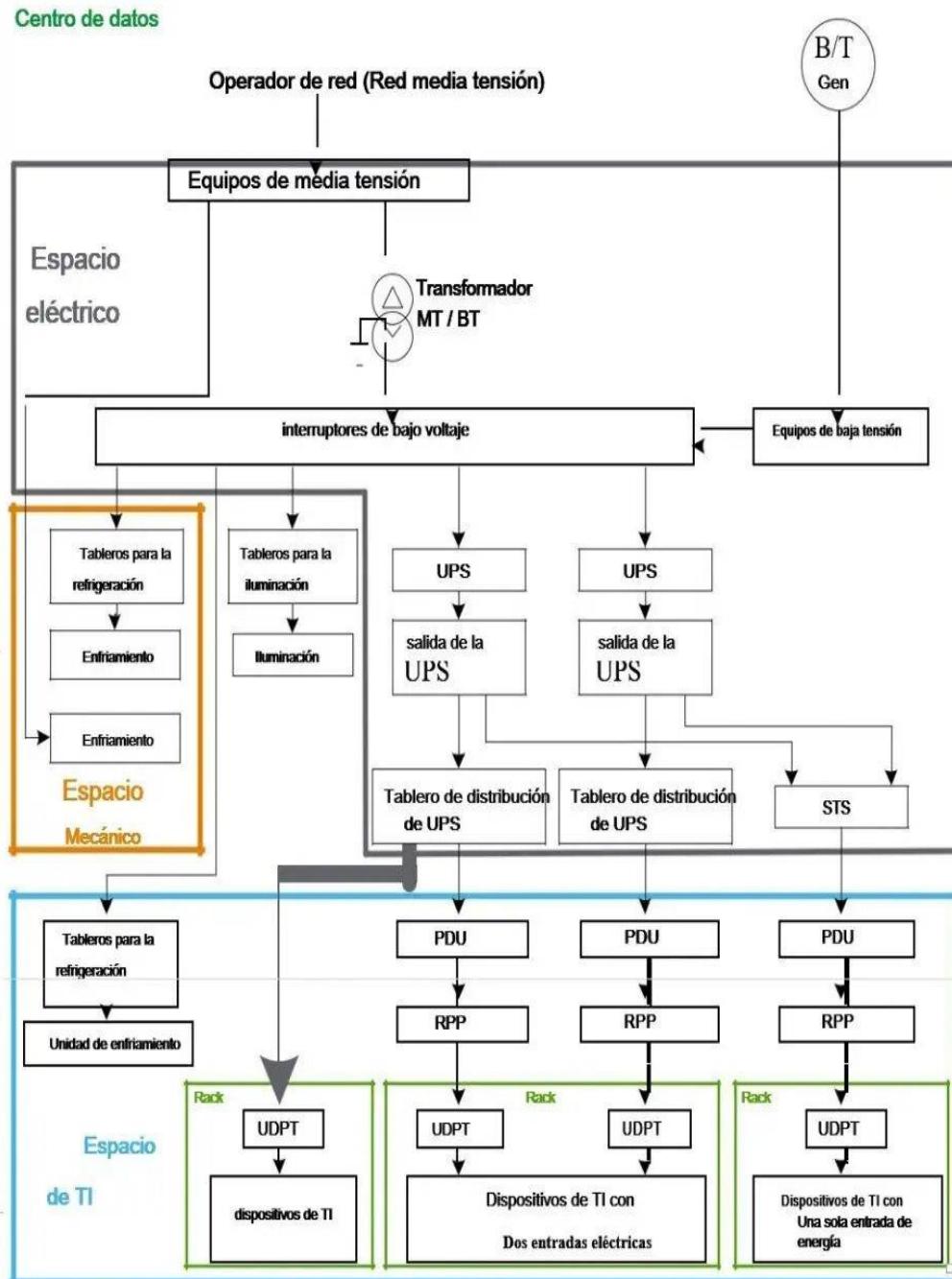
No.	Nombre	Descripción	Versión
1	Diagrama unifilar Bancario.pdf	Diagrama eléctrico Centro de Datos	V1
2	Restauración_Base_Datos.pdf	Restauración de Base de datos de la entidad bancaria.	V1

Nota. Tabla con los nombres de los documentos que se relacionan con el DRP.

Fuente: elaboración propia.

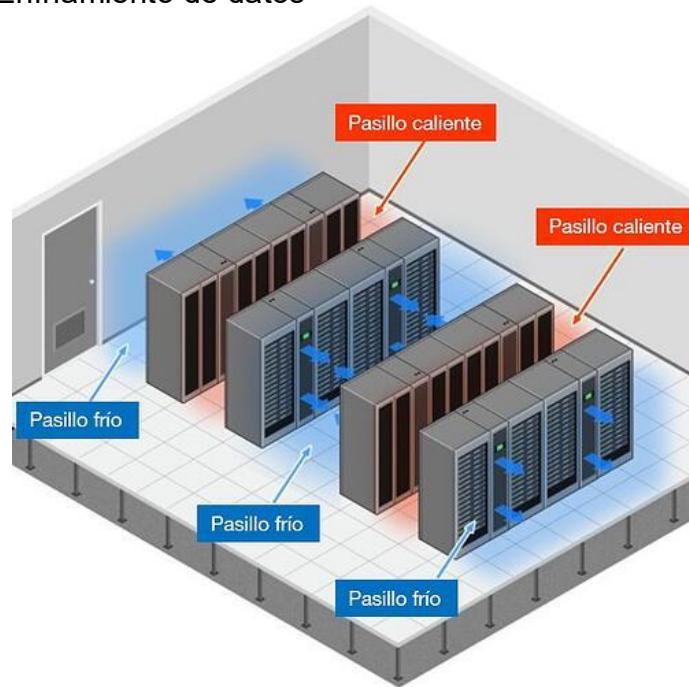
## Mapa de distribución Eléctrica y Enfriamiento de Datos

Figura 13. Mapa de distribución eléctrica y enfriamiento de datos



Nota. Diagrama que Describe la conexión eléctrica y el enfriamiento de los servidores y base de datos. Fuente: elaboración propia.

**Figura 14.** Enfriamiento de datos

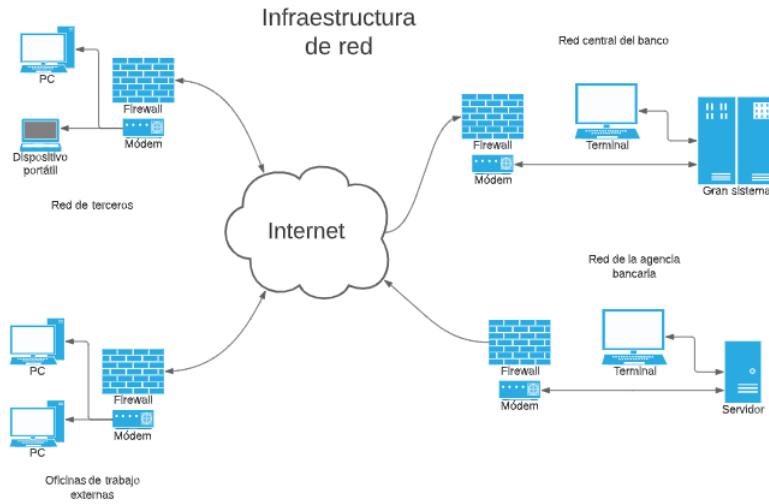


Nota. Diagrama que Describe el enfriamiento de los servidores y base de datos.

Fuente: elaboración propia.

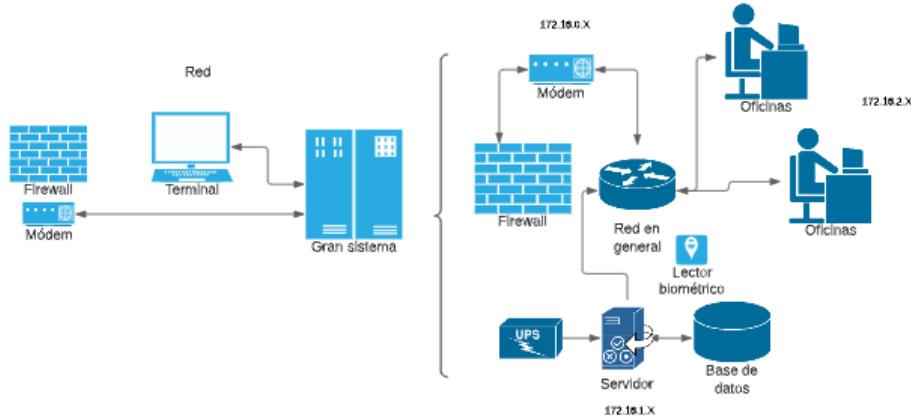
### Mapa de red de centro de datos

**Figura 15.** Mapa de red general



Nota: Se ilustra de manera general cómo funciona la conexión del banco con demás agencias y terceros. Fuente: Elaboración propia.

**Figura 16.** Mapa de red específica



Nota: Se ilustra de manera específica la red de alguna agencia. Fuente: Elaboración propia.

### Mapa de Red Banca Electrónica

La banca electrónica utiliza una red de comunicaciones segura y encriptada para permitir que los clientes realicen transacciones financieras en línea. Esta red se compone de varios elementos, como servidores, enrutadores, conmutadores y firewalls, que trabajan juntos para garantizar que la información del cliente se mantenga segura y protegida.

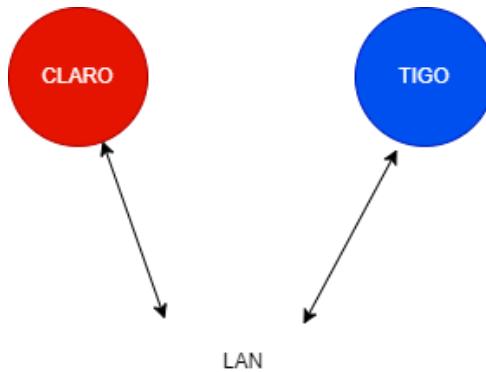
Los servidores son computadoras especializadas que ejecutan aplicaciones de banca electrónica, mientras que los enrutadores y conmutadores se utilizan para enviar y recibir información a través de la red. Los firewalls actúan como barreras de seguridad para proteger la red de intrusiones no autorizadas.

La distribución de redes para la banca electrónica puede variar según el tamaño y la complejidad de la institución financiera. Algunas instituciones pueden utilizar una red centralizada, en la que todos los servidores y dispositivos se encuentran en una sola

ubicación, mientras que otras pueden utilizar una red distribuida, en la que los servidores y dispositivos están dispersos en varias ubicaciones.

En cualquier caso, la seguridad de la red es una prioridad clave en la banca electrónica, y las instituciones financieras trabajan continuamente para mejorar sus sistemas de seguridad y protección contra amenazas cibernéticas.

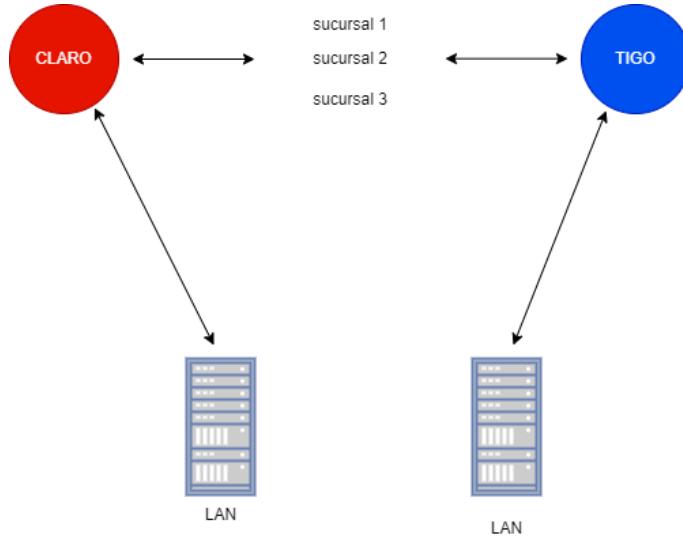
**Figura 17.** IP'S usadas en el sistema



VLAN ID	Name	Dirección IP
130	Administrativa	172.16.32.x
131	Lan	172.16.33.x
132	WirelessCorp	172.16.34.x
133	WirelessGuest	172.16.35.x
134	Voz	172.16.36.x
135	Video	172.16.37.x
136	Symbol	172.16.38.x
137	Smart-tv	172.16.39.x

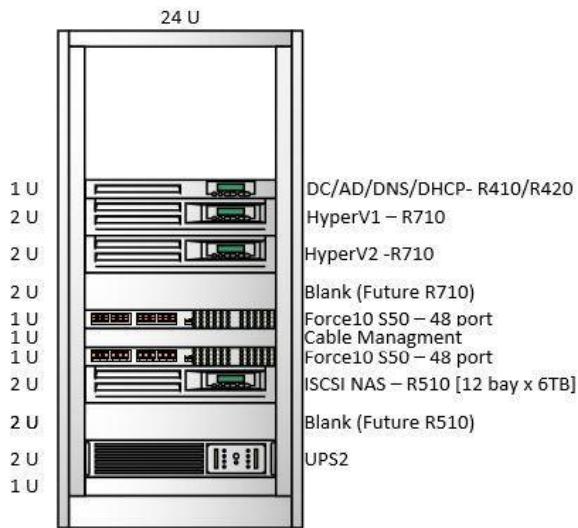
Nota. La figura describe como están distribuidas el uso de las IP'S. Fuente:  
elaboración propia.

**Figura 18.** Mapa de conexión a servidores



Nota. La figura describe como están distribuidos los servicios entre las diferentes LAN'S. Fuente: elaboración propia.

**Figura 19.** Mapa de equipos (Racks) en Centro de Datos



Nota. La figura describe como están distribuido los racks en el centro de Datos.

## **Recuperación Banca Electrónica**

Objetivo del plan de recuperación: Este plan tiene como objetivo establecer los procedimientos y protocolos necesarios para garantizar la rápida recuperación de la banca electrónica en caso de una falla o interrupción del servicio.

### ***Equipo de respuesta***

Definición del equipo de respuesta: El equipo de respuesta estará conformado por personal técnico y de seguridad de la información, quienes estarán encargados de coordinar las acciones necesarias para la recuperación de la banca electrónica.

Designación de roles y responsabilidades: Cada miembro del equipo de respuesta tendrá roles y responsabilidades específicas durante el proceso de recuperación, los cuales deben estar claramente definidos y comunicados.

### ***Procedimientos de detección y notificación***

Sistema de monitoreo y alerta temprana: Se establecerá un sistema de monitoreo y alerta temprana que permita detectar de manera inmediata cualquier falla o interrupción del servicio.

***Procedimientos de notificación:*** Se establecerán procedimientos claros para notificar al equipo de respuesta y a los usuarios de la banca electrónica en caso de una falla o interrupción del servicio.

### ***Procedimientos de recuperación***

Identificación de la falla: En caso de que se presente una falla, se debe identificar la causa de esta para poder implementar las medidas correctivas necesarias.

**Priorización de las acciones:** El equipo de respuesta debe priorizar las acciones necesarias para recuperar el servicio lo más pronto posible y minimizar el impacto en los usuarios de la banca electrónica.

**Restablecimiento del servicio:** Una vez que se han realizado las acciones necesarias, se procederá al restablecimiento del servicio de la banca electrónica. Es importante realizar pruebas para verificar que el servicio está funcionando correctamente.

**Evaluación post-falla:** Despues de restablecer el servicio, se debe realizar una evaluación post-falla para identificar las causas de esta y tomar medidas preventivas para evitar que se repita en el futuro.

#### ***Procedimientos de comunicación con los usuarios***

**Comunicación en caso de falla:** Se establecerán procedimientos claros para comunicar de manera oportuna a los usuarios de la banca electrónica en caso de una falla o interrupción del servicio.

**Información a los usuarios:** Es importante brindar información clara y precisa sobre la falla y el proceso de recuperación para mantener informados a los usuarios de la banca electrónica.

#### ***Procedimientos de entrenamiento y simulación***

**Entrenamiento del equipo de respuesta:** Es importante que el equipo de respuesta esté entrenado y familiarizado con los procedimientos establecidos en este plan de recuperación.

**Simulaciones periódicas:** Se realizarán simulaciones periódicas para verificar la efectividad del plan de recuperación y asegurarse de que todos los miembros del equipo estén familiarizados con los procedimientos establecidos.

### ***Actualización y revisión del plan de recuperación***

**Revisión periódica del plan:** Se revisará periódicamente este plan de recuperación para asegurarse de que esté actualizado y sea efectivo.

**Actualización del plan:** En caso de que se identifiquen cambios significativos en la banca electrónica o en el entorno operativo, se actualizará.

**Tabla 17.** Escenarios de fallos

Escenario de fallo	Impacto	Objetivos de recuperación	Tiempo máximo de recuperación	Nivel de servicio durante la recuperación
<b>Falla en el servidor</b>	La banca electrónica no está disponible	Restaurar el servicio de la banca electrónica	4 horas	No disponible durante la recuperación
<b>Error en la base de datos</b>	Los datos de los clientes pueden ser incorrectos o inaccesibles	Restaurar los datos de la base de datos y garantizar la integridad de los datos	6 horas	No disponible durante la recuperación
<b>Error de programación</b>	Los clientes pueden experimentar problemas al realizar transacciones	Identificar y corregir el error de programación	2 horas	Disponible con algunas limitaciones durante la recuperación
<b>Ataque cibernético</b>	La seguridad de los datos de los clientes está comprometida	Restaurar la seguridad de los datos y garantizar la confidencialidad de la información	12 horas	No disponible durante la recuperación

Nota. La tabla describe los escenarios de fallo, el impacto y los objetivos que se requieren para su recuperación exitosa con los tiempos máximos. Fuente: elaboración propia.

## **Instructivo de recuperación aplicación/base de datos banca electrónica**

La recuperación de una base de datos de banca electrónica puede ser un proceso complejo y delicado, pero aquí hay algunos pasos que puedes seguir:

- Identifica el problema: Lo primero que debes hacer es identificar el problema en la base de datos. Puede ser una falla de hardware o software, un ataque cibernético, un error humano, entre otros.
- Detén la actividad en la base de datos: Detén toda actividad en la base de datos lo antes posible para evitar que se produzcan daños adicionales.
- Realiza una copia de seguridad: Si tienes una copia de seguridad de la base de datos, intenta restaurarla. Asegúrate de que la copia de seguridad esté actualizada y sea compatible con la versión actual de la base de datos.
- Intenta recuperar la base de datos: Si no tienes una copia de seguridad o la copia de seguridad no es suficiente, intenta recuperar la base de datos utilizando herramientas de recuperación de datos o contratando un servicio de recuperación de datos profesional.
- Revisa la integridad de la base de datos: Una vez que hayas recuperado la base de datos, revisa su integridad. Comprueba que todos los datos estén presentes y sean precisos. Si hay algún problema, intenta solucionarlo.
- Restaura la actividad en la base de datos: Una vez que la base de datos esté recuperada y verificada, restaura la actividad en la base de datos de manera gradual. Asegúrate de que todo esté funcionando correctamente y de que los usuarios puedan acceder a sus cuentas sin problemas.

Es importante tener en cuenta que la recuperación de una base de datos de banca electrónica puede ser un proceso complejo y es recomendable contar con un equipo de profesionales capacitados en el manejo de bases de datos y seguridad informática. Además, es importante tener un plan de contingencia en caso de una posible falla en la base de datos.

**Tabla 18.** Inventario de servidores de centros de datos

Servidor	SRV-DC01	SRV-DB01	SRV-APP01	SRV-FILE01	SRV-MAIL01
Rol	Servidor de aplicaciones	Servidor de base de datos	Servidor de aplicaciones	Servidor de archivos	Servidor de correo electrónico
Modelo	HP ProLiant DL360 G9	Dell PowerEdge R740	HPE ProLiant DL380 Gen10	NetApp AFF A220	Cisco UCS C220 M5
Sistema Operativo	Windows Server 2019	Red Hat Enterprise Linux 7	Windows Server 2019	ONTAP 9.9	Microsoft Exchange Server 2016
Número de procesadores	2	2	2	2	2
Número de núcleos por procesador	10	12	18	18	16
Cantidad de procesadores	40	48	72	72	64
CPU	Intel Xeon E5-2640 v4	Intel Xeon Gold 6240	Intel Xeon Gold 6244	Intel Xeon Gold 6248	Intel Xeon Gold 6244
Almacenamiento	Almacenamiento en disco duro SAS	Almacenamiento en disco duro SAS	Almacenamiento en disco duro SAS	Almacenamiento en discos duros SAS y SSD	Almacenamiento en unidad de estado sólido (SSD)

<b>Cantidad de almacenamiento</b>	4 TB	8 TB	4 TB	200 TB	1 TB
<b>Marca</b>	Hewlett Packard Enterprise	Dell Technologies	Hewlett Packard Enterprise	NetApp	Cisco
<b>Servidor</b>	<b>SRV-WEB01</b>	<b>SRV-RESP01</b>	<b>SRV-VIRT01</b>	<b>SRV-WSUS01</b>	<b>SRV-SEG01</b>
<b>Rol</b>	Servidor WEB	Servidor de respaldo	Servidor de virtualización	Servidor de continuidad	Servidor de seguridad
<b>Modelo</b>	IBM System x3650 M5	Dell EMC PowerEdge R740	Supermicro SuperServer 6028U-TR4T+	Lenovo ThinkSystem SR630	Huawei FusionServer RH5885H V3
<b>Sistema Operativo</b>	CentOS 7	Windows Server 2016	VMware ESXi 7.0	VMware ESXi 6.7	Ubuntu Server 20.04
<b>Número de procesadores</b>	2	2	2	1	2
<b>Número de núcleos por procesador</b>	10	18	22	8	24
<b>Cantidad de procesadores</b>	40	72	88	16	96
<b>CPU</b>	Intel Xeon E5-2680 v4	Intel Xeon Gold 6248	Intel Xeon E5-2699 v4	Intel Xeon Silver 4210	Intel Xeon Platinum 8280
<b>Almacenamiento</b>	Almacenamiento en unidad de estado sólido (SSD)	Almacenamiento en discos duros SAS	Almacenamiento en disco duro SAS	Almacenamiento en disco duro SATA	Almacenamiento en disco duro SAS
<b>Cantidad de almacenamiento</b>	1 TB	10 TB	20 TB	2 TB	12 TB

<b>Marca</b>	IBM	Dell EMC	Supermicro	Lenovo	Huawei
--------------	-----	----------	------------	--------	--------

Nota. La tabla los servidores que el banco hace uso para sus procesos considerados en este documento. Fuente: elaboración propia.

**Tabla 19.** Información de red de servidores de centros de datos

	<b>Dirección IP</b>	<b>Dirección MAC</b>	<b>Subnet Mask</b>	<b>Usuario registrado</b>	<b>Domain/Workgroup</b>
<b>SRV-DC01</b>	10.1.1.11	00:0C:29:F7:4C:14	srv-dc01.company.local	255.255.255.0	admin
<b>SRV-DB01</b>	10.1.1.12	00:50:56:C0:00:08	srv-db01.company.local	255.255.255.0	dbadmin
<b>SRV-APP01</b>	10.1.1.13	00:50:56:C0:00:09	srv-app01.company.local	255.255.255.0	appadmin
<b>SRV-FILE01</b>	10.1.1.14	00:50:56:C0:00:10	srv-file01.company.local	255.255.255.0	fileadmin
<b>SRV-MAIL01</b>	10.1.1.15	00:50:56:C0:00:11	srv-mail01.company.local	255.255.255.0	mailadmin
<b>SRV-WEB01</b>	10.1.1.16	00:50:56:C0:00:12	srv-web01.company.local	255.255.255.0	webadmin
<b>SRV-RESP01</b>	10.1.1.17	00:50:56:C0:00:13	srv-print01.company.local	255.255.255.0	printadmin
<b>SRV-VIRT01</b>	10.1.1.18	00:50:56:C0:00:14	srv-vpn01.company.local	255.255.255.0	vpnadmin

<b>SRV-WSUS01</b>	10.1.1.19	00:50:56:C0:00:15	srv-wsus01.company.local	255.255.255.0	wsusadmin
<b>SRV-SEG01</b>	10.1.1.20	00:50:56:C0:00:16	srv-antivirus01.company.local	255.255.255.0	antivirusadmin

Nota. La tabla describe como se encuentra la conexión de los servidores a disposición del banco. Fuente: elaboración propia.

### **Análisis de Riesgo**

Un análisis de riesgo es un proceso sistemático para identificar, evaluar y controlar los riesgos asociados con una actividad, proyecto, proceso o sistema. El análisis de riesgo en los ámbitos bancarios es utilizado para la evaluación y gestión de los riesgos asociados con las actividades financieras y de inversión. El proceso de análisis de riesgo en una entidad bancaria generalmente involucra lo siguiente:

- Identificación de los riesgos
- Evaluación de los riesgos
- Desarrollo de estrategias de mitigación
- Monitoreo continuo

Es importante que este proceso de análisis de riesgo sea un proceso continuo y dinámico, ya que los riesgos y las estrategias de mitigación pueden cambiar en base al tiempo, por lo tanto, se debe de tener en cuenta los cambios de los flujos de activos críticos.

Los procesos críticos identificados analizados en procesos y servicios bancarios son los procesos que aportan un continuo cambio y evolución sistemática y de carácter

importante para que el negocio continúe prestando el servicio, en base a eso se analizan los siguientes procesos:

- Proceso de tipo de cambio
- Proceso de token de seguridad banca en línea
- Proceso de Alta disponibilidad de banca en línea
- Proceso de validación de cuentas ACH y propias

**Tabla 20.** Tabla de riesgos

#	Riesgo	Consecuencia	Acción
1	Proceso de consulta en el tipo de cambio monetario del banco.	Genera mal funcionamiento al momento de que los servicios externos y propios utilicen el WebService de consulta para verificar el tipo de cambio de moneda nacional e internacional.	1. Determinar el origen del incidente. 2. Monitoreo constante. 3. Implementación de mecanismos de seguridad en contra de ataques de negación de servicios.
2	Proceso de generación de token de seguridad para la banca en línea.	Afecta a la seguridad de los usuarios que utilizan los diferentes servicios con los que cuenta la banca en línea, al no generarse el token de seguridad los usuarios no pueden ingresar y hacer uso de las opciones.	1. Generación de políticas de seguridad para la continuidad del servicio. 2. Alta disponibilidad del servicio. 3. Limitar el tiempo de validez de los tokens.

			<p>4. Verificar las solicitudes de generación de token.</p> <p>5. Aplicar permisos de seguridad.</p> <p>6. Monitorear continuamente el servicio.</p>
3	Proceso de alta disponibilidad en el servicio de publicación de banca en línea.	Afecta a la alta disponibilidad de las aplicaciones expuestas para usuarios internos y externos como lo son (banca en línea, validaciones, WS, etc.).	<p>1. Implementar redundancia en servidores, redes e infraestructura de almacenamiento.</p> <p>2. Implementar balanceadores de carga.</p> <p>3. Implementar plan de recuperación ante desastres.</p> <p>4. Monitorear continuamente el rendimiento.</p> <p>5. Contar con mantenimientos periódicos.</p>
4	Proceso de validación de cuentas ACH y de cuentas propias del banco.	La no validación de las cuentas al momento que los usuarios quieran ingresar una nueva cuenta ya sea	<p>1. Determinar el origen del incidente.</p>

	<p>de otros bancos o de cuentas propias del banco, este proceso afecta al flujo monetario en servicios digitales.</p>	<p>2. Verificación de identidad del usuario.</p> <p>3. Verificación de cuentas bancarias, validación de la información de la cuenta.</p> <p>4. Autenticación de dos factores.</p> <p>5. Monitoreo constante.</p>
--	---	--

Nota. Dentro de este se describe los riesgos lo que puede ser la fuente y la acción recomendada para mitigar o eliminarlo. Fuente: elaboración propia.

Para la identificación de los procesos críticos de la institución se procede a la indicación de los procesos que se determinaron como más importantes y que tienen un nivel de importancia en el flujo informático como servicios que se proporcionan a los clientes finales. Estos procesos informáticos se identifican y evalúan cual es el nivel de riesgo afectado y las consecuencias de cada uno.

Los procesos informáticos bancarios pueden incluir la gestión de cuentas, transferencias electrónicas, procesamiento de tarjetas de crédito, procesamiento de cheques, entre otros. Cualquier falla o brecha de seguridad en estos procesos puede tener consecuencias graves para los clientes del banco y para la institución bancaria en sí misma. Por lo tanto, es fundamental realizar un análisis de riesgos para procesos informáticos bancarios.

## Evaluación del riesgo

Para la evaluación del riesgo en procesos bancarios se evalúan las vulnerabilidades y las amenazas en los procesos críticos de los servicios y de tecnologías digitales de información, con el fin de poder identificar y mitigar los riesgos asociados. Para llevar a cabo el análisis de riesgo informático en procesos bancarios es necesario utilizar diferentes técnicas y herramientas, como pruebas de penetración, evaluación de vulnerabilidades, análisis de amenazas y evaluación de impacto en el negocio.

Con base a los resultados del análisis, se pueden establecer medidas de seguridad y controles para la reducción de ataques cibernéticos y proteger la integridad, confidencialidad y disponibilidad de los datos y sistemas. Estos controles pueden incluir la implementación de firewalls, sistemas de detección de intrusiones, cifrado de datos y la capacitación de empleados en seguridad informática.

**Tabla 21.** Procesos bancarios de mayor riesgo

#	Nombre	Descripción	Tipo	Ubicación	Critico
1	Proceso de consulta en el tipo de cambio monetario del banco.	Consulta del tipo de cambio en moneda internacional.	Consulta (virtual)	Centro de datos	SI
2	Proceso de generación de token de seguridad para la banca en línea.	Generación de token de seguridad para usuarios de banca en línea.	Generado (virtual)	Centro de datos	SI
3	Proceso de alta disponibilidad en el servicio de publicación de web del banco	Alta disponibilidad de los servicios	Servidores (físico)	Centro de datos	SI
4	Proceso de validación de cuentas ACH y de cuentas propias del banco.	Validar cuentas ACH de otros bancos y de cuentas propias.	Consulta (virtual)	Centro de Datos	SI

Nota. Dentro de este se describe los riesgos lo que puede ser la fuente y la acción recomendada para mitigar o eliminarlo. Fuente: elaboración propia.

**Tabla 22.** Cálculo de probabilidad

cualitativo	Cuantitativo	Descripción
<b>Media</b>	2	La amenaza puede suceder a lo sumo una vez al mes
<b>Media</b>	2	La amenaza puede suceder a lo sumo una vez al mes
<b>Alta</b>	1	La amenaza puede suceder a lo sumo una vez al año
<b>Media</b>	2	La amenaza puede suceder a lo sumo una vez al mes

Nota. Establece de manera cualitativa y cuantitativamente la probabilidad de riesgo. Fuente: elaboración propia.

**Tabla 23.** Cálculo de impacto

cualitativo	Cuantitativo	Descripción
<b>Media</b>	2	El daño derivado de la materialización de la amenaza tiene consecuencias para la institución.
<b>Media</b>	2	El daño derivado de la materialización de la amenaza tiene consecuencias para la institución.
<b>Alta</b>	1	El daño derivado de la materialización de la amenaza tiene consecuencias graves para la institución.

<b>Media</b>	2	El daño derivado de la materialización de la amenaza tiene consecuencias para la institución.
--------------	---	---

Nota. Establece de manera cualitativa y cuantitativamente impacto riesgo. Fuente: elaboración propia.

## **Matriz de Riesgo**

Es una herramienta utilizada en la gestión de riesgos para visualizar y priorizar los riesgos potenciales asociados con un proyecto, proceso o sistema. La matriz de riesgo también se conoce como matriz de probabilidad-impacto, matriz de evaluación de riesgos o matriz de valoración de riesgos.

La matriz de riesgo generalmente se representa como una tabla o matriz que muestra los riesgos identificados en el eje horizontal y el eje vertical, respectivamente. Cada riesgo se evalúa según dos criterios: la probabilidad de que ocurra y el impacto que tendría en el proyecto, proceso o sistema en caso de que ocurriera. Por lo general, la probabilidad se mide en términos de baja, media o alta, mientras que el impacto se mide en términos de bajo, medio o alto.

La intersección de la probabilidad y el impacto de cada riesgo se representa en la matriz de riesgo como una celda o cuadrante, y se le asigna una prioridad o nivel de riesgo en función de la evaluación. Los riesgos con alta probabilidad e impacto se consideran de alta prioridad y deben ser tratados con medidas de mitigación, mientras que los riesgos con baja probabilidad e impacto pueden ser aceptados o monitoreados sin medidas de mitigación.

**Tabla 24.** Matriz de riesgo de activos

Activo	Valor del activo	Probabilidad de ocurrencia (Amenaza)	Amenaza	Vulnerabilidad	Probabilidad de ocurrencia (Vulnerabilidad)	Impacto	Riesgo	Incidente de Seguridad	Tipo de tratamiento
Base de datos	4	3	inyección SQL	Malas prácticas de programación del desarrollador.	3	4	Moderado	Compromete la integridad	Mitigar
Aplicación Web	4	3	Ataque de denegación de servicios.	Falta configuración incorrecta de WAF.	4	3	Alto	Compromete la integridad	Mitigar
		3	Caída del servidor	Saturación de los recursos del servidor	3	5	Moderado	Compromete la disponibilidad	Aceptar
		5	Acceso no autorizado a servidor	Mala configuración de VPN	3	3	Crítico	Compromete la confidencialidad	Eliminar
Infraestructura	3	5	Pérdida de conexión a internet	Falla por parte de proveedores ISP	4	4	Crítico	Compromete la disponibilidad	Mitigar

Activo	Valor del activo	Probabilidad de ocurrencia (Amenaza)	Amenaza	Vulnerabilidad	Probabilidad de ocurrencia (Vulnerabilidad)	Exposición o Probabilidad (Amenaza x Vulnerabilidad)	Impacto	Riesgo	Incidente de Seguridad	Tipo de tratamiento (Aceptar, mitigar, eliminar, transferir (compartir))
Base de Datos	4	4	destrucción de registros	Falta de Implementación de copias de seguridad periódicas	2		4	Moderado	Compromete la integridad y confiabilidad	Aceptar
		3	Acceso no autorizado	Mal manejo de roles y perfiles en bases de datos, faltas de esquemas de seguridad	3		3	Moderado	Compromete la confidencialidad	Mitigar
Aplicación Web	4	3	Caída del servidor	Saturación de los recursos del servidor	3		5	Moderado	Compromete la disponibilidad	Aceptar
		4	Exposición de credenciales.	Falta de cifrado de datos	3		3	Alto	Compromete la integridad y confiabilidad	Eliminar
		4	Robo de información	Falta de métodos de validación de identidad del usuario.	2		4	Moderado	Compromete la confidencialidad	Eliminar

		5	Acceso no autorizado a servidor	Mala configuración de VPN	3		3	Crítico	Compromete la confidencialidad	Eliminar
Infraestructura	3	5	Pérdida de conexión a internet	Falla por parte de proveedores ISP	4		4	Crítico	Compromete la disponibilidad	Mitigar
<b>Proceso: Generación de token de seguridad para la banca en línea</b>										

Activo	Valor del activo	Probabilidad de ocurrencia	Amenaza	Vulnerabilidad	Probabilidad de ocurrencia	Exposición Probabilidad	Impacto	Total , riesgo	Riesgo	Incidente de Seguridad	Tipo de tratamiento
Infraestructura	3	5	Pérdida de conexión a internet	Falla por parte de proveedores ISP	4	20	4	300	Crítico	Compromete la disponibilidad	Mitigar
	3	3	Falla del hardware de servidor critico	Mala configuración en servidores	3	9	4	81	Moderado	Compromete la disponibilidad	Mitigar
	3	5	Ataque cibernético	puestas de ingreso, falta de políticas, puertos expuestos	5	25	4	375	Crítico	Compromete la disponibilidad	Mitigar
	3	4	Errores de configuración en la red	falta de configuración a nivel de infraestructura	4	16	3	192	Moderado	Compromete la disponibilidad	Mitigar

	3	2	Interrupción del suministro eléctrico	falta de planificación	2	4	2	24	Modera	Compro mete la disponibiliad	Mitigar
	3	3	fallas de software	Mala configuración de equipos	3	9	3	81	Modera	Compro mete la disponibiliad	Mitigar
	3	4	Problemas de continuidad de red	falta de planificación	4	16	4	192	Modera	Compro mete la disponibiliad	Mitigar
<b>Proceso: Alta Disponibilidad en servicio de publicación de banca en línea</b>											

Activo	Valor del activo	Probabilidad de ocurrencia	Amenaza	Vulnerabilidad	Probabilidad de ocurrencia	Impacto	Riesgo	Incidente de Seguridad	Tipo de tratamiento
Base de datos	4	3	inyección SQL	Malas prácticas de programación del desarrollador.	3	4	Moderado	Compromete la integridad	Mitigar
		4	destrucción de registros	Falta de Implementación de copias de seguridad periódicas	2	4	Moderado	Compromete la integridad y confiabilidad	Aceptar
		3	Acceso no autorizado	Mal manejo de roles y perfiles en bases de	3	3	Moderado	Compromete la confidencialidad	Mitigar

				datos, faltas de esquemas de seguridad					
<b>Aplicación Web</b>	4	3		Falta configuración incorrecta de WAF.	4	3	Alto	Compromete la integridad	Mitigar
		3	Caída del servidor	Saturación de los recursos del servidor	3	5	Moderado	Compromete la disponibilidad	Aceptar
<b>Infraestructura</b>	3	5	Pérdida de conexión a internet	Falla por parte de proveedores ISP	4	4	Crítico	Compromete la disponibilidad	Mitigar
<b>Proceso: Validación de cuentas ACH y propias</b>									

Nota. Planeación de los activos y los riesgos que fueron identificado y su correspondiente evaluación. Fuente: elaboración propia.

### Plan de tratamiento

El plan de tratamiento de riesgos se crea después de realizar una evaluación y una matriz de riesgos, y es una parte clave de la gestión de riesgos. El objetivo del plan de tratamiento de riesgos es establecer un conjunto de medidas para reducir la probabilidad y/o el impacto de los riesgos identificados. Estas medidas pueden incluir:

- Evitar el riesgo: Eliminar la fuente de riesgo o cambiar la actividad para evitar el riesgo por completo.
- Transferir el riesgo: Desviar el riesgo a otra parte, como una compañía de seguros o un tercero.
- Mitigar el riesgo: Reducir la probabilidad y/o el impacto del riesgo mediante la implementación de medidas de control, como políticas de seguridad, capacitación de empleados, redundancia de sistemas, entre otras.
- Aceptar el riesgo: Reconocer el riesgo y decidir no tomar medidas de mitigación, ya sea porque el costo de las medidas es mayor que el riesgo en sí o porque no es posible reducirlo significativamente.

**Tabla 25.** Plan de tratamiento

Riesgo identificado	Probabilidad	Impacto	Nivel de prioridad	Medidas de mitigación	Responsable	Fecha de implementación
Pérdida de datos	Alta	Alto	Alta	Implementación de medidas de seguridad, copias de respaldo y sistemas de recuperación de datos	Equipo de seguridad informática	30 de abril de 2023

<b>Interrupción del servicio</b>	Media	Alto	Media	Implementación de medidas de redundancia, actualizaciones y mantenimiento preventivo	Equipo de soporte informático	15 de mayo de 2023
<b>Acceso no autorizado</b>	Media	Medio	Media	Implementación de medidas de autenticación, control de acceso y monitorización de actividad	Equipo de seguridad informática	1 de junio de 2023
<b>Brechas de seguridad</b>	Baja	Alto	Media	Implementación de medidas de seguridad, auditorías de seguridad y pruebas de penetración	Equipo de seguridad informática	15 de junio de 2023
<b>Errores del usuario</b>	Alta	Bajo	Baja	Capacitación y entrenamiento de los usuarios, implementación de controles de entrada de datos	Equipo de soporte informático	30 de junio de 2023

Riesgo identificado	Probabilidad	Impacto	Nivel de prioridad	Medidas de mitigación	Responsable	Fecha de implementación
<b>Errores en la entrada de tipo de cambio</b>	Alta	Medio	Alta	Implementación de controles de entrada de datos, revisión y validación por un segundo usuario, automatización de procesos de validación	Equipo de contabilidad	30 de abril de 2023

<b>Cambios en las tasas de cambio sin autorización</b>	Media	Alto	Media	Implementación de medidas de seguridad, monitoreo y auditoría de los cambios de tasas de cambio, verificación de la autorización para realizar cambios	Equipo de auditoría	15 de mayo de 2023
<b>Falta de actualización de las tasas de cambio</b>	Baja	Bajo	Baja	Implementación de un calendario de actualización de tasas de cambio, automatización de actualizaciones, seguimiento de la actualización	Equipo de contabilidad	1 de junio de 2023
<b>Uso de tasas de cambio obsoletas</b>	Media	Medio	Media	Implementación de un proceso de revisión y actualización periódica de las tasas de cambio, automatización de procesos de actualización	Equipo de contabilidad	15 de junio de 2023

Riesgo identificado	Probabilidad	Impacto	Nivel de prioridad	Medidas de mitigación	Responsable	Fecha de implementación
<b>Generación de tokens débiles</b>	Alta	Alto	Alta	Implementación de un algoritmo de generación de tokens seguro, uso de claves criptográficas fuertes, uso de algoritmos de hash seguros	Equipo de seguridad informática	30 de abril de 2023
<b>Pérdida o robo de tokens</b>	Media	Alto	Media	Implementación de medidas de seguridad física para almacenamiento de tokens, monitoreo y auditoría de la emisión y uso de tokens, implementación de un proceso para revocar y reemplazar tokens perdidos o robados	Equipo de seguridad informática	15 de mayo de 2023
<b>Ataques de fuerza bruta</b>	Alta	Medio	Alta	Implementación de medidas de seguridad para limitar la frecuencia de intentos de autenticación, monitoreo y alerta en caso de intentos fallidos de autenticación, implementación de medidas de bloqueo de cuentas después de un número determinado de intentos fallidos	Equipo de seguridad informática	30 de mayo de 2023

<b>Tokens expirados o revocados en uso</b>	Baja	Medio	Baja	Implementación de un proceso de monitoreo de tokens expirados o revocados, implementación de medidas de bloqueo o alerta en caso de uso de tokens expirados o revocados	Equipo de seguridad informática	15 de junio de 2023
--	------	-------	------	---	---------------------------------	---------------------

Riesgo identificado	Probabilidad	Impacto	Nivel de prioridad	Medidas de mitigación	Responsable	Fecha de implementación
<b>Cuentas fraudulentas</b>	Media	Alto	Alta	Implementación de una validación de identidad sólida para la creación de cuentas, monitoreo constante de las cuentas para detectar actividad inusual, implementación de un proceso de verificación de cuentas de alto riesgo	Equipo de seguridad informática	30 de abril de 2023
<b>Ataques de suplantación de identidad</b>	Media	Alto	Alta	Implementación de medidas de autenticación de dos factores para la verificación de identidad, monitoreo constante de las cuentas para detectar actividad inusual, implementación de un proceso de verificación	Equipo de seguridad informática	15 de mayo de 2023

				de cuentas de alto riesgo		
<b>Pérdida o robo de credenciales de acceso</b>	Baja	Alto	Media	Implementación de medidas de seguridad física para el almacenamiento de credenciales de acceso, implementación de medidas de autenticación de dos factores para el acceso a la información de la cuenta	Equipo de seguridad informática	30 de mayo de 2023
<b>Errores humanos en la validación de cuentas</b>	Alta	Medio	Media	Implementación de un proceso de verificación de cuentas por pares, implementación de medidas de control de calidad en la validación de cuentas	Equipo de validación de cuentas	15 de junio de 2023

Nota. Planteamiento del tratamiento de los riesgos anteriormente planteados.

Fuente: elaboración propia.

## **¿Qué estándar del sistema de Gestión de Continuidad del Negocio implementaría?**

Se implementaría la norma ISO 22301, debido a que este establece un marco para la correcta gestión del negocio con objetivos claros con el objetivo de crear, mantener y mejorar un sistema de gestión de continuidad, esto con la finalidad de poder garantizarle a la agencia bancaria que sus procesos tengan buenos soportes y esta pueda continuar sus operaciones ante cualquier interrupción. Claramente este estándar es uno con los mayores grados de madurez y que contempla todo en la organización siendo de mucho beneficio hacia esta.

Dentro de las etapas y características de este estándar se encuentran los siguientes que benefician grandemente estos procesos bancarios:

### **Comprensión del contexto de la organización**

Dentro de esta etapa, la entidad bancaria plantearía y comprendería su contexto, es decir, sus procesos, las variables que estas incluyen son los factores internos y externos que pueden afectar su capacidad para garantizar la continuidad de sus operaciones críticas. Además, identifica y comprende cada requisito relevante para cada parte interesada dentro de estos procesos, como la alta administración, la seguridad, la auditoria, entre otros, esto con la finalidad de comprender en su totalidad el contexto y considerar cada aspecto que sea necesario mantenerlo en la continuidad del negocio.

### **Liderazgo y compromiso**

En esta se debe de declarar bien quienes serán la alta dirección de la organización que deberá de liderar la implementación del sistema de gestión de continuidad y comprometerse a proporcionar los recursos necesarios. También en donde se abarque

la cultura de la empresa y los valores de la organización enfocados en la continuidad del negocio y gestiones de riesgos, para garantizar una transparencia completa en esta alta gerencia y total responsabilidad con cada proceso que se cree.

### **Planificación**

Para la planificación la entidad bancaria debe de encargar al departamento indicado para conllevar la planificación y establecer claramente los objetivos y políticas que tendrá la continuidad del negocio en conjunto con la alta directiva, para poder identificar cada proceso desde el menos significante hasta los más críticos para la entidad, esto también comprende la evaluación de los riesgos en cualquier ámbito.

### **Implementación**

En esta etapa, la organización debe implementar los procesos y controles necesarios para garantizar la continuidad de sus operaciones críticas, estos que fueron planteados en la planificación. Esto puede incluir planes de contingencia y recuperación de desastres, así como la implementación de medidas de mitigación y controles preventivos, los cuales son de suma importancia para la entidad bancaria, esto claramente ayudara con la continuidad de negocio lo cual es fundamental para esta, además de que esta etapa es crítica por lo que la alta gerencia debe de estar involucrada ante cualquier adversidad y poder tomar acciones inmediatas.

### **Evaluación de la capacidad de respuesta**

En esta etapa, la entidad bancaria debe de plantear un control para la evaluación regular de capacidad de su sistema de continuidad del negocio para responder a las interrupciones y garantizar la continuidad de sus operaciones críticas, de esta manera logrará mantener su sistema listo ante cualquier adversidad en la que pueda encontrarse.

Esto puede incluir pruebas y simulaciones de desastres, revisiones periódicas y evaluaciones de la efectividad del sistema de continuidad del negocio.

### **Mejora continua**

En esta etapa, la entidad bancaria debe llevar a cabo acciones de mejora continua para mejorar la efectividad de su sistema para garantizar que pueda adaptarse a los cambios en el contexto y los requisitos de las partes interesadas que involucra cada proceso que quieran mantener. Esto puede incluir la revisión y actualización de políticas, nuevos objetivos, la mejora de procesos y controles, la implementación de nuevas tecnologías, entre otros, con el fin de mantener el sistema actualizado, seguro y con su capacidad de respuesta alta, de esta manera encontrarán muy efectiva esta implementación de la norma 22301.

## Ciclo de vida

Finalmente, algo muy importante por lo que es muy conocido este estándar es acerca de su ciclo de vida, la cual propone una mejora continua todo el tiempo como un sistema que se mejora conforme el tiempo avanza, dentro este ciclo de vida se caracterizan estos puntos: planificar, hacer, verificar y actuar, proveyendo este tipo de ciclo en la siguiente figura:

**Figura 20.** Ciclo de vida del estándar 22301



Nota. Imagen sobre el ciclo de vida del estándar 22301. Fuente: Inter empresas ([https://www.interempresas.net/FeriaVirtual/Catalogos\\_y\\_documentos/87942/Continuidad\\_Negocio-ISO-22301.pdf](https://www.interempresas.net/FeriaVirtual/Catalogos_y_documentos/87942/Continuidad_Negocio-ISO-22301.pdf)).

### Planificar

Dentro esta etapa de vida, se identificaría los procesos y servicios bancarios críticos para la continuidad del negocio, como se puede ver en la imagen anterior en esta se plantean los objetivos y políticas para el sistema de gestión de continuidad, con la base de esto realizar un análisis de impacto y riesgo de los procesos y servicios

identificados, para que finalmente se proceda con la creación de los planes de contingencia y recuperación ante las adversidades que puedan ocurrir.

### ***Hacer***

En esta etapa se tiene que implementar los controles planteados en la planificación que son medidas de mitigación y prevención de los riesgo planteados de los servicios bancarios, como se ve en la figura anterior en esta se involucra a todas las partes interesadas y la gestión en sí, además también se comprende como la implementación del sistema de seguridad y la asignación de responsables tanto como procesos pequeños dentro de la organización hasta procesos grandes de telecomunicaciones, los cuales puedan perjudicar en el funcionamiento de los servicios bancarios.

### ***Verificar***

Dentro de este punto claramente se trata de verificar lo implementado sobre los servicios y procesos bancarios que se identificaron para que los controles sean verificados y así poder evaluar la capacidad de respuesta de estos, para garantizar una pronta reacción. En este mismo paso se puede mejorar o actualizar lo que ya se ha implementado.

### ***Actuar***

Finalmente, en actuar pues se consideran tomar medidas correctivas y preventivas basadas en los resultados de las pruebas realizadas en la etapa de verificación, y encontrar en esos procesos críticos algunos puntos débiles claramente identificados con KPI (indicadores de desempeño) para poder realizar acciones correspondientes.

## Administración de la continuidad de negocio

### Plan de concientización a los usuarios

#### **Objetivo general**

Planificar el proceso para sensibilizar y capacitar a cada uno de los empleados de la organización con el fin de que conozcan los peligros a los que se encuentran expuestos y que acciones pueden tomar ante cualquier incidente para evitar la interrupción de los servicios o disminuir el impacto.

#### **Objetivos específicos**

**Figura 21.** Plan de concientización de usuarios



Nota. Propuesta de plan de concientización hacia los usuarios del banco.

Fuente: elaboración propia.

En el programa se tienen tres objetivos que van de la mano y en secuencia, ya que uno depende del anterior para garantizar el impacto y aprendizaje que se desea obtener en cada fase.

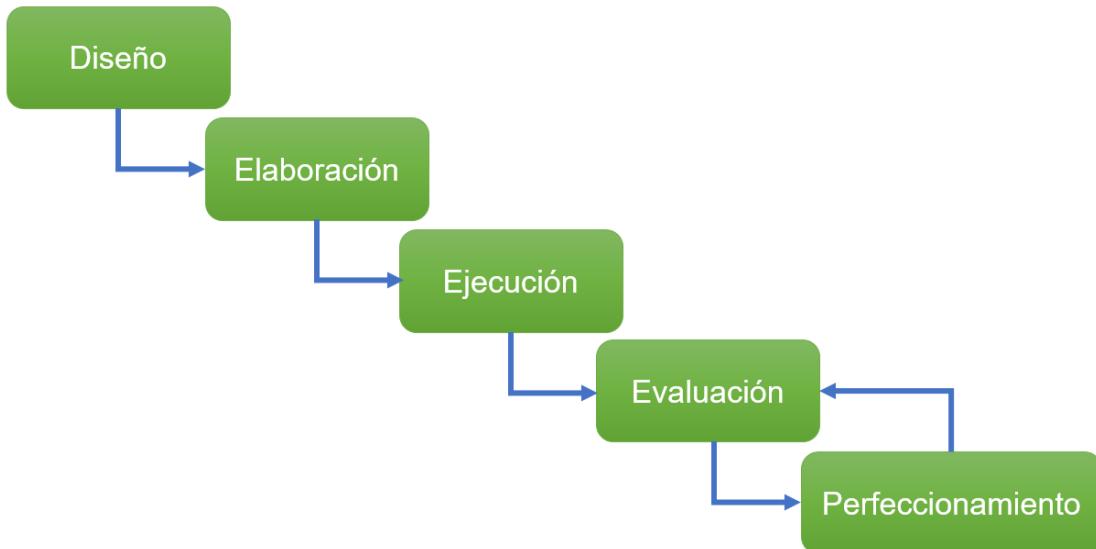
- Sensibilizar: Crear responsabilidad a través de un estímulo presentado, con el fin de que el empleado entienda la importancia de tomar acciones preventivas a los diferentes riesgos.
- Ejercitar: Se buscará crear hábitos en los empleados que garanticen la protección de los procesos y continuidad de la operación, a través de diferentes métodos y dinámicas incluidas dentro de la capacitación.

- Enseñar: Brindar conocimiento acerca de los riesgos que pueden perjudicar a la empresa de tal manera que sus operaciones se detengan.

Dentro del plan se pretende establecer los temas de aprendizaje para las áreas de acuerdo con las tareas que realizan o sistemas que sean de su uso diario, definir quienes recibirán los temas propuestos y cuánto tiempo durará la capacitación aproximadamente. Con el fin de que todos los colaboradores de la empresa estén capacitados y preparados para ejecutar y darle mantenimiento y seguimiento al plan de gestión de riesgos en cada una de las áreas de la organización sin importar que no sean técnicos certificados o expertos en informática ya que en cada área existe el riesgo de detener las operaciones por cualquier evento repentino.

### **Fases del plan de concientización a los usuarios**

**Figura 22.** Fases del plan de concientización



Nota. Etapas o las fases de la creación y ejecución del plan de concientización de los usuarios. Fuente: elaboración propia.

## 1. Diseño

Se detallan las necesidades y prioridades de la empresa respecto al tema de continuidad del negocio para definir y apoyar la elaboración del modelo de capacitación.

### Necesidades de la empresa

- Se deben definir las responsabilidades que asumirán los empleados en caso de presentarse una emergencia y establecer cómo será la comunicación dentro de la estructura organizacional.
- Instaurar un método para gestionar los riesgos que pongan en peligro la operación de la empresa.
- Dar confianza a los proveedores y clientes que la empresa tiene contemplado cualquier situación desafortunada y un plan para actuar.
- Identificar vulnerabilidades en los procesos críticos de la empresa.
- Conocer las diferentes amenazas a la que se encuentran expuestos las personas o sistemas que tienen parte en los procesos críticos
- Calcular la probabilidad que ocurran las diferentes amenazas descritas en el punto anterior.
- Proveer a cada empleado las herramientas necesarias para ejecutar hábitos que garanticen la continuidad de sus operaciones.
- Dar a conocer a los empleados los planes de acción si llega a ocurrir un incidente.

### Modelo de capacitación

Se llevará a cabo un modelo parcialmente descentralizado, es decir, la sede principal definirá el método y estrategia de capacitación, pero si la empresa tiene diferentes sedes, cada sede será responsable de hacer llegar el plan a todos sus

empleados. Se define de esta forma ya que cada sede en especifica puede variar un poco el plan de acuerdo con los sistemas utilizados en su sede.

## 2. Elaboración del diseño

**Tabla 26.** Modelo de capacitación

Capacitación	Objetivo	Audiencia objetivo	Frecuencia	Metología	Duración	Carácter	Observaciones
El ABCD de la gestión de riesgos general	Conocer los conceptos básicos de la gestión de riesgos (probabilidad, impacto, exposición, disparador, mitigación, contingencia, etc.)	Todos los empleados.	Semestral	Plataforma de aprendizaje e-learning	12 horas	Obligatorio	Cada nuevo empleado que ingrese a la organización debe recibir esta capacitación de inmediato.
Concientización de seguridad	Garantizar que cada empleado pueda reconocer que actividades o errores pueden afectar a procesos de la empresa.	Todos los empleados.	Semestral	Plataforma de aprendizaje e-learning	5 horas	Obligatorio	Cuando ingresa un nuevo colaborador debe esperar la siguiente fecha para recibir la capacitación.
Gestión de riesgos especializado en la empresa	Dar a conocer el proceso para la gestión de riesgos en la empresa, como pueden reportarlo, con quien deben reportarlo, cual es el procedimiento estandar que se manejará en la empresa.	Todos los empleados.	Semestral	Plataforma de aprendizaje e-learning	3 horas	Obligatorio	Cada nuevo empleado que ingrese a la organización debe recibir esta capacitación de inmediato.
Principios de seguridad especializado en procesos de informática	Dar a conocer los principios de seguridad que toda persona que trabaje en un área de IT deba conocer.	Empleados de áreas de informática	Trimestral	Plataforma de aprendizaje e-learning	6 horas	Obligatorio	Cuando ingresa un nuevo colaborador al área de IT debe recibir la capacitación de inmediato.
Principios básicos de seguridad	Dar a conocer los principios básicos de seguridad para personas que no sean estudiantes de informática.	Todos los empleados. (menos el área de IT)	Semestral	Plataforma de aprendizaje e-learning	7 horas	Obligatorio	Cada nuevo empleado que ingrese a la organización debe recibir esta capacitación de inmediato.
Introducción a la evaluación de riesgos	Determinar directrices y acciones que se deben de tomar en cuenta al evaluar un riesgo.	Empleados de áreas de informática	Anual	Plataforma de aprendizaje e-learning	7 horas	Opcional	

Nota. Planteamiento acerca de la capacitación objetivo y otros puntos. Fuente:  
elaboración propia.

**Nota importante:** Cada curso tiene actividades de práctica interactivas y un examen final no solamente para evaluar el aprendizaje, sino también para crear hábitos y buenas prácticas en cada empleado de la empresa, sin importar el área a la que pertenezca.

### **3. Ejecución**

#### **Comunicación y aprobación de la junta directiva y gerentes**

Por medio de una reunión se dará a conocer todo el proceso establecido, cuánto tiempo llevará y costos del plan de concientización a los empleados, debido a que se seleccionó el modelo parcialmente descentralizado, en dicha reunión deben estar presentes la junta directiva y el gerente de cada sucursal para que puedan estar enterados y aprobar dicho plan, validar y evaluar si es viable el tiempo establecido o si se necesitarán realizar modificaciones debido a algún contratiempo.

Luego de ser aprobado el plan de concientización a los empleados se iniciaría la fase de ejecución.

#### **Comunicación a los empleados**

A los empleados de la organización se les dará a conocer por medio de correo electrónico boletines informativos simples y claros acerca del plan de capacitación para que cada área pueda tener en cuenta el tiempo que llevarán las capacitaciones y con base a eso organizar proyectos siguientes a realizar.

Luego de que toda la empresa esté debidamente informada se iniciarían las capacitaciones.

#### **Cronograma de ejecución**

Para cada capacitación cada gerente encargado de su sede será responsable de velar por que los empleados cumplan la capacitación en un periodo determinado de un mes, dividiéndolo en semanas, para tomar el curso será un tiempo de 1 a 15 días no hábiles y para la evaluación de la misma forma serán de a 1 15 días no hábiles, la evaluación tiene como fin examinar a los participantes el grado de aprendizaje sobre los temas tratados.

**Tabla 27.** Cronograma de ejecución

Capacitación	Fase	Mes 1				Mes 2				Mes 3				Mes 4				Mes 5				
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	
El ABCD de la gestión de riesgos general	Ejecución		■																			
	Evaluación			■	■																	
Concientización de seguridad	Ejecución					■	■															
	Evaluación							■	■													
Gestión de riesgos especializado en la empresa	Ejecución							■	■	■												
	Evaluación									■	■	■										
Principios de seguridad especializado en procesos de informática	Ejecución													■	■							
	Evaluación															■	■					
Principios básicos de seguridad	Ejecución																		■	■		
	Evaluación																			■	■	
Introducción a la evaluación de riesgos	Ejecución																	■	■			
	Evaluación																			■	■	

Nota. Programa de ejecución de la capacitación hacia los usuarios. Fuente:  
elaboración propia.

### Sanciones por incumplimiento al plan de concientización

- Será tomado como falta grave con carta al expediente del empleado:
  - La no realización de los cursos caracterizados como obligatorios en el tiempo establecido.
  - Obtener una puntuación de menos del 90% en las evaluaciones de cada capacitación.
  - Si no realiza el 100% de horas estipuladas por cada curso.

## 4. Evaluación

Posterior a la realización de las capacitaciones se deberá medir la efectividad de estas mediante diversos métodos que se seleccionaron y se detallan a continuación:

### Métodos para evaluar la efectividad de las capacitaciones

- Simulacros de incidentes.
- Cuestionario vía Google form de forma anónima para evaluar cada módulo de las capacitaciones.

- Cuestionario vía Google forma de forma anónima para dar una puntuación al instructor y brindar retroalimentación.

## 5. Perfeccionamiento

De no ser satisfactoria la nota de los empleados en cada evaluación se deberá redefinir el plan de capacitación, los temas brindados, la forma de realizar las actividades y las evaluaciones.

Para modificar o mejorar el plan de capacitación adicional se debe tomar en cuenta los cambios en las políticas de la empresa durante el transcurso de los seis meses, cambios en las políticas legales que rodean a la empresa, avances en herramientas de tecnología, implementaciones de nuevos sistemas en la organización o nuevas técnicas de ingeniería social que surjan durante el tiempo de los 6 meses de capacitación.

### ¿Cuáles Estrategias implementaría para?

#### Negocio:

Al momento de presentarse inconvenientes con los sistemas de la Entidad Financiera estos afectan directamente a los usuarios(clientes) de dicha institución. Al no contar con sistemas estables se corre el riesgo de que los usuarios dejen de disponer por un periodo de tiempo de las gestiones o servicios que la entidad provee, esto afecta tanto al cliente como a la entidad. Es por ello por lo que como entidad financiera buscamos mejorar constantemente el manejo de mantenimiento, mejoras y controles de los sistemas.

Ante dichos inconvenientes los cuales se han presentado se buscan como entidad poder mejorar la estadía del cliente, es por ello por lo que se implementan beneficios que pueden ser una ventaja para los clientes, entre esos beneficios se encuentra:

- Beneficios de descuentos en comercios autorizados mediante tarjetas de promociones.
- Acumulación de puntos canjeables en comercios autorizados.
- Disminución en tasas de interés acorde al historial crediticio y financiero del cliente.
- Facilidad para la adquisición de préstamos.

Estos son algunos de los beneficios que como entidad financiera se busca proveer a nuestros clientes, dependiendo como se den los eventos y los acuerdos que se pueden establecer.

El objetivo principal de la entidad es poder brindarle servicios de calidad a nuestros clientes. Es por ello por lo que se busca adecuar los servicios definidos.

### **Tecnología:**

Como estrategia definida ante eventos que pueden presentarse y ocasionan bajas en los sistemas, es necesario poder definir una estrategia. Dicha estrategia podrá ser el control de como poder ejecutar de manera eficiente según se requiere ante los eventos que se presenten, para ello se define lo siguiente:

- **Definición de equipos:** se debe de contar con un equipo preparando y conocedor de los sistemas, flujos, configuraciones y todo conocimiento el cual se considere importante, esto debido a que ante alguna situación que comprometa la estabilidad del sistema de la entidad deben de tomar decisiones eficientes para poder restablecer los sistemas en el menor tiempo posible.

- **Evaluaciones del riesgo:** al realizar la evaluación de los riesgos se podrá realizar un filtro y clasificación de la probabilidad de impacto que se tenga y como poder reaccionar ante los mismos.
- **Determinar el impacto:** cada riesgo maneja un grado de impacto diferente, es por ello se deben de analizar y poder determinar su probabilidad.
- **Planificar la respuesta:** al pasar por las fases anteriores y conocer sobre los posibles riesgos a mitigar, se debe de contar con un plan de respuesta que permita definir los planes de acción a tomar según sea el caso. En esta fase se definen tiempos, procedimientos, buenas prácticas y todo aquello que se considere necesario para la restauración de los sistemas.
- **Consolidación del plan:** al comprender las amenazas, riesgos, impacto y como responder ante las mismas, se define un plan de gestión de crisis, esto como una estrategia plasmada de manera escrita y su vez se comunica de manera verbal. Esta debe de contar con un protocolo de activación y contactos de emergencia que permitan abordar y atacar el problema de raíz.
- **Revisión y actualización:** si el plan de crisis definido se encuentra completo es necesario revisarlo y actualizarlo al menos dos veces al año para poder clasificar nuevos riesgos potenciales que puedan surgir conforme el paso del tiempo.

## **Acuerdos con Proveedores**

### **Acuerdo de Nivel de Servicio**

#### **Disponibilidad de Servicio**

Los componentes de Software forman parte de la organización y su funcionamiento son fundamental para que los sistemas puedan funcionar adecuadamente y se pueden considerar como disponibles.

#### **Tareas de Mantenimiento**

Los intervalos de mantenimiento deberán ser aprobados para trabajos de mantenimiento periódicos, programados o no programados en los sistemas de la Entidad Financiera y sus proveedores. Es necesario poder asegurar las operaciones de los sistemas que se llevan en curso y llevar actualizaciones o mejoras necesarias. Toda la limitación a la disponibilidad a través de este tipo de gestiones debe realizarse en horarios establecidos.

Se tiene como regla establecida realizar mantenimientos, actualizaciones, mejoras u otro tipo de acciones necesarias en diferentes horarios:

- Horario 1: De lunes a viernes en el transcurso de 12:00 am a 4 am.
- Horario 2: viernes, sábado y domingo de 12:00 a 3:30 am.
- Dependiendo la criticidad del evento se pueden realizar acciones en cualquier momento.

Existen casos excepcionales en donde se necesita poder realizar cambios o mejoras inmediatas, estas no tienen un horario específico y se pueden realizar en cualquier momento dependiendo la criticidad del evento presentado.

Como entidad se debe de contar con la responsabilidad de comunicarle al personal correspondiente la causa del por qué se realizarán mantenimientos o acciones necesarias para poder restablecer el sistema o los sistemas afectados, también deberá indicarse el tiempo estimado de la suspensión de servicio y el tiempo aproximado en reanudación del servicio. Estos tiempos tienen a variar dependiendo la problemática.

### **Incumplimiento del Nivel de Servicio**

Si los niveles de servicio garantizados no pudiesen ser respetados, la Entidad deberá de computar al cliente una compensación acorde a lo establecido. Esto quedara por escrito y firmado debido al incumplimiento presentado. La compensación se detalla de la siguiente manera.

**Tabla 28.** Tabla indicadora de incumplimiento del servicio

Disponibilidad de Servicio	Compensación
<b>98% a 99.8%</b>	10%
<b>95% a 97.9%</b>	20%
<b>90% a 94.9%</b>	30%
<b>89.9% o menos</b>	50%

Nota. Describe los niveles de incumplimiento al nivel de servicio. Fuente:  
elaboración propia.

### **Política de la Continuidad del Negocio**

#### **Administración del Plan:**

Se debe de contar con un personal asignado como responsable quien deberá de mantener actualizada la política y se encargará del cumplimiento de:

- Gestionar cambios al plan.

- Gestionar la autorización del plan y divulgar el mismo únicamente con las personas autorizadas.

#### **Autorización y Divulgación del Plan:**

Si el plan sufre alguna actualización o alteración esta debe de ser autorizada para poder así confirmar la nueva versión del plan y posterior divulgarlo a las personas autorizadas, tomando en cuenta que únicamente el Comité asignado podrá autorizar.

#### **Evaluación del Plan:**

El plan establecido está sujeto a actualizaciones, generalmente se tiene definido que el plan debe de verificarse cada cuatro meses y a su vez debe de ser autorizado, esto permitirá mitigar riesgos, identificar amenazas, debilidades y puntos de mejora.

#### **Activación del Plan:**

El plan únicamente se podrá activar si el Comité de Control de Riesgos junto con el gerente de informática llegan a la conclusión de que el evento presentado requiere que se actúe de manera inmediata evitando grandes consecuencias a la entidad.

#### **Declaración del Plan:**

El plan debe de declararse aproximadamente 30 minutos después de la primera interrupción de operaciones que se efectúan normalmente, posterior a ello el Gerente de informática debe de comunicar al Comité lo siguiente:

- La Criticidad establecida según la evaluación.
- Las Estrategias definidas para la restauración de los sistemas afectados

- Tiempo estimado de restauración
- Información adicional considerada como relevante

### **Desactivación del Plan:**

El Gerente General será el encargado de comunicar al comité de Control de Riesgos si se ha finalizado la declaración del desastre y se haya restaurado y regresado a la normalidad. Posterior a ello el Comité toma la decisión de la Desactivación del plan.

### **Competencia del Personal**

Ante ciertos incidentes generados el personal de la entidad financiera debe de estar debidamente especializada para poder reaccionar de una manera efectiva ante cualquier crisis. Se debe de contar con un equipo debidamente capacitado y a su vez haber realizado simulaciones de eventos en las que se ponen a práctica su conocimiento, toma de decisiones y la integración que puedan tener como equipo para poder resolverlo lo más pronto posible, tomando en cuenta que una Entidad Bancaria no puede tener sus servicios no disponibles.

Es por ello por lo que la Entidad Bancaria realiza planes, manuales, políticas y define personas específicas para poder liderar y a su vez capacitar a su personal constantemente para prepararlos ante eventos desconocidos y con probabilidad alta de impacto.

### **Control de Registros**

Para tener un control de registros se debe de trabajar junto con el Comité de gestión de riesgos para poder implementar nuevas políticas, procedimientos, acciones, controles, implementaciones de ISO, simulaciones de eventos

inesperados, planes de acción y otros controles que se consideren necesarios, a su vez si ya se tienen implementados los mencionados anteriormente, entonces se debe de entrar en un proceso de validación y actualización de los mismos, debido a que constantemente surgen nuevos riesgos, vulnerabilidades y amenazas de criticidad elevada, por lo que es necesario una constante actualización de nuestros planes y bases implementadas para un mejor manejo de tiempos y estrategias ante un evento presentado.

## Conclusiones

- El análisis de riesgo es una herramienta fundamental para la mitigación de incidentes en los procesos de la institución. Este proceso permite poder responder de manera proactiva a las amenazas de seguridad, minimizando así el riesgo de pérdida de información, interrupción de servicios, fraude, entre otros.
- La aplicación de las recomendaciones y observaciones de la auditoría realizada permitirán a la organización seguir evolucionando en su mejora continua, esto le permitirá a la organización mantener todos sus procesos seguros y con la capacidad de mitigar cualquier incidente.
- Contar con un plan de recuperación ante desastres permitirá que se puedan tener claros los incidentes que se pueden producir y también las diversas maneras en las cuales se puede dar una solución a las situaciones que se pudieran enfrentar.
- Tener una lista de contactos de las personas clave de cada empresa que se encarga de proveer los servicios involucrados con los procesos críticos facilitará la comunicación en caso de un incidente que afecte las operaciones.

### Referencias bibliográficas

- Santos D. (sin fecha). Análisis de riesgos. [Página web]  
<https://blog.hubspot.es/marketing/analisis-de-riesgos>
- Sotres Cruz P. (2012). Matriz de riesgos. [Página web]  
<https://asana.com/es/resources/risk-matrix-template>
- Team Asana. (2022). ISO 22301 Continuidad del negocio. [Archivo PDF]  
<https://www.interempresas.net>
- Anthony Rázuri. (2019). Desarrollo de un Sistema de Gestión de Continuidad de Negocio en una entidad financiera, basado en la ISO. [Tesis de ingeniería industrial, Universidad del Perú. Decana de América]. <http://cybertesis.unmsm.edu.pe/>

Universidad Mariano Gálvez de Guatemala

Facultad de Ingeniería de Sistemas de Información

Maestría de seguridad informática

Gestión de Proyectos



**Proyecto Final**

**Aplicación Móvil Gestión y Atención de Clientes**

*Cristian Rosales*

Nota:40/40

Cristian Waldemar Rosales Meléndez Firmado digitalmente por Cristian Waldemar Rosales Meléndez  
Fecha: 2022.03.19 08:43:31 -06'00'

Alumnos	Carné	Email	Coordinador
Cristian Elí del Cid Rodríguez	1293-07-1719	cdelcidr1@miumg.edu.gt	x
Wagner Aníbal Orózco López	1293-13-4370	worozcol1@miumg.edu.gt	
Ricardo Isaac Marroquín Montenegro	1293-13-9353	rmarroquinm2@miumg.edu.gt	
Bryan Orlando Aguirre Sagastume	1293-17-646	baguirres@miumg.edu.gt	
Ricardo Alejandro Pérez Rodríguez	1293-17-1255	rperezr8@miumg.edu.gt	

Guatemala 23 de enero del 2022

	<b>Índice</b>
Índice .....	2
Introducción.....	4
Visión.....	5
Objetivos.....	5
General.....	5
Específicos.....	5
Antecedentes.....	5
Marco Conceptual.....	6
Grupo de Procesos de Iniciación .....	7
Acta de Constitución del Proyecto .....	7
Lista de Interesados - Por Rol General en el Proyecto – .....	10
Registro de Interesados.....	11
Clasificación de Interesados (Modelo de Prominencia) .....	12
Información del Proyecto .....	13
Propósito y Justificación del Proyecto.....	13
Grupo de Procesos Planificación .....	14
Descripción del Proyecto y Entregables.....	14
Enunciado del Alcance .....	14
Descripción de Roles .....	16
Matriz de Asignación de responsabilidades .....	28
Estructura de Desglose del Trabajo (EDT).....	29
Organigrama del Proyecto .....	30
Cronograma de Hitos Principales .....	31
Diagrama de Red del Proyecto .....	32
Costeo del Proyecto .....	33
Presupuesto Estimado.....	35
Plan de Gestión de la Configuración .....	36
Documentación de Requisitos del Proyecto .....	38
Plan de Gestión de Cambios .....	41
Plan de Gestión de la Calidad.....	42

Plan de Gestión de los Recursos.....	45
Plan de Gestión de las Comunicaciones .....	47
Identificación y Evaluación Cualitativa de Riesgos .....	48
Plan de Respuesta a los Riesgos .....	50
Enunciado del Trabajo Relativo a Adquisiciones (SOW) .....	52
Grupo de Procesos Ejecución .....	56
Lección aprendida.....	56
Encuesta de Satisfacción Sobre el Trabajo en Equipo .....	57
Evaluación de Competencias Generales.....	59
Acta de Reunión de Coordinación del Proyecto.....	84
Registro de Incidentes .....	86
Grupo de Procesos de Monitoreo .....	87
Informe de métricas de calidad.....	87
Solicitud de Cambio .....	89
Estado de las Solicitudes de Cambio.....	90
Reporte de Performance del Proyecto Final .....	92
Conclusiones.....	95
Referencias .....	96
Anexos .....	97
Logo PilloPhone .....	97
Inicio de aplicativo .....	97

## **Introducción**

En el presente documento presenta el proceso de implementación y de documentación de las diferentes actividades efectuadas en la práctica de gestión de proyectos con el fin de poder ejecutar un despliegue de proyecto exitoso, en su mayoría los documentos adjuntos proveen la información tanto para poder proceder con el desarrollo como para poder llevar a cabo la documentación posterior a la implementación de la aplicación.

El documento recopila la información referente al despliegue de un aplicativo móvil para la atención y gestión de clientes dentro de la organización Pillophone, en el cual tanto los clientes internos como externos tendrán la capacidad de realizar solicitudes al departamento técnico y dar el respectivo seguimiento, mientras por otra parte el departamento de TI tendrá la capacidad de poder dar el seguimiento pertinente a cada una de las solicitudes, logrando de esta forma una mejora sustancial en los tiempos de atención y en la satisfacción de los clientes de forma individual mientras al mismo tiempo se logra la implementación adecuada de una gobierno de TI bajo las premisas de ITIL y COBIT.

## Visión

Ser la empresa líder a nivel nacional en soluciones de telecomunicaciones, preferida en el mercado y modelo en el sector empresarial.

## Objetivos

### General

Tener reconocimiento por buen servicio en el ámbito de telecomunicaciones a nivel nacional e internacional.

### Específicos

- Aumentar las sucursales en el país para que la cobertura y servicios prestados sea de una mejor calidad.
- Mejorar constantemente la infraestructura para que la empresa esté a la vanguardia con la tecnología y mejore la calidad del servicio prestado.
- Mejorar a nivel de software la seguridad y atención al cliente para que se mantenga una comunión con los clientes.

## Antecedentes

La iniciativa de la empresa PilloPhone surgió en el año 2,005 como resultado de que los servicios prestados por la única empresa de telecomunicaciones existente en ese momento no cumplían con las necesidades de los ciudadanos del país. Esta empresa era pionera en esta área y, por lo tanto, brindaba servicios de alta calidad, sin embargo, con el paso de los años no mejoró al mismo paso que los avances tecnológicos. Debido a esto se dieron las pláticas con los socios para iniciar las investigaciones relacionadas a la empresa para una posible adquisición con el motivo de mejorar los servicios prestados y asimismo estar a la vanguardia tecnológicamente.

A inicios de 2,007, luego de investigaciones exhaustivas a cargo de nuestro equipo de trabajo se llegó a la conclusión de iniciar las negociaciones con esta empresa. Meses después estas se llevaron a cabo y en septiembre se concluyeron. En este momento comenzaron los trabajos para perfeccionar el funcionamiento de la empresa en puntos primordiales como la mejora en la infraestructura y software.

Actualmente somos una empresa que brinda servicios como: telefonía, cable e internet. Hemos tratado de tener un crecimiento a lo largo de nuestra trayectoria, logrando esto por medio de cubrir las necesidades de nuestros clientes con al menos una agencia en cada municipio y un equipo excelente de profesionales, apoyando así

el talento nacional brindando empleos y oportunidades mientras mejoramos las telecomunicaciones a nivel nacional.

### Marco Conceptual

- **4g:** Es la cuarta generación de tecnologías de telefonía móvil y que trajo consigo unas velocidades mayores a las de 301 Mbit/s con un radio de 8 MHz.
- **Banda ancha:** Red de cualquier tipo con una elevada capacidad para transportar información en la velocidad de transmisión de esta, y que además permite la conexión de varias redes en un único cable.
- **Call Center:** Es un centro de llamadas donde personas, previamente cualificadas para ello, realizan y/o reciben llamadas con el objetivo de ofrecer un servicio telefónico o de atención.
- **CRM:** es una solución de gestión de las relaciones con clientes, orientada normalmente a gestionar tres áreas básicas: la gestión comercial, el marketing y el servicio postventa o de atención al cliente.
- **Roaming:** Es la posibilidad de un dispositivo inalámbrico de utilizar una cobertura de red distinta a la principal y que le permite conectarse a redes secundarias.
- **Softphone:** Es el resultado de la combinación de los términos software y telephone. Se utiliza para realizar llamadas a otros softphones o a otros teléfonos convencionales usando un VoIP o ToIP.
- **Telecomunicación:** es toda transmisión y recepción de señales de cualquier naturaleza, típicamente electromagnéticas, que contengan signos, sonidos, imágenes o, en definitiva, cualquier tipo de información que se desee comunicar a cierta distancia.
- **Teleoperador:** Empresa que ofrece servicios telefónicos, televisivos o telemáticos. También se le conoce como teleoperador a la persona que atiende al público a través del teléfono.
- **VoIP:** Las siglas VoIP quieren decir 'Voice over Internet Protocol' o 'Voz sobre Protocolo de Internet'. Se trata de una tecnología que permite realizar llamadas a través de Internet a un precio más barato y con mayor accesibilidad y comodidad.
- **WAN:** Red de computadoras que une varias redes locales, aunque sus miembros no estén todos en una misma ubicación física.
- **Wireframe:** Es una representación visual de objetos tridimensionales, como aquellos empleados en el desarrollo y diseño de productos.

## Grupo de Procesos de Iniciación

### Acta de Constitución del Proyecto

<b>CONTROL DE VERSIONES</b>					
<b>Versión</b>	<b>Hecha por</b>	<b>Revisada por</b>	<b>Aprobada por</b>	<b>Fecha</b>	<b>Motivo</b>
1.0	Cristian E. del Cid	Cristian W. Rosales	Cristian W. Rosales	20/01/2022	Creación inicial de Acta

<b>NOMBRE DEL PROYECTO</b>	<b>SIGLAS DEL PROYECTO</b>
Aplicación Móvil Gestión y Atención de Clientes	AMGC

**FINALIDAD DEL PROYECTO:** DESCRIBIR EL FIN ÚLTIMO, PROPÓSITO GENERAL, U OBJETIVO DE NIVEL SUPERIOR POR EL CUAL SE EJECUTA EL PROYECTO, MENCIONANDO EL ENLACE CON PROGRAMAS, PORTAFOLIOS, O ESTRATEGIAS DE LA ORGANIZACIÓN.

Proveer un entorno centralizado para la atención a los clientes.

**OBJETIVOS DEL PROYECTO:** DESCRIBIR LOS OBJETIVOS HACIA LOS CUALES SE DEBE DIRIGIR EL TRABAJO DEL PROYECTO EN TÉRMINOS DE LA TRIPLE RESTRICCIÓN, DEFINIENDO LOS OBJETIVOS MEDIBLES DEL PROYECTO Y LOS CRITERIOS DE ÉXITO ASOCIADOS.

<b>CONCEPTO</b>	<b>OBJETIVOS</b>	<b>CRITERIO DE ÉXITO</b>
<b>1. ALCANCE</b>	El alcance del proyecto incluye el diseño, desarrollo y puesta en marcha de una aplicación móvil que permita a los usuarios acceder de forma eficaz y rápida tanto a la solicitud de asistencia técnica como al seguimiento de estas.	Aprobación del área de aseguramiento de la calidad (QA) con respecto a las pantallas establecidas.
<b>2. CRONOGRAMA</b>	Concluir el proyecto en el plazo de tiempo indicado al departamento.	Cumplir el proyecto en 10 semanas, del 25 enero 2021 al 5 abril 2021
<b>3. COSTO</b>	Cumplir con el presupuesto estimado del proyecto (\$. 16,000.00)	No exceder el presupuesto previamente establecido.

**DEFINICIÓN DE REQUISITOS DEL PROYECTO:** DESCRIBIR LOS REQUERIMIENTOS FUNCIONALES, NO FUNCIONALES, DE CALIDAD, ETC., DEL PROYECTO.

#### 1. Requerimientos del Cliente

- a. Los clientes deberán contar con ingreso bajo las políticas de seguridad de la organización y con el uso del “Single-Sign On” que esta proporciona.
- b. Entregar un informe semanal de las actividades realizadas, las cuales serán validadas tanto por el departamento de seguridad como por la PMO de la organización.
- c. Entregar un documento final que contenga tanto las actividades efectuadas, los accesos maestros de la aplicación y el acceso al entorno de desarrollo para el equipo de mantenimiento de la aplicación.

**DESCRIPCIÓN GENERAL DEL PROYECTO, LÍMITES Y ENTREGABLES CLAVE:** *DEFINIR EL PROYECTO DE FORMA GENERAL, DEFINIR LOS LÍMITES DEL PROYECTO, ASÍ COMO LOS ENTREGABLES CLAVE.*

El proyecto **Aplicación Móvil Gestión y Atención de Clientes**, consiste en la realización del diseño, implementación y puesta en marcha de una aplicación contando con los principales entregables:

El sistema por desarrollar deberá satisfacer las siguientes **funcionalidades básicas**:

- Ofrecer una interfaz simple y amigable tanto para la gestión de peticiones e incidencias por parte del departamento correspondiente, como para los usuarios externos.
- Lograr una completa integración con la gestión de tareas de los departamentos de soporte para una mejor atención de las peticiones del servicio recibidas.
- Facilitar, para los usuarios externos, la consulta de todas las incidencias reportadas al área técnica, teniendo una visualización unificada y más precisa de la situación actual de cada una de estas.
- Disponer una visión detallada de las actuaciones o seguimientos completados por el área técnica durante la resolución de una solicitud, así como obtener un resumen de los tiempos totales utilizados para la resolución de cada caso.

Los **entregables** previstos para el desarrollo son los siguientes:

- Análisis, diseño de la interfaz de registro y puesta en producción de la interfaz, así como elaboración de un manual detallado y proceso de capacitación para los usuarios finales.
- Documentación de los resultados obtenidos.

**RIESGOS GENERALES DEL PROYECTO:** *DESCRIBIR LOS RIESGOS GENERALES DEL PROYECTO.*

R01	Como parte de los riesgos físicos, una de las posibles problemáticas encontradas es la falta de iluminación en el área de trabajo del equipo de infraestructura.
R02	Como parte de los riesgos organizacionales, la falta de adaptación para equipos colaborativos en modelo de mando matricial.
R03	Como parte del riesgo ergonómico, parte del equipo de los puestos de trabajo no cuenta con escritorios de altura ajustable.
R04	Parte del equipo eléctrico aún se encuentra en proceso de estructuración en el área donde el equipo de infraestructura se encontrará laborando, por lo que se contará temporalmente con riesgos de seguridad
R05	Debido a los constantes cambios implementados de parte del gobierno, puede contarse con manifestaciones que pongan en riesgo las fichas de finalización del proyecto
R06	Se puede contar con retraso en la entrega de equipo como servidores
R07	Se tiene el riesgo de cierres temporales derivados de la pandemia que impidan la movilidad del equipo de trabajo
R08	Se tiene el riesgo de desastres naturales que puedan impedir el óptimo trabajo e implementación del proyecto

**CRONOGRAMA DE HITOS DEL PROYECTO:** *MENCIONAR TODOS LOS HITOS DE MANERA CRONOLÓGICA, COLOCANDO SUS FECHAS PROGRAMADAS DE INICIO Y FIN.*

HITOS	FECHAS PROGRAMADAS
Inicio del proyecto	25 Enero 2022
Documentación de requisitos y análisis	09 Febrero 2022
Documentación de diseño del sistema	24 Febrero 2022
Solución técnica	11 Marzo 2022
Material formativo y de divulgación	26 Marzo 2022
Fin del proyecto	5 Abril 2022

<b>RECURSOS FINANCIEROS DEL PROYECTO:</b> MENCIONAR LOS RECURSOS FINANCIEROS ASIGNADOS AL PROYECTO.		
<b>CONCEPTO</b>	<b>CONCEPTO</b>	<b>MONTO</b>
Personal	Programadores	\$3,000
	Equipo infraestructura	\$3,000
Materiales		\$1000
Maquinas		\$2,500
Otros Costos		\$1,500
	<b>Total Presupuesto Base</b>	\$10,500
Reserva Contingencias		\$3,000
Reserva Gestión		\$2,000
	<b>Total Presupuesto</b>	\$16,000
<b>LISTA DE INTERESADOS CLAVE:</b> MENCIONAR LOS PRINCIPALES INTERESADOS DEL PROYECTO.		
Daniel Ortiz → DC - Gerente General Raúl Rivera → DC - Asistente de Proyectos Luis Chan → CA - Jefe de Área de Cobranza Marta Godínez → CA – Jefe de Área de Planteamiento Diego Ruiz → CA - Coordinador Marcus López → DC - Recursos Humanos Tulio Lira → DC - Recursos Humanos		
<b>REQUISITOS DE APROBACIÓN DEL PROYECTO:</b> DESCRIBIR EN QUÉ CONSISTE EL ÉXITO DEL PROYECTO, QUIÉN DECIDE SI EL PROYECTO TIENE ÉXITO Y QUIÉN FIRMA LA APROBACIÓN DEL PROYECTO.		
El proyecto podrá catalogarse como completado con éxito, si se la puesta en marcha es completada en el plazo de tiempo solicitado, con el presupuesto previamente asignado y demostrando satisfacción de clientes tanto internos como externos. La aprobación se proporcionará de parte de la gerencia del departamento de TI.		
<b>CRITERIOS DE CULMINACIÓN DEL PROYECTO:</b> MENCIONAR LAS CONDICIONES QUE SE DEBEN CUMPLIR PARA CERRAR O CANCELAR EL PROYECTO O FASE.		
El proyecto será cerrado o cancelado siempre y cuando la organización desista del proyecto o no lo considere como necesidad.		
<b>DESIGNACIÓN DEL DIRECTOR DE PROYECTO:</b> ESCRIBIR EL NOMBRE DEL DIRECTOR DE PROYECTO (PROJECT MANAGER) ASIGNADO, SU RESPONSABILIDAD Y SU NIVEL DE AUTORIDAD.		
<b>NOMBRE</b>	Cristian E. del Cid (CD)	<b>NIVEL DE AUTORIDAD</b>
<b>REPORTA A</b>	Cristian W. Rosales (CR)	Exigir el cumplimiento de los entregables del proyecto
<b>SUPERVISA A</b>	Wagner Orozco (WO), Ricardo Pérez (RP), Bryan Aguirre (BA), Ricardo Marroquín (RM)	
<b>PATROCINADOR QUE AUTORIZA EL PROYECTO:</b> MENCIONAR AL PATROCINADOR DEL PROYECTO, ASÍ COMO LA ENTIDAD A LA QUE PERTENECE, EL CARGO QUE OCUPA Y LA FECHA DE ELABORACIÓN DEL ACTA DE CONSTITUCIÓN DEL PROYECTO.		
<b>NOMBRE</b>	<b>EMPRESA</b>	<b>CARGO</b>
Daniel Ortiz	Pillophone	Gerente General
		22/01/2022

Fuente: (Dharma Consulting, 2022)

## Lista de Interesados - Por Rol General en el Proyecto –

<b>CONTROL DE VERSIONES</b>					
Versión	Hecha por	Revisada por	Aprobada por	Fecha	Motivo
1.0	Wagner Orózco	Cristian W. Rosales	Cristian W. Rosales	20/01/2022	Versión inicial

NOMBRE DEL PROYECTO	SIGLAS DEL PROYECTO
Aplicación Móvil Gestión y Atención de Clientes	<b>AMGC</b>

<b>ROL GENERAL</b>	<b>INTERESADOS</b>
PATROCINADOR	Daniel Ortiz
EQUIPO DE PROYECTO	<p style="margin-left: 20px;">DIRECTOR DE PROYECTO: Cristian E. del Cid (CD)</p> <p style="margin-left: 20px;">EQUIPO DE GESTIÓN DE PROYECTO Cristian del Cid Bryan Aguilar Ricardo Marroquín Ricardo Rodríguez Wagner Orózco</p> <p style="margin-left: 20px;">OTROS MIEMBROS DEL EQUIPO DE PROYECTO</p>
DIRECTOR DE PORTAFOLIOS	Luis Chan
DIRECTOR DE PROGRAMAS	Marta Godínez
PERSONAL DE LA OFICINA DE PROYECTOS	Diego Ruiz
GERENTES DE OPERACIONES	Raúl Rivera
GERENTES FUNCIONALES	Raúl Rivera Luis Chan
USUARIOS / CLIENTES	Usuarios finales a quienes se les da la atención. Usuarios que utilizarán la aplicación móvil para la gestión.
PROVEEDORES / SOCIOS DE NEGOCIOS	Otros
OTROS INTERESADOS	Cristian Rosales

Fuente: (Dharma Consulting, 2022)

## Registro de Interesados

CONTROL DE VERSIONES					
Versión	Hecha por	Revisada por	Aprobada por	Fecha	Motivo
1.0	RP	DO	DO	22-01-22	Versión original

NOMBRE DEL PROYECTO	SIGLAS DEL PROYECTO
Aplicación Móvil Gestión y Atención de Clientes	AMGC

INFORMACIÓN DE IDENTIFICACIÓN					INFORMACIÓN DE EVALUACIÓN				CLASIFICACIÓN DE LOS INTERESADOS	
NOMBRE	EMPRESA Y PUESTO	UBICA-CIÓN	ROL EN EL PROYECTO	INFORMACIÓN DE CONTACTO	REQUISITOS PRINCIPALES	EXPECTATIVAS PRINCIPALES	INFLUENCIA POTENCIAL	FASE DE MAYOR INTERÉS	INTERNO / EXTERNO	PARTIDARIO / NEUTRAL / RETICENTE
Daniel Ortiz	DC-Gerente General	Guatemala	Patrocinador	9658-4596 Dortiz@hotmail.com		Que el Cliente quede satisfecho con el Proyecto	Fuerte	Todo el proyecto	Interno	Apoyo
Cristian del Cid	DC-Asistente de Proyectos	Guatemala	Director de Proyecto	9658-4596 Cdelcid@hotmail.com	Cumplir con Plan de Proyecto	Que el Proyecto sea culminado exitosamente	Fuerte	Todo el proyecto	Interno	Apoyo
Luis Chan	CA- Jefe de Área de Cobranza	Guatemala	Coordinador del Proyecto	9658-4596 Lchan@hotmail.com	Que se Desarrolle el Programa		Fuerte	Implementación de desarrollo	Externo	Neutral
Marta Godínez	CA – Jefe de Área de Planteamiento	Guatemala	Comité de Control de Cambios	9658-45969 Mgodinez@hotmail.com	Que se Desarrolle el Programa		Mediana	Implementación de desarrollo	Externo	Neutral
Diego Ruiz	CA- Coordinador	Guatemala	Comité de Control de Cambios	9658-4599 Druiz@hotmail.com	Que se Desarrolle el Programa		Fuerte	Implementación de desarrollo	Externo	Neutral
Marcus López	DC- Recursos Humanos	Guatemala	Asistente de Aula	9658-4599 Mlopez@hotmail.com	Funcionamiento correcto de la aplicación	Cumplir bien con su rol en el proyecto	Bajo	Funcionamiento del aplicativo en concreto	Interno	Neutral
Tulio Lira	DC- Recursos Humanos	Guatemala	Asistente de Aula	9658-4599 Tlira@hotmail.com	Funcionamiento correcto de la aplicación	Cumplir bien con su rol en el proyecto	Bajo	Informes	Interno	Neutral

Fuente: (Dharma Consulting, 2022)

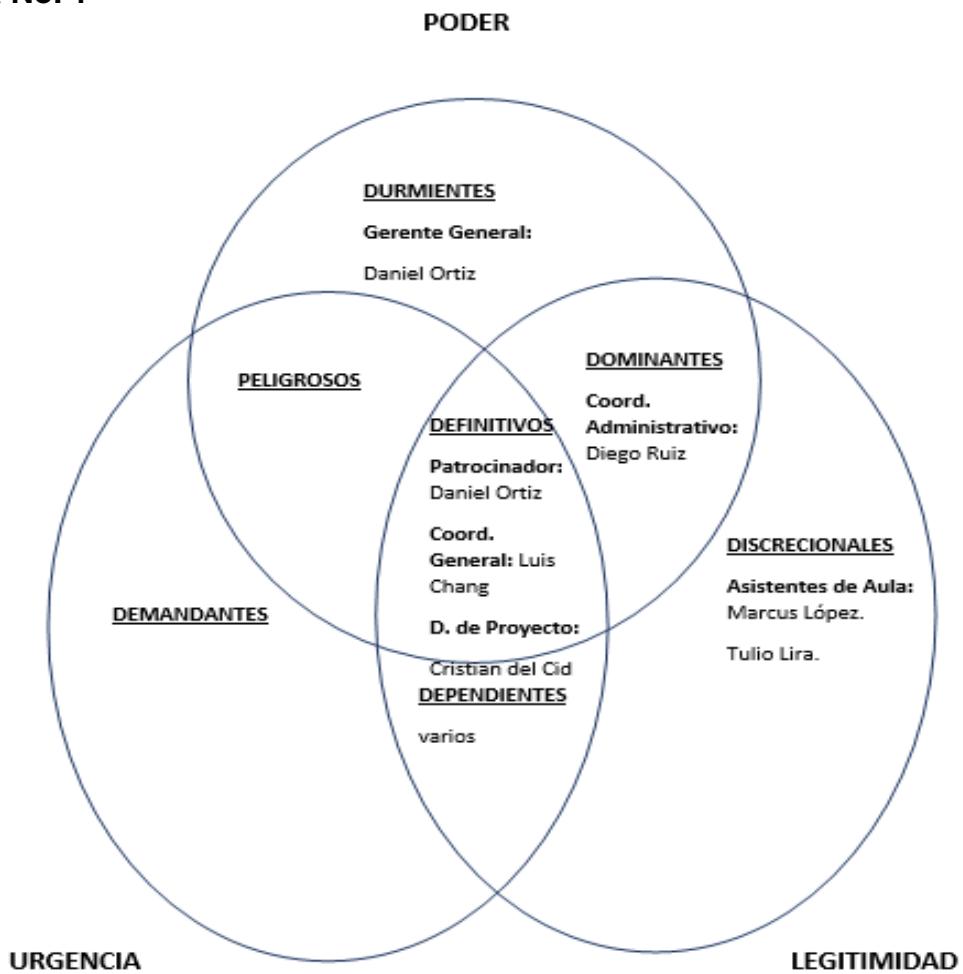
## Clasificación de Interesados (Modelo de Prominencia)

CONTROL DE VERSIONES					
Versión	Hecha por	Revisada por	Aprobada por	Fecha	Motivo
1.0	RM	DO	DO	22-01-2022	Versión Inicial

NOMBRE DEL PROYECTO	SIGLAS DEL PROYECTO
Aplicación Móvil Gestión y Atención de Clientes	AMGC

Fuente: (Dharma Consulting, 2022)

Figura No. 1



Fuente: Elaboración propia.

## **Información del Proyecto**

El Proyecto pretende proveer una aplicación móvil que proporcione la facilidad de manejo de clientes para la organización PilloPhone, este proyecto de desarrollo será implementado de forma local con el fin de poder tener un control estricto sobre los servidores de la organización y el funcionamiento y disponibilidad del servicio.

El equipo de trabajo se tomará tanto de personal interno como externo proveyendo un esquema organizacional matricial con el fin de poder facilitar el proceso de implementación y despliegue.

## **Propósito y Justificación del Proyecto**

PilloPhone no cuenta con una aplicación que le permita llevar a cabo el seguimiento adecuado de los casos de soporte. Actualmente se lleva a cabo la implementación de un nuevo sistema de gobierno de TI bajo las premisas de ITIL y COBIT por lo que es necesario contar con una aplicación para el seguimiento de los casos tanto internos como externos que permita a su vez a los usuarios finales proveer retroalimentación con respecto a el soporte solicitado.

La implementación de una aplicación de gestión permitirá que la organización puede hacer un seguimiento y administración de los recursos tanto humanos como de tiempo y lograr una mejora en el tiempo de respuesta a cada uno de los incidentes.

## Grupo de Procesos Planificación

### Descripción del Proyecto y Entregables

#### Enunciado del Alcance

CONTROL DE VERSIONES					
Versión	Hecha por	Revisada por	Aprobada por	Fecha	Motivo
1.0	BA, RP	CR	CR	26/01/22	Versión Original

NOMBRE DEL PROYECTO	SIGLAS DEL PROYECTO
<b>Aplicación Móvil de Gestión y Atención de Clientes</b>	<b>AMGC</b>

<b>DESCRIPCIÓN DEL ALCANCE DEL PRODUCTO:</b> DESCRIBIR LAS CARACTERÍSTICAS DEL PRODUCTO, SERVICIO, O RESULTADO DESCrito EN EL ACTA DE CONSTITUCIÓN DEL PROYECTO Y EN EL DOCUMENTO DE REQUISITOS.
1. Lograr que la aplicación móvil desarrollada permita a los usuarios realizar solicitudes de asistencia técnica con seguimiento de procesos de una manera eficaz y rápida.
2. Desarrollar inicios de sesión con credenciales y "Single-Sign On" siguiendo estrictamente las políticas de seguridad de la organización.
3. Proveer de informes en períodos semanales al departamento de seguridad sobre las diferentes actividades realizadas, los cuales deberá de aprobar dicho departamento.
4. Proveer de documentación el cual contenga toda actividad efectuada, accesos maestros a la aplicación y accesos al entorno de desarrollo para futuros mantenimientos.

<b>ENTREGABLES DEL PROYECTO:</b> CUALQUIER PRODUCTO, RESULTADO O CAPACIDAD DE PRESTAR UN SERVICIO, ÚNICO Y VERIFICABLE, QUE DEBE PRODUCIRSE PARA COMPLETAR UN PROCESO, UNA FASE O UN PROYECTO.	
<b>FASE DEL PROYECTO</b>	<b>ENTREGABLES</b>
<b>1.0 Toma y Análisis de requerimientos</b>	- Documento completo con los requerimientos del aplicativo. - Especificaciones del sistema.
<b>2.0 Diseño de estructura e interfaces gráficas</b>	- Diseños de interfaz gráfica. - Diseños de algoritmos. - Diccionario de datos. - Estándares de programación. - Técnicas de implementación recomendadas.
<b>3.0 Desarrollo de la Aplicación</b>	- Descripción de las entradas y salidas. - Diseño final del sistema. - Manual técnico. - Manual de usuario. - Aplicación funcional.

<b>4.0 Pruebas de aplicación</b>	<ul style="list-style-type: none"> <li>- Plan de desarrollo de pruebas.</li> <li>- Diseño y documentación de pruebas.</li> <li>- Resultado de pruebas realizadas.</li> </ul>
<b>5.0 Implementación y puesta en marcha</b>	<ul style="list-style-type: none"> <li>- Planes de contingencia.</li> <li>- Guía de revisión de instalación.</li> <li>- Informe de instalación.</li> </ul>
<b>6.0 Evaluación y verificación de resultados</b>	<ul style="list-style-type: none"> <li>- Informe de resultados.</li> <li>- Carta de aceptación del sistema.</li> </ul>

<b>CRITERIOS DE ACEPTACIÓN DEL PRODUCTO:</b> CONJUNTO DE REQUISITOS QUE DEBEN CUMPLIRSE ANTES QUE SE ACEPTE EL PRODUCTO DEL PROYECTO.	
<b>CONCEPTOS</b>	<b>CRITERIOS DE ACEPTACIÓN</b>
<b>1. TÉCNICOS</b>	Se debe de cumplir con éxito la puesta en marcha del aplicativo en el tiempo estipulado.
<b>2. DE CALIDAD</b>	El sistema deberá haber aprobado los mayores estándares de calidad aprobando las pruebas a profundidad en ambientes reales.
<b>3. ADMINISTRATIVOS</b>	El sistema de información debe de cumplir con el correcto procedimiento de procesos y seguimientos de procesos con la documentación debidamente guardada de manera segura.
<b>4. COMERCIALES</b>	Se deberá de cumplir lo estipulado en el contrato.
<b>5. SOCIALES</b>	Aumentar la satisfacción de los clientes con el servicio al cliente brindado por la empresa con la ayuda de la aplicación.

<b>EXCLUSIONES DEL PROYECTO:</b> IDENTIFICA LO QUE SE EXCLUYE DEL PROYECTO. INDICAR EXPLÍCITAMENTE LO QUE SE ENCUENTRA FUERA DEL ALCANCE DEL PROYECTO.	
1. Comercialización	
2. Publicidad	
3. Mercadeo de la aplicación	
4. Actualizaciones por requerimientos adicionales no mencionados inicialmente	
5. Mantenimientos post entrega	

Fuente: (Dharma Consulting, 2022)

## Descripción de Roles

CONTROL DE VERSIONES								
Versión	Hecha por	Revisada por	Aprobada por	Fecha	Motivo			
1.0	BA, RP	CR	CR		Versión Original			
NOMBRE DEL PROYECTO			SIGLAS DEL PROYECTO					
<b>Aplicación móvil de Gestión y Atención de Clientes</b>			<b>AMGC</b>					
NOMBRE DEL ROL								
PATROCINADOR								
<b>OBJETIVOS DEL ROL:</b> OBJETIVOS QUE DEBE LOGRAR EL ROL DENTRO DEL PROYECTO (¿PARA QUÉ SE HA CREADO EL ROL?).								
Es la persona que patrocina el proyecto, es el principal interesado en el éxito del proyecto, y por tanto la persona que apoya, soporta y defiende el proyecto.								
<b>RESPONSABILIDADES:</b> TEMAS PUNTUALES POR LOS CUALES ES RESPONSABLE (¿DE QUÉ ES RESPONSABLE?).								
<ul style="list-style-type: none"> <li>• Aprobar el Acta de Constitución del Proyecto.</li> <li>• Aprobar el Enunciado del Alcance del Proyecto.</li> <li>• Aprobar el Plan de Proyecto.</li> <li>• Aprobar el Cierre del proyecto.</li> <li>• Aprobar todos los Informes de Sesión de los cursos que se van a dictar.</li> <li>• Proveer de requerimientos y especificaciones del sistema.</li> <li>• Revisar los Informes Mensuales del Servicio que se deben enviar al cliente.</li> <li>• Revisar el Informe Final del Servicio que se envía al cliente.</li> </ul>								
<b>FUNCIONES:</b> FUNCIONES ESPECÍFICAS QUE DEBE CUMPLIR (¿QUÉ DEBE REALIZAR PARA LOGRAR SUS OBJETIVOS Y CUBRIR SUS RESPONSABILIDADES?).								
<ul style="list-style-type: none"> <li>• Firmar el Contrato del servicio.</li> <li>• Iniciar el proyecto.</li> <li>• Aprobar la planificación del proyecto.</li> <li>• Monitorear el estado general del proyecto.</li> <li>• Cerrar el proyecto y el Contrato del Servicio.</li> <li>• Gestionar el Control de Cambios del proyecto.</li> <li>• Gestionar los temas contractuales con el Cliente.</li> <li>• Asignar recursos al proyecto.</li> <li>• Designar y empoderar al Director de Proyecto.</li> <li>• Ayudar en la solución de problemas y superación de obstáculos del proyecto.</li> </ul>								
<b>NIVELES DE AUTORIDAD:</b> QUÉ DECISIONES PUEDE TOMAR CON RELACIÓN AL ALCANCE, CRONOGRAMA, COSTO, CALIDAD, RECURSOS Y MATERIALES, PLANES Y PROGRAMAS, INFORMES Y ENTREGABLES, ADQUISICIONES, CONTRATOS, PROVEEDORES, ETC.								
<ul style="list-style-type: none"> <li>• Decide sobre recursos asignados al proyecto.</li> <li>• Decide sobre modificaciones a las líneas base del proyecto.</li> <li>• Decide sobre planes y programas del proyecto.</li> </ul>								
<b>REPORTA A:</b> A QUIÉN REPORTA DENTRO DEL PROYECTO.								

<b>SUPERVISA A:</b> A QUIÉNES SUPERVISA DENTRO DEL PROYECTO.	
Director de Proyecto	
<b>REQUISITOS DEL ROL:</b> QUÉ REQUISITOS DEBEN CUMPLIR LAS PERSONAS QUE ASUMAN EL ROL.	
<b>CONOCIMIENTOS:</b> QUÉ TEMAS, MATERIAS, O ESPECIALIDADES DEBE CONOCER, MANEJAR O DOMINAR.	
<b>HABILIDADES:</b> QUÉ HABILIDADES ESPECÍFICAS DEBE POSEER Y EN QUÉ GRADO.	
<b>EXPERIENCIA:</b> QUÉ EXPERIENCIA DEBE TENER, SOBRE QUÉ TEMAS O SITUACIONES, Y DE QUÉ NIVEL.	
<b>OTROS:</b> OTROS REQUISITOS ESPECIALES TALES COMO GÉNERO, EDAD, NACIONALIDAD, ESTADO DE SALUD, CONDICIONES FÍSICAS, ETC.	

NOMBRE DEL ROL	Director del proyecto
<b>OBJETIVOS DEL ROL:</b> OBJETIVOS QUE DEBE LOGRAR EL ROL DENTRO DEL PROYECTO (¿PARA QUÉ SE HA CREADO EL ROL?).	Es la persona que gestiona el proyecto, es el principal responsable del éxito del proyecto, además es la persona que asume el liderazgo y la administración de cada recurso del proyecto para lograr los objetivos fijados por el patrocinador.
<b>RESPONSABILIDADES:</b> TEMAS PUNTUALES POR LOS CUALES ES RESPONSABLE (¿DE QUÉ ES RESPONSABLE?).	<ul style="list-style-type: none"> <li>• Elaborar el Acta de constitución del proyecto</li> <li>• Elaborar el Enunciado del Alcance del Proyecto.</li> <li>• Elaborar el Plan de Proyecto.</li> <li>• Elaborar el informe de estado del proyecto.</li> <li>• Realizar la reunión de coordinación semanal.</li> <li>• Elaborar el Cierre del proyecto.</li> <li>• Aprobar las oficinas y bienes adquiridos por la empresa.</li> <li>• Elaborar todos los Informes de Sesión de los cursos que se van a dictar.</li> <li>• Elaborar los Informes Mensuales del Servicio que se deben enviar al cliente.</li> <li>• Elaborar el Informe Final del Servicio que se envía al cliente.</li> </ul>
<b>FUNCIONES:</b> FUNCIONES ESPECÍFICAS QUE DEBE CUMPLIR (¿QUÉ DEBE REALIZAR PARA LOGRAR SUS OBJETIVOS Y CUBRIR SUS RESPONSABILIDADES?).	<ul style="list-style-type: none"> <li>• Ayudar al patrocinador a iniciar el proyecto</li> <li>• Planificar el proyecto</li> <li>• Ejecutar el proyecto.</li> <li>• Controlar el proyecto.</li> <li>• Cerrar el proyecto.</li> <li>• Ayudar a gestionar el control de cambios del proyecto.</li> <li>• Ayudar a gestionar los temas contractuales con el cliente.</li> <li>• Gestionar los recursos del proyecto.</li> <li>• Solucionar problemas y superar los obstáculos del proyecto.</li> </ul>

**NIVELES DE AUTORIDAD:** QUÉ DECISIONES PUEDE TOMAR CON RELACIÓN AL ALCANCE, CRONOGRAMA, COSTO, CALIDAD, RECURSOS Y MATERIALES, PLANES Y PROGRAMAS, INFORMES Y ENTREGABLES, ADQUISICIONES, CONTRATOS, PROVEEDORES, ETC.

- Decide sobre la programación detallada de los recursos asignados al proyecto.
- Decide sobre la información y los entregables del proyecto.
- Decide sobre los proveedores y contratos del proyecto, siempre y cuando no excedan lo presupuestado.

**REPORTA A:** A QUIÉN REPORTA DENTRO DEL PROYECTO.

Patrocinador.

**SUPERVISA A:** A QUIÉNES SUPERVISA DENTRO DEL PROYECTO.

- Jefe de equipo de desarrollo de software.
- Jefe de análisis y testing.
- Encargado de base de datos.
- Analista de seguridad.
- Director de IT

**REQUISITOS DEL ROL:** QUÉ REQUISITOS DEBEN CUMPLIR LAS PERSONAS QUE ASUMAN EL ROL.

<b>CONOCIMIENTOS:</b> QUÉ TEMAS, MATERIAS, O ESPECIALIDADES DEBE CONOCER, MANEJAR O DOMINAR.	<ul style="list-style-type: none"> <li>• Gestión de proyectos según la guía del PMBOK</li> <li>• Conocimientos sobre desarrollo de aplicaciones en Android y Apple.</li> <li>• Conocimientos en metodologías agiles y desarrollo de software.</li> </ul>
<b>HABILIDADES:</b> QUÉ HABILIDADES ESPECÍFICAS DEBE POSEER Y EN QUÉ GRADO.	<ul style="list-style-type: none"> <li>• Liderazgo.</li> <li>• Comunicación.</li> <li>• Negociación.</li> <li>• Solución de conflictos.</li> <li>• Motivación.</li> </ul>
<b>EXPERIENCIA:</b> QUÉ EXPERIENCIA DEBE TENER, SOBRE QUÉ TEMAS O SITUACIONES, Y DE QUÉ NIVEL.	<ul style="list-style-type: none"> <li>• Gestión de proyectos según la guía del PMBOK (3 años)</li> <li>• Experiencia en desarrollo de aplicaciones Android y Apple (3 años)</li> <li>• Conocimiento sobre servicios al cliente.</li> </ul>
<b>OTROS:</b> OTROS REQUISITOS ESPECIALES TALES COMO GÉNERO, EDAD, NACIONALIDAD, ESTADO DE SALUD, CONDICIONES FÍSICAS, ETC.	

**NOMBRE DEL ROL**

Director de IT

**OBJETIVOS DEL ROL:** OBJETIVOS QUE DEBE LOGRAR EL ROL DENTRO DEL PROYECTO (¿PARA QUÉ SE HA CREADO EL ROL?).

Es la persona encargada sobre redes, hardware, software y toda operación informática que se lleva a cabo tanto de la decisión sobre que utilizar y verificar que todo lo implementado se encuentre correcto.

**RESPONSABILIDADES:** TEMAS PUNTUALES POR LOS CUALES ES RESPONSABLE (¿DE QUÉ ES RESPONSABLE?).

- Realizar documento de toma de requerimientos y especificaciones del sistema.
- Evaluar necesidades tecnológicas.
- Establecer recursos o tecnologías a usar en un corto y largo plazo.

- Elaborar un plan de arquitectura para la aplicación.
- Aprobar los recursos para el desarrollo de la aplicación sobre tecnologías a implementar
- Planes de contingencia.
- Guía de revisión de instalación.
- Informe de instalación.
- Administrar el sistema de información utilizado.

**FUNCIONES:** FUNCIONES ESPECÍFICAS QUE DEBE CUMPLIR (¿QUÉ DEBE REALIZAR PARA LOGRAR SUS OBJETIVOS Y CUBRIR SUS RESPONSABILIDADES?).

- Gestionar las operaciones técnicas de desarrollo de la aplicación y base de datos.
- Hacer todo lo posible por alcanzar un alta de calidad en la aplicación y satisfacción del cliente sobre las herramientas utilizadas.
- Gestionar medidas de seguridad eficaces tanto físicas como políticas sobre el software y hardware utilizado.
- Garantizar una buena política de recuperación sobre un caso de desastre.
- Llevar a cabo actualizaciones a futuro sobre el software y hardware utilizado.

**NIVELES DE AUTORIDAD:** QUÉ DECISIONES PUEDE TOMAR CON RELACIÓN AL ALCANCE, CRONOGRAMA, COSTO, CALIDAD, RECURSOS Y MATERIALES, PLANES Y PROGRAMAS, INFORMES Y ENTREGABLES, ADQUISICIONES, CONTRATOS, PROVEEDORES, ETC.

- Decide sobre la programación detallada de los recursos asignados al proyecto.
- Decide sobre los proveedores y contratos del proyecto, siempre y cuando no excedan lo presupuestado.

**REPORTA A:** A QUIÉN REPORTA DENTRO DEL PROYECTO.

Director del proyecto.

**SUPERVISA A:** A QUIÉNES SUPERVISA DENTRO DEL PROYECTO.

- Jefe de desarrollo del software.
- Encargado de la base de datos.
- Analista de seguridad.
- Jefe de análisis y testing.

**REQUISITOS DEL ROL:** QUÉ REQUISITOS DEBEN CUMPLIR LAS PERSONAS QUE ASUMAN EL ROL.

<b>CONOCIMIENTOS:</b> QUÉ TEMAS, MATERIAS, O ESPECIALIDADES DEBE CONOCER, MANEJAR O DOMINAR.	<ul style="list-style-type: none"> <li>• Gestión de proyectos según la guía del PMBOK</li> <li>• Conocimientos sobre desarrollo de aplicaciones en Android y Apple.</li> <li>• Conocimientos en metodologías agiles y desarrollo de software.</li> <li>• Conocimientos de base de datos.</li> <li>• Conocimientos sobre redes.</li> <li>• Conocimientos de seguridad.</li> </ul>
<b>HABILIDADES:</b> QUÉ HABILIDADES ESPECÍFICAS DEBE POSEER Y EN QUÉ GRADO.	<ul style="list-style-type: none"> <li>• Liderazgo.</li> <li>• Comunicación.</li> <li>• Negociación.</li> <li>• Solución de conflictos.</li> <li>• Motivación.</li> </ul>

<b>EXPERIENCIA:</b> <i>QUÉ EXPERIENCIA DEBE TENER, SOBRE QUÉ TEMAS O SITUACIONES, Y DE QUÉ NIVEL.</i>	<ul style="list-style-type: none"> <li>• Gestión de proyectos según la guía del PMBOK (3 años)</li> <li>• Experiencia en desarrollo de aplicaciones Android y Apple (3 años)</li> <li>• Conocimiento sobre servicios al cliente.</li> <li>• Experiencia como director de IT (3 años).</li> </ul>
<b>OTROS:</b> <i>OTROS REQUISITOS ESPECIALES TALES COMO GÉNERO, EDAD, NACIONALIDAD, ESTADO DE SALUD, CONDICIONES FÍSICAS, ETC.</i>	

<b>NOMBRE DEL ROL</b>
<b>Jefe de desarrollo de software</b>
<b>OBJETIVOS DEL ROL:</b> <i>OBJETIVOS QUE DEBE LOGRAR EL ROL DENTRO DEL PROYECTO (¿PARA QUÉ SE HA CREADO EL ROL?).</i>
Es la persona encargada del grupo de desarrolladores de la aplicación, de organizar y gestionar las diferentes áreas de desarrollo para lograr obtener los resultados esperados en el tiempo establecido.
<b>RESPONSABILIDADES:</b> <i>TEMAS PUNTUALES POR LOS CUALES ES RESPONSABLE (¿DE QUÉ ES RESPONSABLE?).</i>
<ul style="list-style-type: none"> <li>• Supervisar y coordinar los recursos informáticos.</li> <li>• Planificar el desarrollo, adquisición de sistemas.</li> <li>• Supervisar y mandar a prueba los módulos desarrollados para su aprobación.</li> <li>• Conducir el proceso sobre en la puesta de funcionamiento de la aplicación.</li> <li>• Intervenir y dar asesorías en cualquier tarea de desarrollo.</li> <li>• Diseños de interfaz gráfica.</li> <li>• Diseños de algoritmos.</li> <li>• Estándares de programación.</li> <li>• Técnicas de implementación recomendadas.</li> <li>• Descripción de las entradas y salidas.</li> <li>• Diseño final del sistema.</li> <li>• Manual técnico.</li> <li>• Manual de usuario.</li> <li>• Aplicación funcional.</li> </ul>
<b>FUNCIONES:</b> <i>FUNCIONES ESPECÍFICAS QUE DEBE CUMPLIR (¿QUÉ DEBE REALIZAR PARA LOGRAR SUS OBJETIVOS Y CUBRIR SUS RESPONSABILIDADES?).</i>
<ul style="list-style-type: none"> <li>• Gestionar los recursos informáticos.</li> <li>• Supervisar cada fase de desarrollo del software y guiar al equipo.</li> <li>• Documentar y mandar a aprobación de los módulos desarrollados.</li> <li>• Monitorear cada proceso de puesta de funcionamiento asegurando el éxito.</li> <li>• Asesorar al equipo de desarrollo y a la directiva sobre asuntos de informática.</li> </ul>
<b>NIVELES DE AUTORIDAD:</b> <i>QUÉ DECISIONES PUEDE TOMAR CON RELACIÓN AL ALCANCE, CRONOGRAMA, COSTO, CALIDAD, RECURSOS Y MATERIALES, PLANES Y PROGRAMAS, INFORMES Y ENTREGABLES, ADQUISICIONES, CONTRATOS, PROVEEDORES, ETC.</i>
<ul style="list-style-type: none"> <li>• Decide sobre recursos asignados al equipo de desarrollo.</li> </ul>

- |   |
|---|
| <ul style="list-style-type: none"> <li>Decide sobre modificaciones a los procesos de desarrollo del proyecto.</li> <li>Decide sobre planes y programas del proyecto.</li> </ul> |
|---|

**REPORTA A:** A QUIÉN REPORTA DENTRO DEL PROYECTO.

Director de proyecto.

Director de IT.

**SUPERVISA A:** A QUIÉNES SUPERVISA DENTRO DEL PROYECTO.

Equipo de desarrollo de la aplicación.

**REQUISITOS DEL ROL:** QUÉ REQUISITOS DEBEN CUMPLIR LAS PERSONAS QUE ASUMAN EL ROL.

<b>CONOCIMIENTOS:</b> QUÉ TEMAS, MATERIAS, O ESPECIALIDADES DEBE CONOCER, MANEJAR O DOMINAR.	Guía del PMBOK. Metodologías de desarrollo agiles. Herramientas de desarrollo: MVC, Azure, otros. Manejo de herramientas de ambientes de desarrollo. Conocimiento de programación de lenguajes, arquitecturas y paradigmas. Conocimientos sobre comunicación de aplicaciones tales como: SOA, servicios Web, SOAP, REST, otros.
<b>HABILIDADES:</b> QUÉ HABILIDADES ESPECÍFICAS DEBE POSEER Y EN QUÉ GRADO.	<ul style="list-style-type: none"> <li>Liderazgo.</li> <li>Comunicación.</li> <li>Solución de conflictos.</li> <li>Motivación.</li> <li>Trabajo sobre presión.</li> <li>Compañerismo.</li> </ul>
<b>EXPERIENCIA:</b> QUÉ EXPERIENCIA DEBE TENER, SOBRE QUÉ TEMAS O SITUACIONES, Y DE QUÉ NIVEL.	Experiencia laboral en desarrollo de aplicaciones móviles (5 años) Experiencia laboral en construcción de aplicaciones informáticas utilizando servicios en la nube (3 años).
<b>OTROS:</b> OTROS REQUISITOS ESPECIALES TALES COMO GÉNERO, EDAD, NACIONALIDAD, ESTADO DE SALUD, CONDICIONES FÍSICAS, ETC.	

**NOMBRE DEL ROL**

**Jefe de Análisis y testing**

**OBJETIVOS DEL ROL:** OBJETIVOS QUE DEBE LOGRAR EL ROL DENTRO DEL PROYECTO (¿PARA QUÉ SE HA CREADO EL ROL?).

Es la persona que se encarga de aprobar los diferentes módulos desarrollados después de haberlos sometidos a diferentes pruebas comprobando su calidad y regresando a desarrollo nuevamente todos aqueos que no hayan pasado las pruebas.

**RESPONSABILIDADES:** TEMAS PUNTUALES POR LOS CUALES ES RESPONSABLE (¿DE QUÉ ES RESPONSABLE?).

- Realizar el control de calidad del aplicativo.
- Plan de desarrollo de pruebas.
- Diseño y documentación de pruebas.
- Reportar fallas al jefe de desarrollo de software sobre la aplicación.
- Llevar seguimiento de controles de calidad.

**FUNCIONES:** FUNCIONES ESPECÍFICAS QUE DEBE CUMPLIR (¿QUÉ DEBE REALIZAR PARA LOGRAR SUS OBJETIVOS Y CUBRIR SUS RESPONSABILIDADES?).

- Planificar un plan de testing.
- Definir situaciones para realizar pruebas.
- Realizar pruebas a módulos que se integren.
- Planificar y ejecutar casos de prueba.
- Realizar varias pruebas como performance, instalación, aceptación, usabilidad.
- Analizar, reportar y seguir errores encontrados en los diferentes módulos.
- Maximizar la calidad del módulo desarrollado encontrando cualquier inconveniente en este.

**NIVELES DE AUTORIDAD:** QUÉ DECISIONES PUEDE TOMAR CON RELACIÓN AL ALCANCE, CRONOGRAMA, COSTO, CALIDAD, RECURSOS Y MATERIALES, PLANES Y PROGRAMAS, INFORMES Y ENTREGABLES, ADQUISICIONES, CONTRATOS, PROVEEDORES, ETC.

- Decide sobre recursos asignados al equipo de testing.
- Decide sobre modificaciones a las diferentes pruebas planificadas.

**REPORTA A:** A QUIÉN REPORTA DENTRO DEL PROYECTO.

Director del proyecto.

Director de IT.

**SUPERVISA A:** A QUIÉNES SUPERVISA DENTRO DEL PROYECTO.

Equipo de testing

**REQUISITOS DEL ROL:** QUÉ REQUISITOS DEBEN CUMPLIR LAS PERSONAS QUE ASUMAN EL ROL.

<b>CONOCIMIENTOS:</b> QUÉ TEMAS, MATERIAS, O ESPECIALIDADES DEBE CONOCER, MANEJAR O DOMINAR.	<ul style="list-style-type: none"> <li>• Conocimientos de software.</li> <li>• Conocimientos sobre desarrollo de software.</li> <li>• Conocimiento sobre metodologías agiles.</li> <li>• Conocimientos sobre herramientas de testing y seguimiento de testing.</li> <li>• Conocimientos sobre pruebas manuales.</li> <li>• Conocimientos sobre pruebas automatizadas.</li> </ul>
<b>HABILIDADES:</b> QUÉ HABILIDADES ESPECÍFICAS DEBE POSEER Y EN QUÉ GRADO.	<ul style="list-style-type: none"> <li>• Ser Responsabilidad y ético.</li> <li>• Pensamiento analítico y crítico.</li> <li>• Capacidad de trabajar en equipo.</li> <li>• Capacidad en trabajar bajo presión.</li> <li>• Facilidad en incorporar nuevos procesos o módulos.</li> <li>• Capacidad de utilización de métricas en las diferentes pruebas de desempeño.</li> </ul>
<b>EXPERIENCIA:</b> QUÉ EXPERIENCIA DEBE TENER, SOBRE QUÉ TEMAS O SITUACIONES, Y DE QUÉ NIVEL.	<p>Tener experiencia en testing de aplicaciones móviles (2 años)</p> <p>Tener experiencia con uso de herramientas de testing automatizado como Zira o alguna herramienta de pruebas (2 años).</p>
<b>OTROS:</b> OTROS REQUISITOS ESPECIALES TALES COMO GÉNERO, EDAD, NACIONALIDAD, ESTADO DE SALUD, CONDICIONES FÍSICAS, ETC.	

**NOMBRE DEL ROL**

Encargado de base de datos

<b>OBJETIVOS DEL ROL:</b> <i>OBJETIVOS QUE DEBE LOGRAR EL ROL DENTRO DEL PROYECTO (¿PARA QUÉ SE HA CREADO EL ROL?).</i>	
Es la persona encargada de crear un modelo eficiente, efectivo y seguro para almacenar la información obtenida y generada de los clientes, que sea optima y escalable además de mantenerla cuando esta se encuentre en funcionamiento.	
<b>RESPONSABILIDADES:</b> <i>TEMAS PUNTUALES POR LOS CUALES ES RESPONSABLE (¿DE QUÉ ES RESPONSABLE?).</i>	
<ul style="list-style-type: none"> <li>• Crear y realizar la Normalización de la base de datos.</li> <li>• Administración y gestionar la base de datos.</li> <li>• Diccionario de datos.</li> </ul>	
<b>FUNCIONES:</b> <i>FUNCIONES ESPECÍFICAS QUE DEBE CUMPLIR (¿QUÉ DEBE REALIZAR PARA LOGRAR SUS OBJETIVOS Y CUBRIR SUS RESPONSABILIDADES?).</i>	
<ul style="list-style-type: none"> <li>• Crear y modificar la base de datos.</li> <li>• Optimizar la base de datos Normalizándola.</li> <li>• Aplicar tecnologías para mantener la base de datos seguro.</li> <li>• Monitorear el uso y la capacidad de la base de datos.</li> <li>• Garantizar y optimizar la seguridad, estabilidad e integridad de la base de datos.</li> <li>• Garantizar el respaldo de la información haciendo respaldos.</li> <li>• Mantener y dar mantenimiento a la base de datos.</li> <li>• Permitir la realización de auditorías, cambios y actualizaciones.</li> </ul>	
<b>NIVELES DE AUTORIDAD:</b> <i>QUÉ DECISIONES PUEDE TOMAR CON RELACIÓN AL ALCANCE, CRONOGRAMA, COSTO, CALIDAD, RECURSOS Y MATERIALES, PLANES Y PROGRAMAS, INFORMES Y ENTREGABLES, ADQUISICIONES, CONTRATOS, PROVEEDORES, ETC.</i>	
<ul style="list-style-type: none"> <li>• Decide sobre recursos asignados al desarrollo de la base de datos.</li> <li>• Decide sobre modificaciones a la base de datos</li> <li>• Decide sobre planes, auditorias, mantenimientos, otros, sobre la base de datos.</li> </ul>	
<b>REPORTA A:</b> <i>A QUIÉN REPORTA DENTRO DEL PROYECTO.</i>	
Director del proyecto. Director de IT.	
<b>SUPERVISA A:</b> <i>A QUIÉNES SUPERVISA DENTRO DEL PROYECTO.</i>	
Ninguno.	
<b>REQUISITOS DEL ROL:</b> <i>QUÉ REQUISITOS DEBEN CUMPLIR LAS PERSONAS QUE ASUMAN EL ROL.</i>	
<b>CONOCIMIENTOS:</b> <i>QUÉ TEMAS, MATERIAS, O ESPECIALIDADES DEBE CONOCER, MANEJAR O DOMINAR.</i>	<ul style="list-style-type: none"> <li>• Conocimientos sobre SQL, no-SQL.</li> <li>• Conocimientos sobre DML, DDL.</li> <li>• Conocimientos sobre respaldos y recuperaciones.</li> <li>• Conocimientos sobre redes y configuración de motores.</li> <li>• Conocimientos sobre consola, Linux server, Windows server, otros.</li> <li>• Haber finalizado los estudios universitarios.</li> <li>• Poseer certificado de Oracle.</li> </ul>
<b>HABILIDADES:</b> <i>QUÉ HABILIDADES ESPECÍFICAS DEBE POSEER Y EN QUÉ GRADO.</i>	<ul style="list-style-type: none"> <li>• Responsable y proactivo</li> <li>• Pensamiento analítico y crítico.</li> <li>• Capacidad en trabajar bajo presión.</li> </ul>

<b>EXPERIENCIA:</b> <i>QUÉ EXPERIENCIA DEBE TENER, SOBRE QUÉ TEMAS O SITUACIONES, Y DE QUÉ NIVEL.</i>	<ul style="list-style-type: none"> <li>• Haber creado base de datos.</li> <li>• Haber administrado base de datos (3 años).</li> <li>• Poseer experiencia en realizar respaldos y recuperaciones.</li> </ul>
<b>OTROS:</b> <i>OTROS REQUISITOS ESPECIALES TALES COMO GÉNERO, EDAD, NACIONALIDAD, ESTADO DE SALUD, CONDICIONES FÍSICAS, ETC.</i>	

<b>NOMBRE DEL ROL</b>	
<b>ANALISTA DE SEGURIDAD</b>	
<b>OBJETIVOS DEL ROL:</b> <i>OBJETIVOS QUE DEBE LOGRAR EL ROL DENTRO DEL PROYECTO (¿PARA QUÉ SE HA CREADO EL ROL?).</i>	
Diseñar, desarrollar, implementar y mantener los procesos y estrategias que permitan reducir riesgos para los activos y la plataforma tecnológica de la organización.	
<b>RESPONSABILIDADES:</b> <i>TEMAS PUNTUALES POR LOS CUALES ES RESPONSABLE (¿DE QUÉ ES RESPONSABLE?).</i>	
<ul style="list-style-type: none"> <li>• Evaluar la vulnerabilidad del sistema.</li> <li>• Realizar las pruebas e indicar el resultado de estas.</li> <li>• Proponer estrategias de mitigación de riesgos.</li> <li>• Implementar estrategias de mitigación de riesgos.</li> <li>• Planificar, implementar, monitorear y mejorar las medidas de seguridad de la organización.</li> </ul>	
<b>FUNCIONES:</b> <i>FUNCIONES ESPECÍFICAS QUE DEBE CUMPLIR (¿QUÉ DEBE REALIZAR PARA LOGRAR SUS OBJETIVOS Y CUBRIR SUS RESPONSABILIDADES?).</i>	
<ul style="list-style-type: none"> <li>• Definir la arquitectura de la seguridad de la red.</li> <li>• Potenciar la cultura de seguridad informática.</li> <li>• Prevención de nuevos riesgos.</li> <li>• Supervisar la implementación de los sistemas diseñados.</li> <li>• Controlar la implementación de controles sobre seguridad informática.</li> </ul>	
<b>NIVELES DE AUTORIDAD:</b> <i>QUÉ DECISIONES PUEDE TOMAR CON RELACIÓN AL ALCANCE, CRONOGRAMA, COSTO, CALIDAD, RECURSOS Y MATERIALES, PLANES Y PROGRAMAS, INFORMES Y ENTREGABLES, ADQUISICIONES, CONTRATOS, PROVEEDORES, ETC.</i>	
<ul style="list-style-type: none"> <li>• Admitir o denegar el avance de una función desarrollada del sistema.</li> <li>• Entrega reportes sobre las pruebas de seguridad realizadas a las funcionalidades.</li> </ul>	
<b>REPORTA A:</b> <i>A QUIÉN REPORTA DENTRO DEL PROYECTO.</i>	
Director del proyecto. Director de IT.	
<b>SUPERVISA A:</b> <i>A QUIÉNES SUPERVISA DENTRO DEL PROYECTO.</i>	
No ejerce supervisión.	
<b>REQUISITOS DEL ROL:</b> <i>QUÉ REQUISITOS DEBEN CUMPLIR LAS PERSONAS QUE ASUMAN EL ROL.</i>	
<b>CONOCIMIENTOS:</b> <i>QUÉ TEMAS, MATERIAS, O ESPECIALIDADES DEBE CONOCER, MANEJAR O DOMINAR.</i>	<ul style="list-style-type: none"> <li>• Normativas de seguridad.</li> <li>• Servicios de seguridad.</li> <li>• Software de seguridad.</li> <li>• Identificación de los requerimientos para la implementación del protocolo de seguridad informática.</li> </ul>

	<ul style="list-style-type: none"> <li>• Leyes y estándares de seguridad.</li> </ul>
<b>HABILIDADES:</b> <i>QUÉ HABILIDADES ESPECÍFICAS DEBE POSEER Y EN QUÉ GRADO.</i>	<ul style="list-style-type: none"> <li>• Pensamiento crítico.</li> <li>• Evaluación de riesgos.</li> <li>• Resolución de problemas.</li> <li>• Implementación de estrategias creativas.</li> <li>• Atención a los detalles.</li> <li>• Conocimientos en HTML, Java y Python.</li> <li>• Comunicación asertiva.</li> </ul>
<b>EXPERIENCIA:</b> <i>QUÉ EXPERIENCIA DEBE TENER, SOBRE QUÉ TEMAS O SITUACIONES, Y DE QUÉ NIVEL.</i>	1 año de experiencia en labores relacionadas con el cargo.
<b>OTROS:</b> <i>OTROS REQUISITOS ESPECIALES TALES COMO GÉNERO, EDAD, NACIONALIDAD, ESTADO DE SALUD, CONDICIONES FÍSICAS, ETC.</i>	
<b>NOMBRE DEL ROL</b>	<b>AUXILIAR DE TESTING</b>
<b>OBJETIVOS DEL ROL:</b> <i>OBJETIVOS QUE DEBE LOGRAR EL ROL DENTRO DEL PROYECTO (¿PARA QUÉ SE HA CREADO EL ROL?).</i>	Asegurar la calidad de un software a lo largo de todas sus fases.
<b>RESPONSABILIDADES:</b> <i>TEMAS PUNTUALES POR LOS CUALES ES RESPONSABLE (¿DE QUÉ ES RESPONSABLE?).</i>	<ul style="list-style-type: none"> <li>• Verificar que el software no tenga fallos</li> <li>• Revisar especificaciones del producto</li> <li>• Garantizar que el producto está listo para el público</li> </ul>
<b>FUNCIONES:</b> <i>FUNCIONES ESPECÍFICAS QUE DEBE CUMPLIR (¿QUÉ DEBE REALIZAR PARA LOGRAR SUS OBJETIVOS Y CUBRIR SUS RESPONSABILIDADES?).</i>	<ul style="list-style-type: none"> <li>• Crear un plan de pruebas y testing.</li> <li>• Probar los programas de software de automatización.</li> <li>• Simular el rendimiento del producto y evaluar los resultados.</li> <li>• Identificar los problemas de los productos mediante el uso de sistemas de seguimiento de errores.</li> <li>• Crear bases de datos de defectos de productos conocidos y analizar estos problemas.</li> <li>• Asesoramiento sobre el diseño de productos para reducir los posibles problemas.</li> <li>• Mejorar las estrategias de pruebas.</li> </ul>
<b>NIVELES DE AUTORIDAD:</b> <i>QUÉ DECISIONES PUEDE TOMAR CON RELACIÓN AL ALCANCE, CRONOGRAMA, COSTO, CALIDAD, RECURSOS Y MATERIALES, PLANES Y PROGRAMAS, INFORMES Y ENTREGABLES, ADQUISICIONES, CONTRATOS, PROVEEDORES, ETC.</i>	<ul style="list-style-type: none"> <li>• Admitir o denegar una funcionalidad desarrollada de acuerdo con el resultado de las pruebas realizadas.</li> <li>• Dar el visto bueno de que el proyecto está finalizado para la entrega del cliente.</li> </ul>
<b>REPORTA A:</b> <i>A QUIÉN REPORTA DENTRO DEL PROYECTO.</i>	
Director de Proyecto. Analista y tester.	

Director de IT.	
<b>SUPERVISA A:</b> A QUIÉNES SUPERVISA DENTRO DEL PROYECTO.	
<b>REQUISITOS DEL ROL:</b> QUÉ REQUISITOS DEBEN CUMPLIR LAS PERSONAS QUE ASUMAN EL ROL.	
<b>CONOCIMIENTOS:</b> QUÉ TEMAS, MATERIAS, O ESPECIALIDADES DEBE CONOCER, MANEJAR O DOMINAR.	<ul style="list-style-type: none"> <li>• Ingeniería Informática o Educación IT.</li> <li>• Control de las normas de calidad de la industria.</li> <li>• Métodos estadísticos.</li> <li>• Métodos y técnicas de calidad.</li> <li>• Manejo de Microsoft Project.</li> <li>• Manejo de Microsoft Visio.</li> </ul>
<b>HABILIDADES:</b> QUÉ HABILIDADES ESPECÍFICAS DEBE POSEER Y EN QUÉ GRADO.	<ul style="list-style-type: none"> <li>• Capacidad de análisis y juicio crítico.</li> <li>• Actitud de perfeccionamiento.</li> <li>• Planificación y organización.</li> <li>• Buenas relaciones interpersonales.</li> <li>• Liderazgo.</li> <li>• Redacción de informes.</li> <li>• Orientación a resultados.</li> <li>• Trabajo en equipo.</li> <li>• Dinamismo.</li> <li>• Atención al detalle.</li> <li>• Comunicación oral y escrita.</li> <li>• Capacidad para enseñar o impartir conocimientos.</li> </ul>
<b>EXPERIENCIA:</b> QUÉ EXPERIENCIA DEBE TENER, SOBRE QUÉ TEMAS O SITUACIONES, Y DE QUÉ NIVEL.	1 año de experiencia en labores relacionadas al cargo.
<b>OTROS:</b> OTROS REQUISITOS ESPECIALES TALES COMO GÉNERO, EDAD, NACIONALIDAD, ESTADO DE SALUD, CONDICIONES FÍSICAS, ETC.	
<b>NOMBRE DEL ROL</b>	
<b>AUXILIAR ADMINISTRATIVO</b>	
<b>OBJETIVOS DEL ROL:</b> OBJETIVOS QUE DEBE LOGRAR EL ROL DENTRO DEL PROYECTO (¿PARA QUÉ SE HA CREADO EL ROL?).	
Bajo supervisión directa realiza actividades de apoyo a las labores administrativas, según las operaciones propias de la institución, para fines de contribuir al eficiente desarrollo del área.	
<b>RESPONSABILIDADES:</b> TEMAS PUNTUALES POR LOS CUALES ES RESPONSABLE (¿DE QUÉ ES RESPONSABLE?).	
<ul style="list-style-type: none"> <li>• Velar por la protección de documentos confidenciales.</li> <li>• Recibir y despachar correspondencia.</li> <li>• Llevar control de gastos y solicitudes de fondos para la ejecución de diversas actividades.</li> <li>• Llevar el registro y control del suministro de material gastable y otros insumos del departamento y los Centros de Atención.</li> <li>• Tener al día la agenda.</li> </ul>	
<b>FUNCIONES:</b> FUNCIONES ESPECÍFICAS QUE DEBE CUMPLIR (¿QUÉ DEBE REALIZAR PARA LOGRAR SUS OBJETIVOS Y CUBRIR SUS RESPONSABILIDADES?).	

- Asistir al encargado del departamento y los demás encargados de las diferentes divisiones.
- Coordinar y ejecutar labores administrativas según normas y procedimientos establecidos.
- Archivar correspondencia y documentos según sistema establecido.
- Mantener actualizado los murales y administrar los buzones de sugerencias.
- Presentar informe de las labores realizadas.
- Cumplir las metas y los compromisos asignados conforme a la naturaleza del cargo.
- Realizar otras tareas afines y complementarias, conforme a lo asignado por su superior inmediato.
- Atención de llamadas telefónicas.
- Atender visitas.
- Recibir documentos.
- Comunicar todo lo relacionado con su trabajo al departamento al que pertenece.
- Encontrarse al día de la tramitación de expedientes.
- Conocer los procesos desarrollados por las Administraciones Públicas con las que el departamento tenga relación.

**NIVELES DE AUTORIDAD:** QUÉ DECISIONES PUEDE TOMAR CON RELACIÓN AL ALCANCE, CRONOGRAMA, COSTO, CALIDAD, RECURSOS Y MATERIALES, PLANES Y PROGRAMAS, INFORMES Y ENTREGABLES, ADQUISICIONES, CONTRATOS, PROVEEDORES, ETC.

Toma decisiones sobre contrato de nuevo personal, llamadas de atención o incluso un despido.

**REPORTA A:** A QUIÉN REPORTA DENTRO DEL PROYECTO.

Director de Proyecto.

**SUPERVISA A:** A QUIÉNES SUPERVISA DENTRO DEL PROYECTO.

**REQUISITOS DEL ROL:** QUÉ REQUISITOS DEBEN CUMPLIR LAS PERSONAS QUE ASUMAN EL ROL.

<b>CONOCIMIENTOS:</b> QUÉ TEMAS, MATERIAS, O ESPECIALIDADES DEBE CONOCER, MANEJAR O DOMINAR.	<ul style="list-style-type: none"> <li>• Redacción.</li> <li>• Archivo.</li> <li>• Manejo de Office.</li> <li>• Herramienta informática especializada.</li> </ul>
<b>HABILIDADES:</b> QUÉ HABILIDADES ESPECÍFICAS DEBE POSEER Y EN QUÉ GRADO.	<ul style="list-style-type: none"> <li>• Trabajo en equipo.</li> <li>• Vocación de servicio.</li> <li>• Integridad.</li> <li>• Juicio.</li> <li>• Dinamismo.</li> <li>• Planificación y Organización.</li> <li>• Análisis numérico.</li> <li>• Atención al detalle.</li> <li>• Comunicación oral y escrita.</li> </ul>
<b>EXPERIENCIA:</b> QUÉ EXPERIENCIA DEBE TENER, SOBRE QUÉ TEMAS O SITUACIONES, Y DE QUÉ NIVEL.	Seis meses en labores relacionadas con el cargo.
<b>OTROS:</b> OTROS REQUISITOS ESPECIALES TALES COMO GÉNERO, EDAD, NACIONALIDAD, ESTADO DE SALUD, CONDICIONES FÍSICAS, ETC.	

Fuente: (Dharma Consulting, 2022)

## Matriz de Asignación de responsabilidades

CONTROL DE VERSIONES					
Versión	Hecha por	Revisada por	Aprobada por	Fecha	Motivo
1.0	RM	CR	CR	26/02/2022	Versión Inicial

NOMBRE DEL PROYECTO	SIGLAS DEL PROYECTO
Aplicación Móvil Gestión y Atención de Clientes	AMGC

ENTREGABLES	ROLES / PERSONAS									
	PP	PM	DIT	JEDS	JAT	EBD	AS	AT	AA	
1.0 Toma y Análisis de requerimientos		R								
1.1 Documento completo con los requerimientos del aplicativo.	A	V	R	P			P	P	P	
1.2 Especificaciones del sistema.	A	V	R	P			P	P	P	
2.0 Diseño de estructura e interfaces gráficas				R	P	P	P			
2.1 Diseños de interfaz gráfica.		A	V	R	P	P	P			
2.2 Diseños de algoritmos.		A	V	R	P	P	P			
2.3 Diccionario de datos.				A	V	R	P	P	P	
2.4 Estándares de programación.		A	V	R	P		P			
2.5 Técnicas de implementación recomendadas.		A	V	R	P	P	P			
3.0 Desarrollo de la Aplicación			A	R	P	P	P	P	P	
3.1 Descripción de las entradas y salidas.			A	R	P	P	P	P	P	
3.2 Diseño final del sistema.		A	V	R	P	P	P	P	P	
3.3 Manual técnico.		A	V	R	P	P	P	P	P	
3.4 Manual de usuario.		A	V	R	P	P	P	P	P	
3.5 Aplicación funcional.		A	V	R	P	P	P	P	P	
4.0 Pruebas de aplicación		V	A	V	R	P	P	P		
4.1 Plan de desarrollo de pruebas.		V	A	V	R	P	P	P		
4.2 Diseño y documentación de pruebas.		V	A	V	R	P	P	P		
4.3 Resultado de pruebas realizadas.		V	A	V	R	P	P	P		
5.0 Implementación y puesta en marcha	A	V	R	P	P	P				
5.1 Planes de contingencia.	A	V	R	P	P	P				
5.2 Guía de revisión de instalación.	A	V	R	P	P	P				
5.3 Informe de instalación.	A	V	R	P	P	P				
6.0 Evaluación y verificación de resultados	A	R	P	P	P					
6.1 Informe de resultados.	A	R	P	P	P					
6.2 Carta de aceptación del sistema.	A	R	P	P	P					

### Códigos de Responsables:

**R** = RESPONSABLE  
**P** = PARTICIPA  
**V** = REVISA  
**A** = APRUEBA

### Códigos de Roles PF:

**PP**=Patrocinador del Proyecto  
**PM**=Project Manager  
**DIT**=Director de IT  
**JEDS**=Jefe de equipo desarrollo de software  
**JAT**=Jefe de análisis y testing  
**EBD**=Encargado de base de datos  
**AS**=Analista de seguridad  
**AT**=Auxiliar de testing  
**AA**=Auxiliar Administrativo

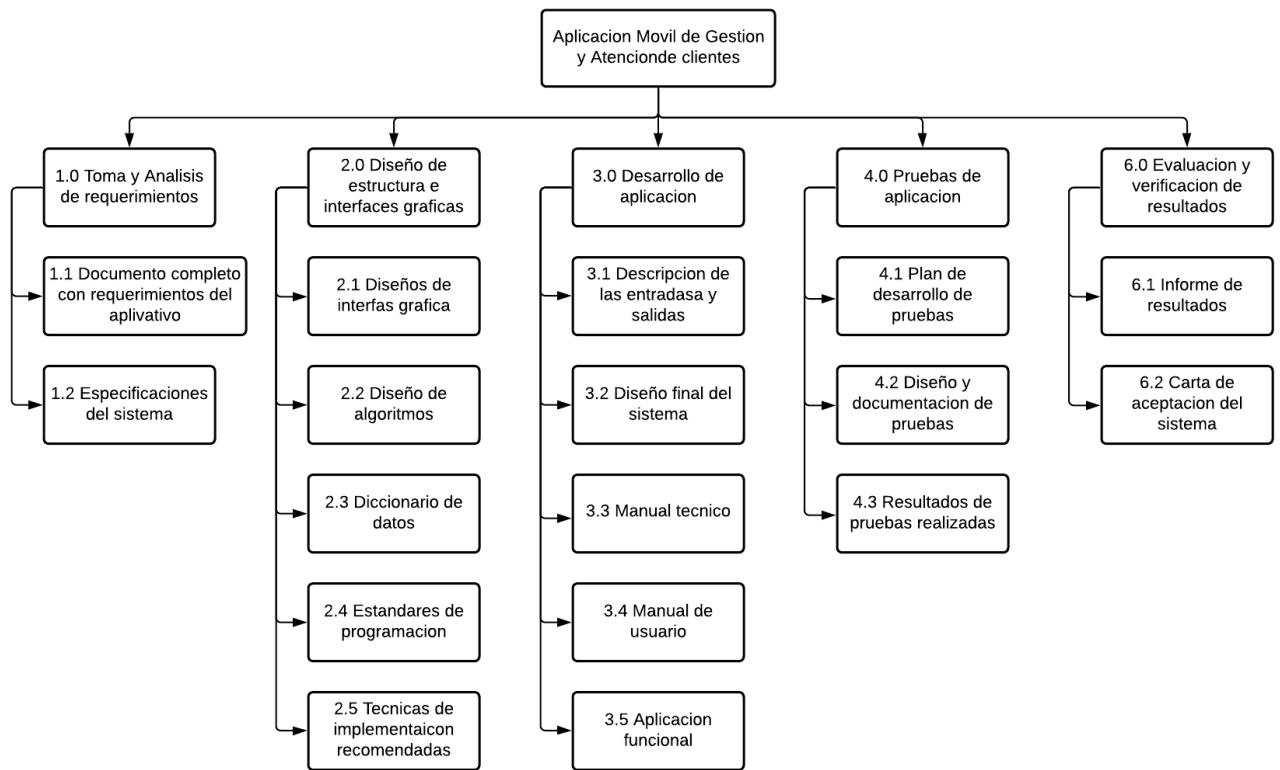
Fuente: (Dharma Consulting, 2022)

## Estructura de Desglose del Trabajo (EDT)

CONTROL DE VERSIONES					
Versión	Hecha por	Revisada por	Aprobada por	Fecha	Motivo
1.0	RM	CR	CR	31/01/2022	Versión Original
NOMBRE DEL PROYECTO			SIGLAS DEL PROYECTO		
<b>Aplicación Móvil de Gestión y Atención de Clientes</b>			<b>AMGC</b>		

Fuente: (Dharma Consulting, 2022)

**Figura No. 2**



Fuente: Elaboración Propia

## Organigrama del Proyecto

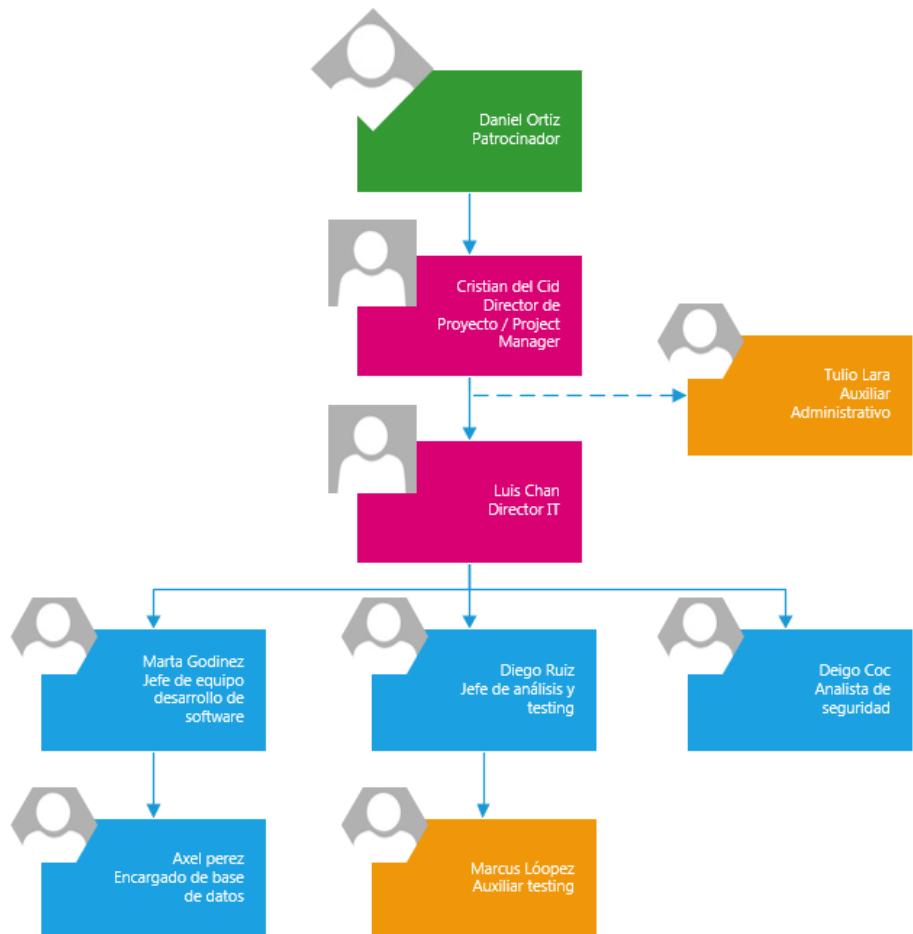
CONTROL DE VERSIONES					
Versión	Hecha por	Revisada por	Aprobada por	Fecha	Motivo
1.0	WO	CR	CR	31/01/2022	ORGANIGRAMA DEL PROYECTO

NOMBRE DEL PROYECTO	SIGLAS DEL PROYECTO
Aplicación Móvil Gestión y Atención de Clientes	AMGC

Fuente: (Dharma Consulting, 2022)

**Figura No. 3**



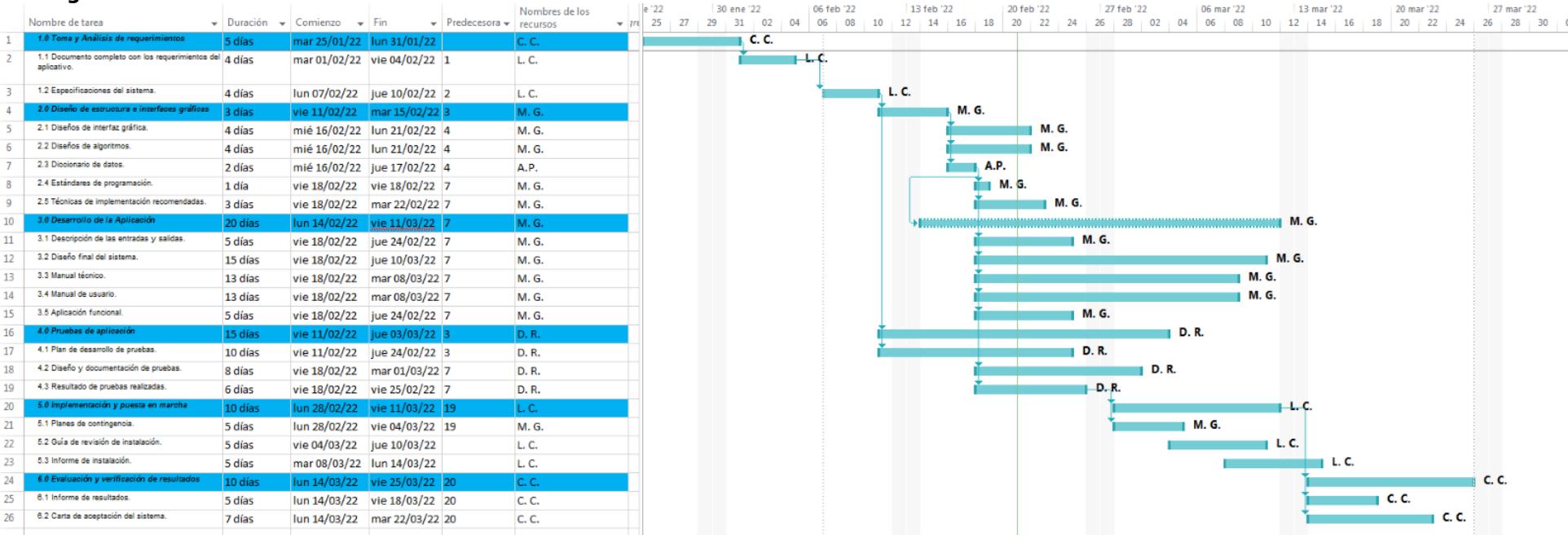
Fuente: Elaboración propia

## Cronograma de Hitos Principales

CONTROL DE VERSIONES					
Versión	Hecha por	Revisada por	Aprobada por	Fecha	Motivo
1.0					CRONOGRAMA DEL PROYECTO

NOMBRE DEL PROYECTO	SIGLAS DEL PROYECTO
Aplicación Móvil Gestión y Atención de Clientes	AMGC

Figura No. 4



Fuente: Elaboracion Propria

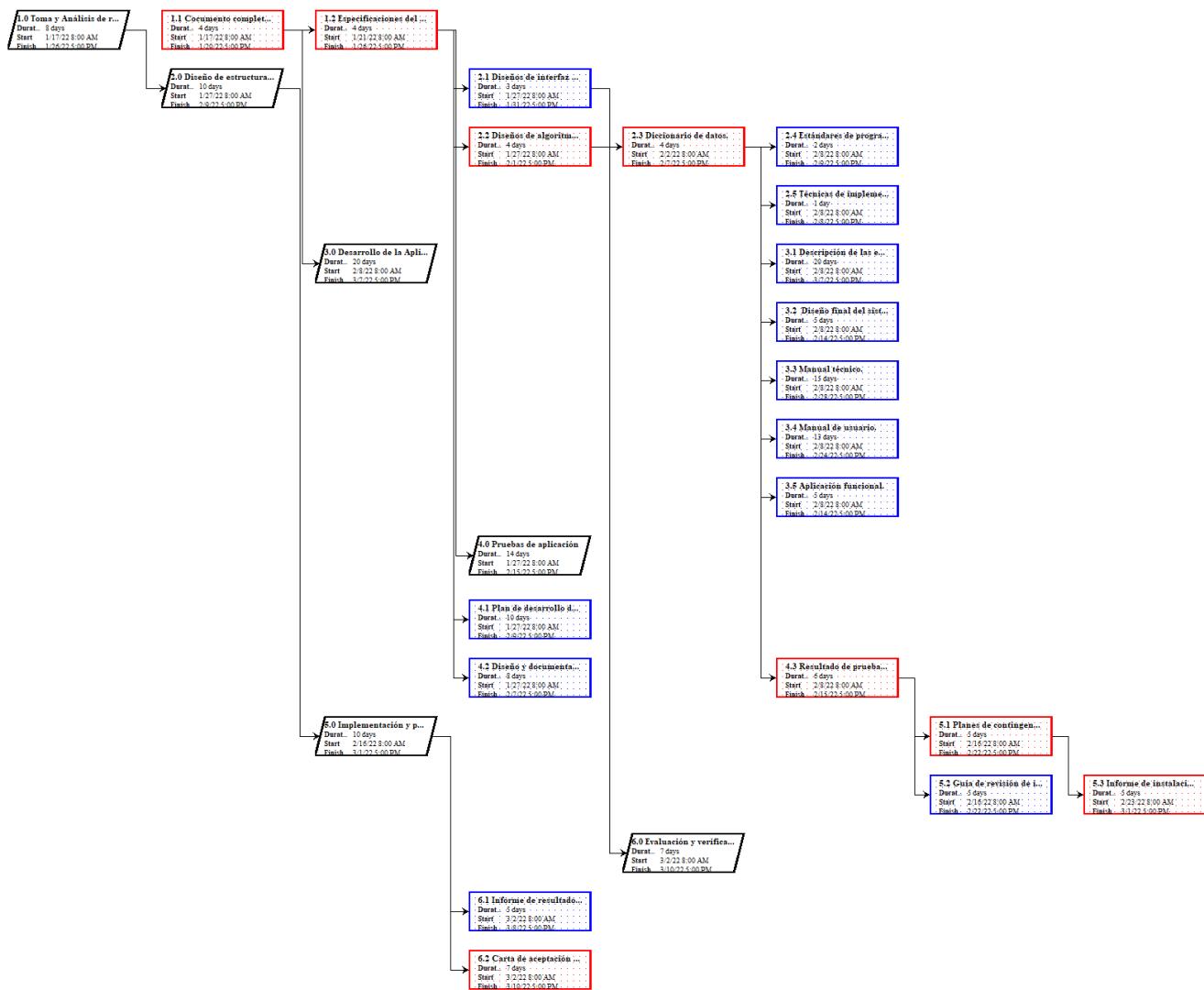
## Diagrama de Red del Proyecto

CONTROL DE VERSIONES					
Versión	Hecha por	Revisada por	Aprobada por	Fecha	Motivo
1.0	WO	CR	CR	21/02/22	Versión Original

NOMBRE DEL PROYECTO	SIGLAS DEL PROYECTO
Aplicación móvil de gestión y atención de clientes	AMGC

Fuente: (Dharma Consulting, 2022)

Figura No. 5



Fuente: Elaboración Propia

## **Costeo del Proyecto**

## **CONTROL DE VERSIONES**

Versión	Hecha por	Revisada por	Aprobada por	Fecha	Motivo
1.0	WO	CR	CR	21/02/22	Versión original

<b>NOMBRE DEL PROYECTO</b>	<b>SIGLAS DEL PROYECTO</b>
<b>Aplicación Móvil Gestión y Atención de Clientes</b>	<b>AMGC</b>

4.0	Plan de desarrollo de pruebas	D.R.	1	1	7500	7500									
	Diseño y documentación de pruebas	D.R.	1	1	3500	3500									
	Resultado de Pruebas Realizadas	D.R.	1	1	1500	1500									
5.0	Planes de contingencia	M.G.	1	1	2550	2550									
	Guía de revisión de instalación	L.C	1	1	2000	2000									
	Informe de instalación	L.C.	1	1	1700	1700									
6.0	Informe de resultados	C.C.	1	1	2600	2600									
	Carta de aceptación del sistema	C.C.	1	1	1000	1000									

Fuente: (Dharma Consulting, 2022)

## Presupuesto Estimado

CONTROL DE VERSIONES					
Versión	Hecha por	Revisada por	Aprobada por	Fecha	Motivo
1.0	RP	CR	CR	21/02/22	Versión original
NOMBRE DEL PROYECTO			SIGLAS DEL PROYECTO		
Aplicación Móvil Gestión y Atención de Clientes			AMGC		
PROYECTO	FASE	ENTREGABLE	MONTO \$		
Aplicativo móvil para Pillophone	<b>1.0 Toma y Análisis de requerimientos</b>	1.1 Documento completo con los requerimientos del aplicativo 1.2 Especificaciones del sistema.	3,000 2,500		
	<b>Total Fase</b>			<b>5,500</b>	
	<b>2.0 Diseño de estructura e interfaces gráficas</b>	2.1 Diseños de interfaz gráfica. 2.2 Diseños de algoritmos. 2.3 Diccionario de datos. 2.4 Estándares de programación. 2.5 Técnicas de implementación recomendadas.	3,550 4,000 1,000 2,500 1,600		
	<b>Total Fase</b>			<b>12,650</b>	
	<b>3.0 Desarrollo de la Aplicación</b>	3.1 Descripción de las entradas y salidas. 3.2 Diseño final del sistema. 3.3 Manual técnico. 3.4 Manual de usuario. 3.5 Aplicación funcional.	2,300 8,500 1,450 1,450 10,000		
	<b>Total Fase</b>			<b>23,700</b>	
	<b>4.0 Pruebas de aplicación</b>	4.1 Plan de desarrollo de pruebas. 4.2 Diseño y documentación de pruebas. 4.3 Resultado de pruebas realizadas.	7,500 3,500 1,500		
	<b>Total Fase</b>			<b>12,500</b>	
	<b>5.0 Implementación y puesta en marcha</b>	5.1 Planes de contingencia. 5.2 Guía de revisión de instalación. 5.3 Informe de instalación.	2,550 2,000 1,700		
	<b>Total Fase</b>			<b>6,250</b>	
	<b>6.0 Evaluación y verificación de resultados</b>	6.1 Informe de resultados.	2,600 1,000		

		6.2 Carta de aceptación del sistema.			
<b>Total Fase</b>			<b>3,600</b>		
<b>TOTAL FASES</b>			64,200		
<b>Reserva de Contingencia</b>			6,420		
<b>Reserva de Gestión</b>			6,420		
<b>PRESUPUESTO TOTAL DEL PROYECTO</b>			77,040		

Fuente: (Dharma Consulting, 2022)

## Plan de Gestión de la Configuración

CONTROL DE VERSIONES					
Versión	Hecha por	Revisada por	Aprobada por	Fecha	Motivo
1.0	RM	CR	CR	17/02/2022	Versión Original

NOMBRE DEL PROYECTO	SIGLAS DEL PROYECTO
Aplicación móvil de gestión y atención de clientes	AMGC

ROLES DE LA GESTIÓN DE LA CONFIGURACIÓN: ROLES QUE SE NECESITAN PARA OPERAR LA GESTIÓN DE LA CONFIGURACIÓN.				
NOMBRE DEL ROL	PERSONA ASIGNADA	RESPONSABILIDADES	NIVELES DE AUTORIDAD	
Director de Proyecto	CC	Supervisar el funcionamiento de la Gestión de la Configuración.	Toda autoridad sobre el proyecto y sus funciones.	
Gestor de Configuración	LC	Ejecutar todas las tareas de Gestión de la Configuración.	Autoridad para operar las funciones de Gestión de la Configuración.	
Inspector de Aseguramiento de Calidad	DR	Auditar la Gestión de la Configuración.	Auditar la Gestión de la configuración según indique el Director de Proyecto.	
Miembros del Equipo de Proyecto	Varios	Consultar la información de Gestión de la Configuración según sus niveles de autoridad.	Depende de cada miembro, se especifica para cada artefacto y cada CI (Ítem de Configuración)	

## PLAN DE DOCUMENTACIÓN: CÓMO SE ALMACENARÁN Y RECUPERARÁN LOS DOCUMENTOS Y OTROS ARTEFACTOS DEL PROYECTO.

DOCUMENTOS O ARTEFACTOS	FORMATO (E=ELECTRÓNICO H=HARD COPY)	ACCESO RÁPIDO NECESARIO	DISPONIBILIDAD AMPLIA NECESARIA	SEGURIDAD DE ACCESO	RECUPERACIÓN DE INFORMACIÓN	RETENCIÓN DE INFORMACIÓN
Acta de Constitución del Proyecto	E	Disponible online	A todos los Interesados	Lectura general Modificación restringida	Backup primario y almacena miento secundario	Durante todo el proyecto
Plan de Proyecto	E	Disponible online	A todos los Interesados	Lectura general Modificación restringida	Backup primario y almacena miento secundario	Durante todo el proyecto

Informe de Performance del proyecto	E	Disponible on-line	A todos los Interesados	Lectura general Modificación restringida	Backup primario y almacenamiento secundario	Durante todo el proyecto
Solicitud de Cambio	E	Disponible on-line	A todos los Interesados	Lectura general Modificación restringida	Backup primario y almacenamiento secundario	Durante todo el proyecto
Log de Control de Solicitudes de Cambio	E	Disponible on-line	A todos los Interesados	Lectura general Modificación restringida	Backup primario y almacenamiento secundario	Durante todo el proyecto
Informe de Cierre de Proyecto	E	Disponible on-line	A todos los Interesados	Lectura general Modificación restringida	Backup primario y almacenamiento secundario	Durante todo el proyecto

**ÍTEMES DE CONFIGURACIÓN (CI):** OBJETOS DEL PROYECTO SOBRE LOS CUALES SE ESTABLECERÁN Y MANTENDRÁN DESCRIPCIONES DE LA LÍNEA BASE DE LOS ATRIBUTOS FUNCIONALES Y FÍSICOS, CON EL FIN DE MANTENER CONTROL DE LOS CAMBIOS QUE LOS AFECTAN.

CÓDIGO DEL ÍTEM DE CONFIGURACIÓN	NOMBRE DEL ÍTEM DE CONFIGURACIÓN	CATEGORÍA 1=FÍSICO 2=DOCUMENTO 3=FORMATO 4=REGISTRO	FUENTE P=PROYECTO C=CONTRATISTA V=PROVEEDOR E=EMPRESA	FORMATO (SOFTWARE + VERSIÓN + PLATAFORMA)	OBSERVACIONES
1.1 .	Documento completo con los requerimientos del aplicativo	2	P	ORIGINAL IMPRESO	Firmado
3.3	Manual técnico.	2	P	PDF	Firmado y aprobado
3.4	Manual de usuario.	2	P	PDF	Firmado y aprobado
4.2	Diseño y documentación de pruebas.	3	P	PDF	Firmado y aprobado
5.3	Informe de instalación.	3	P	PDF	Firmado y aprobado
6.1	Informe de resultados.	3	P	PDF	Firmado y aprobado

**GESTIÓN DEL CAMBIO:** ESPECIFICAR EL PROCESO DE GESTIÓN DEL CAMBIO O ANEXAR EL PLAN DE GESTIÓN DEL CAMBIO.

Ver Plan de Gestión del Cambio adjunto al Plan de Gestión del Proyecto.

**CONTABILIDAD DE ESTADO Y MÉTRICAS DE CONFIGURACIÓN:** ESPECIFICAR EL REPOSITORIO DE INFORMACIÓN, EL REPORTE DE ESTADO Y MÉTRICAS A USAR.

- El Repositorio de Información de los documentos del proyecto será una carpeta con la estructura del EDT para la organización interna de sus subcarpetas.
- El Repositorio de Información para los CI's (Configuration Items) será el Diccionario EDT que residirá en la carpeta antes mencionada.
- En cualquier momento se podrá mostrar una cabecera con la historia de versiones de los documentos y artefactos del proyecto, así como se podrá consultar todas las versiones de los CI's.
- No se llevarán métricas del movimiento y la historia de los documentos, artefactos, y CI's para este proyecto.

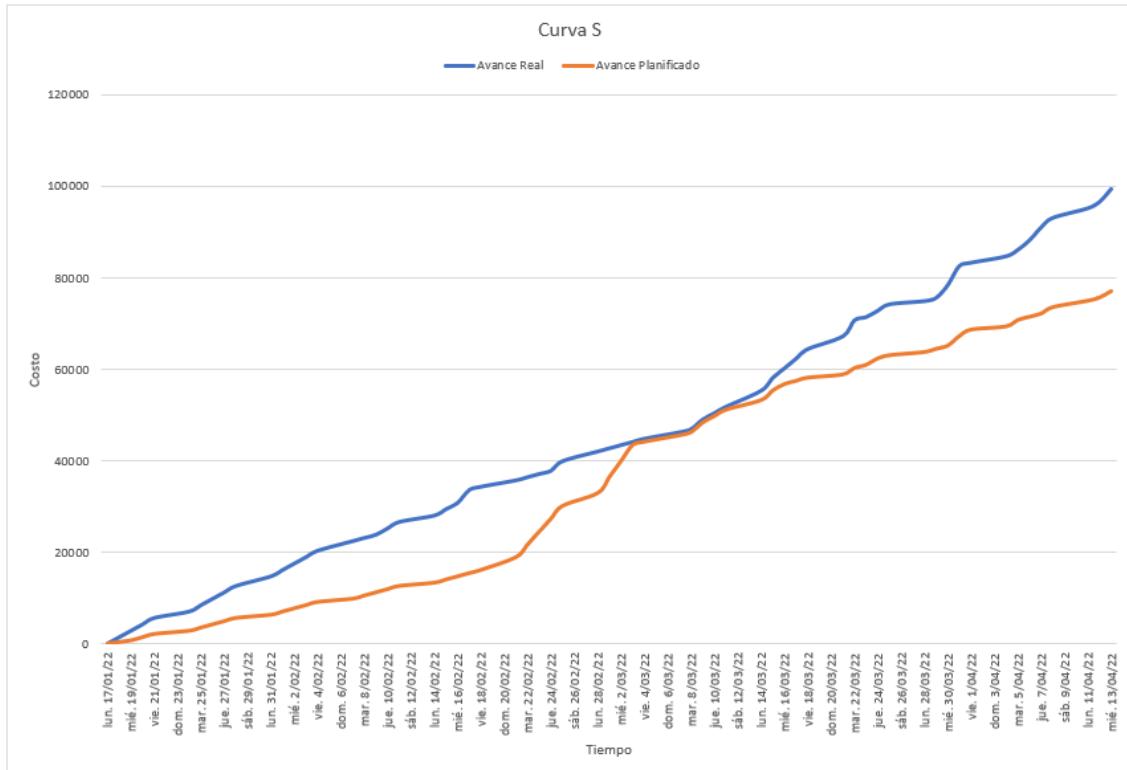
**VERIFICACIÓN Y AUDITORÍAS DE CONFIGURACIÓN:** ESPECIFICAR CÓMO SE ASEGURARÁ LA COMPOSICIÓN DE LOS ÍTEMES DE CONFIGURACIÓN, Y CÓMO SE ASEGURARÁ EL CORRECTO REGISTRO, EVALUACIÓN, APROBACIÓN, RASTREO E IMPLEMENTACIÓN EXITOSA DE LOS CAMBIOS A DICHOS ÍTEMES.

Las verificaciones y auditorías de la integridad de la configuración serán rutinarias y bisemanales, realizadas por el Inspector de Aseguramiento de Calidad, donde se comprobará:

- Integridad de la información de los CI's.
- Exactitud y reproducibilidad de la historia de los CI's

Fuente: (Dharma Consulting, 2022)

**Figura No. 6**



Fuente: Elaboración Propia

## Documentación de Requisitos del Proyecto

CONTROL DE VERSIONES					
Versión	Hecha por	Revisada por	Aprobada por	Fecha	Motivo
1.0	CD	CR	CR	18/02/2022	Dato inicial

NOMBRE DEL PROYECTO	SIGLAS DEL PROYECTO
Aplicación Móvil de Gestión y Atención de Clientes	AMGC

I. REQUISITOS DEL NEGOCIO: DESCRIBIR LAS NECESIDADES DE ALTO NIVEL DE LA ORGANIZACIÓN; TALES COMO OPORTUNIDADES DE NEGOCIO Y RAZONES POR LAS QUE SE HA EMPRENDIDO EL PROYECTO.			
CÓDIGO DEL REQUISITO	DESCRIPCIÓN DEL REQUISITO	FUENTE	PRIORIDAD
RE01	Debe contarse con un contrato que establezca la formalización del proyecto	Contacto	Muy Alto

RE02	La organización desea obtener la totalidad de beneficios al finalizar el proyecto	Entrevista	Alto
RE05	la organización debe obtener una carta indicando la finalización exitosa del proyecto	Entrevista	Alto
RE20	La organización debe obtener un documento con el fin de confirmar su conformidad con el servicio	Contacto	Muy alto
RE21	Debe entregarse un informe cada 15 días y un informe final (este último a modo de resumen total del proyecto)	Contacto	Muy alto

**II. REQUISITOS DE LOS INTERESADOS:** DESCRIBIR DETALLADAMENTE LAS NECESIDADES DE LOS INTERESADOS O GRUPO DE INTERESADOS.

CÓDIGO DEL REQUISITO	DESCRIPCIÓN DEL REQUISITO	FUENTE	PRIORIDAD
RE07	El personal administrativo que cuente con acceso a la información de los clientes no debe por ningún motivo hacer publica dicha información	Contacto	Muy Alto
RE09	Los participantes en el proceso de desarrollo deben hacer uso de las buenas prácticas incluidas tanto en los lineamientos de ITIL, COBIT y el PMBOK	Contacto	Alto
RE18	La organización debe recibir un informe semanal del avance del proyecto, haciendo para esto uso del sistema utilizado para la gestión del cronograma (Project) presentado en formato PDF	Contacto	Alto
RE22	Debe entregarse a la junta directiva un informe final que contenga un manual de procedimiento estándar de operación (SOP) de la herramienta en cuestión, diagramas principales y el algoritmo base del sistema, en un plazo no mayor de quince (15) días calendario	Contacto	Muy Alto
RE25	Debe entregarse a la gerencia del departamento de IT un acta que contenga la información recabada en las reuniones de cada "Sprint" con el fin de poder proveer la documentación de los incidentes en el proceso de desarrollo	Contacto	Alto

**III. REQUISITOS DE SOLUCIONES:** DESCRIBIR LAS FUNCIONES Y CARACTERÍSTICAS DEL PRODUCTO, SERVICIO O RESULTADO, QUE SATISFAGA LOS REQUERIMIENTOS DEL NEGOCIO Y DE LOS INTERESADOS.

**3.1 REQUISITOS FUNCIONALES:** DESCRIBIR EL FUNCIONAMIENTO DEL PRODUCTO. SE PUEDE INCLUIR ACCIONES, PROCESOS, DATOS E INTERACCIONES QUE EL PRODUCTO DEBE EJECUTAR.

CÓDIGO DEL REQUISITO	DESCRIPCIÓN DEL REQUISITO	FUENTE	PRIORIDAD
----------------------	---------------------------	--------	-----------

RE03	Debe proveerse a los departamentos involucrados en el uso de la herramienta un curso de uso básico de la misma	Contacto	Muy alto
RE11	Debe proveerse una capacitación básica visual (video) con fines educativos hacia el cliente o usuario final (personas que ingresaran la solicitud de gestión)	Contacto	Alto
RE12	Debe proveerse con un mínimo de un (1) mes de antelación los requerimientos mínimos de servidor para el despliegue de la aplicación	Contacto	Muy alto
RE15	La aplicación debe contar con una conexión a el sistema de inicio de sesión (SSO) único de la organización, con el fin de que tanto los empleados como los clientes puedan hacer uso del mismo usuario de autenticación	Contacto	Muy alto

**3.2 REQUISITOS No FUNCIONALES:** DESCRIBIR LAS CONDICIONES O CUALIDADES AMBIENTALES REQUERIDAS PARA QUE EL PRODUCTO SEA EFECTIVO. SE PUEDE INCLUIR NIVEL DE SERVICIO, CAPACIDAD DE SOPORTE, FIABILIDAD, SEGURIDAD, RENDIMIENTO, ETC.

CÓDIGO DEL REQUISITO	DESCRIPCIÓN DEL REQUISITO	FUENTE	PRIORIDAD
RE23	Los desarrolladores deben contar con los accesos al sistema de forma remota con el fin de poder reunir las condiciones óptimas de trabajo en caso de cambio de condiciones acorde a la pandemia y los requisitos de la salubridad	Contacto	Muy alto
RE04	El equipo del proyecto debe proveer el informe de sus avances acorde al cronograma establecido	Contacto	Muy alto
RE06	Los equipos deben recibir una transcripción de la capacitación del sistema	Contacto	Alto
RE08	Cada departamento debe recibir de forma independiente los procedimientos estándar de operación (SOP) del sistema	Contacto	Alto

**IV. REQUISITOS DE TRANSICIÓN Y PREPARACIÓN:** DESCRIBIR LAS CAPACIDADES TEMPORALES; TALES COMO LA CONVERSIÓN DE DATOS Y REQUISITOS DE ENTRENAMIENTO, NECESARIOS PARA LA TRANSICIÓN DEL ESTADO ACTUAL AL ESTADO FUTURO DESEADO.

CÓDIGO DEL REQUISITO	DESCRIPCIÓN DEL REQUISITO	FUENTE	PRIORIDAD

RE24	En el proceso de puesta en marcha de la aplicación el proceso de transición del sistema de entorno de calidad al entorno productivo no debe sobrepasar los treinta (30) días calendario	Contacto	Muy alto
RE10	El proceso de transición del entorno de pruebas al entorno de calidad deberá quedar documentado de forma adecuada, con el fin de poder efectuar un proceso de pruebas correcto.	Contacto	Muy alto

**V. REQUISITOS DEL PROYECTO:** DESCRIBIR LAS ACCIONES, PROCESOS U OTRAS CONDICIONES QUE SE NECESITAN PARA CUMPLIR EL PROYECTO. SE PUEDE INCLUIR FECHAS DE HITOS, OBLIGACIONES CONTRACTUALES, RESTRICCIONES, ETC.

CÓDIGO DEL REQUISITO	DESCRIPCIÓN DEL REQUISITO	FUENTE	PRIORIDAD
RE17	Los integrantes del equipo de proyecto deberán ser provistos de los equipos adecuados para ejecutar sus labores	Entrevista	Muy alto
RE13	Los integrantes del equipo de proyecto deberán ser provistos de las licencias correspondientes a sus asignaciones para ejecutar sus labores	Entrevista	Muy alto
RE19	La organización de ser satisfecha con un nivel mínimo del noventa por ciento (90%)	Entrevista	Muy alto
RE14	El equipo de desarrollo debe cumplir con el cien por ciento (100%) de las cláusulas del proyecto	Entrevista	Muy alto

**VI. REQUISITOS DE CALIDAD:** DESCRIBIR LAS CONDICIONES O CRITERIOS NECESARIOS PARA VALIDAR EL ÉXITO DEL PROYECTO ENTREGADO, O EL CUMPLIMIENTO DE OTROS REQUISITOS DEL PROYECTO. SE PUEDE INCLUIR PRUEBAS, CERTIFICACIONES, VALIDACIONES, ETC.

CÓDIGO DEL REQUISITO	DESCRIPCIÓN DEL REQUISITO	FUENTE	PRIORIDAD
RE16	El sistema implementado debe contar con una calificación mínima de 4.5 de 5.0 de satisfacción del cliente o usuario final, la cual será recopilada y medida a través de encuestas dentro de la sesión	Entrevista	Muy alto

Fuente: (Dharma Consulting, 2022)

## Plan de Gestión de Cambios

CONTROL DE VERSIONES					
Versión	Hecha por	Revisada por	Aprobada por	Fecha	Motivo
1.0	BA	CR	CR	17/02/22	Versión Original

NOMBRE DEL PROYECTO	SIGLAS DEL PROYECTO
---------------------	---------------------

<b>Aplicación móvil de gestión y atención de clientes</b>	<b>AMGC</b>
<b>ACTIVIDADES DE REQUISITOS:</b> DESCRIBIR CÓMO SE PLANIFICARÁN, MONITOREARÁN Y REPORTARÁN ESTAS ACTIVIDADES.	
<ul style="list-style-type: none"> <li>Los requisitos son sugeridos por los principales interesados del proyecto, durante el proceso de iniciación y planificación del proyecto.</li> <li>Los requisitos serán descritos en la Documentación de Requisitos.</li> </ul>	
<b>ACTIVIDADES DE GESTIÓN DE LA CONFIGURACIÓN:</b> DESCRIPCIÓN DE CÓMO SE INICIARÁN LAS ACTIVIDADES DE CAMBIOS AL PRODUCTO, SERVICIO O REQUERIMIENTO; CÓMO SE ANALIZARÁN LOS IMPACTOS; CÓMO SE RASTREARÁN, MONITOREARÁN, Y REPORTARÁN, Y CUÁLES SON LOS NIVELES DE AUTORIZACIÓN REQUERIDOS PARA APROBAR DICHOS CAMBIOS.	
<p>Para las actividades de cambio al producto, servicio o requerimiento se realizará lo siguiente:</p> <ul style="list-style-type: none"> <li>Cualquier Interesado puede presentar la Solicitud de Cambio, donde se detalla el porqué del cambio solicitado.</li> <li>El Comité de Control de Cambios evaluará el impacto en el proyecto (a nivel de costos, tiempos, alcance y principalmente el tipo) de las solicitudes de cambios presentadas, y dependiendo del análisis decidirán quién es el encargado de revisar el cambio o si debe de pasar por el Proceso General de Gestión de Cambios descrito en el Plan de Gestión de Cambios.</li> <li>Si el cambio ha sido aprobado, se implementará el cambio.</li> <li>Se hará un seguimiento del cambio, para ver los efectos positivos o negativos que tenga en el proyecto.</li> </ul>	
<b>PROCESO DE PRIORIZACIÓN DE REQUISITOS:</b> DESCRIBIR CÓMO SE PRIORIZARÁN LOS REQUISITOS.	
<p>La priorización de los requisitos se realizará en base a la Documentación de Requisitos, de acuerdo con el nivel de prioridad y el grado de complejidad de cada requisito documentado. Este proceso será realizado por el equipo de gestión del proyecto durante la planificación del proyecto, y será aprobado por el Director de Proyecto para luego presentarlo y aprobarlo por el Patrocinador.</p>	
<b>MÉTRICAS DEL PRODUCTO:</b> DESCRIBIR LAS MÉTRICAS QUE SE USARÁN Y SUSTENTAR PORQUÉ SE USARÁN.	
<p>El grado de satisfacción promedio en la encuesta final de los clientes respecto a la atención brindada debe ser como mínimo 4.5 de 5.0, caso contrario se realizará un seguimiento de los comentarios brindados para mejorar y tomar las acciones correctivas necesarias.</p>	
<b>ESTRUCTURA DE TRAZABILIDAD:</b> DESCRIBIR LOS ATRIBUTOS DE REQUISITOS QUE SE CAPTURARÁN EN LA MATRIZ DE TRAZABILIDAD Y ESPECIFICAR CONTRA QUE OTROS DOCUMENTOS DE REQUISITOS DEL PROYECTO SE HARÁ LA TRAZABILIDAD.	
<p>En la Matriz de Trazabilidad se documentará la siguiente información:</p> <ul style="list-style-type: none"> <li>Atributos de Requisitos, que incluye: código, descripción, sustento de inclusión, propietario, fuente, prioridad, versión, estado actual, fecha de cumplimiento, nivel de estabilidad, grado de complejidad y criterio de aceptación.</li> <li>Trazabilidad hacia: <ul style="list-style-type: none"> <li>Necesidades, oportunidades, metas y objetivos del negocio.</li> <li>Objetivos del proyecto.</li> <li>Alcance del proyecto, entregables de la EDT.</li> <li>Diseño del producto.</li> <li>Desarrollo del producto.</li> <li>Estrategia de prueba.</li> <li>Escenario de prueba.</li> <li>Requerimiento de alto nivel.</li> </ul> </li> </ul>	

Fuente: (Dharma Consulting, 2022)

## Plan de Gestión de la Calidad

CONTROL DE VERSIONES					
Versión	Hecha por	Revisada por	Aprobada por	Fecha	Motivo
1.0	RM	CR	CR	17/02/2022	Versión Original

NOMBRE DEL PROYECTO	SIGLAS DEL PROYECTO

<b>Aplicación móvil de gestión y atención de clientes</b>	<b>AMGC</b>
---	-------------

<b>ESTÁNDAR O NORMA DE CALIDAD APLICABLE</b>	
<b>PAQUETE DE TRABAJO</b>	<b>ESTÁNDAR O NORMA DE CALIDAD APLICABLE</b>
<b>1.0 Toma y Análisis de requerimientos</b>	METODO Y NORMA EXIGIDA POR <b>AMGC</b>
<b>2.0 Diseño de estructura e interfaces gráficas</b>	METODO Y NORMA EXIGIDA POR <b>AMGC</b>
<b>3.0 Desarrollo de la Aplicación</b>	METODO Y NORMA EXIGIDA POR <b>AMGC</b>
<b>4.0 Pruebas de aplicación</b>	METODO Y NORMA EXIGIDA POR <b>AMGC</b>
<b>5.0 Implementación y puesta en marcha</b>	METODO Y NORMA EXIGIDA POR <b>AMGC</b>
<b>6.0 Evaluación y verificación de resultados</b>	METODO Y NORMA EXIGIDA POR <b>AMGC</b>
<b>OBJETIVOS DE CALIDAD</b>	
El Performance del Proyecto obtenga un Índice de Desempeño del Costo Acumulado (CPI) mayor o igual a 0.95 para poder ir acorde al costo planificado del Proyecto.	
El Performance del Proyecto obtenga un Índice de Desempeño del Cronograma Acumulado (SPI) mayor o igual a 0.95 para poder ir acorde al cronograma planificado del Proyecto.	
La satisfacción del cliente en relación con el producto del proyecto sea un nivel mayor o igual 4.0 de un rango del (1 al 5) sobre la gestión del proyecto y producto final.	
<b>ROLES PARA LA GESTIÓN DE LA CALIDAD:</b> ESPECIFICAR LOS ROLES QUE SERÁN NECESARIOS EN EL EQUIPO DE PROYECTO PARA DESARROLLAR LOS ENTREGABLES Y ACTIVIDADES DE GESTIÓN DE LA CALIDAD.	
<b>ROL No 1 :</b>	<p><i>Objetivos del rol:</i> Responsable ejecutivo y final de la calidad del proyecto.</p> <p><i>Funciones del rol:</i> Revisar, aprobar, y tomar acciones correctivas para mejorar la calidad.</p> <p><i>Niveles de autoridad:</i> Aplicar a discreción los recursos de Dharma para el proyecto, renegociar contratos.</p> <p><i>Reporta a:</i> Alta Gerencia</p> <p><i>Supervisa a:</i> Director del Proyecto</p> <p><i>Requisitos de conocimientos:</i> Gestión de Proyectos y Gestión en General.</p> <p><i>Requisitos de habilidades:</i> Liderazgo, Comunicación, Negociación, Motivación, y Solución de Conflictos.</p> <p><i>Requisitos de experiencia:</i> Mas de 12 años de experiencia en acciones relacionadas al puesto.</p>
<b>ROL No 2 :</b>	<p><i>Objetivos del rol:</i> Gestionar operativamente la calidad.</p> <p><i>Funciones del rol:</i> Revisar estándares, revisar entregables, aceptar entregables o disponer su reproceso, deliberar para generar acciones correctivas, aplicar acciones correctivas.</p> <p><i>Niveles de autoridad:</i> Exigir cumplimiento de entregables al Equipo de Proyecto</p> <p><i>Reporta a:</i> Patrocinador del Proyecto</p> <p><i>Supervisa a:</i> Equipo del proyecto</p> <p><i>Requisitos de conocimientos:</i> Gestión de Proyectos.</p> <p><i>Requisitos de habilidades:</i> Liderazgo, Comunicación, Negociación, Motivación, y Solución de Conflictos.</p> <p><i>Requisitos de experiencia:</i> 3 años de experiencia en el cargo</p>
<b>ROL No 3 :</b>	<p><i>Objetivos del rol:</i> Elaborar los entregables con la calidad requerida y según estándares.</p> <p><i>Funciones:</i> Elaborar los entregables. <i>del rol</i></p> <p><i>Niveles de autoridad:</i> Aplicar los recursos que se le han asignado</p> <p><i>Reporta a:</i> Director del Proyecto</p>

	<i>Supervisa a:</i> Ninguno
	<i>Requisitos de conocimientos:</i> Gestión de Proyectos y las especialidades que le tocan según sus entregables asignados.
	<i>Requisitos de habilidades:</i> Específicas según los entregables
	<i>Requisitos de experiencia:</i> Específicas según los entregables

<b>REVISIONES DE CALIDAD</b>	
<b>ENTREGABLES/ PROCESOS</b>	<b>REVISIONES DE CALIDAD</b>
<b>1.0 Toma y Análisis de requerimientos</b>	Revisión Estándar
<b>2.0 Diseño de estructura e interfaces gráficas</b>	Revisión y diseño según Iso 9001
<b>3.0 Desarrollo de la Aplicación</b>	Revisión y diseño según Iso 9001
<b>4.0 Pruebas de aplicación</b>	Revisión Estándar
<b>5.0 Implementación y puesta en marcha</b>	Revisión Estándar
<b>6.0 Evaluación y verificación de resultados</b>	Revisión de modelos de formatos
<b>ACTIVIDADES DE CONTROL Y GESTIÓN DE LA CALIDAD</b>	
<b>ACTIVIDADES DE CONTROL DE LA CALIDAD</b>	El Control de Calidad se ejecutará revisando los entregables para ver si están conformes o no.
	Los resultados de estas mediciones se consolidarán y se enviarán al proceso de Gestionar la calidad.
	Asimismo, en este proceso se hará la medición de las métricas y se informará al proceso de Gestionar la Calidad.
	Los entregables que han sido reprocesados se volverán a revisar para verificar si ya se han vuelto conformes.
<b>ACTIVIDADES DE GESTIÓN DE LA CALIDAD</b>	Gestionar la Calidad se realizará monitoreando continuamente la performance del trabajo, los resultados del control de calidad, y sobre todo las métricas.
	De esta manera se descubrirá tempranamente cualquier necesidad de auditoría de procesos, o de mejora de procesos.
	Los resultados se formalizarán como solicitudes de cambio y/o acciones correctivas/preventivas.
	Asimismo, se verificará que dichas solicitudes de cambio, y/o acciones correctivas/preventivas se hayan ejecutado y hayan sido efectivas
<b>HERRAMIENTAS DE CALIDAD</b>	
Las hojas de verificación: Organiza los hechos de manera que se facilite la recopilación de un conjunto de datos útiles sobre un posible problema de calidad.	
Los diagramas de Pareto: Identificar las pocas fuentes clave responsables de la mayor parte de los efectos de los problemas	
<b>PROCEDIMIENTOS RELEVANTES DE LA CALIDAD</b>	
1 .Para Mejora de Procesos. 2. Para Auditorías de Procesos. 3. Para Reuniones de Aseguramiento de Calidad. 4. Para Resolución de Problemas.	

Fuente: (Dharma Consulting, 2022)

## Plan de Gestión de los Recursos

CONTROL DE VERSIONES												
Versión	Hecha por	Revisada por	Aprobada por	Fecha	Motivo							
1.0	CD	CR	CR	18/02/22	Versión original							
NOMBRE DEL PROYECTO			SIGLAS DEL PROYECTO									
<b>Aplicación Móvil de Gestión y Atención de Clientes</b>			<b>AMGC</b>									
<b>IDENTIFICACIÓN DE LOS RECURSOS:</b> MÉTODOS PARA IDENTIFICAR Y CUANTIFICAR EL EQUIPO Y LOS RECURSOS FÍSICOS NECESARIOS.												
RECURSOS		CANTIDAD										
Patrocinador		1										
Director de Proyecto / Gerente de proyectos		1										
Director IT		1										
Jefe de equipo desarrollo de software y equipo		12										
Jefe de análisis y testing		4										
Encargado de base de datos y equipo		3										
Analista de seguridad y equipo		4										
Auxiliar de testing		1										
Auxiliar Administrativo		1										
Nota: Adjuntar Cuadro de Adquisiciones de Recursos del Proyecto.												
<b>ADQUISICIÓN DE RECURSOS:</b> Guías sobre el modo en que se debe adquirir el equipo y los recursos físicos del proyecto.												
Auxiliar Administrativo												
Nota: Adjuntar Cuadro de Adquisiciones de Recursos del Proyecto.												
<b>ROLES Y RESPONSABILIDADES:</b> NOMBRE DEL ROL, NIVELES DE AUTORIDAD, RESPONSABILIDAD Y COMPETENCIA.												
Ver Descripción de Roles – versión 1.0												
Nota: Adjuntar Descripción de Roles.												
<b>ORGANIGRAMA DEL PROYECTO:</b> ESPECIFICAR EL ORGANIGRAMA DEL PROYECTO.												
Ver Organigrama del Proyecto – versión 1.0												
Nota: Adjuntar Organigrama del Proyecto.												
<b>GESTIÓN DE LOS RECURSOS DEL EQUIPO DE PROYECTO:</b> ¿CÓMO DEFINIR, PROVEER PERSONAL, ADMINISTRAR Y EVENTUALMENTE LIBERAR LOS RECURSOS DEL EQUIPO DE PROYECTO?												
En base a los siguientes documentos:												
<ul style="list-style-type: none"> <li>• Acta de Constitución</li> <li>• Plan para la Dirección del Proyecto</li> <li>• Documentos del Proyecto</li> </ul>												
Se obtiene toda la información necesaria para la Gestión de Recursos de proyecto:												
<ul style="list-style-type: none"> <li>• Plan de Gestión de los Recursos</li> <li>• Acta de Constitución del Equipo</li> <li>• Actualización de los Documentos del Proyecto</li> </ul>												

**CAPACITACIÓN:** ESTRATEGIAS DE CAPACITACIÓN PARA LOS MIEMBROS DEL EQUIPO.

Siempre se deben aprovechar los cursos de la empresa y la oportunidad de agregar a los miembros con poca experiencia a que hagan equipo con los más experimentados para que se vayan preparando y tener más personal experimentado para que la empresa posea de líderes mejor preparados, por lo cual es bueno para la empresa implementar cierta cantidad de horas para el crecimiento de su personal.

Siempre sé que se dé la oportunidad en un proyecto con varios directores muy experimentados es conveniente que se haga mentoring, es decir, que pueda ayudar a un empleado a poder ser mejor enseñándole lo que no se pueda estudiar en los libros y que sea de su propia experiencia para preparar a futuras generaciones.

**DESARROLLO DEL EQUIPO:** MÉTODOS PARA DESARROLLAR EL EQUIPO.

Los métodos por implementar para obtener un mejor desarrollo del equipo son:

- Desarrollar habilidades interpersonales y de equipo
- Desarrollar habilidades analíticas
- Análisis sobre estructuración de equipo.
- Programación de capacitaciones
- Realizar evaluaciones de desempeño del equipo.

**CONTROL DE RECURSOS:** LOS MÉTODOS PARA ASEGURAR QUE LOS RECURSOS FÍSICOS ADECUADOS ESTÉN DISPONIBLES CUANDO SEAN NECESARIOS Y QUE LA ADQUISICIÓN DE RECURSOS FÍSICOS SEA OPTIMIZADA PARA LAS NECESIDADES DEL PROYECTO. INCLUIR INFORMACIÓN SOBRE LA GESTIÓN DE INVENTARIO, EQUIPOS Y SUMINISTROS.

Los métodos para garantizar el uso a tiempo de dispositivos físicos y toda herramienta física que sea necesaria para el proyecto son las siguientes:

- Desarrollo de plan enfocado a solución de posibles problemas
- Datos recurrentes de desempeño en los procesos
- Uso de datos para análisis de actividades dentro de la información de la dirección del proyecto.
- Desarrollar habilidades sociales, de equipo e interpersonales.

**PLAN DE RECONOCIMIENTO:** ¿QUÉ RECONOCIMIENTO Y RECOMPENSA SE DARÁ A LOS MIEMBROS DEL EQUIPO?

Los jefes tienen un sistema para reconocimiento de habilidades y desarrollo interpersonal y colaborativo dentro de la empresa para garantizar un buen ambiente laboral y desarrollo de habilidades, la compensación se basa en lo siguiente:

- Puntualidad 20%
- Desempeño 30%
- Aumento de habilidades prácticas (20 horas-año)15%
- Aumento de habilidades (soft 10 horas-año)15%
- Colaboración entre equipo (12 horas - año)20%

La suma de estos datos representa en un bono del salario actual de entre 60% al 150%.

Fuente: (Dharma Consulting, 2022)

## Plan de Gestión de las Comunicaciones

CONTROL DE VERSIONES					
Versión	Hecha por	Revisada por	Aprobada por	Fecha	Motivo
1.0	WO	CR	CR	24/02/2022	PLAN DE GESTIÓN DE LAS COMUNICACIONES

NOMBRE DEL PROYECTO	SIGLAS DEL PROYECTO
Aplicación Móvil de Gestión y Atención de Clientes	AMGC

REQUISITOS DE COMUNICACIÓN DE INTERESADOS	INFORMACIÓN A SER COMUNICADA	RAZONES DE LA DISTRIBUCIÓN	PROGRAMA / FRECUENCIA	RESPONSABLE DE COMUNICAR	RESPONSABLE DE APROBAR	PERSONAS /GRUPOS RECEPTORES	MÉTODOS O TECNOLOGÍAS DE COMUNICACIÓN
Actualización de proyecto	Actualización de Proyecto	Informar las actualizaciones	Quincenal	Director de Proyecto	Director de Proyecto	Equipo de proyecto	Oficios
Avances de Proyecto	Avances de proyecto	Informar los avances	Semanal	Jefe de equipo de desarrollo	Director de proyecto	Equipo de proyecto	Correos electrónicos
Alcance de Cambios	Alcance de cambios	Comunicar los cambios	Cuando se requiera	Director de Proyecto	Director de Proyecto	Equipo de proyecto	Cartas
Emergencias	Emergencias en el proyecto	Emergencias	Cuando se requiera	Director de Proyecto	Director de Proyecto	Equipo de Proyecto	Reuniones Meet

**RECURSOS ASIGNADOS:** MENCIONA LOS RECURSOS ASIGNADOS PARA LAS ACTIVIDADES DE COMUNICACIÓN, INCLUIDOS EL TIEMPO Y EL PRESUPUESTO.

Patrocinador
Director de Proyecto / Gerente de Proyectos
Director IT
Jefe de desarrollo

MÉTODO PARA ACTUALIZAR Y REFINAR EL PLAN DE GESTIÓN DE LAS COMUNICACIONES:	DEFINA EL MÉTODO PARA ACTUALIZAR Y REFINAR EL PLAN DE GESTIÓN DE LAS COMUNICACIONES A MEDIDA QUE EL PROYECTO AVANZA Y SE DESARROLLA.
Oficios	
Correos electrónicos	
Cartas	

Reuniones Meet
<b>GLOSARIO DE TERMINOLOGÍA COMÚN:</b> GLOSARIO DE TÉRMINOS, NOMBRES, CONCEPTOS, FÓRMULAS, ETC.
Actualización: Alude a lograr que algo se vuelva actual, es decir conseguir que algo este al día.
Avances: Hace referencia al acto y resultado de avanzar.
<b>DIAGRAMAS DE FLUJO DE LA INFORMACIÓN:</b> DIAGRAMAS DE FLUJO DE LA INFORMACIÓN QUE CIRCULA DENTRO DEL PROYECTO, LOS FLUJOS DE TRABAJO CON LA POSIBLE SUCESIÓN DE AUTORIZACIONES, LA LISTA DE INFORMES Y LOS PLANES DE REUNIONES, ETC.
UML
De objetos
<b>RESTRICCIONES:</b> RESTRICCIONES DERIVADAS DE UNA LEGISLACIÓN O NORMATIVA ESPECÍFICA DE LA TECNOLOGÍA, DE LAS POLÍTICAS DE LA ORGANIZACIÓN, ETC.
Reuniones meet no más de dos a la semana a menos que sea de fuerza mayor.

Fuente: (Dharma Consulting, 2022)

## Identificación y Evaluación Cualitativa de Riesgos

CONTROL DE VERSIONES					
Versión	Hecha por	Revisada por	Aprobada por	Fecha	Motivo
1.0	RM	CR	CR	26/02/2022	Versión Original

NOMBRE DEL PROYECTO	SIGLAS DEL PROYECTO
Aplicación móvil de Gestión y Atención de Clientes	AMGC

PROBABILIDAD	VALOR NUMÉRICO	IMPACTO	VALOR NUMÉRICO
Muy Improbable	0.1	Muy Bajo	0.05
Relativamente Probable	0.3	Bajo	0.10
Probable	0.5	Moderado	0.20
Muy Probable	0.7	Alto	0.40
Casi Certeza	0.9	Muy Alto	0.80

TIPO DE RIESGO	PROBABILIDAD X IMPACTO
Muy Alto	Mayor a 0.50
Alto	Menor a 0.50
Moderado	Menor a 0.30
Bajo	Menor a 0.10
Muy Bajo	Menor a 0.05

CÓDIGO DEL RIESGO	DESCRIPCIÓN DEL RIESGO	CAUSA RAÍZ	TRIGGER	ENTREGABLES AFECTADOS	ESTIMACIÓN DE PROBABILIDAD	OBJETIVO AFECTADO	ESTIMACIÓN DE IMPACTO	PROB X IMPACTO	TIPO DE RIESGO
R001	Debido a una insuficiente definición de alcance y/o identificación de los interesados, podría suceder que se generen nuevos requisitos lo cual ocasionaría cambios en el cronograma, mayores costos, y/o una baja calidad del servicio	Inadecuada comunicación con la alta gerencia vulnerando la definición de alcance y/o identificación de los interesados.		<b>Todo el Proyecto</b>	0.1	Alcance	0.10	0.01	Muy Bajo
						Cronograma	0.10	0.01	
						Costo	0.10	0.01	
						Calidad	0.10	0.01	
						<b>TOTAL PROBABILIDAD X IMPACTO</b>		<b>0.04</b>	
R002	Debido a procesos inadecuados de aseguramiento y control de calidad, se podría generar deficiencias en el material lo cual ocasionaría una baja calidad del servicio.	Procesos inadecuados de aseguramiento y control de calidad.		<b>1.0 Toma y Análisis de requerimientos 2.0 Diseño de estructura e interfaces gráficas 3.0 Desarrollo de la Aplicación 4.0 Pruebas de aplicación</b>	0.1	Alcance	0.20	0.02	Bajo
						Cronograma	0.20	0.02	
						Costo	0.20	0.02	
						Calidad	0.10	0.001	
						<b>TOTAL PROBABILIDAD X IMPACTO</b>		<b>0.06</b>	
R003	Pérdida económica por daño en los equipos de cómputo que se usan el equipo de TI	Equipos que no funcionan adecuadamente por algún motivo natural o no	Equipos no funcionan adecuadamente o no funcionan	<b>3.0 Desarrollo de la Aplicación 4.0 Pruebas de aplicación</b>	0.5	Alcance			Moderado
						Cronograma	0.20	0.1	
						Costo	0.20	0.1	
						Calidad	0.20	0.1	
						<b>TOTAL PROBABILIDAD X IMPACTO</b>		<b>0.30</b>	
R004	Problemas de adaptación a los cambios regulatorios y normativos de la empresa por parte de los usuarios.	Problemas de adaptabilidad con los usuarios, que utilizan la aplicación	Pérdida en la cartera de usuarios	<b>Todo el Proyecto</b>	0.5	Alcance	0.20	<b>0.1</b>	Alto
						Cronograma	0.20	0.1	
						Costo	0.20	0.1	
						Calidad	0.20	0.1	
						<b>TOTAL PROBABILIDAD X IMPACTO</b>		<b>0.40</b>	
R005	Equipo de cómputo desactualizado	Mala gestión del equipo, configuraciones, seguridad.	Propenso a virus y malwares	<b>Todo el Proyecto</b>	0.5	Alcance	0.20	0.1	Muy Alto
						Cronograma	0.40	0.2	
						Costo	0.40	0.2	
						Calidad	0.20	0.1	
						<b>TOTAL PROBABILIDAD X IMPACTO</b>		<b>0.60</b>	

Fuente: (Dharma Consulting, 2022)

## Plan de Respuesta a los Riesgos

CONTROL DE VERSIONES					
Versión	Hecha por	Revisada por	Aprobada por	Fecha	Motivo
1.0	BA	CR	CR	28/02/22	Versión Original

NOMBRE DEL PROYECTO	SIGLAS DEL PROYECTO
Aplicación Móvil de Gestión y Atención de Clientes	AMGC

CÓDIGO DEL RIESGO	AMENAZA / OPORTUNIDAD	DESCRIPCIÓN DEL RIESGO	CAUSA RAÍZ	TRIGGER	ENTREGABLES AFECTADOS	PROBABILIDAD POR IMPACTO TOTAL	TIPO DE RIESGO	RESPONSABLE DEL RIESGO	RESPUESTAS PLANIFICADAS	TIPO DE RESPUESTA	RESPONSABLE DE LA RESPUESTA	FECHA PLANIFICADA	PLAN DE CONTINGENCIA	
R005	Amenaza	Equipo de cómputo desactualizado	Mala gestión del equipo, configuraciones, seguridad.	Propenso a virus y malwares	Todo el Proyecto	0.60	Muy Alto	CD	1. Revisar y analizar las actualizaciones posibles a realizar.	Mitigar	CD	Una vez al mes	Registrar problema, equipo y posible solución.	
									2. Analizar los equipos posibles a actualizar	Mitigar	CD	Una vez al mes		
									3. Instalar actualizaciones	Mitigar	CD	Una vez al mes		
R004	Amenaza	Problemas de adaptación a los cambios regulatorios y normativos de la empresa por parte de los usuarios.	Problemas de adaptabilidad con los usuarios, que utilizan la aplicación	Pérdida en la cartera de usuarios	Todo el Proyecto	0.40	Alto	CD	1. Analizar las encuestas de satisfacción de los usuarios.	Mitigar	CD	Al notar una caída en los usuarios activos	Establecer un equipo que pruebe la aplicación cada cierto tiempo y reporten posibles mejores.	
									2. Analizar los cambios propuestas y el impacto que conlleva.	Mitigar	CD	Al notar una caída en los usuarios activos		

R003	Amenaza	Pérdida económica por daño en los equipos de cómputo que se usan el equipo de TI	Equipos que no funcionan adecuadamente por algún motivo natural o no	Equipos no funcionan adecuadamente o no funcionan	3.0 Desarrollo de la Aplicación 4.0 Pruebas de aplicación	0.30	Moderado	CD	1. Tener un inventario de equipos con fecha de compra y registros de mantenimientos.  2. Analizar equipos y concluir en una solución para mejorar	Mitigar	CD	Al adquirir nuevos equipos o dar mantenimiento.	Tener un equipo encargado de realizar pruebas a los equipos cada cierto tiempo para medir su rendimiento.
R002	Amenaza	Debido a procesos inadecuados de aseguramiento y control de calidad, se podría generar deficiencias en el material lo cual ocasionaría una baja calidad del servicio.	Procesos inadecuados de aseguramiento y control de calidad.		1.0 Toma y Análisis de requerimientos 2.0 Diseño de estructura e interfaces gráficas 3.0 Desarrollo de la Aplicación 4.0 Pruebas de aplicación	0.06	Bajo	CD	1. Se debe aplicar la metodología de la empresa para la inspección de los materiales.	Mitigar	CD	En el control de calidad de materiales.	Evaluación del impacto. Revisar y corregir dichos materiales y los próximos a utilizar en las demás secciones.
									2. Realizar inspección cruzada al material.	Mitigar	CD	En el control de calidad de materiales.	
R001	Amenaza	Debido a una insuficiente definición de alcance y/o identificación de los interesados, podría suceder que se generen nuevos requisitos lo cual ocasionaría cambios en el cronograma, mayores costos, y/o una baja calidad del servicio	Inadecuada comunicación con la alta gerencia vulnerando la definición de alcance y/o identificación de los interesados.		Todo el Proyecto	0.04	Muy Bajo	DO/CD	1. Coordinación continua con representantes del cliente	Mitigar	DO	Acción Continua	Analizar causa y realizar acciones correctivas de acuerdo con los nuevos requisitos.
									2. Cláusula de flexibilidad en el contrato con el cliente.	Mitigar	CD	En la firma del contrato	

Fuente: (Dharma Consulting, 2022)

## Enunciado del Trabajo Relativo a Adquisiciones (SOW)

CONTROL DE VERSIONES					
Versión	Hecha por	Revisada por	Aprobada por	Fecha	Motivo
1.0	CD	CR	CR	24/02/2022	Versión inicial

NOMBRE DEL PROYECTO	SIGLAS DEL PROYECTO
<b>Aplicación Móvil de Gestión y Atención de Clientes</b>	<b>AMGC</b>

DESCRIPCIÓN GENERAL DEL PRODUCTO/SERVICIO A ADQUIRIR
<b>ANTECEDENTES:</b> DESCRIBIR BREVEMENTE LA NECESIDAD A SATISFACER, LA LÍNEA DE TIEMPO DE LA NECESIDAD DEL PRODUCTO/SERVICIO, LAS PERSONAS CLAVES QUE PARTICIPAN EN LA ADQUISICIÓN DEL PRODUCTO/SERVICIO, SOLUCIONES ALTERNATIVAS Y ENFOQUE PROUESTO.
PilloPhone desea actualizar su modelo de gestión de incidencias y atención al cliente con la implementación de una nueva aplicación móvil que se encuentre disponible tanto para clientes externos como para clientes internos.  La aplicación contara con las siguientes características: <ul style="list-style-type: none"><li>• Interfaz simple, la interfaz debe ser intuitiva y fácil de utilizar para los clientes externos.</li><li>• Integración de departamento de soporte, el departamento de soporte debe contar con acceso a un sistema que permita monitorear, dar seguimiento y proveer soporte a los clientes externos.</li></ul>
La persona clave para llevar a cavo algún seguimiento con relación a la aplicación es:  Cristian del Cid → Gerente de proyecto  En caso de no contar con infraestructura disponible en la organización para poder ejecutar la puesta en producción del aplicativo para la fecha estimada de terminación se realizará un levantado de la aplicación en un servidor Azure dentro del entorno de producción de la organización, el cual ejecutará los servicios necesarios hasta el momento en que se encuentre disponible la infraestructura física o que se indique la continuidad en el modelo del aplicativo de parte de la organización.
<b>PROPÓSITO/OBJETIVOS:</b> DESCRIBIR EL PROPÓSITO/OBJETIVO QUE LA ORGANIZACIÓN ESPERA CONSEGUIR CON EL PRODUCTO/SERVICIO.
Se tiene como objetivo mejorar el ambiente en el cual tanto los clientes como los operarios de mantenimiento y atención al cliente manejan los incidentes.
<b>BENEFICIOS PREVISTOS:</b> DESCRIBIR BREVEMENTE LO QUE EL PROYECTO PUEDE OBTENER A TRAVÉS DE LA ADQUISICIÓN DEL PRODUCTO/SERVICIO.
Cumplir con los tiempos estándares de soporte a los clientes y realizar un mejor monitoreo de los incidentes en la cola de atención, logrando de esta forma mejorar el prestigio de la organización.
<b>SOFTWARE O TECNOLOGÍA DE PRODUCTOS PROPUESTOS:</b> DESCRIBIR BREVEMENTE CUALQUIER SOFTWARE O TECNOLOGÍA NUEVA QUE SE IMPLEMENTARÁ COMO PARTE DEL PRODUCTO/SERVICIO.

- El servidor propuesto debe contar con al menos
- RAM: 16 GB
  - Procesador: 8 núcleos (Intel Core i7-11700K)
  - Sistema operativo Linux
  - Espacio el disco: 2TB

**PROCESOS DEL NEGOCIO AFECTADOS:** DESCRIBIR BREVEMENTE CAMBIOS IMPORTANTES EN LA MANERA DE HACER NEGOCIOS CUANDO SE ADQUIERA EL PRODUCTO/SERVICIO.

No hay cambios

**INTERESADOS/USUARIOS FINALES AFECTADOS:** IDENTIFICAR LAS PERSONAS O GRUPOS CUYO TRABAJO SE VERÁ AFECTADO DURANTE Y DESPUÉS DE LA ADQUISICIÓN DEL PRODUCTO/SERVICIO.

En caso de no contar con las especificaciones indicadas en el documento se verán afectados:

- Empleados del departamento de soporte
- Empleados del departamento de atención al cliente
- Usuarios finales (Clientes)

**ALCANCE DETALLADO:** DEFINIR UNA LISTA DETALLADA DE LOS REQUISITOS ESPECÍFICOS QUE EL PRODUCTO/SERVICIO DEBE SATISFACER. TAMBIÉN SE DEBE DEFINIR UNA LISTA DE LOS ENTREGABLES QUE SE GENERARÁN, ASÍ COMO TAMBIÉN LOS ENTREGABLES QUE SE EXCLUYEN DEL ALCANCE.

**REQUISITOS:** LISTAR LOS REQUISITOS FUNCIONALES Y NO FUNCIONALES.

- Debe proveerse a los departamentos involucrados en el uso de la herramienta un curso de uso básico de la misma
- Debe proveerse una capacitación básica visual (video) con fines educativos hacia el cliente o usuario final (personas que ingresaran la solicitud de gestión)
- Debe proveerse con un mínimo de un (1) mes de antelación los requerimientos mínimos de servidor para el despliegue de la aplicación
- La aplicación debe contar con una conexión a el sistema de inicio de sesión (SSO) único de la organización, con el fin de que tanto los empleados como los clientes puedan hacer uso del mismo usuario de autenticación
- Los desarrolladores deben contar con los accesos al sistema de forma remota con el fin de poder reunir las condiciones óptimas de trabajo en caso de cambio de condiciones acorde a la pandemia y los requisitos de la salubridad
- El equipo del proyecto debe proveer el informe de sus avances acorde al cronograma establecido
- Los equipos deben recibir una transcripción de la capacitación del sistema
- Cada departamento debe recibir de forma independiente los procedimientos estándar de operación (SOP) del sistema

**ENTREGABLES INCLUIDOS EN EL ALCANCE:** LISTAR LOS ENTREGABLES INCLUIDOS DENTRO DEL ALCANCE DE ESTA ADQUISICIÓN, Y DESCRIBIR BREVEMENTE LAS PRINCIPALES FUNCIONALIDADES Y ATRIBUTOS DEL ENTREGABLE.

ENTREGABLE	DESCRIPCIÓN DEL ENTREGABLE
Computadoras	El equipo de desarrollo deberá contar con equipos adecuados para poder proceder con el desarrollo, estos deben incluir los sistemas y/o programas necesarios para completar el desarrollo.
Sillas	Debe proveerse a cada uno de los integrantes del equipo una silla tipo oficina.
Pizarra	Con el fin de poder ejecutar el proceso bajo la metodología de gestión de proyectos Scrum, se requiere una pizarra para poder llevar a cabo el tablero correspondiente al apartado Kanban.
Tomacorrientes	el número de tomacorrientes necesarios para que todos los equipos electrónicos y sus componentes puedan ser conectados a la energía eléctrica.

Escritorios	Con el fin de poder guardar la sana distancia y debido a las instrucciones giradas de parte del ministerio de salud publica y asistencia social se requiere un escritorio de 150 x 90 centímetros para cada uno de los colaboradores del equipo.
-------------	--

**ENTREGABLES NO INCLUIDOS EN EL ALCANCE:** LISTAR LOS ENTREGABLES QUE HAN SIDO ESPECÍFICAMENTE EXCLUIDOS DEL ALCANCE DE ESTA ADQUISICIÓN Y DESCRIBIR BREVEMENTE ESTOS ENTREGABLES.

ENTREGABLE	DESCRIPCIÓN DEL ENTREGABLE
Provisiones para receso	Refrigerio, gaseosas y bebidas energizantes quedarán bajo la responsabilidad de cada uno de los colaboradores, con excepción del agua pura.

**CRONOGRAMA:** LISTAR TODOS LOS HITOS Y PRINCIPALES ENTREGABLES INDICANDO LA FECHA DE FINALIZACIÓN PREVISTA PARA CADA UNO DE ELLOS.

HITOS Y PRINCIPALES ENTREGABLES	FECHA DE FINALIZACIÓN PREVISTA
Toma y análisis de requerimientos	31 enero 2022
Diseño de estructura e interfaz grafica	15 febrero 2022
Desarrollo de la aplicación	11 marzo 2022
Pruebas de aplicación	3 marzo 2022
Implementación y puesta en marcha	11 marzo 2022
Evaluación y verificación de resultados	25 marzo 2022

**PRESUPUESTO:** REGISTRAR LAS UNIDADES Y LOS COSTOS ESTIMADOS.

	UNIDADES	COSTOS
TRABAJO TEMPORAL	96 horas	\$2000.00
TRABAJO CONTRATADO	384 horas	\$6500.00
COSTOS NO LABORALES	1 equipo	\$2500.00
<b>TOTAL</b>		<b>\$11,000.00</b>

**LUGAR DE EJECUCIÓN:** DESCRIBIR EL LUGAR DONDE EL TRABAJO SERÁ REALIZADO POR EL PROVEEDOR. EN ALGUNOS CASOS, EL PROVEEDOR PUEDE REALIZAR LA TOTALIDAD O PARTE DE SU TRABAJO EN LA UBICACIÓN DEL CLIENTE. ESTO POR LO GENERAL DEPENDE DEL TIPO DE INDUSTRIA O TRABAJO QUE SE REALIZA. ES IMPORTANTE DEFINIR ESTO EN CASO DE QUE EL CLIENTE REQUIERA QUE EL PROVEEDOR TRABAJE EN SUS INSTALACIONES Y PARA DEFINIR CUALQUIER EQUIPO Y/O ESPACIO DE TRABAJO QUE SERÁ NECESARIO PROPORCIONAR.

- Esto dependerá de el modelo de trabajo implementado ya que puede contar una variación entre: presencial, remoto o híbrido.

**ACTIVIDADES DE TRABAJO:** DESCRIBIR LAS TAREAS QUE LA ELABORACIÓN DEL PRODUCTO/SERVICIO REQUERIRÁ. ESTO DEBE INCLUIR LAS TAREAS QUE NECESITEN COMPLETARSE PARA LA FINALIZACIÓN CON ÉXITO DEL PRODUCTO/SERVICIO, Y EL ORDEN EN QUE DEBERÁN REALIZARSE.

- Verificar que los equipos cuenten tanto con las especificaciones requeridas como con los sistemas necesarios para ejecutar el proceso de desarrollo con normalidad.

**CRITERIOS DE ACEPTACIÓN:** DESCRIBIR LA FORMA EN QUE SE ACEPTARÁ EL PRODUCTO/SERVICIO. LA ACEPTACIÓN DE LOS ENTREGABLES DEBE ESTAR CLARAMENTE DEFINIDA Y COMPRENDIDA POR TODAS LAS PARTES. SE DEBE INCLUIR TAMBIÉN CUÁNDO Y CÓMO LAS PARTES INVOLUCRADAS SABRÁN QUE EL TRABAJO ES ACEPTADO, Y QUIÉN ESTÁ AUTORIZADO A ACEPTAR EL TRABAJO.

**DESCRIPCIÓN DE QUÉ ENTREGABLES ESTÁN SUJETOS A APROBACIÓN:**

- Computadoras
- Sillas
- Escritorios
- Tomas de corriente
- Pizarra

**PERSONA AUTORIZADA A ACEPTAR EL TRABAJO:**

- Cristian del Cid

**DESCRIPCIÓN DE CÓMO EL TRABAJO SERÁ ACEPTADO:**

- Los entregables deben satisfacer los requisitos descritos anteriormente.

**DESCRIPCIÓN DE CUÁNDO EL TRABAJO SERÁ ACEPTADO:**

- El producto final será aceptado en la oficina asignada al equipo de desarrollo

**DESCRIPCIÓN DE DÓNDE EL TRABAJO SERÁ ACEPTADO:**

- Los equipos serán revisadas contra las especificaciones a más tardar una semana antes del inicio del desarrollo.

**OTROS REQUISITOS:** DESCRIBIR OTROS REQUISITOS ESPECIALES, TALES COMO LOS REQUISITOS DE SEGURIDAD (PERSONAL CON AUTORIZACIÓN DE SEGURIDAD Y QUÉ NIVEL, ETC.) O SALUBRIDAD (VACUNAS, EXÁMENES, ETC.).

**Ninguno**

**APROBACIONES:** PERSONAS QUE APRUEBAN EL PRESENTE ENUNCIADO DE TRABAJO.

<b>ROL</b>	<b>NOMBRE</b>	<b>FIRMA</b>	<b>FECHA</b>
Patrocinador	Daniel Ortiz	<i>Daniel Ortiz</i>	24/02/2022

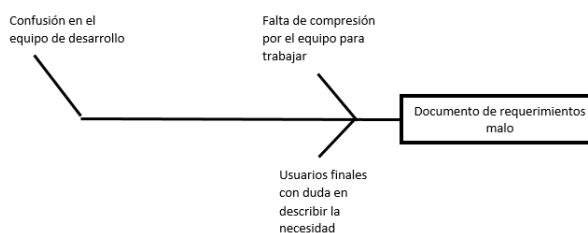
## Grupo de Procesos Ejecución

### Lección aprendida

CONTROL DE VERSIONES																	
Versión	Hecha por	Revisada por	Aprobada por	Fecha	Motivo												
1.0	WO	CR	CR		LECCIÓN APRENDIDA 1												
NOMBRE DEL PROYECTO			SIGLAS DEL PROYECTO														
Aplicación Móvil de Gestión y Atención de Clientes			AMGC														
FASE		ENTREGABLE															
Toma y análisis de requerimientos		Documento con los requerimientos del aplicativo															
TEMAS DE REFERENCIA																	
1	Requerimientos																
<b>DESCRIPCIÓN DEL ENTREGABLE:</b> DESCRIBIR LA INFORMACIÓN DEL ENTREGABLE AFECTADO POR LA LECCIÓN APRENDIDA DE ACUERDO CON EL DICCIONARIO DE LA EDT.																	
<b>Documento con los datos relacionados con la funcionalidad para la aplicación móvil</b>																	
<b>De gestión y atención de clientes</b>																	
<b>DESCRIPCIÓN DEL PROBLEMA:</b> DESCRIBIR EL PROBLEMA SURGIDO DURANTE EL CICLO DE VIDA DEL PROYECTO Y POR EL CUAL SE GENERÓ LA LECCIÓN APRENDIDA.																	
<b>Falta de claridad en lo que se deseaba por parte del usuario final</b>																	
<b>DESCRIPCIÓN DE LAS CAUSAS:</b> DESCRIBIR LAS CAUSAS QUE MOTIVARON EL ORIGEN DEL PROBLEMA Y GENERARON LA LECCIÓN APRENDIDA. (ADJUNTAR DIAGRAMA DE ISHIKAWA)																	
<b>Comunicación clientes - equipo</b>																	
<b>Descripción de requerimientos para la aplicación móvil</b>																	
<b>ACCIONES CORRECTIVAS TOMADAS:</b> DESCRIBIR LAS ACCIONES CORRECTIVAS QUE SE EFECTUARON PARA SOLUCIONAR EL PROBLEMA IDENTIFICADO.																	
<b>Explicarle al cliente después de realizar una toma de requerimientos algunas.</b>																	
<b>RAZONAMIENTO DETRÁS DE LAS ACCIONES:</b> DESCRIBIR EL RAZONAMIENTO DE CÓMO LAS ACCIONES CORRECTIVAS TOMADAS, IMPACTARÁN SOBRE EL PROBLEMA IDENTIFICADO.																	
<b>Mejora en la compresión y comunicación por parte del equipo del proyecto con los clientes finales.</b>																	
<b>RESULTADOS OBTENIDOS:</b> DESCRIPCIÓN DE LOS RESULTADOS OBTENIDOS DESPUÉS DE APLICAR LAS ACCIONES CORRECTIVAS EN EL ENTREGABLE AFECTADO.																	
<b>Un mejor documento con los requisitos de la funcionalidad</b>																	
<b>LECCIÓN APRENDIDA:</b> DESCRIBIR DETALLADAMENTE EL CONOCIMIENTO REUTILIZABLE QUE SE PUEDA APROVECHAR PARA MANEJAR LA PERFORMANCE FUTURA DE PROYECTOS.																	
<b>Realizar de la mejor manera el levantado de requerimientos.</b>																	

Fuente: (Dharma Consulting, 2022)

**Figura No. 7**



Fuente: Elaboración Propia

## Encuesta de Satisfacción Sobre el Trabajo en Equipo

CONTROL DE VERSIONES					
Versión	Hecha por	Revisada por	Aprobada por	Fecha	Motivo
1.0	BA	CR	CR	07/03/22	Versión Original

NOMBRE DEL PROYECTO	SIGLAS DEL PROYECTO
Aplicación Móvil de Gestión y Atención de Clientes	AMGC

<b>I. INTRODUCCIÓN</b>					
<b>DESCRIPCIÓN</b>	<b>NIVEL DE SATISFACCIÓN</b>				
	1 (NADA)	2 (POCO)	3 (MEDIO)	4 (BUENO)	5 (ÓPTIMO)
<b>1. LIDERAZGO:</b> CAPACIDAD DE COMUNICARSE CON EL EQUIPO DE TRABAJO, INFLUIR EN SUS EMOCIONES, PARA COMPARTIR LAS IDEAS DEL EQUIPO, Y EJECUTAR ACCIONES O ACTIVIDADES NECESARIAS PARA EL CUMPLIMIENTO DE LOS OBJETIVOS.				X	
EL LIDERAZGO ES COMPARTIDO EN EL EQUIPO.				X	
SE TOMA EL ROL DE LÍDER DE ACUERDO CON LA SITUACIÓN.				X	
SE CREA INTERDEPENDENCIA DANDO FUERZA, LIBERANDO Y SIRVIENDO A OTROS MIEMBROS DEL EQUIPO.				X	
<b>2. RESPONSABILIDAD:</b> COMPROMISO DE CADA UNO DE LOS MIEMBROS DEL EQUIPO RESPECTO DEL RESULTADO FINAL CONJUNTO.				X	
SE PLANEAN ACTIVIDADES EN TÉRMINOS DEL TIEMPO QUE REQUERIRÁ REALIZARLAS.				X	
LA RESPONSABILIDAD EN EL EQUIPO ES TANTO INDIVIDUAL COMO CONJUNTA.				X	
SE FIJAN OBJETIVOS QUE SIEMPRE SE CUMPLEN, AUTOEXIGIÉNDOSE PLAZOS Y MEJORANDO LA CALIDAD DEL TRABAJO O PROYECTO.				X	
<b>3. OBJETIVOS DEL EQUIPO:</b> SE MOVILIZAN LOS ASPECTOS POSITIVOS Y EL ENTUSIASMO DE LOS MIEMBROS DEL EQUIPO PARA ALCANZAR UN OBJETIVO COMÚN.				X	
SE HACEN APORTES CONCRETOS PARA QUE EL EQUIPO NO PIERDA DE VISTA LOS OBJETIVOS PLANTEADOS.				X	
SE APOYAN Y ALIENTAN LAS ACTIVIDADES EN EQUIPO A FIN DE OBTENER RESULTADOS COMUNES EXITOSOS.				X	
SE MANTIENEN REUNIONES CENTRADAS EN LOS OBJETIVOS PREVISTOS.				X	

<b>4. TRABAJO COLECTIVO:</b> SE GENERAN PRODUCTOS QUE SON FRUTO DEL TRABAJO COLECTIVO DEL EQUIPO, UN GRUPO DE PERSONAS TRABAJANDO JUNTAS CONSTITUYE UN VERDADERO EQUIPO DE TRABAJO.									
SE APOYA EN LA FINALIZACIÓN DE ENTREGABLES DE OTROS MIEMBROS DEL EQUIPO PARA CUMPLIR CON EL OBJETIVO CONJUNTO.				X					
SE DISCUTE, SE DECIDE Y SE TRABAJA CONJUNTAMENTE.				X					
LOS RESULTADOS SE MIDEN EN FORMA DIRECTA MEDIANTE LA EVALUACIÓN DEL PRODUCTO DEL TRABAJO COLECTIVO.				X					
<b>5. RESOLUCIÓN DE PROBLEMAS:</b> SE FOMENTA LA CONFIANZA DE LOS MIEMBROS DEL EQUIPO EN SU PROPIO PENSAMIENTO, PARA APLICAR SUS CONOCIMIENTOS EN RECONOCER, DESCRIBIR, ORGANIZAR Y ANALIZAR LOS ELEMENTOS CONSTITUTIVOS DE UN PROBLEMA PARA IDEAR ESTRATEGIAS QUE LE PERMITAN OBTENER, DE FORMA RAZONADA, UNA SOLUCIÓN CONTRASTADA Y ACORDE A LOS OBJETIVOS DEL EQUIPO Y DEL PROYECTO.									
SE SOLICITAN OPINIONES Y SUGERENCIAS A LOS MIEMBROS DEL EQUIPO PARA LA SOLUCIÓN DE CIERTOS PROBLEMAS.					X				
SE AYUDA A GENERAR NUEVOS CAMINOS PARA EL PENSAMIENTO Y LA REFLEXIÓN SOBRE LOS PROBLEMAS.				X					
SE FOMENTAN LAS DISCUSIONES ABIERTAS PARA LA RESOLUCIÓN DE PROBLEMAS DE MANERA ACTIVA.				X					
<b>6. BUENA COMUNICACIÓN:</b> SE INTERCAMBIA CON EFICACIA, INFORMACIÓN APROPIADA Y RELEVANTE DENTRO DEL EQUIPO, USANDO MÉTODOS APROPIADOS.									
SE COMPARTEN IDEAS Y/O PUNTOS DE VISTA CON OTROS.				X					
EN EL EQUIPO DE TRABAJO SE CREA UN ENTORNO QUE ESTIMULA LA COMUNICACIÓN ABIERTA Y POSITIVA				X					
EXISTE INTERCAMBIO DE INFORMACIÓN Y RETROALIMENTACIÓN ENTRE EL LÍDER Y LOS MIEMBROS DEL EQUIPO.					X				
<b>II. FORTALEZAS Y OPORTUNIDADES DE MEJORA PARA EL EQUIPO</b>									
FORTALEZAS		OPORTUNIDADES DE MEJORA							
El Equipo se encuentra comprometido con los objetivos del proyecto, motivándose y apoyándose continuamente entre los miembros para no perder de vista los objetivos previstos.		El equipo realiza reuniones orientadas a responder las inquietudes de los miembros, exponiendo temas concretos enfocados en los objetivos del proyecto, pero se recomendaría que estas reuniones se realicen con más frecuencia para poder resolver las dudas de los miembros del equipo a medida que estas aparecen, y de esta manera se evitará dejar pasar demasiado tiempo para su resolución.							
El ambiente de trabajo en equipo es amigable, cálido y de aspecto familiar, en el cual los miembros del equipo suelen compartir información del proyecto de manera formal e informal constantemente.		Se ha observado que algunos miembros del equipo no manejan una buena comunicación con el líder del equipo de proyecto, debido a que son un poco reservados y no suelen comunicar sus dudas y/o sus puntos de vista con respecto a diversos temas referentes al proyecto, por ello se recomendaría al líder brindar mayor motivación y una especial atención a estas personas para que puedan expresarse con mayor libertad.							
<b>III. SUGERENCIAS</b>									
Mejorar la comunicación del líder con los miembros del equipo haciendo énfasis en los miembros que no han manejado una buena o poca comunicación hasta el momento.									

Fuente: (Dharma Consulting, 2022)

## Evaluación de Competencias Generales

CONTROL DE VERSIONES					
Versión	Hecha por	Revisada por	Aprobada por	Fecha	Motivo
1.0	CD	CR	CR	07/03/22	Evaluar competencias

NOMBRE DEL PROYECTO	SIGLAS DEL PROYECTO
Aplicación Móvil de Gestión y Atención de Clientes	AMGC

I. CONCEPTO					
<p>LA EVALUACIÓN DE COMPETENCIAS GENERALES, ES UNA HERRAMIENTA DE RETROALIMENTACIÓN, MEDIANTE EL CUAL SE RECOGEN EVIDENCIAS SOBRE LAS COMPETENCIAS GENERALES DEL EVALUADO. EL PROPÓSITO DE LA EVALUACIÓN DE COMPETENCIAS GENERALES ES DAR INFORMACIÓN AL EVALUADO SOBRE LA PERTINENCIA DE SUS COMPETENCIAS EN UN CONTEXTO LABORAL, CON LA FINALIDAD DE AYUDARLO A MEJORAR LOS RESULTADOS DE SU DESEMPEÑO PERSONAL Y PROFESIONAL.</p>					
II. DATOS DEL EVALUADO					
<b>NOMBRE</b>	Luis chan				
<b>ÁREA</b>	IT				
<b>CARGO</b>	Director IT				
III. DATOS DEL EVALUADOR					
RELACIÓN CON EL EVALUADO ( MARCAR CON UNA X)					
<b>Jefe</b>	<input checked="" type="checkbox"/>				
<b>Supervisado</b>					
<b>Cliente</b>					
<b>Colega</b>					
<b>Autoevaluación</b>					
IV. COMPETENCIAS					
<p>"LAS COMPETENCIAS ESTÁN RELACIONADAS CON LAS ACTITUDES, HABILIDADES, Y OTRAS CARACTERÍSTICAS PERSONALES QUE AFECTAN UNA PARTE IMPORTANTE DEL RENDIMIENTO EN EL TRABAJO (ES DECIR, UNO O MÁS ROLES O RESPONSABILIDADES CLAVES), SE PUEDE MEDIR CON ESTÁNDARES ACEPTADOS, Y SE PUEDEN MEJORAR A TRAVÉS DEL ENTRENAMIENTO Y DESARROLLO" (PMI®, 2002).</p>					
V. COMPETENCIAS GENERALES					
<p>"SON LOS COMPORTAMIENTOS ASOCIADOS A DESEMPEÑOS COMUNES A DIVERSAS ORGANIZACIONES Y RAMAS DE ACTIVIDAD PRODUCTIVA, DENTRO DE ESTA DEFINICIÓN SE ENGLOBAN TODAS AQUELLAS CAPACIDADES DE CARÁCTER GENERALISTA, EN EL SENTIDO DE QUE NO ESTARÍAN ORIENTADAS AL DESARROLLO DE NINGUNA TAREA LABORAL ESPECÍFICA, SINO QUE CONSTITUIRÍAN LA BASE DEL SABER PROFESIONAL" (OIT, 2007).</p>					
DESCRIPCIÓN	CALIFICACIÓN				
	1 (NUNCA)	2 (Poco)	3 (MEDIANA MENTE)	4 (HABITUAL MENTE)	5 (SIEMPRE)
<b>1. CALIDAD DE TRABAJO:</b> Conoce los temas del área de la cual es responsable, comprendiendo la esencia de los aspectos complejos para transformarlos en soluciones prácticas, y operables para la organización.				X	
Define objetivos claros, y diseña procesos adecuados, prácticos, y operables en beneficio de todos.				X	
Trabaja con altos estándares de calidad y resultados.			X		
Se mantiene informado y capacitado, desempeñándose con alta eficacia en los contextos cambiantes de la organización.			X		
Apporta ideas y conocimientos a la organización.				X	
<b>2. CAPACIDAD PARA APRENDER:</b> Asimila nueva información y la aplica eficazmente, relacionando la incorporación de nuevos esquemas a su repertorio de conductas habituales.					

<i>INNOVA Y PROPONE AL RESTO DE LA ORGANIZACIÓN NUEVAS HERRAMIENTAS, Y PROCEDIMIENTOS QUE CONTRIBUYEN AL MEJORAMIENTO DEL NEGOCIO.</i>				X	
<i>IDENTIFICA NUEVA INFORMACIÓN, TRASLADÁNDOLA A SU ÁMBITO DE TRABAJO.</i>			X		
<i>ES CONSIDERADO UN REFERENTE DENTRO DE LA ORGANIZACIÓN EN EL MOMENTO DE INCORPORAR CAMBIOS REFERIDOS A PROCEDIMIENTOS, HERRAMIENTAS O CONCEPTOS.</i>					X
<i>ESTÁ ABIERTO A ABANDONAR VIEJAS PRÁCTICAS O MODOS DE LEER LA REALIDAD.</i>		X			
<b>3. HABILIDAD ANALÍTICA (ANÁLISIS DE PRIORIDAD, CRITERIO LÓGICO, SENTIDO COMÚN):</b> REALIZA UN ANÁLISIS LÓGICO, IDENTIFICANDO LOS PROBLEMAS, Y RECONOCIENDO LA INFORMACIÓN SIGNIFICATIVA PARA LA ORGANIZACIÓN.					
<i>COMPRENDE LOS PROCESOS RELATIVOS A SU TRABAJO DENTRO DE LA ORGANIZACIÓN.</i>				X	
<i>IDENTIFICA LA EXISTENCIA DE PROBLEMAS RELACIONADOS CON SU ÁREA.</i>				X	
<i>RECOPILA INFORMACIÓN RELEVANTE, LA ORGANIZA DE FORMA SISTEMÁTICA, Y ESTABLECE RELACIONES CAUSALES.</i>			X		
<i>ESTABLECE RELACIONES ENTRE DATOS NUMÉRICOS Y CONCEPTUALES, PERMITIÉNDOLE RESOLVER PROBLEMAS.</i>			X		
<b>4. CONCIENCIA ORGANIZACIONAL:</b> RECONOCE LOS ATRIBUTOS Y LAS MODIFICACIONES DE LA ORGANIZACIÓN, COMPRENDIENDO E INTERPRETANDO LAS RELACIONES DE PODER DENTRO DE ESTA.					
<i>CONOCE LOS ATRIBUTOS DE LA ORGANIZACIÓN, CAPTANDO CON FACILIDAD LAS MODIFICACIONES QUE EN ELLA SE PRODUCEN.</i>			X		
<i>PRIORIZA LA IMAGEN Y OBJETIVOS ORGANIZACIONALES POR SOBRE SUS OBJETIVOS PERSONALES.</i>				X	
<i>CONSTRUYE REDES DE PERSONAS, DENTRO Y FUERA DE LA ORGANIZACIÓN, A FIN DE QUE PUEDAN APORTARLE INFORMACIÓN VALIOSA PARA LA EMPRESA.</i>				X	
<i>COMPRENDE E INTERPRETA CABALMENTE LAS RELACIONES DE PODER EN Y ENTRE LOS DIFERENTES ACTORES (INTERNAOS Y EXTERNOS) QUE PARTICIPAN EN EL NEGOCIO.</i>					X
<b>5. ORIENTACIÓN A LOS RESULTADOS:</b> ENCAMAÑA SUS ACTOS AL LOGRO DE LO ESPERADO, ACTUANDO CON VELOCIDAD Y SENTIDO DE URGENCIA ANTE DECISIONES IMPORTANTES PARA SATISFACER LAS NECESIDADES DEL CLIENTE, SUPERAR A LOS COMPETIDORES, O MEJORAR LA ORGANIZACIÓN.					
<i>TRABAJA CON OBJETIVOS ESTABLECIDOS, REALISTAS, Y DESAFIANTES.</i>			X		
<i>BRINDA ORIENTACIÓN Y RETROALIMENTACIÓN A SUS COMPAÑEROS DE TRABAJO ACERCA DE SU DESEMPEÑO.</i>				X	
<i>ACTÚA CON VELOCIDAD Y SENTIDO DE URGENCIA ANTE SITUACIONES QUE REQUIEREN ANTICIPARSE A LOS COMPETIDORES O RESPONDER A LAS NECESIDADES DE LOS CLIENTES.</i>		X			
<i>PLANIFICA SU ACTIVIDAD, BUSCANDO INCREMENTAR LA COMPETITIVIDAD DE LA ORGANIZACIÓN.</i>				X	
<b>6. ADAPTABILIDAD AL CAMBIO:</b> SE ADAPTA Y AMOLDA A LOS CAMBIOS, MODIFICANDO LA PROPIA CONDUCTA PARA ALCANZAR DETERMINADOS OBJETIVOS CUANDO SURGEN DIFICULTADES, NUEVOS DATOS O CAMBIOS EN EL MEDIO.					

<i>TIENE UNA AMPLIA VISIÓN DEL MERCADO Y DEL NEGOCIO, QUE LE PERMITE ANTICIPARSE EN LA COMPRENSIÓN DE LOS CAMBIOS QUE SE REQUERIRÁN DENTRO DE LAS POLÍTICAS Y OBJETIVOS DE LA ORGANIZACIÓN.</i>					X
<i>MODIFICA ESTRATEGIAS Y OBJETIVOS DE LA ORGANIZACIÓN, CON CELERIDAD ANTE CAMBIOS EXTERNOS O NUEVAS NECESIDADES.</i>				X	
<i>SE ADAPTA CON VERSATILIDAD, EFICIENCIA, Y VELOCIDAD A DISTINTOS CONTEXTOS SITUACIONALES, MEDIOS Y PERSONAS.</i>				X	
<i>PROMUEVE LA ADAPTABILIDAD AL CAMBIO ENTRE SU EQUIPO DE TRABAJO.</i>			X		
<b>7. ÉTICA:</b> SIENTE Y ACTÚA CONSECUENTEMENTE CON LOS VALORES MORALES, Y LAS BUENAS COSTUMBRES Y PRÁCTICAS PROFESIONALES.					
<i>ESTRUCTURA LA VISIÓN Y MISIÓN ORGANIZACIONALES SOBRE LA BASE DE VALORES MORALES.</i>				X	
<i>ESTABLECE UN MARCO DE TRABAJO QUE RESPETA LAS POLÍTICAS DE LA ORGANIZACIÓN, LOS VALORES MORALES, LAS BUENAS COSTUMBRES Y PRÁCTICAS PROFESIONALES.</i>			X		
<i>SE LE RECONOCE POR SER FIEL A SUS PRINCIPIOS, TANTO EN LO LABORAL COMO EN LOS ÁMBITOS DE SU VIDA.</i>			X		
<i>APORTA Y PROVEE IDEAS PARA MEJORAR EL ACCIONAR DE LA EMPRESA, ADECUÁNDOLO A LOS VALORES Y PRINCIPIOS COMUNES.</i>				X	
<b>8. RESPONSABILIDAD:</b> SE COMPROMETE EN LA REALIZACIÓN DE LAS TAREAS ASIGNADAS. SU INTERÉS POR EL CUMPLIMIENTO DE LO ASIGNADO ESTÁ POR ENCIMA DE SUS PROPIOS INTERESES.					
<i>SE FIJA OBJETIVOS QUE SIEMPRE CUMPLE, AUTOEXIGIÉNDOSE PLAZOS Y MEJORANDO LA CALIDAD DEL TRABAJO O PROYECTO.</i>				X	
<i>MODIFICA CON BUENA PREDISPOSICIÓN LA ORGANIZACIÓN DE SUS TIEMPOS PARA CUMPLIR CON LAS TAREAS ASIGNADAS.</i>				X	
<i>PREFIERE ORGANIZAR, EN PRIMER LUGAR, SUS TAREAS, Y LUEGO DISTRIBUIR EL TIEMPO LIBRE PARA DEDICARSE A OTRAS ACTIVIDADES.</i>				X	
<i>ANTEPONE EL TRABAJO A LAS ACTIVIDADES PERSONALES, AÚN SIN QUE SE LE PIDA, Y EVALÚA ATINADAMENTE LAS OCASIONES EN QUE SE REQUIERE DE SU ESFUERZO EXTRA.</i>				X	

<b>9. TOLERANCIA A LA PRESIÓN:</b> SIGUE ACTUANDO CON EFICACIA EN SITUACIONES DE PRESIÓN DE TIEMPO Y DE DESACUERDO, OPOSICIÓN Y DIVERSIDAD, TRABAJADO CON ALTO DESEMPEÑO EN SITUACIONES DE ALTA EXIGENCIA.									
RESUELVE EFICIENTEMENTE SUS TAREAS AUN CUANDO CONVERGEN AL MISMO TIEMPO PROBLEMAS U OBSTÁCULOS QUE LE EXIGEN MAYORES ESFUERZOS.			X						
MUESTRA SU PREDISPOSICIÓN Y ACTITUD POSITIVA, Y LA TRANSMITE A SUS COMPAÑEROS DE TRABAJO AÚN EN SITUACIONES ESTRESANTES.			X						
PROVEE ALTERNATIVAS PARA EL LOGRO DE LA TAREA, MANTENIENDO LA CALIDAD DESEADA EN SITUACIONES DE ALTA EXIGENCIA.			X						
SE CONDUCE CON PROFESIONALISMO, SIN EXTERIORIZAR DESBORDES EMOCIONALES, EN ÉPOCAS DE TRABAJO QUE REQUIEREN MAYOR ESFUERZO.				X					
<b>10. ORIENTACIÓN AL CLIENTE:</b> AYUDA A LOS CLIENTES, COMPRENDIENDO Y SATISFACIENDO SUS NECESIDADES.									
EL CUIDADO DEL CLIENTE FORMA PARTE DE SU ESTRATEGIA DE TRABAJO.		X							
PLANIFICA SUS ACCIONES CONSIDERANDO LAS NECESIDADES DE LOS CLIENTES.			X						
INDAGA E INFORMA SOBRE NECESIDADES ACTUALES Y POTENCIALES DE LOS CLIENTES.			X						
PRIORIZA LA RELACIÓN A LARGO PLAZO CON EL CLIENTE POR SOBRE BENEFICIOS INMEDIATOS U OCASIONALES.			X						
<b>11. TRABAJO EN EQUIPO:</b> PARTICIPA ACTIVAMENTE EN LA BÚSQUEDA DE UNA META COMÚN, SUBORDINANDO LOS INTERESES PERSONALES A LOS OBJETIVOS DEL EQUIPO.									
ESTA DISPUESTO AL INTERCAMBIO DE INFORMACIÓN CON LOS MIEMBROS DE SU EQUIPO.				X					
MANTIENE SU NIVEL DE RENDIMIENTO EN TAREAS QUE REQUIEREN DE RELACIONES INTERPERSONALES.				X					
ES ABIERTO A RECIBIR NUEVOS COMPAÑEROS EN SU ÁREA DE TRABAJO, COLABORANDO CON ELLOS PARA QUE SE PONGAN RÁPIDAMENTE AL TANTO DE LAS ACTIVIDADES DEL SECTOR.			X						
SE PREOCUPA POR LOGRAR CONSENSO, Y CUIDA QUE NO SE IMPONGAN MODALIDADES DE TRABAJO ARBITRARIAMENTE.				X					
<b>VI. SÍRVASE INDICAR ALGUNAS FORTALEZAS Y OPORTUNIDADES DE MEJORA SOBRE LAS COMPETENCIAS GENERALES DE LA PERSONA EVALUADA:</b>									
<b>FORTALEZAS</b>		<b>OPORTUNIDADES DE MEJORA</b>							
Resulta ser alguien de grandes ideales y con mucha capacidad para trabajar en equipo, aporta buenas ideas y tiene muy buena iniciativa. Es abierto para recibir ideas de otros compañeros.		Podría considerar un poco más al cliente tratándolo de mejor manera y anticiparse a situaciones en donde pueda platicar más. Mejorar sus relaciones con sus inferiores podría mejorar.							
<b>VII. ¿QUÉ LE SUGERIRÍA A LA PERSONA EVALUADA PARA MEJORAR SUS COMPETENCIAS GENERALES?</b>									
<b>SUGERENCIAS</b>									
Mejorar la relación con los clientes y subordinados.									

<b>I. CONCEPTO</b>
LA EVALUACIÓN DE COMPETENCIAS GENERALES, ES UNA HERRAMIENTA DE RETROALIMENTACIÓN, MEDIANTE EL CUAL SE RECOGEN EVIDENCIAS SOBRE LAS COMPETENCIAS GENERALES DEL EVALUADO. EL PROPÓSITO DE LA EVALUACIÓN DE COMPETENCIAS GENERALES ES DAR INFORMACIÓN AL EVALUADO SOBRE LA PERTINENCIA DE SUS COMPETENCIAS EN UN CONTEXTO LABORAL, CON LA FINALIDAD DE AYUDARLO A MEJORAR LOS RESULTADOS DE SU DESEMPEÑO PERSONAL Y PROFESIONAL.

<b>II. DATOS DEL EVALUADO</b>					
<b>NOMBRE</b>	Marta Godínez				
<b>ÁREA</b>	Programas				
<b>CARGO</b>	Director de programas				
<b>III. DATOS DEL EVALUADOR</b>					
<b>RELACIÓN CON EL EVALUADO ( MARCAR CON UNA X)</b>					
<b>Jefe</b>	<input checked="" type="checkbox"/>				
<b>Supervisado</b>					
<b>Cliente</b>					
<b>Colega</b>					
<b>Autoevaluación</b>					
<b>IV. COMPETENCIAS</b>					
<p>"LAS COMPETENCIAS ESTÁN RELACIONADAS CON LAS ACTITUDES, HABILIDADES, Y OTRAS CARACTERÍSTICAS PERSONALES QUE AFECTAN UNA PARTE IMPORTANTE DEL RENDIMIENTO EN EL TRABAJO (ES DECIR, UNO O MÁS ROLES O RESPONSABILIDADES CLAVES), SE PUEDE MEDIR CON ESTÁNDARES ACEPTADOS, Y SE PUEDEN MEJORAR A TRAVÉS DEL ENTRENAMIENTO Y DESARROLLO" (PMI®, 2002).</p>					
<b>V. COMPETENCIAS GENERALES</b>					
<p>"SON LOS COMPORTAMIENTOS ASOCIADOS A DESEMPEÑOS COMUNES A DIVERSAS ORGANIZACIONES Y RAMAS DE ACTIVIDAD PRODUCTIVA, DENTRO DE ESTA DEFINICIÓN SE ENGLOBAN TODAS AQUELLAS CAPACIDADES DE CARÁCTER GENERALISTA, EN EL SENTIDO DE QUE NO ESTARÍAN ORIENTADAS AL DESARROLLO DE NINGUNA TAREA LABORAL ESPECÍFICA, SINO QUE CONSTITUIRÍAN LA BASE DEL SABER PROFESIONAL" (OIT, 2007).</p>					
<b>DESCRIPCIÓN</b>	<b>CALIFICACIÓN</b>				
	<b>1 (NUNCA)</b>	<b>2 (Poco)</b>	<b>3 (MEDIANA MENTE)</b>	<b>4 (HABITUAL MENTE)</b>	<b>5 (SIEMPRE)</b>
<b>1. CALIDAD DE TRABAJO:</b> Conoce los temas del área de la cual es responsable, comprendiendo la esencia de los aspectos complejos para transformarlos en soluciones prácticas, y operables para la organización.				<input checked="" type="checkbox"/>	
Define objetivos claros, y diseña procesos adecuados, prácticos, y operables en beneficio de todos.				<input checked="" type="checkbox"/>	
Trabaja con altos estándares de calidad y resultados.				<input checked="" type="checkbox"/>	
Se mantiene informado y capacitado, desempeñándose con alta eficacia en los contextos cambiantes de la organización.			<input checked="" type="checkbox"/>		
Aporta ideas y conocimientos a la organización.		<input checked="" type="checkbox"/>			
<b>2. CAPACIDAD PARA APRENDER:</b> Asimila nueva información y la aplica eficazmente, relacionando la incorporación de nuevos esquemas a su repertorio de conductas habituales.				<input checked="" type="checkbox"/>	
Innova y propone al resto de la organización nuevas herramientas, y procedimientos que contribuyen al mejoramiento del negocio.				<input checked="" type="checkbox"/>	
Identifica nueva información, trasladándola a su ámbito de trabajo.		<input checked="" type="checkbox"/>			
Es considerado un referente dentro de la organización en el momento de incorporar cambios referidos a procedimientos, herramientas o conceptos.			<input checked="" type="checkbox"/>		
Está abierto a abandonar viejas prácticas o modos de leer la realidad.				<input checked="" type="checkbox"/>	
<b>3. HABILIDAD ANALÍTICA (ANÁLISIS DE PRIORIDAD, CRITERIO LÓGICO, SENTIDO COMÚN):</b> Realiza un análisis lógico, identificando los problemas, y reconociendo la información significativa para la organización.					
Comprende los procesos relativos a su trabajo dentro de la organización.			<input checked="" type="checkbox"/>		

<i>IDENTIFICA LA EXISTENCIA DE PROBLEMAS RELACIONADOS CON SU ÁREA.</i>			X		
<i>RECOPILA INFORMACIÓN RELEVANTE, LA ORGANIZA DE FORMA SISTEMÁTICA, Y ESTABLECE RELACIONES CAUSALES.</i>			X		
<i>ESTABLECE RELACIONES ENTRE DATOS NUMÉRICOS Y CONCEPTUALES, PERMITIÉNDOLE RESOLVER PROBLEMAS.</i>				X	
<b>4. CONCIENCIA ORGANIZACIONAL:</b> RECONOCE LOS ATRIBUTOS Y LAS MODIFICACIONES DE LA ORGANIZACIÓN, COMPRENDIENDO E INTERPRETANDO LAS RELACIONES DE PODER DENTRO DE ESTA.					
<i>CONOCE LOS ATRIBUTOS DE LA ORGANIZACIÓN, CAPTANDO CON FACILIDAD LAS MODIFICACIONES QUE EN ELLA SE PRODUCEN.</i>			X		
<i>PRIORIZA LA IMAGEN Y OBJETIVOS ORGANIZACIONALES POR SOBRE SUS OBJETIVOS PERSONALES.</i>				X	
<i>CONSTRUYE REDES DE PERSONAS, DENTRO Y FUERA DE LA ORGANIZACIÓN, A FIN DE QUE PUEDAN APORTARLE INFORMACIÓN VALIOSA PARA LA EMPRESA.</i>			X		
<i>COMPRENDE E INTERPRETA CABALMENTE LAS RELACIONES DE PODER EN Y ENTRE LOS DIFERENTES ACTORES (INTERNAOS Y EXTERNOS) QUE PARTICIPAN EN EL NEGOCIO.</i>				X	
<b>5. ORIENTACIÓN A LOS RESULTADOS:</b> ENCAMAÑA SUS ACTOS AL LOGRO DE LO ESPERADO, ACTUANDO CON VELOCIDAD Y SENTIDO DE URGENCIA ANTE DECISIONES IMPORTANTES PARA SATISFACER LAS NECESIDADES DEL CLIENTE, SUPERAR A LOS COMPETIDORES, O MEJORAR LA ORGANIZACIÓN.					
<i>TRABAJA CON OBJETIVOS ESTABLECIDOS, REALISTAS, Y DESAFIANTES.</i>				X	
<i>BRINDA ORIENTACIÓN Y RETROALIMENTACIÓN A SUS COMPAÑEROS DE TRABAJO ACERCA DE SU DESEMPEÑO.</i>			X		
<i>ACTÚA CON VELOCIDAD Y SENTIDO DE URGENCIA ANTE SITUACIONES QUE REQUIEREN ANTICIPARSE A LOS COMPETIDORES O RESPONDER A LAS NECESIDADES DE LOS CLIENTES.</i>				X	
<i>PLANIFICA SU ACTIVIDAD, BUSCANDO INCREMENTAR LA COMPETITIVIDAD DE LA ORGANIZACIÓN.</i>			X		
<b>6. ADAPTABILIDAD AL CAMBIO:</b> SE ADAPTA Y AMOLDA A LOS CAMBIOS, MODIFICANDO LA PROPIA CONDUCTA PARA ALCANZAR DETERMINADOS OBJETIVOS CUANDO SURGEN DIFICULTADES, NUEVOS DATOS O CAMBIOS EN EL MEDIO.					
<i>TIENE UNA AMPLIA VISIÓN DEL MERCADO Y DEL NEGOCIO, QUE LE PERMITE ANTICIPARSE EN LA COMPRENSIÓN DE LOS CAMBIOS QUE SE REQUERIRÁN DENTRO DE LAS POLÍTICAS Y OBJETIVOS DE LA ORGANIZACIÓN.</i>		X			
<i>MODIFICA ESTRATEGIAS Y OBJETIVOS DE LA ORGANIZACIÓN, CON CELERIDAD ANTE CAMBIOS EXTERNOS O NUEVAS NECESIDADES.</i>			X		
<i>SE ADAPTA CON VERSATILIDAD, EFICIENCIA, Y VELOCIDAD A DISTINTOS CONTEXTOS SITUACIONALES, MEDIOS Y PERSONAS.</i>				X	
<i>PROMUEVE LA ADAPTABILIDAD AL CAMBIO ENTRE SU EQUIPO DE TRABAJO.</i>				X	
<b>7. ÉTICA:</b> SIENTE Y ACTÚA CONSECUENTEMENTE CON LOS VALORES MORALES, Y LAS BUENAS COSTUMBRES Y PRÁCTICAS PROFESIONALES.					
<i>ESTRUCTURA LA VISIÓN Y MISIÓN ORGANIZACIONALES SOBRE LA BASE DE VALORES MORALES.</i>				X	

<i>ESTABLECE UN MARCO DE TRABAJO QUE RESPETA LAS POLÍTICAS DE LA ORGANIZACIÓN, LOS VALORES MORALES, LAS BUENAS COSTUMBRES Y PRÁCTICAS PROFESIONALES.</i>					X
<i>SE LE RECONOCE POR SER FIEL A SUS PRINCIPIOS, TANTO EN LO LABORAL COMO EN LOS ÁMBITOS DE SU VIDA.</i>					X
<i>APORTA Y PROVEE IDEAS PARA MEJORAR EL ACCIONAR DE LA EMPRESA, ADECUÁNDOLO A LOS VALORES Y PRINCIPIOS COMUNES.</i>					X
<b>8. RESPONSABILIDAD:</b> <i>Se compromete en la realización de las tareas asignadas. Su interés por el cumplimiento de lo asignado está por encima de sus propios intereses.</i>					
<i>SE FIJA OBJETIVOS QUE SIEMPRE CUMPLE, AUTOEXIGIÉNDOSE PLAZOS Y MEJORANDO LA CALIDAD DEL TRABAJO O PROYECTO.</i>					X
<i>MODIFICA CON BUENA PREDISPONSIÓN LA ORGANIZACIÓN DE SUS TIEMPOS PARA CUMPLIR CON LAS TAREAS ASIGNADAS.</i>					X
<i>PREFIERE ORGANIZAR, EN PRIMER LUGAR, SUS TAREAS, Y LUEGO DISTRIBUIR EL TIEMPO LIBRE PARA DEDICARSE A OTRAS ACTIVIDADES.</i>					X
<i>ANTEPONE EL TRABAJO A LAS ACTIVIDADES PERSONALES, AÚN SIN QUE SE LE PIDA, Y EVALÚA ATINADAMENTE LAS OCASIONES EN QUE SE REQUIERE DE SU ESFUERZO EXTRA.</i>					X
<b>9. TOLERANCIA A LA PRESIÓN:</b> <i>Sigue actuando con eficacia en situaciones de presión de tiempo y de desacuerdo, oposición y diversidad, trabajado con alto desempeño en situaciones de alta exigencia.</i>					
<i>RESUELVE EFICIENTEMENTE SUS TAREAS AUN CUANDO CONVERGEN AL MISMO TIEMPO PROBLEMAS U OBSTÁCULOS QUE LE EXIGEN MAYORES ESFUERZOS.</i>				X	
<i>MUESTRA SU PREDISPONSIÓN Y ACTITUD POSITIVA, Y LA TRANSMITE A SUS COMPAÑEROS DE TRABAJO AÚN EN SITUACIONES ESTRESANTES.</i>				X	
<i>PROVEE ALTERNATIVAS PARA EL LOGRO DE LA TAREA, MANTENIENDO LA CALIDAD DESEADA EN SITUACIONES DE ALTA EXIGENCIA.</i>				X	
<i>SE CONDUCE CON PROFESIONALISMO, SIN EXTERIORIZAR DESBORDES EMOCIONALES, EN ÉPOCAS DE TRABAJO QUE REQUIEREN MAYOR ESFUERZO.</i>				X	
<b>10. ORIENTACIÓN AL CLIENTE:</b> <i>Ayuda a los clientes, comprendiendo y satisfaciendo sus necesidades.</i>					
<i>EL CUIDADO DEL CLIENTE FORMA PARTE DE SU ESTRATEGIA DE TRABAJO.</i>			X		
<i>PLANIFICA SUS ACCIONES CONSIDERANDO LAS NECESIDADES DE LOS CLIENTES.</i>				X	
<i>INDAGA E INFORMA SOBRE NECESIDADES ACTUALES Y POTENCIALES DE LOS CLIENTES.</i>				X	
<i>PRIORIZA LA RELACIÓN A LARGO PLAZO CON EL CLIENTE POR SOBRE BENEFICIOS INMEDIATOS U OCASIONALES.</i>					X
<b>11. TRABAJO EN EQUIPO:</b> <i>Participa activamente en la búsqueda de una meta común, subordinando los intereses personales a los objetivos del equipo.</i>					
<i>ESTA DISPUESTO AL INTERCAMBIO DE INFORMACIÓN CON LOS MIEMBROS DE SU EQUIPO.</i>				X	
<i>MANTIENE SU NIVEL DE RENDIMIENTO EN TAREAS QUE REQUIEREN DE RELACIONES INTERPERSONALES.</i>				X	
<i>Es abierto a recibir nuevos compañeros en su área de trabajo, colaborando con ellos para que</i>				X	

SE PONGAN RÁPIDAMENTE AL TANTO DE LAS ACTIVIDADES DEL SECTOR.								
SE PREOCUPA POR LOGRAR CONSENSO, Y CUIDA QUE NO SE IMPONGAN MODALIDADES DE TRABAJO ARBITRARIAMENTE.					X			
<b>VI. SÍRVASE INDICAR ALGUNAS FORTALEZAS Y OPORTUNIDADES DE MEJORA SOBRE LAS COMPETENCIAS GENERALES DE LA PERSONA EVALUADA:</b>								
<b>FORTALEZAS</b>			<b>OPORTUNIDADES DE MEJORA</b>					
Toma la iniciativa ante cualquier problema. Es rápida en tomar decisiones. Tiene precisión con los procesos. Toma de la mejor manera las críticas constructivas. Aporta en ideas en reuniones con los altos mandos.			Podría tener una mejor capacidad de comprensión con sus trabajadores. Puede mejorar con trabajar bajo presión.					
<b>VII. ¿QUÉ LE SUGERIRÍA A LA PERSONA EVALUADA PARA MEJORAR SUS COMPETENCIAS GENERALES?</b>								
<b>SUGERENCIAS</b>								
Puede mejorar en la comunicación con su equipo y darle un mejor apoyo a los integrantes que lo necesiten.								

<b>I. CONCEPTO</b>										
LA EVALUACIÓN DE COMPETENCIAS GENERALES, ES UNA HERRAMIENTA DE RETROALIMENTACIÓN, MEDIANTE EL CUAL SE RECOGEN EVIDENCIAS SOBRE LAS COMPETENCIAS GENERALES DEL EVALUADO. EL PROPÓSITO DE LA EVALUACIÓN DE COMPETENCIAS GENERALES ES DAR INFORMACIÓN AL EVALUADO SOBRE LA PERTINENCIA DE SUS COMPETENCIAS EN UN CONTEXTO LABORAL, CON LA FINALIDAD DE AYUDARLO A MEJORAR LOS RESULTADOS DE SU DESEMPEÑO PERSONAL Y PROFESIONAL.										
<b>II. DATOS DEL EVALUADO</b>										
<b>NOMBRE</b>	Diego Ruiz									
<b>ÁREA</b>	Administración									
<b>CARGO</b>	Personal de la oficina de proyectos									
<b>III. DATOS DEL EVALUADOR</b>										
<b>RELACIÓN CON EL EVALUADO ( MARCAR CON UNA X)</b>										
<b>Jefe</b>	X									
<b>Supervisado</b>										
<b>Cliente</b>										
<b>Colega</b>										
<b>AUTOEVALUACIÓN</b>										
<b>IV. COMPETENCIAS</b>										
"LAS COMPETENCIAS ESTÁN RELACIONADAS CON LAS ACTITUDES, HABILIDADES, Y OTRAS CARACTERÍSTICAS PERSONALES QUE AFECTAN UNA PARTE IMPORTANTE DEL RENDIMIENTO EN EL TRABAJO (ES DECIR, UNO O MÁS ROLES O RESPONSABILIDADES CLAVES), SE PUEDE MEDIR CON ESTÁNDARES ACEPTADOS, Y SE PUEDEN MEJORAR A TRAVÉS DEL ENTRENAMIENTO Y DESARROLLO" (PMI®, 2002).										
<b>V. COMPETENCIAS GENERALES</b>										
"SON LOS COMPORTAMIENTOS ASOCIADOS A DESEMPEÑOS COMUNES A DIVERSAS ORGANIZACIONES Y RAMAS DE ACTIVIDAD PRODUCTIVA, DENTRO DE ESTA DEFINICIÓN SE ENGLOBAN TODAS AQUELLAS CAPACIDADES DE CARÁCTER GENERALISTA, EN EL SENTIDO DE QUE NO ESTARÍAN ORIENTADAS AL DESARROLLO DE NINGUNA TAREA LABORAL ESPECÍFICA, SINO QUE CONSTITUIRÍAN LA BASE DEL SABER PROFESIONAL" (OIT, 2007).										
<b>DESCRIPCIÓN</b>	<b>CALIFICACIÓN</b>									
	<b>1 (NUNCA)</b>	<b>2 (Poco)</b>	<b>3 (MEDIANAMENTE)</b>	<b>4 (HABITUALMENTE)</b>	<b>5 (SIEMPRE)</b>					
<b>1. CALIDAD DE TRABAJO:</b> CONOCE LOS TEMAS DEL ÁREA DE LA CUAL ES RESPONSABLE, COMPRENDIENDO LA ESENCIA DE LOS ASPECTOS COMPLEJOS PARA TRANSFORMARLOS EN SOLUCIONES PRÁCTICAS, Y OPERABLES PARA LA ORGANIZACIÓN.										
DEFINE OBJETIVOS CLAROS, Y DISEÑA PROCESOS ADECUADOS, PRÁCTICOS, Y OPERABLES EN BENEFICIO DE TODOS.			X							

TRABAJA CON ALTOS ESTÁNDARES DE CALIDAD Y RESULTADOS.				X	
SE MANTIENE INFORMADO Y CAPACITADO, DESEMPEÑÁNDOSE CON ALTA EFICACIA EN LOS CONTEXTOS CAMBIANTES DE LA ORGANIZACIÓN.			X		
APORTA IDEAS Y CONOCIMIENTOS A LA ORGANIZACIÓN.				X	
<b>2. CAPACIDAD PARA APRENDER:</b> ASIMILA NUEVA INFORMACIÓN Y LA APLICA EFICAZMENTE, RELACIONANDO LA INCORPORACIÓN DE NUEVOS ESQUEMAS A SU REPERTORIO DE CONDUCTAS HABITUALES.					
INNOVA Y PROPONE AL RESTO DE LA ORGANIZACIÓN NUEVAS HERRAMIENTAS, Y PROCEDIMIENTOS QUE CONTRIBUYEN AL MEJORAMIENTO DEL NEGOCIO.				X	
IDENTIFICA NUEVA INFORMACIÓN, TRASLADÁNDOLA A SU ÁMBITO DE TRABAJO.				X	
ES CONSIDERADO UN REFERENTE DENTRO DE LA ORGANIZACIÓN EN EL MOMENTO DE INCORPORAR CAMBIOS REFERIDOS A PROCEDIMIENTOS, HERRAMIENTAS O CONCEPTOS.				X	
ESTÁ ABIERTO A ABANDONAR VIEJAS PRÁCTICAS O MODOS DE LEER LA REALIDAD.				X	
<b>3. HABILIDAD ANALÍTICA (ANÁLISIS DE PRIORIDAD, CRITERIO LÓGICO, SENTIDO COMÚN):</b> REALIZA UN ANÁLISIS LÓGICO, IDENTIFICANDO LOS PROBLEMAS, Y RECONOCIENDO LA INFORMACIÓN SIGNIFICATIVA PARA LA ORGANIZACIÓN.					
COMPRENDE LOS PROCESOS RELATIVOS A SU TRABAJO DENTRO DE LA ORGANIZACIÓN.			X		
IDENTIFICA LA EXISTENCIA DE PROBLEMAS RELACIONADOS CON SU ÁREA.			X		
RECOPILA INFORMACIÓN RELEVANTE, LA ORGANIZA DE FORMA SISTEMÁTICA, Y ESTABLECE RELACIONES CAUSALES.				X	
ESTABLECE RELACIONES ENTRE DATOS NUMÉRICOS Y CONCEPTUALES, PERMITIÉNDOLE RESOLVER PROBLEMAS.				X	
<b>4. CONCIENCIA ORGANIZACIONAL:</b> RECONOCE LOS ATRIBUTOS Y LAS MODIFICACIONES DE LA ORGANIZACIÓN, COMPRENDIENDO E INTERPRETANDO LAS RELACIONES DE PODER DENTRO DE ESTA.					
CONOCE LOS ATRIBUTOS DE LA ORGANIZACIÓN, CAPTANDO CON FACILIDAD LAS MODIFICACIONES QUE EN ELLA SE PRODUCEN.				X	
PRIORIZA LA IMAGEN Y OBJETIVOS ORGANIZACIONALES POR SOBRE SUS OBJETIVOS PERSONALES.				X	
CONSTRUYE REDES DE PERSONAS, DENTRO Y FUERA DE LA ORGANIZACIÓN, A FIN DE QUE PUEDAN APORTARLE INFORMACIÓN VALIOSA PARA LA EMPRESA.				X	
COMPRENDE E INTERPRETA CABALMENTE LAS RELACIONES DE PODER EN Y ENTRE LOS DIFERENTES ACTORES (INTERNAOS Y EXTERNOS) QUE PARTICIPAN EN EL NEGOCIO.				X	
<b>5. ORIENTACIÓN A LOS RESULTADOS:</b> ENCAMAÑA SUS ACTOS AL LOGRO DE LO ESPERADO, ACTUANDO CON VELOCIDAD Y SENTIDO DE URGENCIA ANTE DECISIONES IMPORTANTES PARA SATISFACER LAS NECESIDADES DEL CLIENTE, SUPERAR A LOS COMPETIDORES, O MEJORAR LA ORGANIZACIÓN.					
TRABAJA CON OBJETIVOS ESTABLECIDOS, REALISTAS, Y DESAFIANTES.			X		
BRINDA ORIENTACIÓN Y RETROALIMENTACIÓN A SUS COMPAÑEROS DE TRABAJO ACERCA DE SU DESEMPEÑO.				X	
ACTÚA CON VELOCIDAD Y SENTIDO DE URGENCIA ANTE SITUACIONES QUE REQUIEREN ANTICIARSE A LOS COMPETIDORES O RESPONDER A LAS NECESIDADES DE LOS CLIENTES.				X	

PLANIFICA SU ACTIVIDAD, BUSCANDO INCREMENTAR LA COMPETITIVIDAD DE LA ORGANIZACIÓN.			X		
<b>6. ADAPTABILIDAD AL CAMBIO:</b> SE ADAPTA Y AMOLDA A LOS CAMBIOS, MODIFICANDO LA PROPIA CONDUCTA PARA ALCANZAR DETERMINADOS OBJETIVOS CUANDO SURGEN DIFICULTADES, NUEVOS DATOS O CAMBIOS EN EL MEDIO.					
TIENE UNA AMPLIA VISIÓN DEL MERCADO Y DEL NEGOCIO, QUE LE PERMITE ANTICIARSE EN LA COMPRENSIÓN DE LOS CAMBIOS QUE SE REQUERIRÁN DENTRO DE LAS POLÍTICAS Y OBJETIVOS DE LA ORGANIZACIÓN.					X
MODIFICA ESTRATEGIAS Y OBJETIVOS DE LA ORGANIZACIÓN, CON CELERIDAD ANTE CAMBIOS EXTERNOS O NUEVAS NECESIDADES.					X
SE ADAPTA CON VERSATILIDAD, EFICIENCIA, Y VELOCIDAD A DISTINTOS CONTEXTOS SITUACIONALES, MEDIOS Y PERSONAS.					X
PROMUEVE LA ADAPTABILIDAD AL CAMBIO ENTRE SU EQUIPO DE TRABAJO.					X
<b>7. ÉTICA:</b> SIENTE Y ACTÚA CONSECUENTEMENTE CON LOS VALORES MORALES, Y LAS BUENAS COSTUMBRES Y PRÁCTICAS PROFESIONALES.					
ESTRUCTURA LA VISIÓN Y MISIÓN ORGANIZACIONALES SOBRE LA BASE DE VALORES MORALES.			X		
ESTABLECE UN MARCO DE TRABAJO QUE RESPETA LAS POLÍTICAS DE LA ORGANIZACIÓN, LOS VALORES MORALES, LAS BUENAS COSTUMBRES Y PRÁCTICAS PROFESIONALES.			X		
SE LE RECONOCE POR SER FIEL A SUS PRINCIPIOS, TANTO EN LO LABORAL COMO EN LOS ÁMBITOS DE SU VIDA.			X		
APORTA Y PROVEE IDEAS PARA MEJORAR EL ACCIONAR DE LA EMPRESA, ADECUÁNDOLO A LOS VALORES Y PRINCIPIOS COMUNES.					X
<b>8. RESPONSABILIDAD:</b> SE COMPROMETE EN LA REALIZACIÓN DE LAS TAREAS ASIGNADAS. SU INTERÉS POR EL CUMPLIMIENTO DE LO ASIGNADO ESTÁ POR ENCIMA DE SUS PROPIOS INTERESES.					
SE FIJA OBJETIVOS QUE SIEMPRE CUMPLE, AUTOEXIGIÉNDOSE PLAZOS Y MEJORANDO LA CALIDAD DEL TRABAJO O PROYECTO.			X		
MODIFICA CON BUENA PREDISPONSIÓN LA ORGANIZACIÓN DE SUS TIEMPOS PARA CUMPLIR CON LAS TAREAS ASIGNADAS.			X		
PREFIERE ORGANIZAR, EN PRIMER LUGAR, SUS TAREAS, Y LUEGO DISTRIBUIR EL TIEMPO LIBRE PARA DEDICARSE A OTRAS ACTIVIDADES.			X		
ANTEPONE EL TRABAJO A LAS ACTIVIDADES PERSONALES, AÚN SIN QUE SE LE PIDA, Y EVALÚA ATINADAMENTE LAS OCASIONES EN QUE SE REQUIERE DE SU ESFUERZO EXTRA.			X		
<b>9. TOLERANCIA A LA PRESIÓN:</b> SIGUE ACTUANDO CON EFICACIA EN SITUACIONES DE PRESIÓN DE TIEMPO Y DE DESACUERDO, OPOSICIÓN Y DIVERSIDAD, TRABAJADO CON ALTO DESEMPEÑO EN SITUACIONES DE ALTA EXIGENCIA.					
RESUELVE EFICIENTEMENTE SUS TAREAS AUN CUANDO CONVERGEN AL MISMO TIEMPO PROBLEMAS U OBSTÁCULOS QUE LE EXIGEN MAYORES ESFUERZOS.					X

MUESTRA SU PREDISPOSICIÓN Y ACTITUD POSITIVA, Y LA TRANSMITE A SUS COMPAÑEROS DE TRABAJO AÚN EN SITUACIONES ESTRESANTES.				X					
PROVEE ALTERNATIVAS PARA EL LOGRO DE LA TAREA, MANTENIENDO LA CALIDAD DESEADA EN SITUACIONES DE ALTA EXIGENCIA.				X					
SE CONDUCE CON PROFESIONALISMO, SIN EXTERIORIZAR DESBORDES EMOCIONALES, EN ÉPOCAS DE TRABAJO QUE REQUIEREN MAYOR ESFUERZO.					X				
<b>10. ORIENTACIÓN AL CLIENTE:</b> AYUDA A LOS CLIENTES, COMPRENDIENDO Y SATISFACIENDO SUS NECESIDADES.									
EL CUIDADO DEL CLIENTE FORMA PARTE DE SU ESTRATEGIA DE TRABAJO.				X					
PLANIFICA SUS ACCIONES CONSIDERANDO LAS NECESIDADES DE LOS CLIENTES.			X						
INDAGA E INFORMA SOBRE NECESIDADES ACTUALES Y POTENCIALES DE LOS CLIENTES.				X					
PRIORIZA LA RELACIÓN A LARGO PLAZO CON EL CLIENTE POR SOBRE BENEFICIOS INMEDIATOS U OCASIONALES.					X				
<b>11. TRABAJO EN EQUIPO:</b> PARTICIPA ACTIVAMENTE EN LA BÚSQUEDA DE UNA META COMÚN, SUBORDINANDO LOS INTERESES PERSONALES A LOS OBJETIVOS DEL EQUIPO.									
ESTA DISPUESTO AL INTERCAMBIO DE INFORMACIÓN CON LOS MIEMBROS DE SU EQUIPO.					X				
MANTIENE SU NIVEL DE RENDIMIENTO EN TAREAS QUE REQUIEREN DE RELACIONES INTERPERSONALES.					X				
ES ABIERTO A RECIBIR NUEVOS COMPAÑEROS EN SU ÁREA DE TRABAJO, COLABORANDO CON ELLOS PARA QUE SE PONGAN RÁPIDAMENTE AL TANTO DE LAS ACTIVIDADES DEL SECTOR.				X					
SE PREOCUPA POR LOGRAR CONSENSO, Y CUIDA QUE NO SE IMPONGAN MODALIDADES DE TRABAJO ARBITRARIAMENTE.					X				
<b>VI. SÍRVASE INDICAR ALGUNAS FORTALEZAS Y OPORTUNIDADES DE MEJORA SOBRE LAS COMPETENCIAS GENERALES DE LA PERSONA EVALUADA:</b>									
<b>FORTALEZAS</b>		<b>OPORTUNIDADES DE MEJORA</b>							
Es una persona muy ordenada que le gusta estar analizando lo que hace cada vez. Se adapta muy fácilmente a los cambios, siguiendo el hilo de los procesos. Se enfoca mucho en los resultados.		Puede llegar hacer una persona muy trabajadora que olvida las relaciones personales con sus compañeros. Puede llegar hacer muy tirano con algunas tareas.							
<b>VII. ¿QUÉ LE SUGERIRÍA A LA PERSONA EVALUADA PARA MEJORAR SUS COMPETENCIAS GENERALES?</b>									
<b>SUGERENCIAS</b>									
Puede mejorar bastante en la comunicación con sus compañeros para mejorar con sus relaciones y llegar hacer mejor persona.									

<b>I. CONCEPTO</b>	
LA EVALUACIÓN DE COMPETENCIAS GENERALES, ES UNA HERRAMIENTA DE RETROALIMENTACIÓN, MEDIANTE EL CUAL SE RECOGEN EVIDENCIAS SOBRE LAS COMPETENCIAS GENERALES DEL EVALUADO. EL PROPÓSITO DE LA EVALUACIÓN DE COMPETENCIAS GENERALES ES DAR INFORMACIÓN AL EVALUADO SOBRE LA PERTINENCIA DE SUS COMPETENCIAS EN UN CONTEXTO LABORAL, CON LA FINALIDAD DE AYUDARLO A MEJORAR LOS RESULTADOS DE SU DESEMPEÑO PERSONAL Y PROFESIONAL.	
<b>II. DATOS DEL EVALUADO</b>	
<b>NOMBRE</b>	Raul Rivera
<b>ÁREA</b>	Operaciones
<b>CARGO</b>	Gerente de operaciones
<b>III. DATOS DEL EVALUADOR</b>	
<b>RELACIÓN CON EL EVALUADO ( MARCAR CON UNA X)</b>	

<b>Jefe</b>	
<b>SUPERVISADO</b>	
<b>CLIENTE</b>	
<b>COLEGAS</b>	X
<b>AUTEOVALUACIÓN</b>	

#### **IV. COMPETENCIAS**

"LAS COMPETENCIAS ESTÁN RELACIONADAS CON LAS ACTITUDES, HABILIDADES, Y OTRAS CARACTERÍSTICAS PERSONALES QUE AFECTAN UNA PARTE IMPORTANTE DEL RENDIMIENTO EN EL TRABAJO (ES DECIR, UNO O MÁS ROLES O RESPONSABILIDADES CLAVES), SE PUEDE MEDIR CON ESTÁNDARES ACEPTADOS, Y SE PUEDEN MEJORAR A TRAVÉS DEL ENTRENAMIENTO Y DESARROLLO" (PMI®, 2002).

#### **V. COMPETENCIAS GENERALES**

"SON LOS COMPORTAMIENTOS ASOCIADOS A DESEMPEÑOS COMUNES A DIVERSAS ORGANIZACIONES Y RAMAS DE ACTIVIDAD PRODUCTIVA, DENTRO DE ESTA DEFINICIÓN SE ENGLOBAN TODAS AQUELLAS CAPACIDADES DE CARÁCTER GENERALISTA, EN EL SENTIDO DE QUE NO ESTARÍAN ORIENTADAS AL DESARROLLO DE NINGUNA TAREA LABORAL ESPECÍFICA, SINO QUE CONSTITUIRÍAN LA BASE DEL SABER PROFESIONAL" (OIT, 2007).

<b>DESCRIPCIÓN</b>	<b>CALIFICACIÓN</b>				
	<b>1 (NUNCA)</b>	<b>2 (POCO)</b>	<b>3 (MEDIANAMENTE)</b>	<b>4 (HABITUALMENTE)</b>	<b>5 (SIEMPRE)</b>
<b>1. CALIDAD DE TRABAJO:</b> CONOCE LOS TEMAS DEL ÁREA DE LA CUAL ES RESPONSABLE, COMPRENDIENDO LA ESENCIA DE LOS ASPECTOS COMPLEJOS PARA TRANSFORMARLOS EN SOLUCIONES PRÁCTICAS, Y OPERABLES PARA LA ORGANIZACIÓN.					
DEFINE OBJETIVOS CLAROS, Y DISEÑA PROCESOS ADECUADOS, PRÁCTICOS, Y OPERABLES EN BENEFICIO DE TODOS.				X	
TRABAJA CON ALTOS ESTÁNDARES DE CALIDAD Y RESULTADOS.				X	
SE MANTIENE INFORMADO Y CAPACITADO, DESEMPEÑÁNDOSE CON ALTA EFICACIA EN LOS CONTEXTOS CAMBIANTES DE LA ORGANIZACIÓN.				X	
APORTA IDEAS Y CONOCIMIENTOS A LA ORGANIZACIÓN.					X
<b>2. CAPACIDAD PARA APRENDER:</b> ASIMILA NUEVA INFORMACIÓN Y LA APLICA EFICAZMENTE, RELACIONANDO LA INCORPORACIÓN DE NUEVOS ESQUEMAS A SU REPERTORIO DE CONDUCTAS HABITUALES.					
INNOVA Y PROPONE AL RESTO DE LA ORGANIZACIÓN NUEVAS HERRAMIENTAS, Y PROCEDIMIENTOS QUE CONTRIBUYEN AL MEJORAMIENTO DEL NEGOCIO.				X	
IDENTIFICA NUEVA INFORMACIÓN, TRASLADÁNDOLA A SU ÁMBITO DE TRABAJO.					X
ES CONSIDERADO UN REFERENTE DENTRO DE LA ORGANIZACIÓN EN EL MOMENTO DE INCORPORAR CAMBIOS REFERIDOS A PROCEDIMIENTOS, HERRAMIENTAS O CONCEPTOS.					X
ESTÁ ABIERTO A ABANDONAR VIEJAS PRÁCTICAS O MODOS DE LEER LA REALIDAD.				X	
<b>3. HABILIDAD ANALÍTICA (ANÁLISIS DE PRIORIDAD, CRITERIO LÓGICO, SENTIDO COMÚN):</b> REALIZA UN ANÁLISIS LÓGICO, IDENTIFICANDO LOS PROBLEMAS, Y RECONOCIENDO LA INFORMACIÓN SIGNIFICATIVA PARA LA ORGANIZACIÓN.					
COMPRENDE LOS PROCESOS RELATIVOS A SU TRABAJO DENTRO DE LA ORGANIZACIÓN.				X	
IDENTIFICA LA EXISTENCIA DE PROBLEMAS RELACIONADOS CON SU ÁREA.				X	
RECOPILA INFORMACIÓN RELEVANTE, LA ORGANIZA DE FORMA SISTEMÁTICA, Y ESTABLECE RELACIONES CAUSALES.				X	
ESTABLECE RELACIONES ENTRE DATOS NUMÉRICOS Y CONCEPTUALES, PERMITIÉNDOLE RESOLVER PROBLEMAS.					X

<b>4. CONCIENCIA ORGANIZACIONAL:</b> RECONOCE LOS ATRIBUTOS Y LAS MODIFICACIONES DE LA ORGANIZACIÓN, COMPRENDIENDO E INTERPRETANDO LAS RELACIONES DE PODER DENTRO DE ESTA.					
CONOCE LOS ATRIBUTOS DE LA ORGANIZACIÓN, CAPTANDO CON FACILIDAD LAS MODIFICACIONES QUE EN ELLA SE PRODUCEN.				X	
PRIORIZA LA IMAGEN Y OBJETIVOS ORGANIZACIONALES POR SOBRE SUS OBJETIVOS PERSONALES.				X	
CONSTRUYE REDES DE PERSONAS, DENTRO Y FUERA DE LA ORGANIZACIÓN, A FIN DE QUE PUEDAN APORTARLE INFORMACIÓN VALIOSA PARA LA EMPRESA.					X
COMPRENDE E INTERPRETA CABALMENTE LAS RELACIONES DE PODER EN Y ENTRE LOS DIFERENTES ACTORES (INTERNAOS Y EXTERNOS) QUE PARTICIPAN EN EL NEGOCIO.				X	
<b>5. ORIENTACIÓN A LOS RESULTADOS:</b> ENCAMAÑA SUS ACTOS AL LOGRO DE LO ESPERADO, ACTUANDO CON VELOCIDAD Y SENTIDO DE URGENCIA ANTE DECISIONES IMPORTANTES PARA SATISFACER LAS NECESIDADES DEL CLIENTE, SUPERAR A LOS COMPETIDORES, O MEJORAR LA ORGANIZACIÓN.					
TRABAJA CON OBJETIVOS ESTABLECIDOS, REALISTAS, Y DESAFIANTES.				X	
BRINDA ORIENTACIÓN Y RETROALIMENTACIÓN A SUS COMPAÑEROS DE TRABAJO ACERCA DE SU DESEMPEÑO.				X	
ACTÚA CON VELOCIDAD Y SENTIDO DE URGENCIA ANTE SITUACIONES QUE REQUIEREN ANTICIPARSE A LOS COMPETIDORES O RESPONDER A LAS NECESIDADES DE LOS CLIENTES.				X	
PLANIFICA SU ACTIVIDAD, BUSCANDO INCREMENTAR LA COMPETITIVIDAD DE LA ORGANIZACIÓN.				X	
<b>6. ADAPTABILIDAD AL CAMBIO:</b> SE ADAPTA Y AMOLDA A LOS CAMBIOS, MODIFICANDO LA PROPIA CONDUCTA PARA ALCANZAR DETERMINADOS OBJETIVOS CUANDO SURGEN DIFICULTADES, NUEVOS DATOS O CAMBIOS EN EL MEDIO.					
TIENE UNA AMPLIA VISIÓN DEL MERCADO Y DEL NEGOCIO, QUE LE PERMITE ANTICIPARSE EN LA COMPRENSIÓN DE LOS CAMBIOS QUE SE REQUERIRÁN DENTRO DE LAS POLÍTICAS Y OBJETIVOS DE LA ORGANIZACIÓN.			X		
MODIFICA ESTRATEGIAS Y OBJETIVOS DE LA ORGANIZACIÓN, CON CELERIDAD ANTE CAMBIOS EXTERNOS O NUEVAS NECESIDADES.				X	
SE ADAPTA CON VERSATILIDAD, EFICIENCIA, Y VELOCIDAD A DISTINTOS CONTEXTOS SITUACIONALES, MEDIOS Y PERSONAS.				X	
PROMUEVE LA ADAPTABILIDAD AL CAMBIO ENTRE SU EQUIPO DE TRABAJO.					X
<b>7. ÉTICA:</b> SIENTE Y ACTÚA CONSECUENTEMENTE CON LOS VALORES MORALES, Y LAS BUENAS COSTUMBRES Y PRÁCTICAS PROFESIONALES.					
ESTRUCTURA LA VISIÓN Y MISIÓN ORGANIZACIONALES SOBRE LA BASE DE VALORES MORALES.				X	
ESTABLECE UN MARCO DE TRABAJO QUE RESPETA LAS POLÍTICAS DE LA ORGANIZACIÓN, LOS VALORES MORALES, LAS BUENAS COSTUMBRES Y PRÁCTICAS PROFESIONALES.				X	
SE LE RECONOCE POR SER FIEL A SUS PRINCIPIOS, TANTO EN LO LABORAL COMO EN LOS ÁMBITOS DE SU VIDA.				X	

<i>APORTA Y PROVEE IDEAS PARA MEJORAR EL ACCIONAR DE LA EMPRESA, ADECUÁNDOLA A LOS VALORES Y PRINCIPIOS COMUNES.</i>				X	
<b>8. RESPONSABILIDAD:</b> <i>SE COMPROMETE EN LA REALIZACIÓN DE LAS TAREAS ASIGNADAS. SU INTERÉS POR EL CUMPLIMIENTO DE LO ASIGNADO ESTÁ POR ENCIMA DE SUS PROPIOS INTERESES.</i>					
<i>SE FIJA OBJETIVOS QUE SIEMPRE CUMPLE, AUTOEXIGIÉNDOSE PLAZOS Y MEJORANDO LA CALIDAD DEL TRABAJO O PROYECTO.</i>				X	
<i>MODIFICA CON BUENA PREDISPOSICIÓN LA ORGANIZACIÓN DE SUS TIEMPOS PARA CUMPLIR CON LAS TAREAS ASIGNADAS.</i>			X		
<i>PREFIERE ORGANIZAR, EN PRIMER LUGAR, SUS TAREAS, Y LUEGO DISTRIBUIR EL TIEMPO LIBRE PARA DEDICARSE A OTRAS ACTIVIDADES.</i>				X	
<i>ANTEPONE EL TRABAJO A LAS ACTIVIDADES PERSONALES, AÚN SIN QUE SE LE PIDA, Y EVALÚA ATINADAMENTE LAS OCASIONES EN QUE SE REQUIERE DE SU ESFUERZO EXTRA.</i>					X
<b>9. TOLERANCIA A LA PRESIÓN:</b> <i>SIGUE ACTUANDO CON EFICACIA EN SITUACIONES DE PRESIÓN DE TIEMPO Y DE DESACUERDO, OPOSICIÓN Y DIVERSIDAD, TRABAJADO CON ALTO DESEMPEÑO EN SITUACIONES DE ALTA EXIGENCIA.</i>					
<i>RESUELVE EFICIENTEMENTE SUS TAREAS AUN CUANDO CONVERGEN AL MISMO TIEMPO PROBLEMAS U OBSTÁCULOS QUE LE EXIGEN MAYORES ESFUERZOS.</i>					X
<i>MUESTRA SU PREDISPOSICIÓN Y ACTITUD POSITIVA, Y LA TRANSMITE A SUS COMPAÑEROS DE TRABAJO AÚN EN SITUACIONES ESTRESANTES.</i>					X
<i>PROVEE ALTERNATIVAS PARA EL LOGRO DE LA TAREA, MANTENIENDO LA CALIDAD DESEADA EN SITUACIONES DE ALTA EXIGENCIA.</i>					X
<i>SE CONDUCE CON PROFESIONALISMO, SIN EXTERIORIZAR DESBORDES EMOCIONALES, EN ÉPOCAS DE TRABAJO QUE REQUIEREN MAYOR ESFUERZO.</i>					X
<b>10. ORIENTACIÓN AL CLIENTE:</b> <i>AYUDA A LOS CLIENTES, COMPRENDIENDO Y SATISFACIENDO SUS NECESIDADES.</i>					
<i>EL CUIDADO DEL CLIENTE FORMA PARTE DE SU ESTRATEGIA DE TRABAJO.</i>				X	
<i>PLANIFICA SUS ACCIONES CONSIDERANDO LAS NECESIDADES DE LOS CLIENTES.</i>			X		
<i>INDAGA E INFORMA SOBRE NECESIDADES ACTUALES Y POTENCIALES DE LOS CLIENTES.</i>			X		
<i>PRIORIZA LA RELACIÓN A LARGO PLAZO CON EL CLIENTE POR SOBRE BENEFICIOS INMEDIATOS U OCASIONALES.</i>		X			
<b>11. TRABAJO EN EQUIPO:</b> <i>PARTICIPA ACTIVAMENTE EN LA BÚSQUEDA DE UNA META COMÚN, SUBORDINANDO LOS INTERESES PERSONALES A LOS OBJETIVOS DEL EQUIPO.</i>					
<i>ESTA DISPUESTO AL INTERCAMBIO DE INFORMACIÓN CON LOS MIEMBROS DE SU EQUIPO.</i>				X	
<i>MANTIENE SU NIVEL DE RENDIMIENTO EN TAREAS QUE REQUIEREN DE RELACIONES INTERPERSONALES.</i>				X	
<i>ES ABIERTO A RECIBIR NUEVOS COMPAÑEROS EN SU ÁREA DE TRABAJO, COLABORANDO CON ELLOS PARA QUE SE PONGAN RÁPIDAMENTE AL TANTO DE LAS ACTIVIDADES DEL SECTOR.</i>				X	
<i>SE PREOCUPA POR LOGRAR CONSENSO, Y CUIDA QUE NO SE IMPONGAN MODALIDADES DE TRABAJO ARBITRARIAMENTE.</i>				X	
<b>VI. SÍRVASE INDICAR ALGUNAS FORTALEZAS Y OPORTUNIDADES DE MEJORA SOBRE LAS COMPETENCIAS GENERALES DE LA PERSONA EVALUADA:</b>					
<b>FORTALEZAS</b>			<b>OPORTUNIDADES DE MEJORA</b>		

Es una persona enfocada en el trabajo. Es una persona muy responsable que dedica bastante tiempo en enfocarse que toda operación se lleve a cabo a tiempo y bien hecha.	Su falta de relación con los clientes lo vuelve alguien propenso a no simpatizar con los clientes.
<b>VII. ¿QUÉ LE SUGERIRÍA A LA PERSONA EVALUADA PARA MEJORAR SUS COMPETENCIAS GENERALES?</b>	
<b>SUGERENCIAS</b>	
La relación con los clientes es de suma importancia y si debe rendir cuentas debe considerar una buena relación	

<b>I. CONCEPTO</b>					
<p><i>LA EVALUACIÓN DE COMPETENCIAS GENERALES, ES UNA HERRAMIENTA DE RETROALIMENTACIÓN, MEDIANTE EL CUAL SE RECOGEN EVIDENCIAS SOBRE LAS COMPETENCIAS GENERALES DEL EVALUADO. EL PROPÓSITO DE LA EVALUACIÓN DE COMPETENCIAS GENERALES ES DAR INFORMACIÓN AL EVALUADO SOBRE LA PERTINENCIA DE SUS COMPETENCIAS EN UN CONTEXTO LABORAL, CON LA FINALIDAD DE AYUDARLO A MEJORAR LOS RESULTADOS DE SU DESEMPEÑO PERSONAL Y PROFESIONAL.</i></p>					
<b>II. DATOS DEL EVALUADO</b>					
<b>NOMBRE</b>	Diego Coc				
<b>ÁREA</b>	Seguridad				
<b>CARGO</b>	Analista de seguridad				
<b>III. DATOS DEL EVALUADOR</b>					
<b>RELACIÓN CON EL EVALUADO ( MARCAR CON UNA X)</b>					
<b>Jefe</b>	X				
<b>Supervisado</b>					
<b>Cliente</b>					
<b>Colega</b>					
<b>Autoevaluación</b>					
<b>IV. COMPETENCIAS</b>					
<p>"LAS COMPETENCIAS ESTÁN RELACIONADAS CON LAS ACTITUDES, HABILIDADES, Y OTRAS CARACTERÍSTICAS PERSONALES QUE AFECTAN UNA PARTE IMPORTANTE DEL RENDIMIENTO EN EL TRABAJO (ES DECIR, UNO O MÁS ROLES O RESPONSABILIDADES CLAVES), SE PUEDE MEDIR CON ESTÁNDARES ACEPTADOS, Y SE PUEDEN MEJORAR A TRAVÉS DEL ENTRENAMIENTO Y DESARROLLO" (PMI®, 2002).</p>					
<b>V. COMPETENCIAS GENERALES</b>					
<p>"SON LOS COMPORTAMIENTOS ASOCIADOS A DESEMPEÑOS COMUNES A DIVERSAS ORGANIZACIONES Y RAMAS DE ACTIVIDAD PRODUCTIVA, DENTRO DE ESTA DEFINICIÓN SE ENGLOBAN TODAS AQUELLAS CAPACIDADES DE CARÁCTER GENERALISTA, EN EL SENTIDO DE QUE NO ESTARÍAN ORIENTADAS AL DESARROLLO DE NINGUNA TAREA LABORAL ESPECÍFICA, SINO QUE CONSTITUIRÍAN LA BASE DEL SABER PROFESIONAL" (OIT, 2007).</p>					
<b>DESCRIPCIÓN</b>	<b>CALIFICACIÓN</b>				
	<b>1 (NUNCA)</b>	<b>2 (Poco)</b>	<b>3 (MEDIANA MENTE)</b>	<b>4 (HABITUAL MENTE)</b>	<b>5 (SIEMPRE)</b>
<b>1. CALIDAD DE TRABAJO:</b> CONOCE LOS TEMAS DEL ÁREA DE LA CUAL ES RESPONSABLE, COMPRENDIENDO LA ESENCIA DE LOS ASPECTOS COMPLEJOS PARA TRANSFORMARLOS EN SOLUCIONES PRÁCTICAS, Y OPERABLES PARA LA ORGANIZACIÓN.			X		
DEFINE OBJETIVOS CLAROS, Y DISEÑA PROCESOS ADECUADOS, PRÁCTICOS, Y OPERABLES EN BENEFICIO DE TODOS.			X		
TRABAJA CON ALTOS ESTÁNDARES DE CALIDAD Y RESULTADOS.			X		
SE MANTIENE INFORMADO Y CAPACITADO, DESEMPEÑÁNDOSE CON ALTA EFICACIA EN LOS CONTEXTOS CAMBIANTES DE LA ORGANIZACIÓN.			X		
APORTA IDEAS Y CONOCIMIENTOS A LA ORGANIZACIÓN.			X		
<b>2. CAPACIDAD PARA APRENDER:</b> ASIMILA NUEVA INFORMACIÓN Y LA APLICA EFICAZMENTE, RELACIONANDO LA INCORPORACIÓN DE NUEVOS ESQUEMAS A SU REPERTORIO DE CONDUCTAS HABITUALES.					

<i>INNOVA Y PROPONE AL RESTO DE LA ORGANIZACIÓN NUEVAS HERRAMIENTAS, Y PROCEDIMIENTOS QUE CONTRIBUYEN AL MEJORAMIENTO DEL NEGOCIO.</i>				X	
<i>IDENTIFICA NUEVA INFORMACIÓN, TRASLADÁNDOLA A SU ÁMBITO DE TRABAJO.</i>				X	
<i>ES CONSIDERADO UN REFERENTE DENTRO DE LA ORGANIZACIÓN EN EL MOMENTO DE INCORPORAR CAMBIOS REFERIDOS A PROCEDIMIENTOS, HERRAMIENTAS O CONCEPTOS.</i>				X	
<i>ESTÁ ABIERTO A ABANDONAR VIEJAS PRÁCTICAS O MODOS DE LEER LA REALIDAD.</i>			X		
<b>3. HABILIDAD ANALÍTICA (ANÁLISIS DE PRIORIDAD, CRITERIO LÓGICO, SENTIDO COMÚN):</b> REALIZA UN ANÁLISIS LÓGICO, IDENTIFICANDO LOS PROBLEMAS, Y RECONOCIENDO LA INFORMACIÓN SIGNIFICATIVA PARA LA ORGANIZACIÓN.					
<i>COMPRENDE LOS PROCESOS RELATIVOS A SU TRABAJO DENTRO DE LA ORGANIZACIÓN.</i>			X		
<i>IDENTIFICA LA EXISTENCIA DE PROBLEMAS RELACIONADOS CON SU ÁREA.</i>			X		
<i>RECOPILA INFORMACIÓN RELEVANTE, LA ORGANIZA DE FORMA SISTEMÁTICA, Y ESTABLECE RELACIONES CAUSALES.</i>				X	
<i>ESTABLECE RELACIONES ENTRE DATOS NUMÉRICOS Y CONCEPTUALES, PERMITIÉNDOLE RESOLVER PROBLEMAS.</i>				X	
<b>4. CONCIENCIA ORGANIZACIONAL:</b> RECONOCE LOS ATRIBUTOS Y LAS MODIFICACIONES DE LA ORGANIZACIÓN, COMPRENDIENDO E INTERPRETANDO LAS RELACIONES DE PODER DENTRO DE ESTA.					
<i>CONOCE LOS ATRIBUTOS DE LA ORGANIZACIÓN, CAPTANDO CON FACILIDAD LAS MODIFICACIONES QUE EN ELLA SE PRODUCEN.</i>				X	
<i>PRIORIZA LA IMAGEN Y OBJETIVOS ORGANIZACIONALES POR SOBRE SUS OBJETIVOS PERSONALES.</i>				X	
<i>CONSTRUYE REDES DE PERSONAS, DENTRO Y FUERA DE LA ORGANIZACIÓN, A FIN DE QUE PUEDAN APORTARLE INFORMACIÓN VALIOSA PARA LA EMPRESA.</i>			X		
<i>COMPRENDE E INTERPRETA CABALMENTE LAS RELACIONES DE PODER EN Y ENTRE LOS DIFERENTES ACTORES (INTERNAOS Y EXTERNOS) QUE PARTICIPAN EN EL NEGOCIO.</i>				X	
<b>5. ORIENTACIÓN A LOS RESULTADOS:</b> ENCAMAÑA SUS ACTOS AL LOGRO DE LO ESPERADO, ACTUANDO CON VELOCIDAD Y SENTIDO DE URGENCIA ANTE DECISIONES IMPORTANTES PARA SATISFACER LAS NECESIDADES DEL CLIENTE, SUPERAR A LOS COMPETIDORES, O MEJORAR LA ORGANIZACIÓN.					
<i>TRABAJA CON OBJETIVOS ESTABLECIDOS, REALISTAS, Y DESAFIANTES.</i>				X	
<i>BRINDA ORIENTACIÓN Y RETROALIMENTACIÓN A SUS COMPAÑEROS DE TRABAJO ACERCA DE SU DESEMPEÑO.</i>					X
<i>ACTÚA CON VELOCIDAD Y SENTIDO DE URGENCIA ANTE SITUACIONES QUE REQUIEREN ANTICIPARSE A LOS COMPETIDORES O RESPONDER A LAS NECESIDADES DE LOS CLIENTES.</i>					X
<i>PLANIFICA SU ACTIVIDAD, BUSCANDO INCREMENTAR LA COMPETITIVIDAD DE LA ORGANIZACIÓN.</i>				X	
<b>6. ADAPTABILIDAD AL CAMBIO:</b> SE ADAPTA Y AMOLDA A LOS CAMBIOS, MODIFICANDO LA PROPIA CONDUCTA PARA ALCANZAR DETERMINADOS OBJETIVOS CUANDO SURGEN DIFICULTADES, NUEVOS DATOS O CAMBIOS EN EL MEDIO.					

TIENE UNA AMPLIA VISIÓN DEL MERCADO Y DEL NEGOCIO, QUE LE PERMITE ANTICIPARSE EN LA COMPRENSIÓN DE LOS CAMBIOS QUE SE REQUERIRÁN DENTRO DE LAS POLÍTICAS Y OBJETIVOS DE LA ORGANIZACIÓN.				X	
MODIFICA ESTRATEGIAS Y OBJETIVOS DE LA ORGANIZACIÓN, CON CELERIDAD ANTE CAMBIOS EXTERNOS O NUEVAS NECESIDADES.				X	
SE ADAPTA CON VERSATILIDAD, EFICIENCIA, Y VELOCIDAD A DISTINTOS CONTEXTOS SITUACIONALES, MEDIOS Y PERSONAS.					X
PROMUEVE LA ADAPTABILIDAD AL CAMBIO ENTRE SU EQUIPO DE TRABAJO.				X	
<b>7. ÉTICA:</b> SIENTE Y ACTÚA CONSECUENTEMENTE CON LOS VALORES MORALES, Y LAS BUENAS COSTUMBRES Y PRÁCTICAS PROFESIONALES.					
ESTRUCTURA LA VISIÓN Y MISIÓN ORGANIZACIONALES SOBRE LA BASE DE VALORES MORALES.					X
ESTABLECE UN MARCO DE TRABAJO QUE RESPETA LAS POLÍTICAS DE LA ORGANIZACIÓN, LOS VALORES MORALES, LAS BUENAS COSTUMBRES Y PRÁCTICAS PROFESIONALES.				X	
SE LE RECONOCE POR SER FIEL A SUS PRINCIPIOS, TANTO EN LO LABORAL COMO EN LOS ÁMBITOS DE SU VIDA.				X	
APORTA Y PROVEE IDEAS PARA MEJORAR EL ACCIONAR DE LA EMPRESA, ADECUÁNDOLO A LOS VALORES Y PRINCIPIOS COMUNES.					X
<b>8. RESPONSABILIDAD:</b> SE COMPROMETE EN LA REALIZACIÓN DE LAS TAREAS ASIGNADAS. SU INTERÉS POR EL CUMPLIMIENTO DE LO ASIGNADO ESTÁ POR ENCIMA DE SUS PROPIOS INTERESES.					
SE FIJA OBJETIVOS QUE SIEMPRE CUMPLE, AUTOEXIGIÉNDOSE PLAZOS Y MEJORANDO LA CALIDAD DEL TRABAJO O PROYECTO.					X
MODIFICA CON BUENA PREDISPOSICIÓN LA ORGANIZACIÓN DE SUS TIEMPOS PARA CUMPLIR CON LAS TAREAS ASIGNADAS.				X	
PREFIERE ORGANIZAR, EN PRIMER LUGAR, SUS TAREAS, Y LUEGO DISTRIBUIR EL TIEMPO LIBRE PARA DEDICARSE A OTRAS ACTIVIDADES.					X
ANTEPONE EL TRABAJO A LAS ACTIVIDADES PERSONALES, AÚN SIN QUE SE LE PIDA, Y EVALÚA ATINADAMENTE LAS OCASIONES EN QUE SE REQUIERE DE SU ESFUERZO EXTRA.				X	
<b>9. TOLERANCIA A LA PRESIÓN:</b> SIGUE ACTUANDO CON EFICACIA EN SITUACIONES DE PRESIÓN DE TIEMPO Y DE DESACUERDO, OPOSICIÓN Y DIVERSIDAD, TRABAJADO CON ALTO DESEMPEÑO EN SITUACIONES DE ALTA EXIGENCIA.					
RESUELVE EFICIENTEMENTE SUS TAREAS AUN CUANDO CONVERGEN AL MISMO TIEMPO PROBLEMAS U OBSTÁCULOS QUE LE EXIGEN MAYORES ESFUERZOS.			X		
MUESTRA SU PREDISPOSICIÓN Y ACTITUD POSITIVA, Y LA TRANSMITE A SUS COMPAÑEROS DE TRABAJO AÚN EN SITUACIONES ESTRESANTES.		X			
PROVEE ALTERNATIVAS PARA EL LOGRO DE LA TAREA, MANTeniENDO LA CALIDAD DESEADA EN SITUACIONES DE ALTA EXIGENCIA.		X			

SE CONDUCE CON PROFESIONALISMO, SIN EXTERIORIZAR DESBORDES EMOCIONALES, EN ÉPOCAS DE TRABAJO QUE REQUIEREN MAYOR ESFUERZO.		X			
<b>10. ORIENTACIÓN AL CLIENTE:</b> AYUDA A LOS CLIENTES, COMPRENDIENDO Y SATISFACIENDO SUS NECESIDADES.					
EL CUIDADO DEL CLIENTE FORMA PARTE DE SU ESTRATEGIA DE TRABAJO.		X			
PLANIFICA SUS ACCIONES CONSIDERANDO LAS NECESIDADES DE LOS CLIENTES.		X			
INDAGA E INFORMA SOBRE NECESIDADES ACTUALES Y POTENCIALES DE LOS CLIENTES.			X		
PRIORIZA LA RELACIÓN A LARGO PLAZO CON EL CLIENTE POR SOBRE BENEFICIOS INMEDIATOS U OCASIONALES.			X		
<b>11. TRABAJO EN EQUIPO:</b> PARTICIPA ACTIVAMENTE EN LA BÚSQUEDA DE UNA META COMÚN, SUBORDINANDO LOS INTERESES PERSONALES A LOS OBJETIVOS DEL EQUIPO.					
ESTA DISPUESTO AL INTERCAMBIO DE INFORMACIÓN CON LOS MIEMBROS DE SU EQUIPO.			X		
MANTIENE SU NIVEL DE RENDIMIENTO EN TAREAS QUE REQUIEREN DE RELACIONES INTERPERSONALES.			X		
ES ABIERTO A RECIBIR NUEVOS COMPAÑEROS EN SU ÁREA DE TRABAJO, COLABORANDO CON ELLOS PARA QUE SE PONGAN RÁPIDAMENTE AL TANTO DE LAS ACTIVIDADES DEL SECTOR.			X		
SE PREOCUPA POR LOGRAR CONSENSO, Y CUIDA QUE NO SE IMPONGAN MODALIDADES DE TRABAJO ARBITRARIAMENTE.		X			
<b>VI. SÍRVASE INDICAR ALGUNAS FORTALEZAS Y OPORTUNIDADES DE MEJORA SOBRE LAS COMPETENCIAS GENERALES DE LA PERSONA EVALUADA:</b>					
<b>FORTALEZAS</b>			<b>OPORTUNIDADES DE MEJORA</b>		
Es una persona muy hábil en su trabajo que se compromete con realizarlo bien. Es muy responsable y anda siempre al pendiente de la finalización de cada proceso para identificar posibles vulnerabilidades.			Puede ser que trabaje lento debido a que analiza paso por paso. Puede mejorar su metodología para que no sea tan invasiva en algunos procesos.		
<b>VII. ¿QUÉ LE SUGERIRÍA A LA PERSONA EVALUADA PARA MEJORAR SUS COMPETENCIAS GENERALES?</b>					
<b>SUGERENCIAS</b> -----					

CONTROL DE VERSIONES					
Versión	Hecha por	Revisada por	Aprobada por	Fecha	Motivo
1.0	CD	CR	CR	07/03/02	Evaluar competencias

## RESUMEN DE EVALUACIÓN DE COMPETENCIAS GENERALES

NOMBRE DEL PROYECTO	SIGLAS DEL PROYECTO
Aplicación Móvil de Gestión y Atención de Clientes	AMGC

I. CONCEPTO
LA EVALUACIÓN DE COMPETENCIAS GENERALES, ES UNA HERRAMIENTA DE RETROALIMENTACIÓN, MEDIANTE EL CUAL SE RECOGEN EVIDENCIAS SOBRE LAS COMPETENCIAS GENERALES DEL EVALUADO. EL PROPÓSITO DE LA EVALUACIÓN DE COMPETENCIAS GENERALES ES DAR INFORMACIÓN AL EVALUADO SOBRE LA PERTINENCIA DE SUS COMPETENCIAS EN UN CONTEXTO LABORAL, CON LA FINALIDAD DE AYUDARLO A MEJORAR LOS RESULTADOS DE SU DESEMPEÑO PERSONAL Y PROFESIONAL.
II. DATOS DEL EVALUADO

<b>NOMBRE</b>	Luis chan
<b>ÁREA</b>	IT
<b>CARGO</b>	Director IT

### **III. COMPETENCIAS**

"LAS COMPETENCIAS ESTÁN RELACIONADAS CON LAS ACTITUDES, HABILIDADES, Y OTRAS CARACTERÍSTICAS PERSONALES QUE AFECTAN UNA PARTE IMPORTANTE DEL RENDIMIENTO EN EL TRABAJO (ES DECIR, UNO O MÁS ROLES O RESPONSABILIDADES CLAVES), SE PUEDE MEDIR CON ESTÁNDARES ACEPTADOS, Y SE PUEDEN MEJORAR A TRAVÉS DEL ENTRENAMIENTO Y DESARROLLO" (PMI, 2002).

### **IV. COMPETENCIAS GENERALES**

"SON LOS COMPORTAMIENTOS ASOCIADOS A DESEMPEÑOS COMUNES A DIVERSAS ORGANIZACIONES Y RAMAS DE ACTIVIDAD PRODUCTIVA, DENTRO DE ESTA DEFINICIÓN SE ENGLOBAN TODAS AQUELLAS CAPACIDADES DE CARÁCTER GENERALISTA, EN EL SENTIDO DE QUE NO ESTARÍAN ORIENTADAS AL DESARROLLO DE NINGUNA TAREA LABORAL ESPECÍFICA, SINO QUE CONSTITUIRÍAN LA BASE DEL SABER PROFESIONAL" (OIT, 2007).

<b>DESCRIPCIÓN</b>	<b>CALIFICACIÓN</b>				
	<b>1 (NUNCA)</b>	<b>2 (POCO)</b>	<b>3 (MEDIANAMENTE)</b>	<b>4 (HABITUALMENTE)</b>	<b>5 (SIEMPRE)</b>
<b>1. CALIDAD DE TRABAJO:</b> CONOCE LOS TEMAS DEL ÁREA DE LA CUAL ES RESPONSABLE, COMPRENDIENDO LA ESENCIA DE LOS ASPECTOS COMPLEJOS PARA TRANSFORMARLOS EN SOLUCIONES PRÁCTICAS, Y OPERABLES PARA LA ORGANIZACIÓN.			2	2	
<b>2. CAPACIDAD PARA APRENDER:</b> ASIMILA NUEVA INFORMACIÓN Y LA APLICA EFICAZMENTE, RELACIONANDO LA INCORPORACIÓN DE NUEVOS ESQUEMAS A SU REPERTORIO DE CONDUCTAS HABITUALES.		1	1	1	1
<b>3. HABILIDAD ANALÍTICA (ANÁLISIS DE PRIORIDAD, CRITERIO LÓGICO, SENTIDO COMÚN):</b> REALIZA UN ANÁLISIS LÓGICO, IDENTIFICANDO LOS PROBLEMAS, Y RECONOCIENDO LA INFORMACIÓN SIGNIFICATIVA PARA LA ORGANIZACIÓN.			2	2	
<b>4. CONCIENCIA ORGANIZACIONAL:</b> RECONOCE LOS ATRIBUTOS Y LAS MODIFICACIONES DE LA ORGANIZACIÓN, COMPRENDIENDO E INTERPRETANDO LAS RELACIONES DE PODER DENTRO DE ESTA.			1	2	1
<b>5. ORIENTACIÓN A LOS RESULTADOS:</b> ENCAMA SUS ACTOS AL LOGRO DE LO ESPERADO, ACTUANDO CON VELOCIDAD Y SENTIDO DE URGENCIA ANTE DECISIONES IMPORTANTES PARA SATISFACER LAS NECESIDADES DEL CLIENTE, SUPERAR A LOS COMPETIDORES, O MEJORAR LA ORGANIZACIÓN.		1	1	2	
<b>6. ADAPTABILIDAD AL CAMBIO:</b> SE ADAPTA Y AMOLDA A LOS CAMBIOS, MODIFICANDO LA PROPIA CONDUCTA PARA ALCANZAR DETERMINADOS OBJETIVOS CUANDO SURGEN DIFICULTADES, NUEVOS DATOS O CAMBIOS EN EL MEDIO.			1	2	1
<b>7. ÉTICA:</b> SIENTE Y ACTÚA CONSECUENTEMENTE CON LOS VALORES MORALES, Y LAS BUENAS COSTUMBRES Y PRÁCTICAS PROFESIONALES.			2	2	
<b>8. RESPONSABILIDAD:</b> SE COMPROMETE EN LA REALIZACIÓN DE LAS TAREAS ASIGNADAS. SU INTERÉS POR EL CUMPLIMIENTO DE LO ASIGNADO ESTÁ POR ENCIMA DE SUS PROPIOS INTERESES.				3	
<b>9. TOLERANCIA A LA PRESIÓN:</b> SIGUE ACTUANDO CON EFICACIA EN SITUACIONES DE PRESIÓN DE TIEMPO			3	1	

Y DE DESACUERDO, OPOSICIÓN Y DIVERSIDAD, TRABAJADO CON ALTO DESEMPEÑO EN SITUACIONES DE ALTA EXIGENCIA.				
<b>10. ORIENTACIÓN AL CLIENTE:</b> AYUDA A LOS CLIENTES, COMPRENDIENDO Y SATISFACIENDO SUS NECESIDADES.		1	3	
<b>11. TRABAJO EN EQUIPO:</b> PARTICIPA ACTIVAMENTE EN LA BÚSQUEDA DE UNA META COMÚN, SUBORDINANDO LOS INTERESES PERSONALES A LOS OBJETIVOS DEL EQUIPO.			1	3
<b>V. FORTALEZAS Y OPORTUNIDADES DE MEJORA</b>				
<b>FORTALEZAS</b>		<b>OPORTUNIDADES DE MEJORA</b>		
Resulta ser alguien de grandes ideales y con mucha capacidad para trabajar en equipo, aporta buenas ideas y tiene muy buena iniciativa. Es abierto para recibir ideas de otros compañeros.		Podría considerar un poco más al cliente tratándolo de mejor manera y anticiparse a situaciones en donde pueda platicar más. Mejorar sus relaciones con sus inferiores podría mejorar.		
<b>VI. SUGERENCIAS</b>				
Mejorar la relación con los clientes y subordinados.				

<b>I. CONCEPTO</b>					
<i>LA EVALUACIÓN DE COMPETENCIAS GENERALES, ES UNA HERRAMIENTA DE RETROALIMENTACIÓN, MEDIANTE EL CUAL SE RECOGEN EVIDENCIAS SOBRE LAS COMPETENCIAS GENERALES DEL EVALUADO. EL PROPÓSITO DE LA EVALUACIÓN DE COMPETENCIAS GENERALES ES DAR INFORMACIÓN AL EVALUADO SOBRE LA PERTINENCIA DE SUS COMPETENCIAS EN UN CONTEXTO LABORAL, CON LA FINALIDAD DE AYUDARLO A MEJORAR LOS RESULTADOS DE SU DESEMPEÑO PERSONAL Y PROFESIONAL.</i>					
<b>II. DATOS DEL EVALUADO</b>					
<b>NOMBRE</b>	Marta Godínez				
<b>ÁREA</b>	Programas				
<b>CARGO</b>	Director de programas				
<b>III. COMPETENCIAS</b>					
<i>"LAS COMPETENCIAS ESTÁN RELACIONADAS CON LAS ACTITUDES, HABILIDADES, Y OTRAS CARACTERÍSTICAS PERSONALES QUE AFECTAN UNA PARTE IMPORTANTE DEL RENDIMIENTO EN EL TRABAJO (ES DECIR, UNO O MÁS ROLES O RESPONSABILIDADES CLAVES), SE PUEDE MEDIR CON ESTÁNDARES ACEPTADOS, Y SE PUEDEN MEJORAR A TRAVÉS DEL ENTRENAMIENTO Y DESARROLLO" (PMI, 2002).</i>					
<b>IV. COMPETENCIAS GENERALES</b>					
<i>"SON LOS COMPORTAMIENTOS ASOCIADOS A DESEMPEÑOS COMUNES A DIVERSAS ORGANIZACIONES Y RAMAS DE ACTIVIDAD PRODUCTIVA, DENTRO DE ESTA DEFINICIÓN SE ENGLOBAN TODAS AQUELLAS CAPACIDADES DE CARÁCTER GENERALISTA, EN EL SENTIDO DE QUE NO ESTARÍAN ORIENTADAS AL DESARROLLO DE NINGUNA TAREA LABORAL ESPECÍFICA, SINO QUE CONSTITUIRÍAN LA BASE DEL SABER PROFESIONAL" (OIT, 2007).</i>					
<b>DESCRIPCIÓN</b>			<b>CALIFICACIÓN</b>		
			<b>1 (NUNCA)</b>	<b>2 (POCO)</b>	<b>3 (MEDIANA MENTE)</b>
<b>1. CALIDAD DE TRABAJO:</b> Conoce los temas del área de la cual es responsable, comprendiendo la esencia de los aspectos complejos para transformarlos en soluciones prácticas, y operables para la organización.					2
<b>2. CAPACIDAD PARA APRENDER:</b> Asimila nueva información y la aplica eficazmente, relacionando la incorporación de nuevos esquemas a su repertorio de conductas habituales.					2

<b>3. HABILIDAD ANALÍTICA (ANÁLISIS DE PRIORIDAD, CRITERIO LÓGICO, SENTIDO COMÚN):</b> REALIZA UN ANÁLISIS LÓGICO, IDENTIFICANDO LOS PROBLEMAS, Y RECONOCIENDO LA INFORMACIÓN SIGNIFICATIVA PARA LA ORGANIZACIÓN.			3	2					
<b>4. CONCIENCIA ORGANIZACIONAL:</b> RECONOCE LOS ATRIBUTOS Y LAS MODIFICACIONES DE LA ORGANIZACIÓN, COMPRENDIENDO E INTERPRETANDO LAS RELACIONES DE PODER DENTRO DE ESTA.			2	2					
<b>5. ORIENTACIÓN A LOS RESULTADOS:</b> ENCAMA SUS ACTOS AL LOGRO DE LO ESPERADO, ACTUANDO CON VELOCIDAD Y SENTIDO DE URGENCIA ANTE DECISIONES IMPORTANTES PARA SATISFACER LAS NECESIDADES DEL CLIENTE, SUPERAR A LOS COMPETIDORES, O MEJORAR LA ORGANIZACIÓN.			2	2					
<b>6. ADAPTABILIDAD AL CAMBIO:</b> SE ADAPTA Y AMOLDA A LOS CAMBIOS, MODIFICANDO LA PROPIA CONDUCTA PARA ALCANZAR DETERMINADOS OBJETIVOS CUANDO SURGEN DIFICULTADES, NUEVOS DATOS O CAMBIOS EN EL MEDIO.		1	1	2					
<b>7. ÉTICA:</b> SIENTE Y ACTÚA CONSECUENTEMENTE CON LOS VALORES MORALES, Y LAS BUENAS COSTUMBRES Y PRÁCTICAS PROFESIONALES.				1	3				
<b>8. RESPONSABILIDAD:</b> SE COMPROMETE EN LA REALIZACIÓN DE LAS TAREAS ASIGNADAS. SU INTERÉS POR EL CUMPLIMIENTO DE LO ASIGNADO ESTÁ POR ENCIMA DE SUS PROPIOS INTERESES.					4				
<b>9. TOLERANCIA A LA PRESIÓN:</b> SIGUE ACTUANDO CON EFICACIA EN SITUACIONES DE PRESIÓN DE TIEMPO Y DE DESACUERDO, OPOSICIÓN Y DIVERSIDAD, TRABAJADO CON ALTO DESEMPEÑO EN SITUACIONES DE ALTA EXIGENCIA.				4					
<b>10. ORIENTACIÓN AL CLIENTE:</b> AYUDA A LOS CLIENTES, COMPRENDIENDO Y SATISFACIENDO SUS NECESIDADES.		1	2	1					
<b>11. TRABAJO EN EQUIPO:</b> PARTICIPA ACTIVAMENTE EN LA BÚSQUEDA DE UNA META COMÚN, SUBORDINANDO LOS INTERESES PERSONALES A LOS OBJETIVOS DEL EQUIPO.			3	1					
<b>V. FORTALEZAS Y OPORTUNIDADES DE MEJORA</b>									
<b>FORTALEZAS</b>		<b>OPORTUNIDADES DE MEJORA</b>							
Toma la iniciativa ante cualquier problema. Es rápida en tomar decisiones. Tiene precisión con los procesos. Toma de la mejor manera las críticas constructivas. Aporta en ideas en reuniones con los altos mandos.		Podría tener una mejor capacidad de comprensión con sus trabajadores. Puede mejorar con trabajar bajo presión.							
<b>VI. SUGERENCIAS</b>									
Puede mejorar en la comunicación con su equipo y darle un mejor apoyo a los integrantes que lo necesiten.									

<b>I. CONCEPTO</b>
<i>LA EVALUACIÓN DE COMPETENCIAS GENERALES, ES UNA HERRAMIENTA DE RETROALIMENTACIÓN, MEDIANTE EL CUAL SE RECOGEN EVIDENCIAS SOBRE LAS COMPETENCIAS GENERALES DEL EVALUADO. EL PROPÓSITO DE LA EVALUACIÓN DE COMPETENCIAS GENERALES ES DAR INFORMACIÓN AL EVALUADO SOBRE LA PERTINENCIA DE SUS COMPETENCIAS EN UN CONTEXTO LABORAL, CON LA FINALIDAD DE AYUDARLO A MEJORAR LOS RESULTADOS DE SU DESEMPEÑO PERSONAL Y PROFESIONAL.</i>

<b>II. DATOS DEL EVALUADO</b>					
<b>NOMBRE</b>	Diego Ruiz				
<b>ÁREA</b>	Administración				
<b>CARGO</b>	Personal de la oficina de proyectos				
<b>III. COMPETENCIAS</b>					
<p>"LAS COMPETENCIAS ESTÁN RELACIONADAS CON LAS ACTITUDES, HABILIDADES, Y OTRAS CARACTERÍSTICAS PERSONALES QUE AFECTAN UNA PARTE IMPORTANTE DEL RENDIMIENTO EN EL TRABAJO (ES DECIR, UNO O MÁS ROLES O RESPONSABILIDADES CLAVES), SE PUEDE MEDIR CON ESTÁNDARES ACEPTADOS, Y SE PUEDEN MEJORAR A TRAVÉS DEL ENTRENAMIENTO Y DESARROLLO" (PMI, 2002).</p>					
<b>IV. COMPETENCIAS GENERALES</b>					
<p>"SON LOS COMPORTAMIENTOS ASOCIADOS A DESEMPEÑOS COMUNES A DIVERSAS ORGANIZACIONES Y RAMAS DE ACTIVIDAD PRODUCTIVA, DENTRO DE ESTA DEFINICIÓN SE ENGLOBAN TODAS AQUELLAS CAPACIDADES DE CARÁCTER GENERALISTA, EN EL SENTIDO DE QUE NO ESTARÍAN ORIENTADAS AL DESARROLLO DE NINGUNA TAREA LABORAL ESPECÍFICA, SINO QUE CONSTITUIRÍAN LA BASE DEL SABER PROFESIONAL" (OIT, 2007).</p>					
<b>DESCRIPCIÓN</b>	<b>CALIFICACIÓN</b>				
	<b>1 (NUNCA)</b>	<b>2 (Poco)</b>	<b>3 (MEDIANAMENTE)</b>	<b>4 (HABITUALMENTE)</b>	<b>5 (SIEMPRE)</b>
<b>1. CALIDAD DE TRABAJO:</b> Conoce los temas del área de la cual es responsable, comprendiendo la esencia de los aspectos complejos para transformarlos en soluciones prácticas, y operables para la organización.			2	2	
<b>2. CAPACIDAD PARA APRENDER:</b> Asimila nueva información y la aplica eficazmente, relacionando la incorporación de nuevos esquemas a su repertorio de conductas habituales.				4	
<b>3. HABILIDAD ANALÍTICA (ANÁLISIS DE PRIORIDAD, CRITERIO LÓGICO, SENTIDO COMÚN):</b> Realiza un análisis lógico, identificando los problemas, y reconociendo la información significativa para la organización.			2	2	
<b>4. CONCIENCIA ORGANIZACIONAL:</b> Reconoce los atributos y las modificaciones de la organización, comprendiendo e interpretando las relaciones de poder dentro de esta.				4	
<b>5. ORIENTACIÓN A LOS RESULTADOS:</b> Encamina sus actos al logro de lo esperado, actuando con velocidad y sentido de urgencia ante decisiones importantes para satisfacer las necesidades del cliente, superar a los competidores, o mejorar la organización.			2	2	
<b>6. ADAPTABILIDAD AL CAMBIO:</b> Se adapta y amolda a los cambios, modificando la propia conducta para alcanzar determinados objetivos cuando surgen dificultades, nuevos datos o cambios en el medio.					4
<b>7. ÉTICA:</b> Siente y actúa consecuentemente con los valores morales, y las buenas costumbres y prácticas profesionales.				3	1
<b>8. RESPONSABILIDAD:</b> Se compromete en la realización de las tareas asignadas. Su interés por el cumplimiento de lo asignado está por encima de sus propios intereses.				4	

<b>9. TOLERANCIA A LA PRESIÓN:</b> SIGUE ACTUANDO CON EFICACIA EN SITUACIONES DE PRESIÓN DE TIEMPO Y DE DESACUERDO, OPOSICIÓN Y DIVERSIDAD, TRABAJADO CON ALTO DESEMPEÑO EN SITUACIONES DE ALTA EXIGENCIA.				2	2
<b>10. ORIENTACIÓN AL CLIENTE:</b> AYUDA A LOS CLIENTES, COMPRENDIENDO Y SATISFACIENDO SUS NECESIDADES.		1	2	1	
<b>11. TRABAJO EN EQUIPO:</b> PARTICIPA ACTIVAMENTE EN LA BÚSQUEDA DE UNA META COMÚN, SUBORDINANDO LOS INTERESES PERSONALES A LOS OBJETIVOS DEL EQUIPO.			1	3	
<b>V. FORTALEZAS Y OPORTUNIDADES DE MEJORA</b>					
<b>FORTALEZAS</b>			<b>OPORTUNIDADES DE MEJORA</b>		
Es una persona muy ordenada que le gusta estar analizando lo que hace cada vez. Se adapta muy fácilmente a los cambios, siguiendo el hilo de los procesos. Se enfoca mucho en los resultados.			Puede llegar hacer una persona muy trabajadora que olvida las relaciones personales con sus compañeros. Puede llegar hacer muy tirano con algunas tareas.		
<b>VI. SUGERENCIAS</b>					
Puede mejorar bastante en la comunicación con sus compañeros para mejorar con sus relaciones y llegar hacer mejor persona.					

<b>I. CONCEPTO</b>										
<i>LA EVALUACIÓN DE COMPETENCIAS GENERALES, ES UNA HERRAMIENTA DE RETROALIMENTACIÓN, MEDIANTE EL CUAL SE RECOGEN EVIDENCIAS SOBRE LAS COMPETENCIAS GENERALES DEL EVALUADO. EL PROPÓSITO DE LA EVALUACIÓN DE COMPETENCIAS GENERALES ES DAR INFORMACIÓN AL EVALUADO SOBRE LA PERTINENCIA DE SUS COMPETENCIAS EN UN CONTEXTO LABORAL, CON LA FINALIDAD DE AYUDARLO A MEJORAR LOS RESULTADOS DE SU DESEMPEÑO PERSONAL Y PROFESIONAL.</i>										
<b>II. DATOS DEL EVALUADO</b>										
<b>NOMBRE</b>	Raul Rivera									
<b>ÁREA</b>	Operaciones									
<b>CARGO</b>	Gerente de operaciones									
<b>III. COMPETENCIAS</b>										
<i>"LAS COMPETENCIAS ESTÁN RELACIONADAS CON LAS ACTITUDES, HABILIDADES, Y OTRAS CARACTERÍSTICAS PERSONALES QUE AFECTAN UNA PARTE IMPORTANTE DEL RENDIMIENTO EN EL TRABAJO (ES DECIR, UNO O MÁS ROLES O RESPONSABILIDADES CLAVES), SE PUEDE MEDIR CON ESTÁNDARES ACEPTADOS, Y SE PUEDEN MEJORAR A TRAVÉS DEL ENTRENAMIENTO Y DESARROLLO" (PMI, 2002).</i>										
<b>IV. COMPETENCIAS GENERALES</b>										
<i>"SON LOS COMPORTAMIENTOS ASOCIADOS A DESEMPEÑOS COMUNES A DIVERSAS ORGANIZACIONES Y RAMAS DE ACTIVIDAD PRODUCTIVA, DENTRO DE ESTA DEFINICIÓN SE ENGLOBAN TODAS AQUELLAS CAPACIDADES DE CARÁCTER GENERALISTA, EN EL SENTIDO DE QUE NO ESTARÍAN ORIENTADAS AL DESARROLLO DE NINGUNA TAREA LABORAL ESPECÍFICA, SINO QUE CONSTITUIRÍAN LA BASE DEL SABER PROFESIONAL" (OIT, 2007).</i>										
<b>DESCRIPCIÓN</b>		<b>CALIFICACIÓN</b>								
		<b>1 (NUNCA)</b>	<b>2 (POCO)</b>	<b>3 (MEDIANA MENTE)</b>	<b>4 (HABITUAL MENTE)</b>					
<b>1. CALIDAD DE TRABAJO:</b> CONOCE LOS TEMAS DEL ÁREA DE LA CUAL ES RESPONSABLE, COMPRENDIENDO LA ESENCIA DE LOS ASPECTOS COMPLEJOS PARA TRANSFORMARLOS EN SOLUCIONES PRÁCTICAS, Y OPERABLES PARA LA ORGANIZACIÓN.					3					
					1					

<b>2. CAPACIDAD PARA APRENDER:</b> ASIMILA NUEVA INFORMACIÓN Y LA APLICA EFICAZMENTE, RELACIONANDO LA INCORPORACIÓN DE NUEVOS ESQUEMAS A SU REPERTORIO DE CONDUCTAS HABITUALES.				2	2			
<b>3. HABILIDAD ANALÍTICA (ANÁLISIS DE PRIORIDAD, CRITERIO LÓGICO, SENTIDO COMÚN):</b> REALIZA UN ANÁLISIS LÓGICO, IDENTIFICANDO LOS PROBLEMAS, Y RECONOCIENDO LA INFORMACIÓN SIGNIFICATIVA PARA LA ORGANIZACIÓN.				3	1			
<b>4. CONCIENCIA ORGANIZACIONAL:</b> RECONOCE LOS ATRIBUTOS Y LAS MODIFICACIONES DE LA ORGANIZACIÓN, COMPRENDIENDO E INTERPRETANDO LAS RELACIONES DE PODER DENTRO DE ESTA.				3	1			
<b>5. ORIENTACIÓN A LOS RESULTADOS:</b> ENCAMINA SUS ACTOS AL LOGRO DE LO ESPERADO, ACTUANDO CON VELOCIDAD Y SENTIDO DE URGENCIA ANTE DECISIONES IMPORTANTES PARA SATISFACER LAS NECESIDADES DEL CLIENTE, SUPERAR A LOS COMPETIDORES, O MEJORAR LA ORGANIZACIÓN.				4				
<b>6. ADAPTABILIDAD AL CAMBIO:</b> SE ADAPTA Y AMOLDA A LOS CAMBIOS, MODIFICANDO LA PROPIA CONDUCTA PARA ALCANZAR DETERMINADOS OBJETIVOS CUANDO SURGEN DIFICULTADES, NUEVOS DATOS O CAMBIOS EN EL MEDIO.			1	2	1			
<b>7. ÉTICA:</b> SIENTE Y ACTÚA CONSECUENTEMENTE CON LOS VALORES MORALES, Y LAS BUENAS COSTUMBRES Y PRÁCTICAS PROFESIONALES.				4				
<b>8. RESPONSABILIDAD:</b> SE COMPROMETE EN LA REALIZACIÓN DE LAS TAREAS ASIGNADAS. SU INTERÉS POR EL CUMPLIMIENTO DE LO ASIGNADO ESTÁ POR ENCIMA DE SUS PROPIOS INTERESES.			1	2	1			
<b>9. TOLERANCIA A LA PRESIÓN:</b> SIGUE ACTUANDO CON EFICACIA EN SITUACIONES DE PRESIÓN DE TIEMPO Y DE DESACUERDO, OPOSICIÓN Y DIVERSIDAD, TRABAJADO CON ALTO DESEMPEÑO EN SITUACIONES DE ALTA EXIGENCIA.					4			
<b>10. ORIENTACIÓN AL CLIENTE:</b> AYUDA A LOS CLIENTES, COMPRENDIENDO Y SATISFACIENDO SUS NECESIDADES.	1	2	1					
<b>11. TRABAJO EN EQUIPO:</b> PARTICIPA ACTIVAMENTE EN LA BÚSQUEDA DE UNA META COMÚN, SUBORDINANDO LOS INTERESES PERSONALES A LOS OBJETIVOS DEL EQUIPO.			4					
<b>V. FORTALEZAS Y OPORTUNIDADES DE MEJORA</b>								
<b>FORTALEZAS</b>			<b>OPORTUNIDADES DE MEJORA</b>					
Es una persona enfocada en el trabajo. Es una persona muy responsable que dedica bastante tiempo en enfocarse que toda operación se lleve a cabo a tiempo y bien hecha.			Su falta de relación con los clientes lo vuelve alguien propenso a no simpatizar con los clientes.					
<b>VI. SUGERENCIAS</b>								
La relación con los clientes es de suma importancia y si debe rendir cuentas debe considerar una buena relación								

<b>I. CONCEPTO</b>
<i>LA EVALUACIÓN DE COMPETENCIAS GENERALES, ES UNA HERRAMIENTA DE RETROALIMENTACIÓN, MEDIANTE EL CUAL SE RECOGEN EVIDENCIAS SOBRE LAS COMPETENCIAS GENERALES DEL EVALUADO. EL PROPÓSITO DE LA EVALUACIÓN DE</i>

COMPETENCIAS GENERALES ES DAR INFORMACIÓN AL EVALUADO SOBRE LA PERTINENCIA DE SUS COMPETENCIAS EN UN CONTEXTO LABORAL, CON LA FINALIDAD DE AYUDARLO A MEJORAR LOS RESULTADOS DE SU DESEMPEÑO PERSONAL Y PROFESIONAL.

## II. DATOS DEL EVALUADO

<b>NOMBRE</b>	Diego Coc
<b>ÁREA</b>	Seguridad
<b>CARGO</b>	Analista de seguridad

## III. COMPETENCIAS

"LAS COMPETENCIAS ESTÁN RELACIONADAS CON LAS ACTITUDES, HABILIDADES, Y OTRAS CARACTERÍSTICAS PERSONALES QUE AFECTAN UNA PARTE IMPORTANTE DEL RENDIMIENTO EN EL TRABAJO (ES DECIR, UNO O MÁS ROLES O RESPONSABILIDADES CLAVES), SE PUEDE MEDIR CON ESTÁNDARES ACEPTADOS, Y SE PUEDEN MEJORAR A TRAVÉS DEL ENTRENAMIENTO Y DESARROLLO" (PMI, 2002).

## IV. COMPETENCIAS GENERALES

"SON LOS COMPORTAMIENTOS ASOCIADOS A DESEMPEÑOS COMUNES A DIVERSAS ORGANIZACIONES Y RAMAS DE ACTIVIDAD PRODUCTIVA, DENTRO DE ESTA DEFINICIÓN SE ENGLOBAN TODAS AQUELLAS CAPACIDADES DE CARÁCTER GENERALISTA, EN EL SENTIDO DE QUE NO ESTARÍAN ORIENTADAS AL DESARROLLO DE NINGUNA TAREA LABORAL ESPECÍFICA, SINO QUE CONSTITUIRÍAN LA BASE DEL SABER PROFESIONAL" (OIT, 2007).

DESCRIPCIÓN	CALIFICACIÓN				
	1 (NUNCA)	2 (POCO)	3 (MEDIANAMENTE)	4 (HABITUALMENTE)	5 (SIEMPRE)
<b>1. CALIDAD DE TRABAJO:</b> Conoce los temas del área de la cual es responsable, comprendiendo la esencia de los aspectos complejos para transformarlos en soluciones prácticas, y operables para la organización.			1	3	
<b>2. CAPACIDAD PARA APRENDER:</b> Asimila nueva información y la aplica eficazmente, relacionando la incorporación de nuevos esquemas a su repertorio de conductas habituales.			1	3	
<b>3. HABILIDAD ANALÍTICA (ANÁLISIS DE PRIORIDAD, CRITERIO LÓGICO, SENTIDO COMÚN):</b> Realiza un análisis lógico, identificando los problemas, y reconociendo la información significativa para la organización.			2	2	
<b>4. CONCIENCIA ORGANIZACIONAL:</b> Reconoce los atributos y las modificaciones de la organización, comprendiendo e interpretando las relaciones de poder dentro de esta.			1	3	
<b>5. ORIENTACIÓN A LOS RESULTADOS:</b> Encamina sus actos al logro de lo esperado, actuando con velocidad y sentido de urgencia ante decisiones importantes para satisfacer las necesidades del cliente, superar a los competidores, o mejorar la organización.				2	2
<b>6. ADAPTABILIDAD AL CAMBIO:</b> Se adapta y amolda a los cambios, modificando la propia conducta para alcanzar determinados objetivos cuando surgen dificultades, nuevos datos o cambios en el medio.				3	1
<b>7. ÉTICA:</b> Siente y actúa consecuentemente con los valores morales, y las buenas costumbres y prácticas profesionales.				2	2

<b>8. RESPONSABILIDAD:</b> SE COMPROMETE EN LA REALIZACIÓN DE LAS TAREAS ASIGNADAS. SU INTERÉS POR EL CUMPLIMIENTO DE LO ASIGNADO ESTÁ POR ENCIMA DE SUS PROPIOS INTERESES.				2	2
<b>9. TOLERANCIA A LA PRESIÓN:</b> SIGUE ACTUANDO CON EFICACIA EN SITUACIONES DE PRESIÓN DE TIEMPO Y DE DESACUERDO, OPOSICIÓN Y DIVERSIDAD, TRABAJADO CON ALTO DESEMPEÑO EN SITUACIONES DE ALTA EXIGENCIA.			3	1	
<b>10. ORIENTACIÓN AL CLIENTE:</b> AYUDA A LOS CLIENTES, COMPRENDIENDO Y SATISFACIENDO SUS NECESIDADES.		2	2		
<b>11. TRABAJO EN EQUIPO:</b> PARTICIPA ACTIVAMENTE EN LA BÚSQUEDA DE UNA META COMÚN, SUBORDINANDO LOS INTERESES PERSONALES A LOS OBJETIVOS DEL EQUIPO.		1	3		
<b>V. FORTALEZAS Y OPORTUNIDADES DE MEJORA</b>					
<b>FORTALEZAS</b>			<b>OPORTUNIDADES DE MEJORA</b>		
Es una persona muy hábil en su trabajo que se compromete con realizarlo bien. Es muy responsable y anda siempre al pendiente de la finalización de cada proceso para identificar posibles vulnerabilidades.			Puede ser que trabaje lento debido a que analiza paso por paso. Puede mejorar su metodología para que no sea tan invasiva en algunos procesos.		
<b>VI. SUGERENCIAS</b>					

Fuente: (Dharma Consulting, 2022)

## Acta de Reunión de Coordinación del Proyecto

CONTROL DE VERSIONES					
Versión	Hecha por	Revisada por	Aprobada por	Fecha	Motivo
1.0	RM	CR	CR	07/03/2022	REVISIÓN DEL PROYECTO

Proyecto	APLICACIÓN MÓVIL GESTIÓN Y ATENCIÓN DE CLIENTES (AMGC)		
Fecha y hora	07/03/2022 9:00 AM	Convocada por	DO
Lugar	PILLOPHONE	Facilitador	CD
Objetivo	REVISAR EL ESTADO ACTUAL DEL PROYECTO		

Asistentes		
Persona	Cargo/Área	Empresa
C. del Cid	Director del Proyecto	Pillophone.
D. Ortiz	Gerente General	Pillophone.
Documentación		
Qué se debe leer previamente	<b>Responsable</b>	
Nada		
Qué se debe presentar en la reunión	<b>Responsable</b>	
Acta de reunión	CD	
Informe de desempeño	CD	
Cronograma actualizado	CD	

<b>Agenda</b>		
<b>Actividad</b>	<b>Responsable</b>	<b>Tiempo Programado</b>
Informar esta del proyecto	CD	10 min
Acordar actividades a desarrollar	DO	10 min

<b>Conclusiones</b>	
01	SE CONSULTARÁ EL METODO A UTILIZAR PARA EL ENVIO DE INFORMES
02	SE DEBE PRESENTAR EL DISEÑO DE ALGORITMOS
03	SE DEBEN PRESENTAR LAS TÉCNICAS DE IMPLEMENTACION RECOMENDADAS
04	PRESENTAR RESULTADOS DE PRUEBAS
05	PRESENTAR INFORME DE RESULTADOS

<b>Acciones</b>	<b>Responsable</b>	<b>Fecha Límite</b>	<b>Observaciones</b>
ELABOAR ACTA DE REUNIONES	CD	9/03/2022	
VERIFICAR FORMA DE ENVIO DE INFORMES	CD	09/03/2022	
ELABORAR LAS TECNICAS DE IMPLEMENTACIÓN	CD	11/03/2022	
ELABORAR INFORME DE RESULTADOS	CD	13/03/2022	

<b>Notas Especiales</b>	

Fuente: (Dharma Consulting, 2022)

## Registro de Incidentes

CONTROL DE VERSIONES					
Versión	Hecha por	Revisada por	Aprobada por	Fecha	Motivo
1.0	CD	CR	CR	28/02/2022	Versión inicial

## REGISTRO DE INCIDENTES

NOMBRE DEL PROYECTO	SIGLAS DEL PROYECTO
Aplicación Móvil de Gestión y Atención de Clientes	AMGC

TIPO DE INCIDENTE	INVOLUCRADOS Y FECHA DE INCIDENTE	DESCRIPCIÓN	PRIORIDAD	RESPONSABLES	FECHA DE SOLUCIÓN	ESTADO	SOLUCIÓN FINAL
Importante	Luis Chang Marta Godínez Desarrolladores 18/02/2022	Los equipos proporcionados no cumplen con las especificaciones solicitadas.	Alta	PM	21/02/2022	Aprobado	Se proveyó de equipos diferentes al grupo de desarrolladoras con el fin de poder satisfacer las necesidades del entorno solicitado.
Urgente	Tulio Lira 24/02/2022	Falta de disponibilidad de uno de los desarrolladores debido a complicaciones médicas.	Alta	PM, CR	25/02/2022	Aprobado	Se realizó una reorganización de responsabilidades debido a que el colaborador no estará disponible para completar sus asignaciones por más de 15 días, según suspensión médica.
importante	Marcus Lopez 14/03/2022	El servidor de testing no contaba con las mismas características que el servidor de producción	Alta	ML, AP, DR	16/03/2022	Aprobado	Se procedió con la modificación del entorno de testing con el fin de lograr una coincidencia con el entorno de producción, esto implicó reinstalación de sistemas.

Fuente: (Dharma Consulting, 2022)

## Grupo de Procesos de Monitoreo

### Informe de métricas de calidad

CONTROL DE VERSIONES					
Versión	Hecha por	Revisada por	Aprobada por	Fecha	Motivo
1.0	RM	CR	CR	14/03/2022	VERSIÓN ORIGINAL

NOMBRE DEL PROYECTO	SIGLAS DEL PROYECTO
Aplicación Móvil de Gestión y Atención de Clientes	AMGC

CUADRO DE MÉTRICAS							
FACTOR RELEVANTE DE CALIDAD	MÉTRICA DE CALIDAD	MÉTODO DE MEDICIÓN	OBJETIVO DE CALIDAD	TOLERANCIA(VARIACIÓN PERMISIBLE DE LA MÉTRICA)	MEDICIÓN DE MÉTRICA		OBSERVACIONES
					FECHA	RESULTADO OBTENIDO	
Performance del Proyecto	CPI= Índice de Desempeño del Costo Acumulado.	1. Se recabará información de avances reales, valor ganado, fechas de inicio y fin real, trabajo real, y costo real, los cuales se ingresarán en el MS Project. 2. El MS Project calculará el índice. 3. Este índice se trasladará al Informe Semanal de Proyecto. 4. Se revisará el informe con el Patrocinador y se tomarán las acciones correctivas y/o preventivas pertinentes.	Para el CPI se desea un valor acumulado no menor de 0.95.	± 10%	<ul style="list-style-type: none"> <li>• Frecuencia, semanal.</li> <li>• Medición, martes en la mañana.</li> </ul>	0.96	El sobrecosto ha sido originado por los gastos incurridos en cambios solicitados en el proyecto. Estos cambios se encuentran registrados en el documento "Estado de las Solicitudes de Cambio".
Performance del Proyecto	SPI= Índice de Desempeño del Cronograma Acumulado.	1. Se recabará información de avances reales, valor ganado, fechas de inicio y fin real, trabajo real, y costo real, los cuales se ingresarán en el MS Project. 2. El MS Project calculará el índice. 3.	Para el SPI se desea un valor acumulado no mayor de 0.95.	± 10%	<ul style="list-style-type: none"> <li>• Frecuencia, semanal.</li> <li>• Medición, martes en la mañana.</li> </ul>	0.93	El resultado del indicador muestra que se ha realizado el trabajo conforme a lo planificado. Eficientizando el desarrollo del proyecto.

		Este índice se trasladará al Informe Semanal de Proyecto. 4. Se revisará el informe con el Patrocinador y se tomarán las acciones correctivas y/o preventivas pertinentes.					
Satisfacción de los clientes en el desarrollo de la aplicación	Nivel de Satisfacción = Promedio entre 1 a 5 sobre insumos, equipo de desarrollo, y producto final.	1. Se recaudará la información proveniente de las encuestas que se aplicarán al finalizar cada informe y entrega de resultados a los clientes. 2. La información recaudada será transferida a un archivo Excel, en el cual se hará la tabulación correspondiente. 3. Se obtendrán los resultados de la tabulación. 4. Se revisará el documento con el Patrocinador y se tomarán las acciones correctivas y/o preventivas pertinentes.	Nivel de Satisfacción >= 4.0	± 10%	<ul style="list-style-type: none"> <li>• Frecuencia, una encuesta por cada sesión.</li> <li>• Medición, al día siguiente de la encuesta.</li> </ul>	4.10	Los resultados de las encuestas evidenciaron una satisfacción positiva. Debido a que se ha llevado un buen manejo y organización, así como cumplimiento del cronograma de trabajo apegados a una metodología estilo scrumban.

Fuente: (Dharma Consulting, 2022)

## Solicitud de Cambio

CONTROL DE VERSIONES					
Versión	Hecha por	Revisada por	Aprobada por	Fecha	Motivo
1.0	BA	CR	CR	10/03/22	Versión Original

## SOLICITUD DE CAMBIO N°001

NOMBRE DEL PROYECTO	SIGLAS DEL PROYECTO	SOLICITANTES DEL CAMBIO
Aplicación Móvil de Gestión y Atención de Clientes	AMGC	Comité de Control de Cambios

Tipo de Cambio Requerido											
Generación de Acción Correctiva:	Reparación de Defecto: <input checked="" type="checkbox"/>										
Generación de Acción Preventiva:	Actualizaciones:										
<b>Definición del Problema o Situación Actual:</b> Defina y acote el problema que se va a resolver, distinguiendo el problema de sus causas, y de sus consecuencias. De acuerdo con las encuestas de satisfacción presentadas a los clientes luego de tratar sus gestiones en la aplicación móvil se encontró que faltó indicar la escala que se muestra.											
<b>Descripción detallada del Cambio Solicitado:</b> Especifique con claridad el cambio solicitado, precisando el qué, quién, cómo, cuándo y dónde. Modificar el diseño de la escala en la encuesta de satisfacción que se presenta al finalizar la gestión por un diseño más intuitivo y presentando las instrucciones con la escala y su significado.											
<b>Razón por la que se solicita el Cambio:</b> Especifique con claridad porque motivos o razones solicita el cambio, porque motivos eligen este curso de acción y no otro alternativo, y qué sucedería si el cambio no se realiza. Los usuarios no están entendiendo bien la escala presentada por lo cual tiene efecto en los datos que se recaban de estas.											
<b>Efectos en el Proyecto:</b> Definir el efecto del cambio solicitado a corto o largo plazo en el alcance del proyecto. En el corto plazo    En el largo plazo Ampliación de 2 de la fecha fin del proyecto estipulada.											
<b>Efectos en otros proyectos, programas, portafolios u operaciones.</b> Ninguno											
<b>Efectos extra empresariales en clientes, mercados, proveedores, gobierno, etc.</b> Ninguno											
<b>Observaciones y Comentarios adicionales.</b> Realizar pruebas con un grupo de clientes para validar el nuevo diseño y reportar resultados.											
<b>Revisión del Comité de Control de Cambios.</b> <table border="1"> <tr> <td>Fecha de Revisión</td> <td>11/03/22</td> </tr> <tr> <td>Efectuada Por</td> <td>CR</td> </tr> <tr> <td>Resultados de Revisión (aprobada/rechazada)</td> <td>Aprobada</td> </tr> <tr> <td>Responsable de Aplicar/Informar</td> <td>CD</td> </tr> <tr> <td>Observaciones Especiales</td> <td>Ninguna</td> </tr> </table>		Fecha de Revisión	11/03/22	Efectuada Por	CR	Resultados de Revisión (aprobada/rechazada)	Aprobada	Responsable de Aplicar/Informar	CD	Observaciones Especiales	Ninguna
Fecha de Revisión	11/03/22										
Efectuada Por	CR										
Resultados de Revisión (aprobada/rechazada)	Aprobada										
Responsable de Aplicar/Informar	CD										
Observaciones Especiales	Ninguna										

Fuente: (Dharma Consulting, 2022)

## Estado de las Solicitudes de Cambio

CONTROL DE VERSIONES					
Versión	Hecha por	Revisada por	Aprobada por	Fecha	Motivo
1.0	CD	CR	CR	09/03/2022	Versión Inicial

NOMBRE DEL PROYECTO	SIGLAS DEL PROYECTO
Aplicación Móvil de Gestión y Atención de Clientes	AMGC

Nº DE SOLICITUD DE CAMBIO	SOLICITANTE DEL CAMBIO	TIPO DE CAMBIO REQUERIDO	DESCRIPCIÓN DEL CAMBIO	RESPONSABLE DEL CAMBIO	ESTADO DEL CAMBIO	OBSERVACIONES
1	Comité de control de cambios	Reparación de defecto	Falta de indicador en las encuestas de satisfacción del cliente, esto no permite obtener una métrica optima o adecuada en dicha encuesta.	CD	Aprobado	El cambio solicitado fue aplicado en la encuesta con el fin de reparar el defecto. Se realizo una validación de los datos adicionales para confirmar que la encuesta cumple a totalidad con las necesidades del cliente y de la aplicación.
2	Comité de control de cambios	Acción Correctiva	Cambio en el proveedor de los equipos destinados a ser servidores de aplicación. Debido al retraso en la entrega de los equipos por parte del proveedor, para el levantado y puesta en marcha de la aplicación en entorno operativo el área encargada de dicho procedimiento no tenía la capacidad para ejecutar los procesos	CD	Aprobado	Se realizo una validación de los posibles proveedores, asegurando que estos contaran con los equipos dentro del país para evitar retrasos aduanales. Finalmente se contactó con INTCOMEX, asegurándolo como proveedor de los equipos pertinentes para el despliegue de la aplicación.

			pertinentes. Generando de esta forma un retraso en la fecha de lanzamiento de producto.			
3	Comité de control de cambios	Acción preventiva	Cambio en el material de capacitación para empleados internos. El material destinado para la capacitación de los empleados con accesos adicionales como administradores de departamento fue modificado con el fin de poder proveerles capacitación específica con referencia a sus capacidades dentro del sistema.	CD	Aprobado	<p>Se llevo a cabo el cambio aplicando las acciones como acciones correctivas con el fin de evitar falta de información en el proceso de capacitación contra la ejecución en la práctica del aplicativo.</p> <p>La capacitación posterior a la actualización fue desglosada con el fin de poder proveer una capacitación personalizada por injerencia en el departamento por lo que los gerentes contarán con información adicional a la que los usuarios regulares podrán acceder.</p>

Fuente: (Dharma Consulting, 2022)

## Reporte de Performance del Proyecto Final

CONTROL DE VERSIONES					
Versión	Hecha por	Revisada por	Aprobada por	Fecha	Motivo
1.0	RP	CR	CR	14/03/2022	Versión original

NOMBRE DEL PROYECTO	SIGLAS DEL PROYECTO	PERIODO
Aplicación Móvil de Gestión y Atención de Clientes	AMGC	17-01-22 al 13-04-22

**Estado Actual del Proyecto:** Como está el proyecto a la fecha de corte del periodo.

### 1.- Situación del Alcance

Indicador	Fórmula	Cálculo	Resultado
% avance real	EV / BAC	\$. 99,456.8 / \$. 77,040	129%
% avance planificado	PV / BAC	\$. 99,456.8 / \$. 77,040	130%

### 2.- Eficiencia del Cronograma

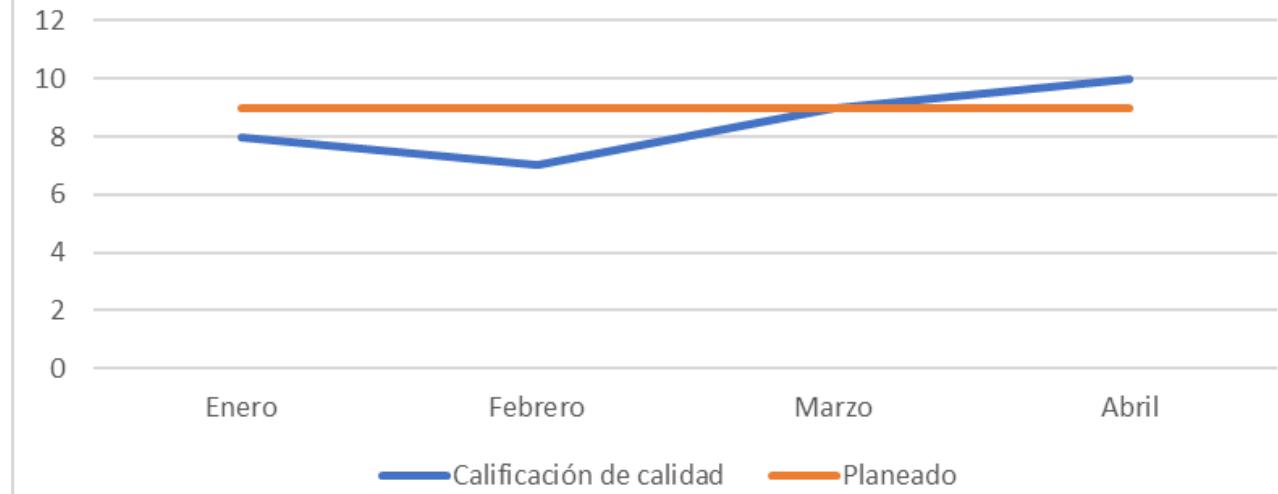
Indicador	Fórmula	Cálculo	Resultado
SV (Variación del Cronograma)	EV – PV	\$. 99,456.8 - \$. 77,040	\$. 22,146.8
SPI (Índice de Desempeño del Cronograma)	EV / PV	\$. 99,456.8 / \$. 77,040	1.30

### 3.- Eficiencia del Costo

Indicador	Fórmula	Cálculo	Resultado
CV (Variación del Costo)	EV – AC	\$. 99,456.8 - \$. 77,040	\$. 22,146.8
CPI (Índice de Desempeño del Costo)	EV / AC	\$. 99,456.8 / \$. 77,040	1.29

### 4.- Cumplimiento de Objetivos de Calidad

#### DESARROLLO DE APP PROYECTO AMGC: Calificación de calidad



Calidad objetivo = 9

**REPORTE DE PROGRESO:** QUÉ SE ALCANZÓ DESDE LA ÚLTIMA VEZ QUE SE PRESENTÓ EL INFORME.

**1.- ALCANCE DEL PERÍODO**

INDICADOR	FÓRMULA	CÁLCULO	RESULTADO
% DE AVANCE PLANIFICADO DE PERÍODO	(PV <sub>j</sub> /BAC) - (PV <sub>i</sub> /BAC)	(\$. 99,456.8 / \$. 77,040) - (\$. 60,234.4 / \$. 56,732.4)	2.29 %
% DE AVANCE REAL DEL PERÍODO	(EV <sub>j</sub> /BAC) - (EV <sub>i</sub> /BAC)	(\$. 99,456.8 / \$. 77,040) - (\$. 60,234.4 / \$. 56,732.4)	2.2 %

**2.- VALOR GANADO DEL PERÍODO**

INDICADOR	FÓRMULA	CÁLCULO	RESULTADO
VALOR GANADO PLANIFICADO	PV <sub>j</sub> - PV <sub>i</sub>	\$. 77,040 - \$. 56,732.4	\$. 20,307.6
VALOR GANADO REAL	EV <sub>j</sub> - EV <sub>i</sub>	\$. 99,456.8 - \$. 60,234.4	\$. 39,222.4

**3.- COSTO DEL PERÍODO**

INDICADOR	FÓRMULA	CÁLCULO	RESULTADO
COSTO PLANIFICADO	PV <sub>j</sub> - PV <sub>i</sub>	\$. 77,040 - \$. 56,732.4	\$. 20,307.6
COSTO REAL	AC <sub>j</sub> - AC <sub>i</sub>	\$. 99,456.8 - \$. 60,234.4	\$. 39,222.4

**4.- EFICIENCIA DEL CRONOGRAMA EN EL PERÍODO**

INDICADOR	FÓRMULA	CÁLCULO	RESULTADO
SV DEL PERÍODO	(EV <sub>j</sub> -EV <sub>i</sub> )-(PV <sub>j</sub> -PV <sub>i</sub> )	(\$. 99,456.8 - \$. 60,234.4) - (\$. 77,040 - \$. 56,732.4)	\$. 18,914.8
SPI DEL PERÍODO	(EV <sub>j</sub> -EV <sub>i</sub> )/(PV <sub>j</sub> -PV <sub>i</sub> )	(\$. 99,456.8 - \$. 60,234.4) / (\$. 77,040 - \$. 56,732.4)	1.93

**5.- EFICIENCIA DEL COSTO EN EL PERÍODO**

INDICADOR	FÓRMULA	CÁLCULO	RESULTADO
CV DEL PERÍODO	(EV <sub>j</sub> -EV <sub>i</sub> )-(AC <sub>j</sub> -AC <sub>i</sub> )	(\$. 99,456.8 - \$. 60,234.4) - (\$. 99,456.8 - \$. 60,234.4)	\$. 0
CPI DEL PERÍODO	(EV <sub>j</sub> -EV <sub>i</sub> )/(AC <sub>j</sub> -AC <sub>i</sub> )	(\$. 99,456.8 - \$. 60,234.4) / (\$. 99,456.8 - \$. 60,234.4)	1

**Pronóstico:** Estimados del comportamiento futuro del proyecto.

**Pronóstico del Costo**

Indicador	Fórmula	Cálculo	Resultado
EAC (estimate at completion)	AC +[(BAC - EV)/CPI]	\$. 99,456.8 + [(\$. 77,040- \$. 99,456.8 )/1]	\$. 77,040
ETC (estimate to complete)	(BAC - EV)/CPI	(\$. 77,040- \$. 99,456.8 )/	\$. -22.416.8
VAC (variance at completion)	BAC - EAC	\$. 77,040 - \$. 77,040	\$. 0

**Pronóstico del Cronograma**

EAC (de tiempo)	0 días útiles
ETC (de tiempo)	0 días útiles
VAC (de tiempo línea base)	0 días útiles
Fecha de Término Planificada	3 de abril del 2022
Fecha de Término Pronosticada	13 de abril del 2022

Estado actual de Problemas y Riesgos.

El proyecto ha sido finalizado y entregado, funcionando al 100%

Únicamente han quedado algunas ideas para agregar más módulos como un subproyecto.

Trabajo terminado durante el periodo.

Ver cronograma N.1 Adjunto

Trabajo a ser realizado en el siguiente periodo.

Ver cronograma N.2 Adjunto

Resumen de cambios aprobados durante el periodo.

Ninguno

Resultados de análisis de variaciones.

Ninguno

Otra información relevante para revisión y discusión.

Ninguno

Fuente: (Dharma Consulting, 2022)

## **Conclusiones**

El proceso de documentación dio pie a poder ejecutar el proyecto de forma ordenada y sistemática, con apoyo adicional de técnicas de gestión de proyectos como Kanban y Scrum que permitieron la organización optima del equipo de desarrollo mientras al mismo tiempo se lograba satisfacer las necesidades del cliente con entregas parciales en cada uno de los “Sprints” o hitos de entrega del proyecto.

Las facilidades de documentación a su vez permitieron el fácil despliegue del aplicativo y la capacidad de poder documentar tanto los logros como cada uno de los cambios y lecciones aprendidas durante el proceso de desarrollo.

## **Referencias**

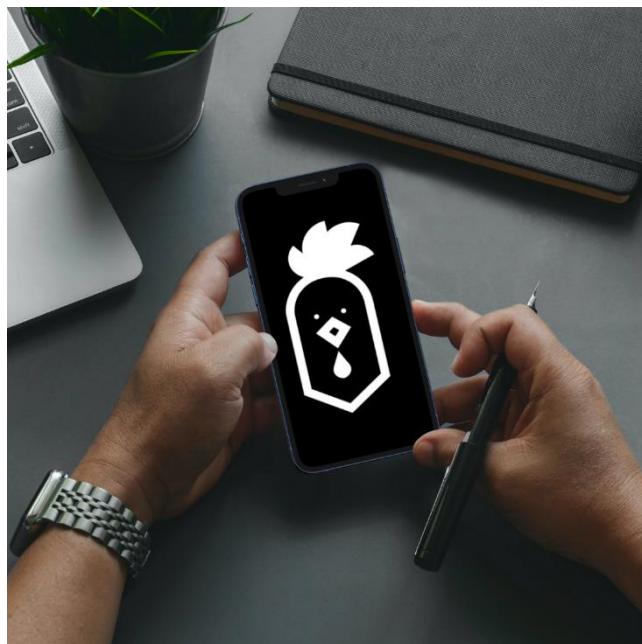
Consulting, D. (2022). *Gestion de Proyectos*. Guatemala: Dharma Consulting.

## Anexos

### Logo PilloPhone



### Inicio de aplicativo



**Universidad Mariano Gálvez de Guatemala**  
**Facultad de Ingeniería en Sistemas de Información**  
**Maestría de Seguridad informática**  
**CMMI**



Proyecto Final

**Implementación de modelo de madurez CMMI**

40/40  
100/100

*Cristian Rosales*

Cristian Waldemar Rosales  
Meléndez

Firmado digitalmente por Cristian Waldemar  
Rosales Meléndez  
Fecha: 2022.06.15 13:56:28 -06'00'

Alumnos	Carne	Email	Coordinador
Cristian Elí del Cid Rodríguez	1293-07-1719	Cdelcidr1@miumg.edu.gt	x
Wagner Aníbal Orózco López	1293-13-4370	worozcol1@miumg.edu.gt	
Ricardo Alejandro Pérez Rodríguez	1293-17-1255	rperezr8@miumg.edu.gt	
Bryan Orlando Aguirre Sagastume	1293-17-646	baguirres@miumg.edu.gt	
Josué Eduardo Pérez Veliz	1293-10-593	Jperezv8@miumg.edu.gt	
Valeriano de Jesús Chete Guzmán	1293-13-3807	vcheteg@miumg.edu.gt	

## Índice

<b>INTRODUCCIÓN.....</b>	<b>1</b>
<b>RESUMEN.....</b>	<b>2</b>
<b>ANTECEDENTES DE LA ORGANIZACIÓN .....</b>	<b>3</b>
VISIÓN DE LA ORGANIZACIÓN.....	4
MISIÓN DE LA ORGANIZACIÓN .....	4
PROPÓSITO DE LA EMPRESA .....	4
<i>Corporación</i> .....	4
<i>Negocio de productos, tecnologías y servicios agrícolas (fertilizantes, agroquímicos, etc.)</i> .....	4
NUESTRA CULTURA .....	4
<i>Verdad e integridad</i> .....	4
<i>Competitividad</i> .....	4
<i>Relaciones de largo plazo</i> .....	4
RESPONSABILIDAD SOCIAL.....	4
<b>JUSTIFICACIÓN DEL PROYECTO.....</b>	<b>6</b>
<b>ESTIMACIÓN .....</b>	<b>7</b>
EST 1.1 DESARROLLE ESTIMACIONES DE ALTO NIVEL PARA REALIZAR EL TRABAJO.....	7
EST 2.1 DESARROLLAR, MANTENER ACTUALIZADO Y UTILIZAR EL ALCANCE DE LO QUE SE ESTÁ ESTIMANDO.....	9
EST 2.2 DESARROLLE Y MANTENGA ESTIMACIONES ACTUALIZADAS PARA EL TAMAÑO DE LA SOLUCIÓN .....	10
EST 2.3 BASADO EN ESTIMACIONES DE TAMAÑO, DESARROLLE Y REGISTRE EL ESFUERZO, LA DURACIÓN Y LAS ESTIMACIONES DE COSTOS Y SU RAZÓN DE SER PARA LA SOLUCIÓN.....	10
EST 3.1 DESARROLLAR Y MANTENER ACTUALIZADO UN MÉTODO DE ESTIMACIÓN REGISTRADO. ....	11
EST 3.2 UTILICE EL REPOSITORIO DE MEDICIÓN DE LA ORGANIZACIÓN Y LOS ACTIVOS DE PROCESO PARA ESTIMAR EL TRABAJO.....	12
<b>PLANIFICACIÓN .....</b>	<b>14</b>
PLAN 1.1 DESARROLLE UNA LISTA DE TAREAS.....	14
TAREA .....	14
ACTIVIDAD.....	14
DURABILIDAD.....	14
GENERACIÓN DE ESPECIFICACIONES ALTAMENTE CORRECTAS CON CLARIDAD Y SIN AMBIGÜEDADES. POR LO QUE LAS RESPONSABLES DEBEN CUMPLIR CON LA OBTENCIÓN, ANÁLISIS Y VALIDES DE LOS REQUERIMIENTOS. ....	14
1 A 2 SEMANAS. DEPENDERÁ DEL TAMAÑO DEL PROYECTO Y DE LA METODOLOGÍA A UTILIZAR. ....	14
EVALUAR Y VERIFICAR LOS REQUERIMIENTOS, PARA ESTABLECER UN DISEÑO DE ESTRUCTURACIÓN ALTO NIVEL DONDE FUNCIONARA EL SISTEMA DE SOFTWARE.....	15
1 SEMANA .....	15
1 SEMANA .....	15
DESARROLLO DE MODELO CONCEPTUAL DE ESTRUCTURA DE DATOS QUE CUMPLA CON LOS ALTOS ESTÁNDARES DE NORMALIZACIÓN PARA BASE DE DATOS RELACIONALES, ASÍ COMO DAR SEGUIMIENTO Y MANTENIMIENTO PARA ACTUALIZACIONES Y MODIFICACIONES ESTE ESTOS, CON EL FIN DE GARANTIZAR LA ESTABILIDAD Y DISPONIBILIDAD DE LOS DATOS. ....	15
1 SEMANA .....	15
ESTABLECER METODOLOGÍA DE DESARROLLO DE SOFTWARE QUE AYUDE A LLEVAR DE FORMA ORDENADA Y CONTROLADA LOS ENTREGABLES DEL PROYECTO. ....	15
3 DÍAS.....	15
DESARROLLO DE CÓDIGO FUENTE CON BASE A LINEAMIENTOS IMPUESTOS DE REQUISITOS FUNCIONALES Y NO FUNCIONALES. ....	15
ENTREGABLES PERIÓDICAS DE 1 SEMANA COMO MÍNIMO.....	15

VERIFICACIÓN Y VALIDACIÓN DE SOFTWARE, CON EL OBJETIVO DE BÚSQUEDA DE ERRORES SOBRE LAS DIFERENTES FUNCIONALIDADES DE CADA UNO DE LOS PROCESOS DE UN SISTEMA DE SOFTWARE.....	15
1 SEMANA .....	15
CONFIGURACIÓN E INSTALACIÓN DE HARDWARE EN ENTORNOS DE DESARROLLO, CAPACITACIÓN Y PRODUCCIÓN. ASÍ COMO TAMBIÉN DAR SEGUIMIENTO S DE ACTUALIZACIONES Y DE VERSIONES PARA CADA UNO DE LOS PROYECTOS.....	15
1 SEMANA A 2 SEMANAS .....	15
PLAN 1.2 ASIGNAR PERSONAS A TAREAS. ....	15
PLAN 2.1 DESARROLLAR Y MANTENER ACTUALIZADO EL ENFOQUE PARA REALIZAR EL TRABAJO. ....	17
PLAN 2.2 PLANIFIQUE LOS CONOCIMIENTOS Y HABILIDADES NECESARIOS PARA REALIZAR EL TRABAJO. ....	17
PLAN 2.3 BASADO EN ESTIMACIONES REGISTRADAS, DESARROLLE Y MANTENGA EL PRESUPUESTO Y EL CRONOGRAMA ACTUALIZADOS.....	18
PLAN 2.4 PLANIFIQUE LA PARTICIPACIÓN DE LAS PARTES INTERESADAS IDENTIFICADAS. ....	19
PLAN 2.5 PLANIFIQUE LA TRANSICIÓN A OPERACIONES Y SOPORTE.....	19
PLAN 2.6 ASEGÚRESE DE QUE LOS PLANES SEAN VIABLES CONCILIANDO LOS RECURSOS DISPONIBLES Y ESTIMADOS....	20
PLAN 2.7 DESARROLLAR EL PLAN DEL PROYECTO, ASEGURAR LA COHERENCIA ENTRE SUS ELEMENTOS Y MANTENERLO ACTUALIZADO. ....	20
PLAN 2.8 REVISE LOS PLANES Y OBTENGA COMPROMISOS DE LAS PARTES INTERESADAS AFECTADAS. ....	21
PLAN 3.2 DESARROLLE UN PLAN Y MANTÉNGALO ACTUALIZADO, UTILIZANDO EL PROCESO DEL PROYECTO, LOS ACTIVOS DEL PROCESO DE LA ORGANIZACIÓN Y EL REPOSITORIO DE MEDICIÓN.....	25
PLAN 3.3 IDENTIFICAR Y NEGOCIAR DEPENDENCIAS CRÍTICAS .....	26
PLAN 3.4 PLANIFIQUE EL ENTORNO DEL PROYECTO Y MANTÉNGALO ACTUALIZADO SEGÚN LOS ESTÁNDARES DE LA ORGANIZACIÓN. ....	27
<b>RESULTADOS OBTENIDOS .....</b>	<b>28</b>
<b>CONCLUSIONES .....</b>	<b>29</b>
<b>RECOMENDACIONES .....</b>	<b>30</b>
<b>REFERENCIAS BIBLIOGRÁFICAS.....</b>	<b>31</b>
<b>ANEXOS.....</b>	<b>1</b>
ANEXO 1 - DIAGRAMA DESARROLLO.....	1

## **Introducción**

El presente documento nace de cubrir las necesidades emergentes de la organización Disagro de Guatemala, en tener un sistema documentado de gestión de planificación y estimación.

Disagro siendo una organización orientada de forma directa al entorno agrícola, muestra la realzad de la mayoría de las organizaciones dentro de nuestra región, ya que, así como la mayoría de estas no cuenta con un sistema de gestión que pueda proveer una guía y ayude a determinar la sostenibilidad de la organización a largo plazo.

El no contar con ningún modelo de gestión para la estimación y planificación, se consideró conveniente la adaptación del “Capability Maturity Model Integration” (CMMI) con un enfoque en los niveles de madures 1, 2 y 3 (niveles de madurez final para estas áreas de practica) con el objeto de poder completar el diseño y alcanzar los parámetros requeridos por el CMMI y con miras a continuar aplicando diferentes niveles en diversas áreas de oportunidad en el futuro.

## Resumen

Teniendo en consideración la existencia de múltiples teorías, modelos y esquemas que pueden ser utilizados para formalizar las labores que se ejecutan dentro de una organización debe denotarse que uno de los modelos más utilizados y debido a su proceso de implementación es CMMI.

El presente trabajo nace de la necesidad de implementar CMMI para poder reafirmar el nivel de madurez de los procesos dentro de la organización Disagro, Guatemala.

Disagro en la actualidad no cuenta con una implementación de madures de procesos por lo que en general todos los procesos cuentan con una implementación empírica y con una falta de generalizada de documentación que tiende a ser la causal raíz de malas prácticas dentro de la organización y a su vez desemboca en resultados deficientes, motivo por el cual se procede en este documento a completar la implementación de dos áreas de practica que pretende ayudar a la organización a mejorar sus procesos de gestión.

## Antecedentes de la Organización

Es una organización internacional de origen guatemalteco, su historia se remonta desde el año 1976 en donde inicio como un negocio de ventas de fertilizantes para los diferentes agricultores guatemaltecos en ese entonces, iniciando con muy poco fue creciendo su mercado y con eso mismo las nuevas líneas de negocio, 4 años después se inició con la línea de negocio de agroquímicos en Guatemala abriendo más puertas para la organización y avanzando rápidamente dentro del mercado de la agricultura guatemalteca.

Entre los años 1985 y 1986 la organización se introdujo dentro del mercado de más maquinarias agrícolas y el negocio de manufactura y distribución de sacos, en donde colocaban a disposición de los agricultores el servicio de alquiler de máquinas para hacer trabajos en sus tierras y en ocasiones ventas de las mismas maquinarias, también se abrió paso en la manufactura de sacos como proveedor de estos para que los agricultores pudiesen trasladar sus productos con mayor confianza y una mejor organización e incluso para almacenarlos.

Luego de 6 años de crecimiento dentro del territorio guatemalteco y toma de bastante experiencia y respeto dentro del mercado agrícola, en el año 1992 la organización se abrió paso al resto del mundo inicialmente con honduras, en donde se inicia con un negocio de fertilizantes dentro de ese territorio el primero fuera de Guatemala, posteriormente de este acto se vio la demanda de los servicios de Disagro por lo que sus ventas y su crecimiento se dio aún más alto, y tocando más territorios externos.

En el año 1996 se inició con la venta de sus productos en Panamá y Costa Rica, siendo un logro total para Disagro, ahora hasta la fecha se incluye a Colombia, Nicaragua y el Salvador como otro país que usa los productos de Disagro.

Dentro de las fechas de 1998 y 2018 se iniciaron nuevas líneas de negocio para la organización, las cuales son:

- Inicio de producción de envases PET y otros tipos de envases (1998).
- Representación de maquinaria industrial (2006).
- Representación de maquinaria de construcción (2013).
- Negocio de plasticultura agrícola (2014).
- Negocio de riego (2016).
- Negocio de semillas de maíz (2018). (Disagro, 2022).

Finalmente, la empresa en el año 2019 decidió dar su paso más grande para sus líneas de negocio, y es una línea fuera de lo común para una empresa agricultora, esto debido al avance tecnológico y el crecimiento de la digitalización en el mundo, y la línea es el lanzamiento de plataforma de agricultura digital y AgritecGEO en conjunto con el inicio del negocio de aplicación inteligente de insumos (AVANTAGRO).

Esta línea nueva de negocio se enfoca bastante en el desarrollo e implementación de hardware o software para toda necesidad que los agricultores

tengan, es decir que realizan productos tecnológicos hechos a la medida para aquellas empresas que necesiten de estas y puedan ser útiles en los diferentes ambientes en el que se encuentra la agricultura o simplemente necesiten llevar el estricto control de sus procesos.

### **Visión de la organización**

“Nuestra visión es ser pioneros y líderes en el desarrollo de una nueva agricultura de altos rendimientos en las cosechas de todos los agricultores.” (Disagro, 2022).

### **Misión de la organización**

“Tenemos la misión de proveer a nuestros clientes con productos y servicios de primera calidad internacional a precios altamente competitivos, a través de nuestra excelencia operativa e innovación tecnológica, fundamentados en la entrega y pasión del mejor y más motivado equipo humano.” (Disagro, 2022).

### **Propósito de la empresa**

#### ***Corporación***

“Más alimentos y desarrollo para la región.” (Disagro, 2022).

#### ***Negocio de productos, tecnologías y servicios agrícolas (fertilizantes, agroquímicos, etc.)***

“Impulsamos la competitividad del agro llevando a nuestros clientes lo más innovador y efectivo del mundo”. (Disagro, 2022).

### **Nuestra Cultura**

#### ***Verdad e integridad***

“Valoramos la verdad e integridad como principio absoluto que rigen todo lo que hacemos. ”(Disagro, 2022).

#### ***Competitividad***

“Somos altamente competitivos, buscando siempre ganar la carrera” (Disagro, 2022).

#### ***Relaciones de largo plazo***

“Construimos relaciones de largo plazo fundamentadas en la confianza, lealtad y el respeto.” (Disagro, 2022).

### **Responsabilidad social**

“Creemos que, como ciudadanos corporativos responsables, debemos contribuir activamente al mejoramiento social, económico y ambiental de las comunidades de las cuales somos parte.” (Disagro, 2022).

“Creemos que, para ser eficaz en las iniciativas de responsabilidad social empresarial, es importante enfocar los esfuerzos en soluciones simples y prácticas, pero que a su vez permiten alcanzar enormes beneficios.” (Disagro, 2022).

“A través de nuestros proyectos y prácticas de responsabilidad social empresarial buscamos ayudar a los más necesitados y generar desarrollo, poniendo en uso nuestras capacidades y habilidades como empresa y como individuos.” (Disagro, 2022).

De acuerdo con lo anterior Disagro se encuentra totalmente comprometida con su responsabilidad de mejorar al medio ambiente, la economía y la sociedad, siendo esto algo de suma importancia para una empresa de este tipo, ya que por su crecimiento y su magnitud a nivel internacional deja mucha huella en donde se encuentra y con estos objetivos que se impone en conjunto con su responsabilidad provee de progreso a todo aquel agricultor que desee emprender y utilice a Disagro como su proveedor ya que provee productos de muy alta calidad a nivel internación y lleva años en el área de la agricultura.

Y ahora en un nuevo comienzo del mundo digital, empieza con su rol con proveer herramientas electrónicas o softwares con lo último de la tecnología para proveer a sus clientes tecnologías de alta calidad dándoles la oportunidad de afrontar esta era de la digitalización y que puedan ir creciendo en conjunto con esta era con sus productos, tales que provee el servicio de productos hechos a la medida por lo que cualquiera que desea uno, pueda implementarlo y funcionarle exactamente como este quisiera, ya que posee 46 años de experiencia en el mercado de la agricultura.

## Justificación del Proyecto

Disagro de Guatemala, es una empresa en constante crecimiento, es bien sabido que una empresa cuando necesita expandirse debe realizarse de forma sistemática con la finalidad de asentarse en el país o región donde quiera establecerse. Actualmente la empresa utiliza una metodología llamada scaling-up, dicha metodología es aplicada a nivel general para definir los objetivos en los próximos años y en los últimos años el área de sistemas se ha convertido en un pilar para el crecimiento de la empresa.

Uno de los factores más importantes que ha ayudado a la empresa a lograr una expansión ha sido el uso de sistemas de información especialmente aquellos que están hechos a la medida.

Actualmente cada unidad de negocio de la empresa puede gestionar la compra de software a terceras personas, y eso ha causado que las unidades de negocio tengan diferente información distribuida en diferentes lugares y al momento de querer consolidar la información se vuelve una tarea titánica.

Sin embargo, el departamento de sistemas cuenta con un área de desarrollo que puede ayudar a las demás áreas de negocio, generando sistemas de alta calidad, con tecnología actualizada, con alta compatibilidad de conexión a los sistemas ya existentes.

Por lo tanto, se ha solicitado hacer una evaluación de los procesos que actualmente se tiene implementados para hacer software a la medida, así como se ha solicitado que dichos procesos puedan ser mejorados a tal grado de alcanzar un nivel de madurez entre eficiencia y eficacia.

Para poder cumplir con la necesidad de la empresa, se ha utilizado el modelo CMMI, aplicado específicamente al proceso de desarrollo de software.

Se han tomado dos áreas de prácticas de CMMI las cuales son estimación y planificación, dichas áreas ayudarán a que desde el inicio del proyecto todos los involucrados puedan saber el tiempo, el esfuerzo y los recursos utilizados.

## Estimación

### **EST 1.1 Desarrolle estimaciones de alto nivel para realizar el trabajo.**

#### **Datos históricos:**

La siguiente estimación es basada en la metodología Scrum la cual utiliza la empresa para desarrollar los diferentes softwares a medida que realiza para sus clientes con la ayuda de algunas otras herramientas como Slack y Jira. De acuerdo con dicha metodología los puntos de historia se evalúan con el método póker (Fibonacci): 1-3-5-8-13, dicha evaluación se realiza con los programadores en una votación para que la puntuación sea más acertada con cada ticket, los programadores tienen una meta mínima de puntos que deben de completar por sprint la cual es de 8.

**Tabla 1:** Registros históricos sobre sprints pasados con el equipo de desarrollo.

Sprints	Puntos de historia propuestos	Puntos de historia completados	Cantidad de programadores	Tiempo
1	41	41	8	2 semanas
2	59	38	8	2 semanas
3	43	39	8	2 semanas
Medias:	48	39		

*Tabla 1. 1 Fuente Elaboración Propia*

Nota. Esta tabla representa algunos datos históricos del equipo de desarrollo con la finalidad de poder realizar una estimación adecuada sobre la duración que cada Sprint debe de tener, la columna Sprint representa la cantidad de datos tomados, la columna: puntos de historia propuestos, son los puntos propuestos a inicio de cada Sprint, la columna: puntos de historia completados, representa la cantidad de puntos completados en los desarrolladores, la última columna representa el tiempo tardado en finalizar el sprint.

La siguiente tabla 2, contiene la estimación de costos que representa el desarrollo del software, dentro de los recursos se encuentra el pago mensual de desarrolladores los cuales son 8 programadores, el pago del director del proyecto, el pago de servicios administrativos representa el pago de 3 personas encargadas de llevar a cabo la documentación y la administración del proyecto, finalmente se encuentran los otros gastos operacionales.

**Tabla 2:** Estimación de gastos.

Recursos	Tiempo de servicio	Valoración por mes	Costo total
Pago mensual de desarrolladores	4.5 meses	Q 128,000.00	Q 576,000.00
Pago mensual de director	5 meses	Q 20,000.00	Q 100,000.00
Pago mensual de servicio administrativo	5 meses	Q 36,000.00	Q 180,000.00
Pago de licencias de software	4.5 meses	Q 1,200.00	Q 5,400.00
Gastos operacionales (servicios básicos)	5 meses	Q 19,000.00	Q 95,000.00
Total:			Q 956,400.00

*Tabla 1. 2 Fuente Elaboración Propia*

La siguiente tabla representa los diferentes sprints estimados para el desarrollo del aplicativo a medida, dentro de la tabla se puede visualizar fechas, el backlog, las diferentes historias de usuarios, duración del sprint, otros. Cabe mencionar que la empresa ya cuenta con su base de datos únicamente falta el nuevo aplicativo.

**Tabla 3:** Estimación de alto nivel del módulo control de inventario.

Fecha inicio	Semana	Product backlog: Desarrollo del aplicativo	Duración	Puntos de historia totales
14/02/2022		Epic: modulo de inicio de sesión	3 semanas	62
		Sprint 1	2 semanas	42
	1	User story: pagina de inicio de sesión		23
	2	User story: pagina de registro		19
		Sprint 2	2 semanas	37
	3	User story: Gestión de cuentas		20
8/03/2022		Epic: Control de almacenes	3 semanas	45
	4	User story: agregar almacenes		17
		Sprint 3	2 semanas	43
	5	User story: editar almacenes		13
	6	User story: eliminar almacenes		15
30/03/2022		Epic: Control de categorías	3 semanas	59
	7	User story: agregar categorías		15
		Sprint 4	2 semanas	44
	8	User story: editar categorías		24
	9	User story: eliminar categorías		20
18/04/2022		Epic: Control de Productos	4 semanas	71
		Sprint 5	2 semanas	35
	10	User story: agregar Productos		16
	11	User story: dar de baja un producto		19
		Sprint 6	2 semanas	36
	12	User story: editar Productos		22
	13	User story: eliminar Productos		14
18/05/2022		Epic: paginas de visualización	2 semanas	81
		Sprint 7	2 semanas	37
	14	User story: visualizar productos por categorías		18
	15	User story: visualizar productos por diferentes filtros		19
1/06/2022		Epic: transferencia de producto	3 semanas	64
		Sprint 8	2 semanas	44
	16	User story: pagina para crear transferencia		21
	17	User story: pagina para introducir transferencia		23
		Sprint 9	2 semanas	20
	18	User story: editar transferencias		20
<b>Totales:</b>			18 semanas	382

*Tabla 1. 3 Fuente Elaboración Propia*

Nota. La columna titulada producto backlog representa todas las acciones a llevar a cabo, cada una se encuentra dividida en Epic el cual denomina cada módulo a desarrollar del aplicativo, la columna puntos de historia totales representa la puntuación total que se le asignó a cada Epic, Sprint y user story.

La siguiente figura únicamente representa el desarrollo de los sprints conforme el tiempo y su duración.

Figura 1. Estimación de desarrollo de cada sprint.

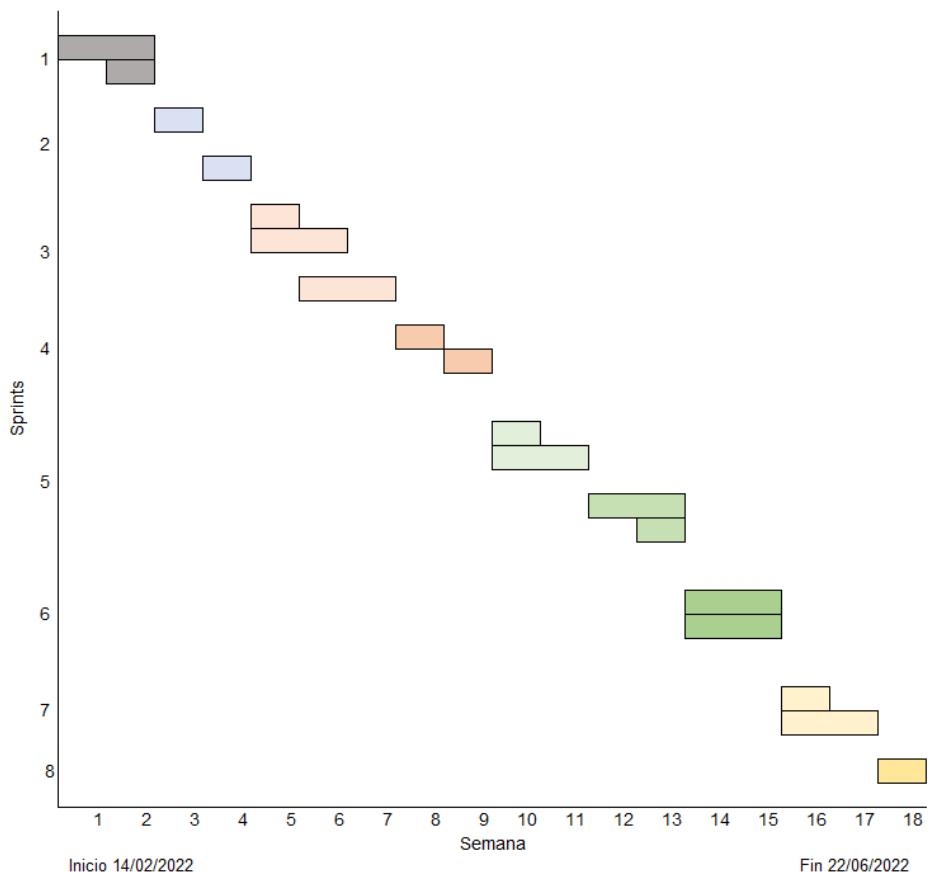


Ilustración 1.1 Fuente: Elaboración Propia

### **EST 2.1 Desarrollar, mantener actualizado y utilizar el alcance de lo que se está estimando.**

Se garantiza que desde este punto se cumplan con los requisitos anclados estimando costos, tiempos en entregables, aumentando la posibilidad de cumplir con los objetivos.

Tarea	Descripción
Estimación de costos	<ul style="list-style-type: none"> <li>• Costos de equipos</li> <li>• Costos de licencias</li> <li>• Costos de atrasos</li> <li>• Costos por sprint</li> <li>• Sueldos</li> <li>• Gastos varios</li> <li>• Costos de Implementación SCRUM</li> <li>• Capacitaciones en DELPHI</li> </ul>
Seguimiento de Cronograma	<ul style="list-style-type: none"> <li>• Requerimientos</li> <li>• Tiempos en los sprint</li> <li>• Análisis de base de datos</li> <li>• Maquetado</li> <li>• Holgura en Sprint</li> <li>• Pruebas</li> </ul>

	<ul style="list-style-type: none"> <li>• Documentación</li> <li>• Tiempo en capacitaciones DELPHI</li> </ul>
Documentación	<ul style="list-style-type: none"> <li>• Documentos de análisis</li> <li>• Diagramas</li> <li>• Manuales de usuario</li> <li>• Manuales técnicos</li> </ul>
Entregables	<ul style="list-style-type: none"> <li>• Diseño Funcional</li> <li>• Módulos</li> <li>• Garantía</li> </ul>
Ambientes	<ul style="list-style-type: none"> <li>• De prueba</li> <li>• Pruebas Integrales</li> <li>• Aceptación de usuario</li> <li>• Posproducción</li> </ul>

Tabla 2. 1 Fuente Elaboración Propia

### EST 2.2 Desarrolle y mantenga estimaciones actualizadas para el tamaño de la solución.

Se llevan a cabo cada uno de los desarrollos y se actualizan las estimaciones adecuándolo al software y la solución que se necesita entregar.

Tarea	Descripción
Seguimiento de DELPHI	<ul style="list-style-type: none"> <li>• Datos accesibles</li> <li>• Rápida Codificación</li> <li>• Compatibilidad con distintas plataformas</li> <li>• Conectividad nativa con diferentes bases de datos</li> <li>• Menor esfuerzo al crear aplicaciones</li> <li>• Simple adaptabilidad e integración</li> </ul>
Cumplimiento de SCRUM	<ul style="list-style-type: none"> <li>• Analizar el tipo de proyecto.</li> <li>• Creación de Backlog.</li> <li>• Planificación de sprint.</li> <li>• Inicio de sprint.</li> <li>• Consultas para ver el panorama general.</li> <li>• Mejora con informes agiles.</li> </ul>

Tabla 2. 1 Fuente Elaboración Propia

### EST 2.3 Basado en estimaciones de tamaño, desarrolle y registre el esfuerzo, la duración y las estimaciones de costos y su razón de ser para la solución.

Se basa en la solución que se le dará al cliente, pero viéndolo desde el punto de nosotros, características, funciones personalizadas, etc.

Tarea	Descripción
-------	-------------

Bases de datos	<ul style="list-style-type: none"> <li>• Normalización exacta de base de datos</li> <li>• Diagnosticar la gestión de la base de datos</li> <li>• Evaluar la gestión de la base de datos</li> <li>• Analizar la situación actual de la base de datos.</li> <li>• Mantenimiento a bases de datos</li> <li>• Diagramas de red</li> <li>• Informe.</li> </ul>
Desarrollo completo	<ul style="list-style-type: none"> <li>• Planificación</li> <li>• Análisis</li> <li>• Diseño</li> <li>• Implementación</li> <li>• Pruebas</li> <li>• Instalación o Despliegue</li> <li>• Uso y mantenimiento</li> <li>• Modelos a utilizar</li> </ul>
Documentación	<ul style="list-style-type: none"> <li>• Definir la documentación</li> <li>• Preparar Manuales</li> </ul>

Tabla 3. 2 Fuente Elaboración Propia

### **EST 3.1 Desarrollar y mantener actualizado un método de estimación registrado.**

#### **Definición del método de estimación**

Como se ha mencionado en los puntos anteriores se utiliza scrum como framework de trabajo, sin embargo, dentro de scrum se utiliza el método de póker que es una derivación del método **Delphi**, de tal forma que todos los técnicos involucrados puedan hacer sus estimaciones.

Este método se realizará siempre que se esté planificando un backlog por lo que se determinara un día a la semana donde se haga dicha planificación, lo importante es mantener el foco en hacer una buena estimación por lo que este día no hay un límite de tiempo para la estimación de las tareas.

Cada colaborador debe tener en cuenta que la estimación es un compromiso el cual debe cumplirse y comprometerse en el tiempo establecido democráticamente.

#### **Actualización del método de estimación**

Si bien el método póker no es algo muy complejo debe acoplarse a cada equipo de trabajo. para lograr una actualización constante al método de estimación se

recomienda realizar una reunión al finalizar cada backlog donde se escuchen las opiniones de los técnicos involucrados en el proyecto.

Una vez recopilada las opiniones evaluar cuales son los puntos de mejora que se pueden aplicar de forma inmediata. Con la finalidad que los puntos de mejora se vean reflejados en la próxima estimación de tareas.

Al mismo tiempo se recomienda a los scrum másteres analizar las estimaciones históricas, evaluar el promedio de las tareas que sean de carácter similar o las tareas que tengan la misma naturaleza de forma que para la siguiente estimación de tareas se tenga un promedio para comenzar las estimaciones.

### **Validación del método de estimación**

Una vez que se tengan los datos registrados según el historial de estimaciones se debe contratar a una empresa externa que haga una evaluación de la efectividad del método, así como las recomendaciones de mejoras que no puedan existir. La empresa para seleccionar debe contar con años de experiencia en el campo y ser reconocida como una fuente confiable.

### **Herramientas**

Para mantener el control sobre las tareas, estimaciones y cumplimiento, como ya se ha mencionado se utilizará Jira, puesto que es una herramienta enfocada en equipos de trabajo basados en scrum, al mismo tiempo que permite obtener paneles de análisis de datos de forma que se pueda visualizar el esfuerzo tareas y demás.

### **EST 3.2 Utilice el repositorio de medición de la organización y los activos de proceso para estimar el trabajo.**

### **Justificaciones**

Cada proyecto de desarrollo cuenta con enfoques muy diferentes, sin embargo, muchos proyectos de programación pueden tener tareas que ya se han realizado en el pasado. Para ello es importante que las tareas actuales sean analizadas con las tareas realizadas en el pasado en proyectos similares.

Es en ese punto donde entra la justificación, todos los scrum masters que utilicen datos históricos deben justificar el uso los datos históricos, de tal forma que la precisión de la estimación de las tareas no se vea afectado por un error de fuente de datos.

### **Actualización y mejoras**

El uso de justificantes en el momento de realizar una estimación debe de ir acompañador de actualizaciones constantes y mejoras continuas. Para ello se debe generar un informe general que ayude a hacer una comparación entre estimaciones pasadas.

La finalidad de dicha comparación es obtener toda la información posible del uso de los recursos y poder ser una herramienta para la toma de decisiones respecto a los recursos de la empresa.

### **Resultados a tomar en consideración**

Si bien para que el instrumento de estimación sea funcional a futuro es importante tener mediciones, tales como:

1. Prioridad de la tarea
  - a. Toda tarea debe tener una prioridad entre alta, media o baja.
2. Duración total de la tarea.
  - a. La duración de la tarea se expresa en horas de trabajo, sin embargo, no se limita a que pueda durar días
3. Costo por personal asignado
  - a. La hora de trabajo de los técnicos tienen un costo estándar por lo que saber cuántas horas se tarda en realizar una tarea, ayudará a determinar el costo total de esta.
4. Calidad
  - a. La calidad se verifica con un experto en Q&A mientras menos errores y menos retornos a desarrollo mejor será la calidad de las tareas.
5. Contexto
  - a. Para poder entender el contexto de la tarea esta debe expresarse como historia de usuario, sin embargo, el técnico asignado a la realización de la tarea de explicar el contexto técnico de la tarea.

Al utilizar Jira como herramienta oficial para controlar, organizar y monitorear las actividades los scrum master deben de mantener siempre los datos actualizados y analizar de forma periódica los activos de la empresa.

## Planificación

### **PLAN 1.1 Desarrolle una lista de tareas.**

Para el desarrollo de software es esencial establecer un conjunto de actividades, estas permiten tener una mejor estimación de todos los elementos que implica. También permite tener una visión clara de los riesgos, costes y tiempo durante la trayectoria del desarrollo del software.

Tabla 4:

*Descripción de tareas.*

Tarea	Descripción
Toma de requerimientos	Etapa inicial, lo cual ayuda comprender para qué se necesita en el desarrollo de un software.
Análisis de la arquitectura	Se analizan todos los componentes necesarios para el desarrollo e implementación del software.
Desarrollo del diseño	Describe la planificación de la solución del desarrollo, así como también ayuda a disminuir los riesgos en la vida del desarrollo del software.
Desarrollo del modelo	Se enfoca en la representación gráfica de la estructura de la información.
Metodología del desarrollo	Se analiza la metodología a utilizar durante todo el desarrollo del software, este dependerá mucho de la dimensión del proyecto.
Desarrollo del software	Es la etapa donde se transforma todos los procesos y requisitos obtenidos a un lenguaje de código fuente.
Pruebas del software	Se verifica las funcionalidades, rendimiento y la experiencia del usuario, con el objetivo de asegurar que no existan errores en proyecto.
Despliegue	Proceso de llevar el proyecto a un entorno de producción, por lo que este proceso puede ser de forma escalonada.

Tabla 5:

*Actividad de ejecución de tareas y durabilidad.*

Tarea	Actividad	Durabilidad
Toma de requerimientos	Generación de especificaciones altamente correctas con claridad y sin ambigüedades. Por lo que las responsables deben cumplir con la obtención, análisis y valides de los requerimientos.	1 a 2 semanas. dependerá del tamaño del proyecto y de la metodología a utilizar.

Análisis de la arquitectura	Evaluar y verificar los requerimientos, para establecer un diseño de estructuración alto nivel donde funcionara el sistema de software.	1 semana
Desarrollo del diseño	Definir los procesos detallados del comportamiento del sistema, por lo que debe cumplir con diseño de datos, arquitectónicos, interfaz y procedimientos.	1 semana
Desarrollo del modelo	Desarrollo de modelo conceptual de estructura de datos que cumpla con los altos estándares de normalización para base de datos relacionales, así como dar seguimiento y mantenimiento para actualizaciones y modificaciones este estos, con el fin de garantizar la estabilidad y disponibilidad de los datos.	1 semana
Metodología del desarrollo	Establecer metodología de desarrollo de software que ayude a llevar de forma ordenada y controlada los entregables del proyecto.	3 días
Desarrollo del software	Desarrollo de código fuente con base a lineamientos impuestos de requisitos funcionales y no funcionales.	Entregables periódicas de 1 semana como mínimo.
Pruebas del software	Verificación y validación de software, con el objetivo de búsqueda de errores sobre las diferentes funcionalidades de cada uno de los procesos de un sistema de software.	1 semana
Despliegue	Configuración e instalación de hardware en entornos de desarrollo, capacitación y producción. Así como también dar seguimientos de actualizaciones y de versiones para cada uno de los proyectos.	1 semana a 2 semanas

Fuente: Elaboración Propia

### PLAN 1.2 Asignar personas a tareas.

Tabla 6:

Asignación de responsables de tareas.

Tarea	Responsables	Colaboradores
Toma de requerimientos	Jefe de proyectos	<ul style="list-style-type: none"> <li>• Jefe de desarrollo</li> </ul>
Análisis de la arquitectura	Jefe de proyectos	<ul style="list-style-type: none"> <li>• Jefe de desarrollo</li> <li>• Equipo de desarrollo</li> </ul>

Desarrollo del diseño	Equipo de desarrollo	N/A
Desarrollo del modelo	Equipo de desarrollo	N/A
Metodología del desarrollo	Jefe de proyectos	<ul style="list-style-type: none"> <li>• Jefe de desarrollo</li> <li>• Equipo de desarrollo</li> </ul>
Desarrollo del software	Equipo de desarrollo	N/A
Pruebas del software	QA	<ul style="list-style-type: none"> <li>• Equipo de desarrollo</li> </ul>
Despliegue	Jefe de desarrollo	<ul style="list-style-type: none"> <li>• Equipo de desarrollo</li> </ul>

Fuente: *Elaboración Propia*

Tabla 7:

Conocimiento o experiencia necesaria para la ejecución de tareas.

Tarea	Conocimiento	Nivel de experiencia
Toma de requerimientos	Capacidad de buena comunicación con los Stakeholders, por lo que debe cumplir con un buen análisis,	Alto
Análisis de la arquitectura	Conocimientos de principios de arquitectura de software, así como también un amplio conocimiento de tecnología.	Alto
Desarrollo del diseño	Debe conocer herramientas específicas para el proceso de formulación de características de una aplicación. También debe conocer principios fundamentales de diseño y metodologías.	Medio
Desarrollo del modelo	Habilidad de manejo y manipulación de base de datos para aplicaciones de construidas con enfoque de modelado de relacionales y no relacionales	Medio
Metodología del desarrollo	Conocimiento amplio de metodologías tradicionales y agiles de desarrollo de software, por lo cual es indispensable tener habilidades para integrar y	Alto

---

	dirigir equipos de trabajo para diferentes tipos de proyectos.	
Desarrollo del software	Análisis y conocimiento amplio de buenas prácticas de programación, así como contar con experiencia en diseño y seguridad de aplicaciones.	Alto
Pruebas del software	Conocimiento amplio para pruebas estructurales, performance, funcionariales y aleatorias de sistemas.	Alto
Despliegue	Conocimiento amplio de manejo de herramientas para automatización para el proceso de despliegue, así como contar con un conocimiento amplio de servidores.	Alto

---

*Fuente: Elaboración Propia*

#### **PLAN 2.1 Desarrollar y mantener actualizado el enfoque para realizar el trabajo.**

A manera de protección de cada una de las actividades se tiene establecido que de acuerdo con los tiempos acordados se revisará con el cliente el entregable dicho con anterioridad. En esta revisión además de verificar el entregable se analizarán en conjunto los objetivos, la viabilidad del enfoque propuesto, los riesgos, los problemas de seguridad y las tecnologías propuestas de las siguientes etapas, de modo que se pueda concluir si estos siguen siendo correctos y de no ser así realizar un ajuste del enfoque haciendo los ajustes de lo mencionado.

#### **PLAN 2.2 Planifique los conocimientos y habilidades necesarios para realizar el trabajo.**

##### **Contrataciones**

Para realizar contrataciones se definen anualmente los conocimientos que debe de poseer un candidato para ser contratado, estos se actualizan anualmente debido al cambio constante de tecnologías que existe. Al definir los conocimientos se realizan versiones preliminares de exámenes posibles, luego de aceptar mínimo tres versiones estas se pasan al departamento de recursos humanos para que se actualice el examen del departamento solicitado. Todos los candidatos que se reúnan deben de obtener al menos 75 puntos para aprobar el examen, de estos se contratan los que hayan obtenido las notas más altas y dependiendo de la cantidad de plazas disponibles.

## Capacitación

La capacitación que se da generalmente es organizacional, por departamento, es decir el departamento completo la recibe de modo que esta sea aprovechada por cada persona. Sin embargo, si algún proyecto necesita en específico capacitarse sobre cierto tema para el desarrollo, únicamente este equipo será llevado a capacitaciones especiales. Incluso si solo cierto personal del equipo cumple con los requisitos para recibir una capacitación necesaria, solo este la recibirá y será el encargado de realizar la tarea para la cual implique este conocimiento.

A final de año se realiza una evaluación de conocimientos para verificar el estado del personal, en caso de que se necesite apoyo en cierta área se decide si se planifica una capacitación general o si cierto empleado necesita realizar un curso de autoaprendizaje dirigido en plataformas de asociados como por ejemplo Platzi.

En el departamento de tecnología se cuenta con diferentes puestos, pero se describen las habilidades y conocimientos necesarios de uno de los más importantes.

Full Stack Developer	
Habilidades	Conocimientos
<ul style="list-style-type: none"> <li>• Aprendizaje Autodidacta</li> <li>• Trabajo en equipo</li> <li>• Paciencia</li> <li>• Comunicación</li> </ul>	<ul style="list-style-type: none"> <li>• HTML</li> <li>• CSS</li> <li>• JavaScript</li> <li>• Python</li> <li>• PHP</li> <li>• Base de datos <ul style="list-style-type: none"> <li>◦ Oracle</li> <li>◦ SQL</li> <li>◦ MySQL</li> </ul> </li> </ul>

Fuente: Elaboración Propia

### PLAN 2.3 Basado en estimaciones registradas, desarrolle y mantenga el presupuesto y el cronograma actualizados.

El desarrollo de presupuesto y cronograma se realiza luego de la etapa de toma de requerimientos y de que el cliente haya firmado que está de acuerdo con estos. Se realiza un presupuesto y cronograma para el desarrollo completo del proyecto con todas las actividades necesarias de cada una de las etapas establecidas en el punto 1.1. En el cronograma se establecen de la mano con encargados del departamento de tecnología la estimación en horas, complejidad, duración y actividades relacionadas de cada una de las tareas, entregables, fechas propuestas para reuniones de revisión interna y revisión con el cliente. Actualmente se trabaja con la herramienta de Jira, en esta se registra el cronograma y de acuerdo con el precio de hora establecido calcula el presupuesto total que se va a manejar. Para que el cronograma tenga una base sólida se revisan los datos históricos de la organización para verificarlo antes de presentarlo con el cliente.

Para mantener el presupuesto y el cronograma actualizados es necesario que durante todo el desarrollo del proyecto los integrantes del equipo registren las horas dedicadas para cada una de las tareas y actualizar el estado de estas. El líder de cada equipo debe velar porque esto se cumpla siempre y presentar los reportes correspondientes a dirección o incluso al cliente si así fue establecido. Con esto la herramienta podrá calcular los costos y tiempos actualizados en el momento. El líder también debe verificar que los tiempos y costos establecidos se estén cumpliendo y tomar acciones de lo contrario.

#### **PLAN 2.4 Planifique la participación de las partes interesadas identificadas.**

Entre las partes interesadas principalmente está el cliente, este puede establecer los encargados a los cuales se deben de reportar los avances realizados con el proyecto. La comunicación con el cliente la tiene asignada el Project manager, este puede transmitir las dudas y hallazgos que se tengan de todo el equipo de trabajo, ellos pueden hablar directamente de modo que se tenga una comunicación rápida y constante. Las reuniones principalmente se deben hacer cuando se establecieron en el cronograma, pero en dado caso se necesite el Project manager puede solicitar una reunión con el cliente.

Además del cliente podemos mencionar a los proveedores, con este se deben realizar reuniones para solicitar un servicio nuevo, ajustes o incluso reportar un problema encontrado en cierto servicio. Las reuniones con este principalmente son antes de iniciar una etapa donde se necesite un servicio nuevo, pero cabe mencionar que también pueden surgir situaciones emergentes por algún problema. En caso de que se tengan socios o patrocinadores por alguna razón, se deben de realizar reuniones para presentar los avances del proyecto cuando sea esencial.

#### **PLAN 2.5 Planifique la transición a operaciones y soporte.**

Para poder hacer una transición a operaciones y soporte del proyecto se debe de cumplir con lo siguiente:

1. Obtener el visto bueno del encargado del proyecto, con este visto bueno se considera que el proyecto está finalizado y pasó todos los estándares de calidad establecidos con anterioridad.
2. Realizar todas las configuraciones correspondientes en los equipos de la otra organización.
3. Confirmar que todas las configuraciones realizadas en los equipos de la otra organización sean correctas realizando pruebas.
4. Implementar el proyecto dentro de la organización.
5. Realizar pruebas de funcionamiento dentro de la organización del cliente.
6. Aprobar las pruebas realizadas de funcionamiento.
7. Preparar un repositorio con permisos para que el cliente lo pueda utilizar, en donde se colocarán todas las fuentes relacionadas con el proyecto.

8. Cargar todos los archivos fuentes en el repositorio preparado.
9. Cargar la documentación y manuales relacionados con el proyecto en un sitio compartido.
10. Realizar una presentación con lo que se va a hacer entrega al cliente.
11. Confirmar la fecha para realizar la presentación de entrega del proyecto.
12. Llevar a cabo reunión de presentación de entrega del proyecto.
13. Pasar documentos de aceptación de entrega y obtener la firma del cliente.

Para el soporte se maneja un sistema de tickets, el proceso es el siguiente:

1. Crear un ticket en la herramienta registrando lo siguiente:
  - a. Error encontrado
  - b. Nivel de urgencia
  - c. Capturas de pantalla
  - d. Descripción del error y funcionamiento esperado.
2. El ticket agregado aparecerá en el sistema para que los integrantes del equipo lo visualicen.
3. Uno de los integrantes del equipo debe de asignarse el ticket de acuerdo con el nivel de urgencia.
4. El encargado del ticket atenderá la solicitud y al finalizar marcará el ticket como resuelto. En dado caso que tenga dudas se las trasladará al Project manager y este al cliente e incluso pueden programar una reunión.
5. El usuario que creó el ticket recibirá un correo indicando que el ticket fue resuelto y debe verificar el cambio.
6. Si la solución es correcta debe marcar el ticket como finalizado, de lo contrario debe poner los comentarios necesarios en el ticket y devolverlo.

#### **PLAN 2.6 Asegúrese de que los planes sean viables conciliando los recursos disponibles y estimados.**

En el caso de que el proyecto incluya servicios de proveedores de terceros se debe realizar generalmente cada año (dependiendo del contrato) una reunión para la renovación del contrato, evaluar la propuesta y en caso de ser necesario realizar las negociaciones correspondientes sobre los puntos que se deben cambiar. Luego de firmar y establecer los nuevos recursos disponibles y estimados se debe de realizar una reunión con el cliente para notificar de los nuevos cambios. Todo esto se debe de realizar pensando en la viabilidad del proyecto y responsabilidad que se tiene con el cliente.

#### **PLAN 2.7 Desarrollar el plan del proyecto, asegurar la coherencia entre sus elementos y mantenerlo actualizado.**

Distintos planes del proyecto se han mencionado a grandes rasgos en el punto 2, tales como:

7. Plan de implicación de las partes interesadas, punto 2.4
8. Plan de comunicación, punto 2.4, primer párrafo
9. Plan de soporte, punto 2.6, segundo párrafo
10. Plan de transición a operaciones, punto 2.6, primer párrafo

**PLAN 2.8 Revise los planes y obtenga compromisos de las partes interesadas afectadas.**

Se mencionan los compromisos de los planes mencionados en el punto anterior.

<b>Plan</b>	<b>Compromisos</b>
Implicación de las partes interesadas	<ul style="list-style-type: none"> <li>• Presentar mensualmente al cliente los avances del proyecto.</li> <li>• Asistir a las reuniones agendadas.</li> </ul>
Comunicación	<ul style="list-style-type: none"> <li>• El horario de comunicación es válido durante el periodo laboral 8 a.m.- 5 p.m.</li> <li>• Obtener una respuesta en menos de 5 horas si es dentro del horario válido. En caso contrario se debe obtener una razón por la cual no se pudo contestar y validarse.</li> <li>• Brindar la información necesaria para resolver la duda presentada.</li> </ul>
Soporte	<ul style="list-style-type: none"> <li>• Incluir toda la información necesaria en el ticket</li> <li>• Resolver el ticket en el tiempo acordado de acuerdo con el nivel de urgencia.</li> <li>• En caso de que el ticket no se pueda resolver en el tiempo acordado se debe de notificar al usuario con los motivos para solicitar más tiempo.</li> <li>• El soporte es válido para funcionalidades establecidas en la toma de requerimiento firmada.</li> </ul>
Transición a operaciones	<ul style="list-style-type: none"> <li>• Asistir a las reuniones agendadas.</li> <li>• Presentar lo acordado en el plan</li> <li>• Revisar únicamente lo firmado en el contrato inicial</li> </ul>

Fuente: *Elaboración Propia*

**PLAN 3.1** Utilice el conjunto de procesos estándar de la organización y las pautas de adaptación para desarrollar, mantener actualizado y seguir el proceso del proyecto.

Con el fin de poder completar un proceso de desarrollo óptimo se toma en consideración dos factores importantes, las fases estándar de desarrollo de un proyecto y el ciclo de vida del desarrollo de software.

### **Fases de desarrollo de proyecto**

Tener en consideración las fases de desarrollo de proyectos permite manejar los detalles a lo largo del desarrollo de un proyecto y poder mantener el orden en los pasos de dicho desarrollo. De forma general las fases son 5:

#### **1. Identificación del proyecto**

Fase en la que se procede con las mediciones tanto del valor como de la viabilidad del proyecto, de forma generalizada se utiliza dos herramientas para decidir si se procede con el proyecto o no:

- a. **Plan de Negocio:** Documento utilizado para justificar la necesidad del proyecto, de forma regular incluye un listado de los beneficios potenciales.
- b. **Estudio Individual:** Documento que contiene una evaluación de las partes del proyecto con los recursos disponibles para confirmar si la implementación de dicho proyecto cuenta con sentido y se apega a las necesidades organizacionales.

#### **2. Planificación del Proyecto**

Cada uno de los proyectos de desarrollo cuenta con necesidades diferentes por lo que el proceso de planificación se encuentra inmerso dentro del proceso (debe tomarse en consideración que la planificación del proceso de desarrollo no se encuentra intrínsecamente ligada a la planificación del proyecto como tal) una planificación efectiva de un proyecto de desarrollo proporciona la adecuada orientación para la obtención de recursos, financiamiento y materiales adicionales necesarios y de forma adicional ayuda con el manejo de riesgos, aceptación y comunicación de beneficios a las partes interesadas en dicho desarrollo.

#### **3. Ejecución del Proyecto**

La ejecución se basa en la construcción de entregables que satisfagan las necesidades de los interesados o clientes. La ejecución depende de manera directa del proceso de planeación ya que de esto dependerá el proceso de desarrollo y/o sprints por tomar.

#### **4. Control del Proyecto**

Con el fin de garantizar las fechas de entrega de cada una de las fases directas de desarrollo, el equipo de desarrollo debe contar con un proceso de supervisión, esto con el fin de evitar que en el proceso de desarrollo se pierda de vista el alcance del proyecto.

## **5. Cierre del Proyecto**

El proceso de cierre de un proyecto proporciona las oportunidades de documentación de incidentes encontrados durante el proceso de desarrollo y apoya en futuras puestas en marcha similares a la entrega realizada. Se considera que el proyecto se encuentra cerrado cuando se realiza la entrega final al cliente o interesados.

Por otra parte, el ciclo de vida del desarrollo de software el cual cuenta con 11 fases, es decir, 6 fases más que el desarrollo de proyectos regular

### **1. Comunicación**

Fase en la que el cliente o interesado se comunica con el equipo de desarrollo para realizar una solicitud de un producto de software específico. Como parte de este contacto se plasman las necesidades específicas y se presenta una solicitud formal para dicho desarrollo.

### **2. Planificación y análisis**

Se procede con el análisis de los requisitos. Con suma atención se realiza un análisis de los requerimientos para confirmar cuales se encuentran poco claros, incompletos, ambiguos, son contradictorios o no son necesarios. Se realizan indagaciones a profundidad teniendo en cuenta a los usuarios clave. Se procede con la división y agrupación de requisitos entre requisitos de usuario, requisitos funcionales y requisitos de sistema.

Se completa la recolección de datos llevando a cabo estudios de software actual, entrevistas con los usuarios finales y desarrolladores.

### **3. Estudios de viabilidad**

Posterior a la recolección de requisitos, se analiza que parte del software cubre las necesidades de cada usuario. Se investiga la viabilidad financiera y tecnológica para saber si el desarrollo solicitado es factible o no.

### **4. Análisis de Sistema**

El equipo de desarrollo asigna recursos y planifica el tiempo de duración del proyecto. Se busca limitaciones del producto y se identifican los impactos del proyecto sobre toda la organización en conjunto.

### **5. Diseño**

En esta fase se inicia un proceso de visualización de la solución con ayuda de las fases anteriores. Se completa un diseño lógico del servicio para posteriormente completar un diseño físico. Se completa la creación de metadatos, diagramas o pseudocódigos.

### **6. Codificación**

Denominada también ‘fase de programación’ se procede con la elección del lenguaje más conveniente y se procede con la creación de programas ejecutables de manera eficiente. El fin de esta fase es lograr la entrega (al final de esta) de un

PMV (producto mínimo viable) o el software completamente desarrollado y listo para su implementación.

## **7. Integración**

El software puede necesitar estar integrado con bibliotecas, bases e datos o con otros programas. Esta fase del SDLC integra el software con las entidades del mundo exterior.

## **8. Pruebas**

De manera regular la fase de pruebas se encuentra ligada de forma directa a la fase de desarrollo entrando en un ciclo continuo hasta completar tanto el desarrollo como las pruebas hasta que la funcionalidad del software desarrollado sea de un cien por ciento.

## **9. Implementación**

Proceso de instalación del software, se evalúa la integración, la adaptabilidad, la potabilidad y se instalan las configuraciones posteriores necesarios.

## **10. Formación**

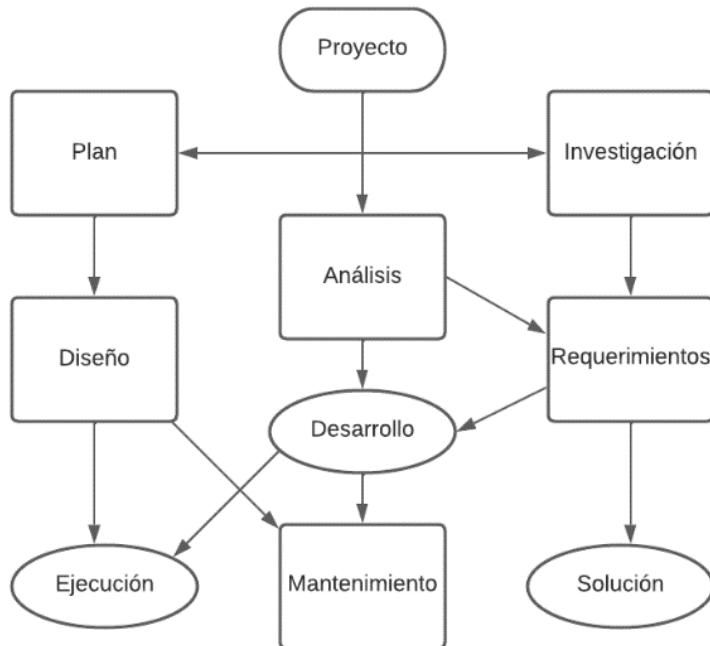
La adaptación del usuario es una de las partes mas importantes dentro del SDLC y para ello deben ofrecerse capacitaciones a cada uno de los usuarios tanto para facilitar la migración al nuevo entorno de software como para reducir la resistencia al cambio. Es importante comprobar el nivel de uso, la experiencia del usuario y resolver cualquier dificultad que pueda surgir.

## **11. Mantenimiento y Funcionamiento**

El mantenimiento es uno de los elementos clave del éxito de un desarrollo de software. Esta fase se minimizan pequeños errores, se confirma el buen funcionamiento del software, su eficiencia y estabilidad. Ya que el desarrollo se encuentra completado se requiere un monitoreo para garantizar que el software se desempeña de forma óptima.

Generalmente el diagrama del SDLC (Systems Development Life Cycle) o Ciclo de vida del desarrollo de software cuenta con el diagrama a continuación.

## Diagrama General SDLC

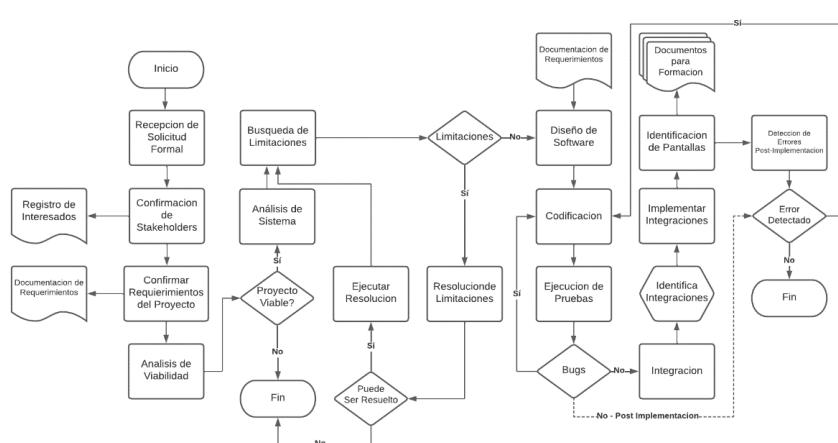


*Ilustración 3. 3 Fuente: Elaboración Propia*

**PLAN 3.2 Desarrolle un plan y manténgalo actualizado, utilizando el proceso del proyecto, los activos del proceso de la organización y el repositorio de medición**

Con el fin de poder proveer de un flujo específico para el proceso de desarrollo que logre cumplir con las expectativas tanto del departamento de desarrollo como con las de los usuarios finales se procede a completar un diagrama que pueda especificar cada uno de los pasos a seguir (dicho diagrama puede verse modificado dependiendo de las necesidades del proyecto).

## Diagrama Desarrollo



*Ilustración 3. 4 Fuente Elaboración Propia (ver anexo 1)*

### **PLAN 3.3 Identificar y negociar dependencias críticas**

Con el fin de poder completar el proceso de identificación de las dependencias o procesos críticos debe comprenderse a cabalidad no solo el proceso, también las definiciones implícitas en la información proporcionada.

#### **Tipos de dependencias**

##### **Dependencias Lógicas**

También conocidas como dependencias causales, estas dependencias son partes de un proyecto que son necesarias para su realización. A menudo representan el resultado final de todas las tareas precedentes y no se pueden ejecutaren paralelo con otras tareas.

##### **Dependencias de recursos**

Las dependencias de recursos son restricciones del proyecto relacionadas con una cantidad limitada de recursos que se tienen para el proyecto. Si hay recursos adicionales disponibles para el proyecto esta dependencia no sería un problema.

##### **Dependencias Preferenciales**

Las dependencias preferenciales son creadas por procesos impuestos por el equipo, pero son necesariamente necesarias para llevar a cabo el proyecto. Por ejemplo, para un editor puede ser necesario hacer una última revisión antes de enviar un artículo a publicar. Aunque se trata de un paso creado por el equipo para garantizar que no haya errores, este paso no es necesario para finalizar el proyecto.

##### **Dependencias Externas**

Las dependencias externas son tareas que dependen de factores externos sobre los que el equipo no tiene control. Las dependencias internas son mas comunes, ya que dependen de cuestiones que el equipo puede controlar. Un buen ejemplo de dependencia externa es cuando un fenómeno meteorológico impide que llegue un envío de fruta fresca a un restaurante.

#### **Listado de Dependencias**

Orden	Tipo	Dependencia	Criticidad
A	Preferenciales	recepción de Solicitud	Media
B	Preferenciales	confirmación de Stakeholders	Media
C	Preferenciales	Requerimientos del Proyecto	Alta
D	Recursos	Análisis de Viabilidad	Baja
E	lógicas	Análisis de Sistema	Alta
F	Recursos	Búsqueda de Limitaciones	Baja
G	Recursos	Ejecución de Resoluciones	Baja
H	Preferenciales	Diseño de Software	Alta
I	lógicas	Elección de Lenguaje de Programación	Media
J	lógicas	Proceso de desarrollo / codificación	Alta

K	Preferenciales	Ejecución de Pruebas	Alta
L	lógicas	Confirmación de Fallos	Alta
M	Externas	Identificación de Integraciones	Media
N	Externas	Proceso de Integración	Media
O	Externas	Identificación de Pantallas	Media
P	Externas	Documentación de Uso	Media
		Detección de Errores Post-	
Q	lógicas	Implementación	Alta
		Reparación de Errores Post-	
R	lógicas	Implementación	Alta

Fuente: Elaboración Propia

### PLAN 3.4 Planifique el entorno del proyecto y manténgalo actualizado según los estándares de la organización.

En la mayoría de los casos, una parte crucial del proceso de planificación del entorno, no obstante, esto puede variar de proyecto en proyecto teniendo en consideración tanto el lenguaje a utilizar como el tipo de proyecto y sus requerimientos. Con el fin de lograr un entorno básico para el departamento de desarrollo confirma la siguiente planificación.

Como entorno básico de desarrollo se requieren de los siguientes componentes:

#### Entorno de Desarrollo

- Servidor Remoto
- Servidor Local (como servidor de respaldo)
- Licencias de desarrollo
  - o Bases de datos
  - o Procesadores de texto
  - o Servicios de Gestión
- Servicio compartido de repositorio y versionado (git)

#### Entorno de Pruebas

- Servicios cloud para testing
- Servidor local dedicado al departamento de QA
- Servicios de testing automatizados

#### Entorno de preproducción / Staging

- Trabajado bajo soluciones Cloud, a no ser que se indique lo contrario por el cliente

#### Entorno de Producción

- Trabajado bajo soluciones Cloud, a no ser que se indique lo contrario por el cliente

Debe tenerse en consideración que dichos requerimientos continúan siendo los requerimientos mínimos y pueden estar sujetos a cambios dependiendo del tipo de proyecto.

## Resultados Obtenidos

### Estimación

- Estimaciones de alto nivel, logrando abordar el tamaño real del trabajo, costos y las incertidumbres de calendario logrando minimizar saturaciones o sobre costos.
- Garantía de que la solución logra cumplir con los objetivos.
- Estimaciones bien definidas, logrando de esta forma un seguimiento óptimo del trabajo y acciones correctivas oportunas.
- Maximización de la consistencia y eficacia en formulación de estimaciones precisas permitiendo alcanzar de forma óptima los objetivos.

### Planificación

- Identificación óptima del trabajo necesario logrando alcanzar las expectativas del usuario final.
- Aseguramiento de tareas específicas.
- Asegurar el éxito del proyecto mediante el enfoque adecuado de las partes interesadas.
- Uso eficaz tanto del personal como del equipo disponible para el manejo del proyecto.
- Gestión oportuna de las acciones correctivas necesarias con el fin de alcanzar los objetivos mediante la detección temprana de desviaciones ya sea presupuestarias o en relación con el cronograma.
- Aseguramiento de los recursos necesarios para la operación y logrando una probabilidad mayor de cubrir a cabalidad las necesidades del usuario final.
- Un logro eficaz y eficiente de los objetivos gracias al establecimiento correcto de procesos.

## Conclusiones

Una vez terminado el proyecto, se pudieron llegar a varias conclusiones, las cuales fueron:

1. Toda actividad que se realice dentro de una empresa debe tener un proceso definido, puesto que al establecer una serie de pasos ordenados ayuda a agilizar los resultados de las actividades.
2. Cada proceso debe ser actualizado constantemente, existen varios momentos donde un proceso debe ser actualizado por completo, uno de ellos es donde la organización ha cambiado de actividades por ende el proceso debe actualizarse. El siguiente momento para hacer una actualización es cuando se busca obtener un grado de madurez y se comienzan a afinar aspectos importantes del proceso actual.
3. Un proceso debe ser ágil y no burocrático. En la actualidad muchos procesos llegan a confundirse con burocracia, de tal forma que existen series de pasos tan extensos y difíciles para las personas, que terminan siendo engorrosos y muy lentos. Un proceso debe ser ágil
4. Como equipo de investigación se llegó a la conclusión que CMMI es una herramienta altamente efectiva siempre que se tenga el apoyo de la gerencia, y una vez que se ha implementado se debe mantener actualizado para que el nivel de madurez no decaiga.

## Recomendaciones

- Se recomienda a la empresa Disagro mantener un estándar alto en la calidad de las pruebas realizadas a los tickets para evitar minimizar la creación de nuevos para arreglar bugs de los anteriores, lo cual compromete los tiempos de entrega de los proyectos.
- Se recomienda al director del proyecto realizar las estimaciones de tiempos de sprints basados en datos históricos y también enfocarse en los tiempos de holguras, esto con la finalidad de obtener un tiempo óptimo y sin contratiempos durante el desarrollo del software.
- Para un cumplimiento correcto del tiempo se le recomienda al director realizar análisis constantes sobre los resultados de los sprints anteriores, para optimizar la estimación de los sprints futuros y poder tomar acciones sobre el tiempo de trabajo cuando este sea necesario.
- Se recomienda el uso de herramientas como Jira en todos los procesos para llevar un correcto control y una amplia vista de lo que se está desarrollando, además de que la implementación de esto traerá muchos más beneficios como el rastreo de actividades, oportunidad de realizar análisis de tiempos, otros.
- Se recomienda al director de proyectos el estudio de su equipo de trabajo con la finalidad de obtener una clara visión de las debilidades y fortalezas de su equipo, con estos datos podrá optimizar las tareas o procesos que ellos desarrollaran.
- Se recomienda al director automatizar tareas simples, como las de petición de acceso a ciertas herramientas o otras solicitudes para evitar contratiempos o malentendidos en el desarrollo del proyecto.

## Referencias Bibliográficas

*Codificación.* (s/f). Github.lo. Recuperado el 9 de junio de 2022, de

<https://argenisosorio.github.io/mdsl-cenditel/codificacion2.html>

Lee, G. (2020, octubre 16). *Tipos de pruebas de software: diferencias y ejemplos.*

LoadView; LoadView by Dotcom-Monitor. <https://www.loadview-testing.com/es/blog/tipos-de-pruebas-de-software-diferencias-y-ejemplos/>

*Metodologías de desarrollo de software: ¿qué son?* (s/f). Becas-santander.com.

Recuperado el 9 de junio de 2022, de <https://www.becas-santander.com/es/blog/metodologias-desarrollo-software.html>

*¿Qué es el desarrollo de software?* (s/f). Ibm.com. Recuperado el 9 de junio de 2022, de

<https://www.ibm.com/es-es/topics/software-development>

Rodriguez, G. J. (2012, enero 15). *Técnicas efectivas para la toma de requerimientos.*

Northware. <https://www.northware.mx/blog/tecnicas-efectivas-para-la-toma-de-requerimientos/>

Disagro (12 de junio del 2022). Quienes somos. Recuperado de:

<https://www.disagro.com/quienes-somos>

Disagro (12 de junio del 2022). Responsabilidad social. Recuperado de:

<https://www.disagro.com/rse>

Chaudhary, M., & Chopra, A. (2017). *CMMI for Development: Implementation Guide.* India: Apress.

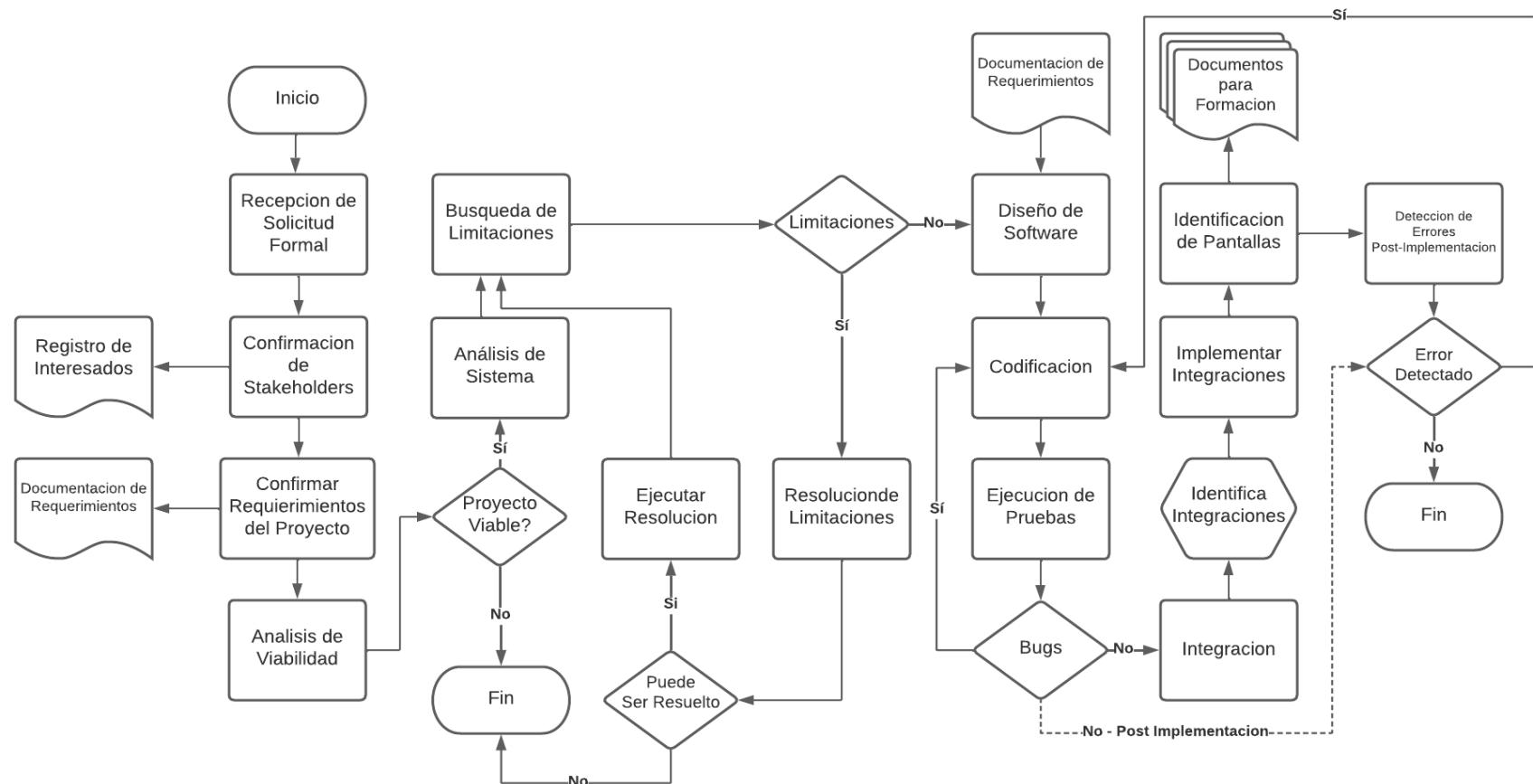
ISACA. (2019). *CMMI V2.0 - Modelo de un vistazo.* Illinois, USA: ISACA.

ISACA. (2022). *V2.0 del modelo CMMI - Visión General.* Illinois, USA: ISACS.

VishnuVarthan, M. (2015). *CMMI High Maturity Handbook.* USA: CreateSpace.

## Anexos

### Anexo 1 - Diagrama Desarrollo



Fuente: Elaboración Propria

UNIVERSIDAD MARIANO GÁLVEZ DE GUATEMALA  
FACULTAD DE INGENIERÍA EN SISTEMAS  
MAESTRÍA EN SEGURIDAD INFORMATICA  
MASTER. HAROLD CANCINOS

~~HO~~  
~~HO~~  
~~HO~~



**Proyecto final: Análisis de las resoluciones JM**

Integrantes:

Haroldo  
Rafael  
Cancinos  
Arbizu

Firmado  
digitalmente por  
Haroldo Rafael  
Cancinos Arbizu  
Fecha: 2023.06.23  
23:36:00 -06'00'

1293-17-646 Bryan Orlando Aguirre Sagastume  
1293-17-1255 Ricardo Alejandro Pérez Rodríguez  
1293-16-14277 Ana Kristina Cifuentes Castañeda  
1293-15-10369 Jonathan Renato del Cid Juárez  
1293-16-13892 Dora Lucrecia Ordoñez Pérez

Guatemala, 16 de junio de 2023

## Índice

Introducción .....	1
¿Porque estas resoluciones nacen e importancia en su implementación/cumplimiento? .....	3
¿Por qué nacen? .....	3
Importancia de implementación: .....	5
Determinar las ventajas para las instituciones supervisadas, sobre la aplicabilidad de las normativas anteriores .....	8
Establecer la relación con otros marcos de referencia o de trabajo sobre ciberseguridad.....	13
Establecer los retos sobre las nuevas disposiciones o actualizaciones y como las entidades abordan las mismas .....	16
Definiciones de roles.....	17
Responsabilidades sobre el cumplimiento y habilidades .....	17
Plan y/o gap análisis que permita establecer el cumplimiento las resoluciones de la junta monetaria en una institución supervisada.....	19
Propuesta de procedimiento para el análisis forense digital de incidentes cibernéticos .....	25
Sanciones y/o penalizaciones por parte de la SIB ante el incumplimiento de dichas resoluciones.....	32
Multas económicas .....	32
Suspensión temporal de operaciones .....	32
Prohibición de actividades específicas.....	33
Responsabilidad penal.....	33
Sanciones administrativas .....	34
Retirada de licencia.....	34

Casos de sanciones en Guatemala .....	34
Conclusiones .....	37
Recomendaciones .....	38
Referencias bibliográficas.....	39
Anexos.....	42

## Índice de figuras

<b>Figura 1.</b> Tabla de detalle de niveles de madurez.....	22
<b>Figura 2.</b> Resultados de dominio planear y organizar marco de referencia COBIT.....	23
<b>Figura 3.</b> Resultados de dominio adquirir e implementar marco de referencia COBIT.....	23
<b>Figura 4.</b> Resultados de dominio entregar y dar soporte marco de referencia COBIT.....	24
<b>Figura 5.</b> Resultados de dominio monitorear y evaluar marco de referencia COBIT.....	24
<b>Figura 6.</b> Resultados generales del nivel de madurez del marco de referencia COBIT.....	25
<b>Figura 7.</b> Procedimiento para el análisis forense digital de incidentes cibernéticos.....	32
<b>Figura 8.</b> Encuesta para la obtención de resultados del nivel de madurez COBIT del dominio planear y organizar en la entidad financiera.....	42

**Figura 9.** Encuesta para la obtención de resultados del nivel de madurez COBIT del dominio entregar y dar soporte en la entidad financiera.....43

**Figura 10.** Encuesta para la obtención de resultados del nivel de madurez COBIT del dominio adquirir e implementar en la entidad financiera.....43

**Figura 11.** Encuesta para la obtención de resultados del nivel de madurez COBIT del dominio monitorear y evaluar en la entidad financiera.....44

## **Índice de Anexos**

**Anexo 1.** Entrevista gestión de riesgos tecnológico y ciberseguridad.....42

**Anexo 2.** Instrumento de evaluación.....42

## Introducción

En la actualidad, la gestión de riesgos en el sector bancario desempeña un papel de suma importancia en la seguridad informática. Mediante este enfoque, se logra identificar, analizar y responder de manera proactiva a los diversos tipos de riesgos que pueden surgir en un proyecto. Contar con una gestión de riesgos efectiva resulta de gran utilidad, ya que permite detectar cualquier riesgo potencial y mitigarlo, evitando así pérdidas monetarias u otras consecuencias negativas.

En el caso específico de Guatemala, existe un organismo gubernamental encargado de regular y supervisar las actividades de las instituciones bancarias: la Superintendencia de Bancos (SIB). Esta institución ha desarrollado una serie de resoluciones, como la JM-102-2011, JM-42-2020 y JM-104-2021, que establecen las pautas para la gestión de riesgos en las instituciones financieras. Estas resoluciones también abordan aspectos como la gestión de inventarios de infraestructura, bases de datos y servicios de tecnología de la información, así como la seguridad de la información, la ciberseguridad y los planes de recuperación ante desastres, entre otros aspectos relevantes.

Es fundamental que todos los bancos y el sector financiero del país cumplan rigurosamente con estas leyes y regulaciones establecidas por la Superintendencia de Bancos. El incumplimiento de dichas normativas podría resultar en irregularidades o sanciones por parte de la mencionada entidad reguladora.

Sin embargo, a pesar de la existencia de estas resoluciones, el campo de la gestión de riesgos en el sector bancario sigue presentando desafíos y oportunidades de mejora. En este contexto, el presente trabajo de maestría tiene como objetivo analizar y ampliar las prácticas actuales de gestión de riesgos en las instituciones financieras de Guatemala, con el fin de proponer estrategias y recomendaciones que fortalezcan aún más la seguridad informática en el sector bancario y contribuyan a la protección de los activos financieros y la confidencialidad de la información de los clientes. A través de este estudio, se espera generar un

mayor conocimiento y conciencia sobre la importancia de la gestión de riesgos y su impacto en la seguridad informática en el sector bancario guatemalteco.

## **¿Porque estas resoluciones nacen e importancia en su implementación/cumplimiento?**

### **¿Por qué nacen?**

Las resoluciones son un instrumento diseñado para abordar y solucionar pautas o conflictos que puedan surgir y afectar a las instituciones financieras en términos económicos, temporales y procesuales. Con el transcurso del tiempo, se han promulgado tres resoluciones de gran relevancia y enfoque específico, especialmente relacionadas con las entidades financieras y su relación con la tecnología. Estas resoluciones tienen como objetivo principal proporcionar pautas claras y directrices fundamentales para garantizar la eficiencia, seguridad y cumplimiento normativo en el ámbito financiero y tecnológico. Su conocimiento y aplicación resultan de suma importancia para las instituciones financieras, ya que les permite adaptarse a los cambios tecnológicos, mantener la confidencialidad y seguridad de la información, así como optimizar sus procesos y operaciones en un entorno cada vez más digitalizado. Josue Theissen en su artículo Reglamento para la Administración del Riesgo Tecnológico en Guatemala indica que:

"Los avances tecnológicos actuales plantean un reto totalmente diferente, debido a muchos factores. Tenemos el advenimiento de la nube, la nube se ha convertido en el habilitador clave de la nueva era digital, cada vez tenemos más usuarios, datos, complejidad en el manejo de los datos, entre otros. Este panorama, tecnológico, ha sido uno de los desencadenantes de la nueva resolución de la Junta Monetaria." (Theissen, 2022).

Las resoluciones JM-102-2011, JM-42-2020 y JM-104-2021 nacieron como respuesta a la creciente dependencia de las entidades financieras del uso de tecnología de la información en sus actividades diarias. A medida que estas instituciones adoptan y utilizan cada vez más la tecnología para mejorar su eficiencia operativa y brindar servicios más rápidos y accesibles, también enfrentan nuevos y complejos desafíos relacionados con la gestión del riesgo tecnológico.

El riesgo tecnológico abarca una amplia gama de amenazas, como fallas en los sistemas informáticos, ataques cibernéticos, brechas de seguridad, robo de datos y fraudes electrónicos. Estos riesgos pueden tener consecuencias significativas, como pérdidas financieras, daños a la reputación, pérdida de confianza de los clientes y perturbación de los servicios financieros.

Esta misma también se creó para abordar esta necesidad y establecer un marco regulatorio que promueva una adecuada gestión del riesgo tecnológico en el sistema financiero de Guatemala. Al implementar y cumplir con esta resolución, las entidades financieras se comprometen a tomar medidas para identificar y mitigar estos riesgos, protegiendo así la estabilidad financiera del sistema.

También busca salvaguardar los activos y la información de las entidades financieras, que manejan una gran cantidad de información sensible y activos financieros. Al implementar controles y medidas de seguridad adecuados, las entidades garantizan la confidencialidad, integridad y disponibilidad de la información, evitando el acceso no autorizado, la pérdida de datos o la manipulación indebida, lo que podría tener graves consecuencias financieras y de reputación.

Además, la resolución establece lineamientos para la gestión de la continuidad del negocio, lo que implica la implementación de planes de contingencia y medidas para garantizar que las entidades financieras puedan mantener la prestación de servicios a sus clientes incluso en situaciones de emergencia. Esto es esencial para evitar interrupciones en los servicios financieros y mantener la confianza de los clientes.

El cumplimiento de estas resoluciones de junta monetaria ayuda a las entidades financieras a cumplir con las regulaciones y normas establecidas por las autoridades competentes. Al implementar las medidas y controles requeridos, las entidades demuestran su compromiso con el cumplimiento normativo y facilitan la supervisión por parte de las autoridades reguladoras, evitando sanciones y repercusiones legales. De acuerdo con Luis Villalobos:

"Si una institución financiera no puede demostrar que está preparada para hacer frente a situaciones adversas, los reguladores pueden imponer

sanciones o requerir cambios en las políticas y procedimientos de esta. En casos extremos, los reguladores pueden incluso exigir a la institución que aumente su capital o reduzca su exposición a ciertos tipos de riesgos." (Villalobos, 2023)

### **Importancia de implementación:**

Es de suma importancia la aplicación de medidas de seguridad en una institución bancaria y de acuerdo CyberSecurity establecen su importancia en el siguiente texto:

"Con La implementación de estas resoluciones a nivel país, en el sector bancario y financiero, es de vital importancia, debido a que es una vía de progreso el cual permite realizar transacciones confiables dentro del sistema financiero y reduce el riesgo de amenazas ciberneticas que atentan a diario contra la integridad, disponibilidad y confidencialidad de los activos en el ciberespacio. Su gestión y cumplimiento dentro de las entidades interesadas permitirá que el sector cuente con ciberseguridad con el objetivo de que puedan detectar, resistir responder y recuperarse rápidamente de un ciberataque." CyberSecurity (2020)

Conforme al texto anterior se declara sumamente la importancia de tener estas resoluciones en cada institución y defender cada aspecto dentro de estas para que su funcionamiento no se vea afectado y no afecten a sus clientes que son el pueblo guatemalteco, además puntos importantes de la implementación son las siguientes:

**Protección de la estabilidad financiera:** El riesgo tecnológico puede tener un impacto significativo en la estabilidad financiera del sistema. Las interrupciones en los sistemas, los fallos de seguridad o los ataques ciberneticos pueden afectar la operatividad de las entidades financieras, interrumpir los servicios y generar pérdidas financieras. Al implementar la resolución, se establecen medidas para identificar y mitigar estos riesgos, contribuyendo así a la protección de la estabilidad financiera del sistema.

**Salvaguardia de los activos y la información:** Las entidades financieras manejan una gran cantidad de información sensible y activos financieros. El cumplimiento de dichas resoluciones de la junta monetaria implica implementar controles y medidas de seguridad adecuados para proteger estos activos y garantizar la confidencialidad, integridad y disponibilidad de la información. Esto es crucial para prevenir el acceso no autorizado, la pérdida de datos o la manipulación indebida de la información, lo que podría tener graves consecuencias financieras y de reputación.

**Continuidad del negocio:** También establece lineamientos para la gestión de la continuidad de los servicios financieros. Esto implica la implementación de planes de contingencia y medidas para garantizar que las entidades financieras puedan mantener la prestación de servicios a sus clientes incluso en situaciones de emergencia, como desastres naturales, fallos tecnológicos o ciberataques. La continuidad del negocio es esencial para evitar interrupciones en los servicios financieros y mantener la confianza de los clientes.

**Cumplimiento normativo y supervisión:** Ayuda a las entidades financieras a cumplir con las regulaciones y normas establecidas por las autoridades competentes. Al implementar las medidas y controles requeridos, las entidades demuestran su compromiso con el cumplimiento normativo y facilitan la supervisión por parte de las autoridades reguladoras. Esto puede ayudar a evitar sanciones y repercusiones legales que podrían derivarse de un incumplimiento normativo.

Inicialmente se publicó la resolución JM-102-2011 luego surgen dos actualizaciones más, siendo la última la nueva resolución JM-104-2021, esto debido a que en la resolución JM-102-2011 se estableció el Reglamento para la Administración del Riesgo tecnológico, sin embargo ante el desarrollo y los crecientes avances de la tecnología y telecomunicaciones que se han generado con mucha rapidez y facilidad para el manejo de la información, el surgimiento de nuevos tipos de servicios, modelos de procesamiento y almacenamiento de información se identificó un incremento del riesgo tecnológico a través de amenazas ciberneticas las cuales buscan poner en riesgo los activos de la información, en el

cual se puede sufrir alguna pérdida o robo de información como consecuencia de las nuevas amenazas cibernéticas que se presentan día con día.

Es por ello por lo que se consideró como necesario derogar la resolución JM-102-2011 y emitir un nuevos Reglamentos para la Administración del Riesgo Tecnológico obteniendo como resultado hasta la fecha la JM-104-2021 la cual permitirá brindar mayor seguridad y fortalecer las políticas y procedimientos relacionadas con el procesamiento y almacenamiento de la información que se maneja en las instituciones, tomando en consideración la contratación de servicios a terceros que en su momento las instituciones consideren como necesario realizar. La implementación de la resolución JM-104-2021 es importante en los grupos financieros del país, ya que dicha resolución brinda un estándar para llevar la administración de riesgos tecnológicos, infraestructura, TI, base de datos, seguridad de la información, ciberseguridad, plan de recuperación ante desastres, procesamiento, almacenamiento, criticidad de la información y disposiciones transitorias.

Como institución financiera es necesario que vele por el cumplimiento de cada uno de los artículos que se establecen en la resolución para tener una mejor organización en los equipos de infraestructura, reducir la probabilidad de ataques por vulnerabilidades encontradas y tener un plan de recuperación que realmente garantice una rápida respuesta ante algún incidente y todo esto con el fin de conservar la integridad, confidencialidad y disponibilidad de la información.

Otra resolución que cabe mencionar y que se encuentra entre la primera y la última es la JM-42-2020, dicha resolución nace con el mismo objetivo principal de la resolución JM-102-2011 que es contar con la implementación de protección ante cualquier amenaza cibernética dentro del sistema bancario y financiero, ante esta resolución se tomó a consideración la propuesta de modificación al Reglamento para la Administración del Riesgo Tecnológico, en la cual a través de dicha resolución se promueve incorporar lo relacionado a la gestión de la ciberseguridad, la designación de un Oficial de Seguridad de la Información, implementación de un Centro de Operaciones de Seguridad Cibernética, la organización de un Equipo de

Respuestas de Incidentes Ciberneticos y a su vez la incorporación de aspectos relacionados a la ciberseguridad en contratación de proveedores. Esta resolución al igual que la JM-102-2011 está dirigida a los bancos y entidades financieras del país, quienes forman parte fundamental de la economía.

## **Determinar las ventajas para las instituciones supervisadas, sobre la aplicabilidad de las normativas anteriores**

Si las Instituciones supervisadas aplican las normativas relacionadas a las resoluciones anteriores obtendrán las ventajas que estas proveen, debido a que tienen por objetivo buscar las buenas prácticas para obtener mejores resultados y estar siempre un paso al frente de los riesgos y acciones desfavorables que puedan darse y afectar en gran medida la ejecución de dichas instituciones.

La resolución JM-102-2011 está conformada por 7 capítulos los cuales describen lo que se requiere implementar en las entidades del sistema financiero, en donde específicamente en los capítulos del dos al siete se describen los lineamientos, políticas, entre otros, que se deben de implementar. En total suman 29 artículos, en donde los primeros 2 únicamente hacen referencia al objetivo de dicha resolución y las definiciones respectivamente. Por lo tanto, las ventajas que se logran aplicar con esta resolución dentro de los capítulos dos al seis son las siguientes:

**Capítulo 2:** Organización para la administración del riesgo tecnológico, como su nombre lo indica, este capítulo se enfoca directamente a políticas, procedimientos, creación y responsabilidad de consejo administrativo, controles de riesgo, entre otros, por lo cual todo lo que incluye en este capítulo se enfoca directamente en proveer estas ventajas:

- Una gestión adecuada enfocada al riesgo tecnológico, con el fin de poder identificar, evaluar y mitigar cada riesgo enfocado a la infraestructura y otros

sistemas, reduciendo la probabilidad de posibles ataques que puedan afectar la integridad de la información.

- Mejora en seguridad sobre la tecnología de la información, basado en políticas y procesos que se deben de implementar, se enfoca mucho en garantizar la seguridad de los sistemas usados.

- Proveer un control total al consejo administrativo, de esta manera este podrá aprobar políticas, conocer cada reporte sobre el comité de gestión de riesgos, conocer cómo se están cumpliendo y a qué nivel se cumple cada política implementada.

- Creación de comité de gestión de riesgo y unidad de administración de riesgos, con esto la ventaja presentada es tener un control total sobre las propuestas de cualquier índole, implementaciones, análisis y revisiones sobre cómo se gestiona el riesgo en la organización para finalmente poder proveer reportes completos y bien detallados hacia el consejo administrativo.

- Creación de plan estratégico de TI, dentro de esta ventaja las instituciones podrán tener un plan estratégico, proyectos y un presupuesto para poder cumplir con sus objetivos alineados con la estrategia del negocio.

- Creación de una organización de TI, cada institución obtendrá una organización de TI con el fin de que el departamento de la institución tenga las capacidades necesarias para poder llevar a cabo sus funciones correctamente y que estas se alineen con el plan estratégico planteado.

- Manual de riesgo tecnológico, la ventaja que comprende este punto es que todo lo planteada sobre el artículo 3 tendrá que estar escrito en un manual el cual se irá actualizando y servirá como base para la institución.

**Capítulo 3:** Infraestructura de TI, sistemas de información, base de datos y servicios de TI: dentro de este capítulo se centra en proveer un control específico sobre los equipos, estructura organización, administración y maneras de adquisición de equipos para las instituciones, algunas ventajas específicas de este capítulo son:

- Creación de un esquema de infraestructura alineado con los procesos principales de la institución.

○ Control y administración sobre inventario de productos tecnológicos, dentro de este punto las ventajas son el estricto control sobre las compras de componentes de infraestructura o software, además de las políticas y procesos específicos de cómo todos estos procesos se realizan por lo que es un gran beneficio administrativo para las instituciones.

○ Designaciones de encargados, dentro de este punto las ventajas son las designaciones oficiales sobre los roles de administrador de base de datos, encargado de infraestructura y los sistemas de información, por lo que se reparten las responsabilidades de dichas áreas a encargados oficiales que deben de responder por su área designada.

**Capítulo 4:** seguridad tecnología de la información: las ventajas sobre este capítulo son varias las cuales comprende como gestiones de seguridad, respaldos y cómo se debe de manejar las operaciones por los canales electrónicos dentro las destacables se encuentran:

○ Gestión de la seguridad: dentro de esta gestión se obtiene las ventajas de conocer los posibles riesgos y cómo estos pueden afectar la empresa según su clasificación, además de poder tener control sobre ellos, monitores y quiénes son los responsables de la gestión de estos.

○ Copias de respaldo, la ventaja que provee esto es tener una integridad completa de la información que manejen a pesar de toda adversidad que pueda sucederles, tanto como hechos naturales hasta hechos intencionales, por lo que las instituciones obtendrán como ventaja una integridad completa de su información.

○ Canales seguros: como ventaja se contará con canales seguros para el envío de información por las redes del sistema y afuera del sistema, para garantizar la completa confidencialidad y registros sobre accesos, es decir bitácoras para la seguridad de los datos.

**Capítulo 5:** Continuidad de operaciones de tecnología de la información: dentro de este capítulo se busca garantizar la continuidad de los procesos críticos de las instituciones a pesar de las adversidades que puedan ocurrirle, dentro las ventajas destacables se encuentran:

- Plan de continuidad de operaciones de TI, como ventaja se obtiene un plan que comprenda los procesos críticos de la institución, los cuales son los causantes de las interrupciones en las operaciones, pudiendo ser por fallas tecnológicas, fenómenos naturales o acontecimientos inesperados, los cuales deben de ser identificados y atacados para poder garantizar el funcionamiento o la pronta recuperación de los sistemas. Esto se realizará mediante un análisis de riesgos, de esta manera se logrará una continuidad de operaciones en la institución.
- Pruebas que garanticen lo planificado para lograr que el plan de continuidad se encuentre siempre disponible y no falle al momento de tener algún problema con el sistema principal.
- Como última ventaja y no la menos importante es tener un equipo o centro de cómputo de respaldo el cual garantizará un funcionamiento pronto a la caída del principal y que los procesos críticos puedan seguir su curso sin mayor pérdida.

**Capítulo 6:** procesamiento de información y tercerización: dentro de este se obtienen las ventajas de poder procesar procesos afuera del territorio nacional y el uso de servicios de terceros, algunas ventajas específicas son:

- Las instituciones pueden hacer uso de sistemas de cómputo propios dentro de cualquier parte del territorio nacional.
- Las instituciones pueden hacer uso de servicios de terceros ya sea adentro o fuera del territorio nacional, pero solo mediante por las empresas que estén de acuerdo de cumplir todo lo de la resolución y específicamente el artículo 25 del capítulo 6 de dicha resolución.

**Capítulo 7:** disposiciones transitorias y finales: ventajas directamente dentro de este capítulo únicamente es que en cualquier caso no previsto y sea de carácter especial por parte de la organización esta puede ser planteada hacia la junta monetaria para su solución.

Por otro lado, dentro de las ventajas destacables que no se encuentran específicamente en la JM-102-2011 si no en las nuevas resoluciones son las siguientes

Para la resolución JM-42-2020 Desafíos del Riesgo Cibernético agrega las siguientes ventajas:

- Las instituciones supervisadas contarán con respaldo ante cualquier ciberataque que les sea dirigido mediante la internet.
- La Administración del Riesgo Tecnológico en las entidades financieras brindará mayor confiabilidad y seguridad en sus cuentahabientes o stakeholders en relación con el manejo de la información.
- Se contará con una cultura de ciberseguridad de la información a nivel nacional en el sector bancario y financiero por medio del programa continuo de capacitación del recurso humano y concientización a los usuarios de las instituciones.
- Se contará con el Equipo de Respuesta de incidentes Cibernéticos, un Comité de Gestión de Riesgos y una unidad de Administración de Riesgos, los cuales deben de estar formados por personal multidisciplinario de las distintas áreas de la institución.
- Cada institución podrá contar con un plan estratégico de TI alineado a su estrategia de negocio.
- Administrar y gestionar el riesgo tecnológico de la institución, tomando en cuenta o considerando la naturaleza, complejidad y volumen de sus operaciones.
- Las instituciones contarán con una guía sobre las Políticas y procedimientos la cual les permitirá tener una adecuada gestión del riesgo tecnológico dentro de la entidad, en donde se encontrarán establecidas las metodologías, herramientas y modelos a seguir en caso de un ciberataque.
- Podrán contar con el respaldo de la Unidad de Administración de Riesgo, en donde en conjunto con el Comité en la Administración del Riesgo Tecnológico, tendrán nuevas propuestas y revisiones de forma anual, en donde se establece un plan de recuperación antes desastres.
- Las entidades podrán realizar operaciones y servicios financieros a través de canales electrónicos de forma confiable y segura.

Luego de la resolución JM-42-2020 surge nuevamente otra actualización la cual es JM-104-2021 dentro de esta se mejoró el Reglamento para la Administración del Riesgo Tecnológico, estas son algunas ventajas destacables que no se encuentran en las resoluciones anteriores:

- Implementar las medidas de seguridad y los controles establecidos por las resoluciones ayudan a proteger la información confidencial y datos sensibles de los clientes y proveedores.
- Optimizar procesos operativos y aumentar la eficiencia en las operaciones bancarias a través de la implementación de tecnologías adecuadas y seguras.
- Estandarizar los procesos de gestión de riesgos tecnológicos entre los distintos bancos de Guatemala.

Cada resolución cuenta con diferentes ventajas al momento de su implementación, es por ello por lo que las instituciones deben de realizar el respectivo análisis ante su implementación y considerar cuáles ventajas son favorables y qué puede obtener a través de ellas, de tal manera mejorar y salvaguardar los procesos propios de la institución y tener una ventaja competitiva ante otras instituciones.

### **Establecer la relación con otros marcos de referencia o de trabajo sobre ciberseguridad**

Cada resolución mencionada anteriormente puede tener o establecer una relación con otros marcos de referencia respecto a ciberseguridad los cuales son necesarios mencionar:

#### **COBIT (Control Objectives for Information and Related Technologies):**

COBIT es un marco de referencia utilizado para la gestión y gobierno de la tecnología de la información en las organizaciones. COBIT se enfoca en ayudar a las entidades financieras a establecer un marco de control y gobierno efectivo sobre

sus procesos y sistemas de información. Dichas resoluciones tienen relación con COBIT en términos de establecer controles y medidas adecuadas para garantizar la confidencialidad, integridad, disponibilidad y cumplimiento normativo de la información en el sistema financiero. COBIT proporciona una estructura para la implementación de las medidas de seguridad y controles requeridos por la resolución, y también ayuda a las entidades financieras a evaluar y mejorar su gobierno y gestión de TI.

COBIT proporciona una metodología de trabajo estructurado y basado en mejores prácticas para garantizar el cumplimiento, calidad y confiabilidad de los sistemas de información, además proporciona una lista de objetivos de control relacionados con diferentes dominios de gobierno de TI, lo que permite a las organizaciones evaluar y mejorar los controles existentes, ofrece una serie de indicadores clave de desempeño y métricas para evaluar y monitorear el desempeño de los procesos de TI, esto ayuda a la entidad financiera a asegurarse de que se están cumpliendo con los requisitos normativos y de cumplimiento de las resoluciones de la JM.

**ISO 27001 (International Organization for Standardization 27001):** ISO 27001 es un estándar internacional para la gestión de la seguridad de la información. Está diseñado para ayudar a las organizaciones a establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información (SGSI). De acuerdo con las resoluciones descritas en este documento se relacionan con ISO 27001 en términos de identificar y gestionar los riesgos tecnológicos y establecer controles de seguridad adecuados en las entidades financieras. ISO 27001 proporciona un conjunto de controles y buenas prácticas para la seguridad de la información que pueden ser útiles para cumplir con los requisitos de seguridad establecidos por la resolución. Además, ISO 27001 también enfatiza la importancia de la gestión de riesgos, la continuidad del negocio y la mejora continua, aspectos relevantes para las resoluciones. Básicamente la ISO 270001 se utiliza para proteger la confidencialidad, integridad y disponibilidad de la información.

**NIST (National Institute of Standards and Technology):** El NIST es una agencia del gobierno de los Estados Unidos que ha desarrollado varios marcos y estándares relacionados con la ciberseguridad. Uno de los más destacados es el Framework for Improving Critical Infrastructure Cybersecurity, comúnmente conocido como el NIST Cybersecurity Framework. Este marco proporciona una guía integral para ayudar a las organizaciones a evaluar y mejorar su postura de ciberseguridad. Las resoluciones JM-102-2011, JM-104-2021 y JM-42-2020 pueden beneficiarse del enfoque del NIST en la identificación de riesgos, la protección de activos y la respuesta a incidentes. El NIST Cybersecurity Framework ofrece una estructura sólida para la gestión de riesgos cibernéticos, que se alinea con los objetivos de la resolución al ayudar a las entidades financieras a fortalecer sus medidas de seguridad y reducir la exposición a amenazas y ataques.

**CIS Controls (Center for Internet Security Controls):** Los CIS Controls son un conjunto de mejores prácticas desarrolladas por el Center for Internet Security para ayudar a las organizaciones a proteger sus sistemas y datos contra ciberataques. Estos controles se centran en medidas específicas para prevenir, detectar y responder a las amenazas cibernéticas. La implementación de los CIS Controls puede ser complementaria con las resoluciones al proporcionar directrices detalladas y prácticas recomendadas para mejorar la seguridad y mitigar riesgos en el entorno tecnológico de las entidades financieras. Los CIS Controls abordan áreas clave como el control de acceso, la protección contra malware, la seguridad de la configuración, la monitorización continua y la respuesta a incidentes, aspectos que son relevantes para el cumplimiento de la resolución.

**ITIL (Information Technology Infrastructure Library):** ITIL es un marco de referencia para la gestión de servicios de tecnología de la información. Aunque no está específicamente centrado en la ciberseguridad, el enfoque de ITIL en la entrega de servicios de TI de calidad puede ser útil para las entidades financieras en la implementación de los controles y procesos requeridos por las resoluciones. ITIL proporciona pautas para la gestión del cambio, la gestión de incidentes, la gestión de problemas y otros aspectos que pueden contribuir a una gestión eficiente del

riesgo tecnológico. Estas prácticas pueden ayudar a las entidades financieras a establecer procesos y controles sólidos para garantizar la continuidad del negocio, mitigar riesgos y mantener la calidad de los servicios financieros.

Tomando en consideración que cada día un mayor número de clientes del sector financiero son usuarios de la banca electrónica, realizan transacciones por internet o pagos a través de dispositivos móviles. Esta adaptación de los modelos de negocio y la explotación de canales digitales pretende aprovechar las ventajas de las tecnologías, que tiene como contrapartida la aparición de nuevos riesgos que se deben prevenir con el fin de mitigar los posibles ataques y situaciones de fraude a los que están expuestos actualmente el sector y, por supuesto, sus usuarios.

En el mundo, gran parte de las comunicaciones y procesos son digitales, con lo cual la ciberseguridad no es una alternativa sino un requisito. Los riesgos cibernéticos que afectan al sector gobierno, al sector privado y a las personas tienen unos impactos y una problemática distintos. Cada una de estas normativas y reglamentos tienen como objetivo mitigar la lucha contra el fraude por medio de canales digitales.

## **Establecer los retos sobre las nuevas disposiciones o actualizaciones y como las entidades abordan las mismas**

Cada resolución requiere de retos establecidos los cuales cada institución debe de tomar en consideración para poder manejar y a su vez implementar. Según Azucena Portillo indica que: "Es muy importante se deben dejar claros cuáles son los roles y responsabilidades que los miembros deben cumplir, qué excepciones existen y qué consecuencias puede haber por incumplimientos de esta." Debido a ello se debe de tomar en consideración:

- Definiciones de roles, responsabilidades sobre el cumplimiento y habilidades del Oficial de Seguridad de la Información y Experto en Informática Forense/Digital.

Respecto a las resoluciones tienen como retos realizar y poder cumplir con los siguientes retos y disposiciones:

### **Definiciones de roles**

- Oficial de seguridad de la información: profesional de tecnología encargado de planificar, controlar, desarrollar y velar por gestiones políticas, además administración sobre administraciones y acciones que tengan que ver con la seguridad de la información dentro de la institución (Jiménez, s.f.).
- Experto en informática forense: persona profesional dedicado a recopilar y analizar datos de sistemas informáticos y medios electrónicos para usarlos como alguna evidencia ante un caso legal sobre investigaciones criminales (Coursera, 2023).

### **Responsabilidades sobre el cumplimiento y habilidades**

- **Responsabilidades del oficial de seguridad de la información**

- Toma de decisiones que cumplan todo lo regulado conforme a la seguridad de TI.
- Creación de comité para gestión de riesgos e iniciación o actualización de centro de operaciones de seguridad informática.
- Establecimiento de equipo que responda y vele porque todos los incidentes informáticos se puedan tratar y resolver.
- Implementación y administración sobre procesos de auditoria tales como: continuidad del negocio, recuperación de desastres e investigación.
- Protección de activos, propiedad digital e intelectual.
- Responsable de coordinar la ejecución de análisis de riesgos en la seguridad de información, esto debe de ser aplicable en toda la organización.
- Crear y actualizar políticas de seguridad informática adicionales a la resolución, siempre y cuando se cumpla con los estándares establecidos en la normativa.

- Responsable de asegurarse que los procesos de seguridad informática de la organización estén funcionando de manera correcta. (Jiménez, s.f.).
- **Habilidades del oficial de seguridad de la información:**
  - Conocimiento avanzado sobre sistemas de información, base de datos, criptografía, redes y las normas legales que rigen sobre su institución.
  - Liderazgo, ser autodidacta, toma de decisiones, comunicación eficaz y trabajo en equipo.
  - Buena capacidad de análisis, resolución de problemas y de estrategia.
  - Conocimiento sobre negocios, innovación y servicio al cliente.
- (Jiménez, s.f.).
- **Responsabilidades del experto en informática forense/Digital:**
  - Realizar investigaciones sobre seguridad de sistemas y violaciones de datos.
  - Restaurar sistemas para la obtención de datos y pruebas
  - Realizar recuperaciones de información ya sea oculta, cifrada, eliminada de cualquier dispositivo.
  - Análisis e identificación de equipos comprometidos en procesos de seguridad.
  - Dar testimonios en juicios, proveer pruebas y todo lo relacionado con procedimientos legales.
  - Redacción de informes forenses sobre información técnica e información digital para procedimientos legales (Cómo convertirse en un experto en forense digital, s.f.).
- **Habilidades del experto en informática forense/Digital:**
  - Que posea buenos valores éticos, además de ser integro y confidencial con lo que realiza.
  - Buena atención y comunicación.
  - Buena educación sobre informática forense con gran capacidad de análisis, deducción y lógica.

- Amplia experiencia y con buenos conocimientos sobre sistemas de información, base de datos, criptografía, redes, las normas legales que rigen sobre su institución y conocimiento de amenazas de seguridad.
- Comprensión sobre el funcionamiento de los dispositivos digitales.
- Conocimiento en base de datos de nube.
- Conocimiento en sistemas operativos de LINUX (Cómo convertirse en un experto en forense digital, s.f.).

### **Plan y/o gap análisis que permita establecer el cumplimiento las resoluciones de la junta monetaria en una institución supervisada**

Un plan o análisis de brechas para verificar el cumplimiento de la resolución debe de comprender lo siguientes puntos:

1. Comprensión total sobre la resolución JM: dentro de este proceso de plan se debe de comprender en totalidad la resolución a comprobar, debido a que con base a ese conocimiento se preparan las herramientas que se utilizarán para la obtención de la información que se requiera para calificar el nivel de cumplimiento, todo dependerá de cómo se realice la evaluación, entre las más utilizadas se encuentran:

- a. Lista de ítems.
- b. Lista de tareas.
- c. Lista de preguntas
- d. Lista de verificación.
- e. checklists.
- f. Hoja de verificación.
- g. Formularios de inspección.

Finalmente, en este paso del plan también debe de considerarse contar con el listado de requisitos de hardware, software y todo lo relacionado con la gestión de riesgos tecnológicos para también comprobar que se tenga un sistema actualizado según indique la resolución.

2. Revisión detallada de los procesos y políticas de la institución: en esta etapa se considera el análisis detallado y revisión de: procesos, documentación, políticas, estándares aplicados, manuales, entre otros, todo lo que sea de interés para el investigador y considere que sea necesario para evaluar el nivel de cumplimiento, en esta misma etapa se harán uso de las herramientas que convengan según como el investigador desee proceder, dentro de estas herramientas se encuentran:

- a. Entrevista.
- b. Obtención de manuales.
- c. Obtención de datos.
- d. Cuestionarios.
- e. Auditoría de software y hardware.
- f. Matrices de evaluación.
- g. Observación.
- h. Grupo focales.
- i. Encuestas longitudinales.

Antes de la realización de la planificación se debe de realizar un estudio de las herramientas más eficaces y que mejor se acoplan a la institución para garantizar el éxito de la recolección de la información.

3. Comprobación de los lineamientos: esta es una de las etapas más importantes dentro de esta planificación, la cual por medio de análisis de todos los datos recopilados de la institución a evaluar y el uso de las herramientas planteadas al inicio se obtendrá el resultado del nivel de cumplimiento, se deberá de proceder con el análisis de los resultados, con base a una matriz o alguna lista que contenga los resultados esperados se deberán de comparar con los resultados obtenidos, de esta manera se podrá encontrar el nivel de cumplimiento, esto se debe de hacer en cada área en la que se obtuvo información respecto la resolución.

4. Documentación de las brechas encontradas: luego de haber finalizado el análisis de datos y obtener el resultado, se debe de escribir el informe detalladamente, aclarando los aspectos en los que la empresa no cumple, remarcar

los cumplidos y finalmente un apartado en donde se coloquen propuestas de mejoras, detalles sobre aspectos encontrados, conclusiones y recomendaciones para futuros análisis.

#### **A. Informe de diagnóstico con nivel de madurez COBIT.**

COBIT se puede definir como un grupo de herramientas de apoyo que es dirigida a los gerentes o altos mandos de una organización, esto para reducir la brecha que puede existir entre los requerimientos de control, temas tecnológicos y riesgos del negocio (Esan, 2016)

Teniendo claro lo que es el marco de trabajo COBIT, se ha diseñado una encuesta con el fin de evaluar el nivel de madurez de los procesos con el marco de referencia COBIT para el gobierno y cumplimiento en la organización. Dicha encuesta fue trasladada al jefe de cumplimiento, ya que es la persona que tienen el conocimiento de los procesos del departamento de TI. La encuesta está compuesta por 69 preguntas las cuales fueron de apoyo a recabar la información necesaria. El objetivo de la encuesta también es identificar si existen buenas prácticas en cuanto al diseño y control de los procesos actuales, adicional también apoya a poder identificar el nivel de madurez de los procesos en la organización. Dicha encuesta puede ser encontrada en el anexo 2 del presente documento.

Para el marco de referencia COBIT existen cuatro dominios en los que fueron evaluados los procesos, los cuales son los siguientes:

1. Planear y organizar (PO).
2. Adquirir e implementar (AI).
3. Entrar y Dar Soporte (DS).
4. Monitorear y Evaluar (ME)

Teniendo en cuenta los dominios en los que fueron evaluados los procesos, se tiene que definir niveles de madurez que nos proporciona el marco de referencia COBIT, los diferentes niveles son los siguientes:

1. No Existente: La organización no ha reconocido que hay problemas por resolver.
2. Inicial: La organización ya tiene conocimiento de problemas existentes y necesita solventarlos.
3. Repetitivo: Se cuenta con procesos en los cuales existen procedimientos similares en diferentes áreas de la organización.
4. Definido: Todos los procedimientos han sido estandarizados y documentados.
5. Administrado: Se puede medir y monitorear el cumplimiento de los procedimientos y tomas medidas en los que no funcionan de manera efectiva.
6. Optimizado: Los procesos son utilizados para la mejora continua del negocio.

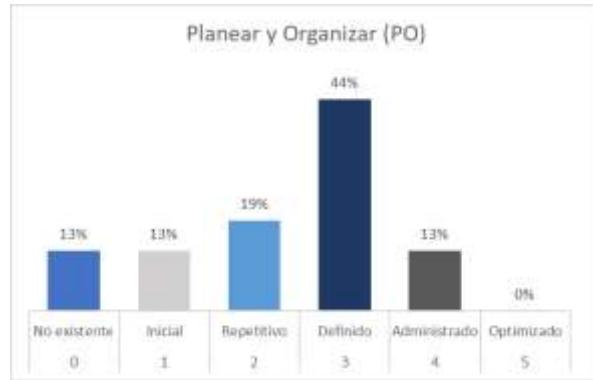
**Figura 1.** Tabla de detalle de niveles de madurez

Nivel	Nombre
0	No existente
1	Inicial
2	Repetitivo
3	Definido
4	Administrado
5	Optimizado

Nota: Son los niveles de madurez que pueden tener los procesos del marco de referencia COBIT. Fuente: Elaboración propia.

Luego de tener claro los niveles de madurez de COBIT y también los dominios, se procede a demostrar los resultados arrojados en la encuesta. Como primer punto se muestran los resultados que se obtuvieron en el domino PLANEAR Y ORGANIZAR (PO).

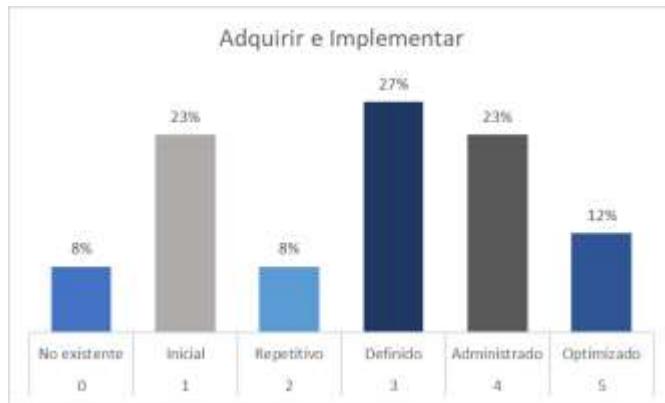
**Figura 2.** Resultados de dominio planear y organizar marco de referencia COBIT.



Nota: Se describe los resultados de la encuesta del dominio planear y organizar. Fuente: Elaboración propia.

Se logra observar que para el dominio PLANEAR Y ORGANIZAR se detecta que los niveles de madurez la organización se encuentra en el nivel 3 como primer lugar con un 44% y como segundo lugar se encuentra en el nivel 2 con el 19%.

**Figura 3.** Resultados de dominio adquirir e implementar marco de referencia COBIT.



Nota: Se describe los resultados de la encuesta del adquirir e implementar. Fuente: Elaboración propia.

Para el dominio de ADQUIRIR E IMPLEMENTAR, predomina el nivel 3 con un 27%, esto indica que aún hay procesos que cuentan con inconvenientes pero que aún falta actuar sobre ellos, pero a pesar de esto, el nivel de madurez de este dominio al igual que el anterior es el nivel 3.

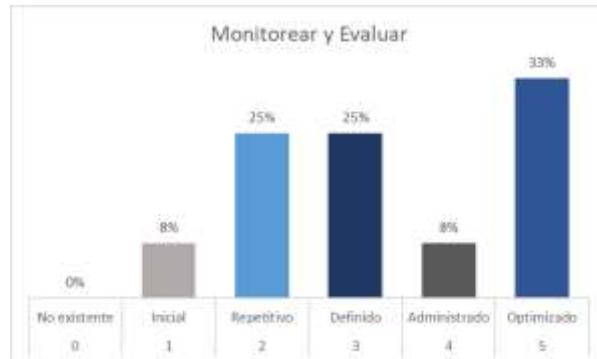
**Figura 4.** Resultados de dominio entregar y dar soporte marco de referencia COBIT.



Nota: Se describe los resultados de la encuesta del dominio entregar u dar soporte. Fuente: Elaboración propia.

Los procesos clasificados dentro del dominio ENTRAR Y DAR SOPORTE se encuentran clasificados en el nivel 2 con el 33%, esto indica que existen procesos que pueden ser replicables a otras áreas de la organización, pero falta mejorar mucho en esta sección.

**Figura 5.** Resultados de dominio monitorear y evaluar marco de referencia COBIT.



Nota: Se describe los resultados de la encuesta del monitorear y evaluar. Fuente: Elaboración propia.

Para el dominio MONITOREAR Y EVALUAR, los procesos en su mayoría se encuentran en el nivel 5 con un 33%, esto quiere decir que se ha aplicado correctamente buenas prácticas a estos procesos y ayudan a la mejora continua del negocio.

Ahora bien, el resultado general de la evaluación de los procesos en la institución es el siguiente:

**Figura 6.** Resultados generales del nivel de madurez del marco de referencia COBIT.



Nota: Se describe el nivel de madurez alcanzado por la organización en los procesos implementados. Fuente: Elaboración propia.

Se logró detectar que el departamento de IT ha alcanzado un nivel de madurez número 3 en sus procesos, ya que es el que predomina con un 29%, esto quiere decir que la mayoría de los procesos del departamento y organización han sido estandarizados y documentados, por lo que las buenas prácticas se han implementado de manera correcta. Aunque como se logra observar en los resultados, existen procesos que se encuentran en los niveles 0,1 y 2, sobre estos se debe de tomar acción para poder minimizar la cantidad de procesos en esos niveles para que todos puedan cumplir un estándar alto, esto brinda una oportunidad de mejora a la organización para que puedan cumplir con la documentación, estandarización y comunicación en todos los procesos de la entidad bancaria.

## **Propuesta de procedimiento para el análisis forense digital de incidentes cibernéticos**

El análisis forense digital desempeña un papel crucial en la respuesta a incidentes cibernéticos en el sector bancario de Guatemala. En este contexto, se propone un procedimiento que cumple con las leyes y regulaciones bancarias del

país. El procedimiento abarca etapas clave, como la recolección de evidencia, el análisis forense, la elaboración de informes y el cumplimiento legal. Se destaca la importancia de proteger la privacidad y cumplir con las regulaciones de protección de datos personales, así como establecer una cadena de custodia sólida. El procedimiento propuesto para cumplir al punto “e” del Artículo 24 es el siguiente:

### **Preparación**

a) Establecer un equipo forense digital: El equipo forense digital debe estar compuesto por profesionales capacitados en análisis forense digital y expertos en leyes y regulaciones bancarias de Guatemala. Se deben asignar roles específicos dentro del equipo, como analistas forenses, expertos en adquisición y análisis de evidencia digital, especialistas en análisis de malware y coordinadores de comunicaciones. Además, es importante que el equipo reciba una formación continua para mantenerse actualizado sobre las últimas técnicas y tendencias en el análisis forense digital en el ámbito bancario.

b) Definir responsabilidades: Cada miembro del equipo forense debe tener responsabilidades claramente definidas y entender su rol en el proceso de análisis forense. Esto incluye designar un líder del equipo para coordinar las actividades, establecer canales de comunicación claros con otros departamentos y asegurarse de que se cumplan los requisitos legales y regulatorios. También se debe establecer una estrecha colaboración con el departamento legal del banco para garantizar que el proceso de análisis forense cumpla con las leyes y regulaciones pertinentes.

c) Crear un plan de respuesta: El banco debe desarrollar un plan de respuesta a incidentes cibernéticos personalizado, adaptado a las leyes y regulaciones bancarias de Guatemala. Este plan debe incluir procedimientos detallados para la detección, notificación, respuesta y recuperación de incidentes cibernéticos. También debe abordar la preservación y adquisición forense de evidencia digital, la gestión de la cadena de custodia y la colaboración con las autoridades competentes. El plan de respuesta debe ser revisado y actualizado regularmente para asegurarse de que esté alineado con los requisitos legales y regulatorios vigentes.

## Recolección de evidencia

- a) Preservación de la escena del incidente: Es crucial preservar la escena del incidente para evitar la alteración o destrucción de la evidencia. El equipo forense debe actuar rápidamente para aislar y asegurar los sistemas y dispositivos afectados. Esto implica asegurar la integridad de los medios de almacenamiento, tomar imágenes forenses de discos duros y otros dispositivos, y recopilar registros y registros de actividad relevantes. Además, se deben mantener registros detallados de todas las acciones tomadas y garantizar la cadena de custodia de la evidencia recolectada.
- b) Obtención de autorización legal: Antes de realizar cualquier actividad de recolección de evidencia, se debe obtener la autorización legal correspondiente de acuerdo con las leyes y regulaciones bancarias de Guatemala. Esto puede implicar obtener órdenes judiciales o solicitar la asistencia de las autoridades competentes. El equipo forense debe trabajar en estrecha colaboración con el departamento legal del banco para garantizar que se cumplan todos los requisitos legales y regulatorios, y que se respeten los derechos de privacidad y protección de datos.
- c) Adquisición forense de datos: Durante la recolección de evidencia, se deben utilizar técnicas y herramientas forenses reconocidas que cumplan con los estándares de adquisición forense de datos en el contexto bancario. Esto implica utilizar software y hardware especializados para realizar copias forenses de los sistemas, dispositivos móviles, registros de red y otros medios digitales relevantes. Es fundamental asegurar que la evidencia se adquiera de manera forensemente sólida, preservando su integridad y autenticidad.
- d) Registro y documentación: Durante el proceso de recolección de evidencia, el equipo forense debe mantener registros detallados y documentar cada paso del proceso. Esto incluye registrar la fecha, hora y ubicación de la recolección de evidencia, así como los detalles de los sistemas y dispositivos involucrados. Además, se deben documentar las técnicas y herramientas utilizadas, los resultados obtenidos y cualquier observación relevante. Esta documentación será fundamental

para respaldar los hallazgos y conclusiones durante el análisis forense y cualquier procedimiento legal posterior.

e) Cumplimiento de la cadena de custodia: La cadena de custodia es un aspecto crítico del análisis forense digital. El equipo forense debe establecer y mantener una cadena de custodia sólida para garantizar la integridad y la trazabilidad de la evidencia recolectada. Esto implica registrar y documentar cada cambio de posesión o custodia de la evidencia, asegurando que se mantenga bajo condiciones seguras y controladas. Se deben seguir los protocolos establecidos por las leyes y regulaciones bancarias de Guatemala, así como las mejores prácticas reconocidas en la gestión de la cadena de custodia.

### **Análisis de la evidencia**

a) Análisis forense digital: Durante el análisis forense de la evidencia recolectada, se deben aplicar técnicas y metodologías forenses reconocidas para identificar las causas del incidente, los métodos utilizados por los atacantes y el alcance del impacto en el banco y sus clientes. Se deben utilizar herramientas forenses avanzadas y realizar análisis exhaustivos de los registros de actividad, archivos de registro, imágenes de disco y otros artefactos digitales relevantes. Todo el proceso de análisis debe llevarse a cabo siguiendo los estándares y las mejores prácticas reconocidas en el campo del análisis forense digital.

b) Análisis de malware: En caso de identificar malware durante el análisis forense, se debe realizar un análisis detallado para comprender su funcionamiento, la forma en que se introdujo en los sistemas del banco y los posibles impactos en la seguridad y la confidencialidad de la información. Esto puede requerir la colaboración con expertos en seguridad informática y la participación de las autoridades competentes, como la Unidad de Delitos Informáticos del Ministerio Público en Guatemala. El análisis de malware debe seguir los protocolos establecidos por las leyes y regulaciones bancarias, así como las mejores prácticas de la industria en materia de análisis y respuesta a incidentes.

c) Análisis de metadatos: Durante el análisis forense, se deben examinar los metadatos asociados con los archivos y las comunicaciones relevantes para el

incidente cibernético. Esto puede incluir metadatos de archivos, metadatos de correos electrónicos, registros de actividad de red, registros de acceso a sistemas, entre otros. El análisis de metadatos puede ayudar a establecer la secuencia de eventos, las relaciones entre los actores involucrados y otros detalles importantes para la investigación. Sin embargo, es fundamental tener en cuenta las leyes de privacidad y protección de datos personales en Guatemala al analizar y utilizar los metadatos recolectados.

d) Análisis de registros de red: Los registros de red desempeñan un papel crucial en el análisis forense digital de incidentes cibernéticos en un banco. Estos registros pueden proporcionar información sobre las actividades de los atacantes, las rutas de acceso utilizadas, los patrones de tráfico sospechosos y otros indicios importantes. El equipo forense debe analizar y correlacionar los registros de red para reconstruir la secuencia de eventos, identificar las vulnerabilidades explotadas y determinar el impacto del incidente en el sistema bancario. El análisis de registros de red debe cumplir con las leyes y regulaciones bancarias de Guatemala, así como las prácticas recomendadas en el manejo de registros y auditoría.

e) Análisis de comunicaciones: Durante el análisis forense, se debe investigar las comunicaciones relacionadas con el incidente cibernético. Esto puede incluir análisis de correos electrónicos, mensajes instantáneos, registros de llamadas y otros medios de comunicación utilizados por los atacantes o involucrados en el incidente. El análisis de comunicaciones puede proporcionar información valiosa sobre los actores involucrados, sus intenciones y las técnicas utilizadas. Sin embargo, es fundamental respetar la privacidad y cumplir con las leyes y regulaciones bancarias relacionadas con la interceptación y el análisis de comunicaciones en Guatemala.

### **Informe forense**

a. Elaboración del informe: Una vez completado el análisis forense, se debe preparar un informe detallado que documente los hallazgos, conclusiones y recomendaciones derivados del análisis. El informe forense debe ser claro, preciso y completo, siguiendo los requisitos legales y regulatorios establecidos por las leyes

bancarias de Guatemala. Debe incluir una descripción del incidente, los sistemas y dispositivos afectados, los métodos utilizados por los atacantes, el impacto en el banco y sus clientes, así como las medidas recomendadas para mitigar futuros incidentes. El informe debe presentar la evidencia recolectada de manera ordenada y estructurada, respaldando cada conclusión y recomendación con los datos y los análisis correspondientes.

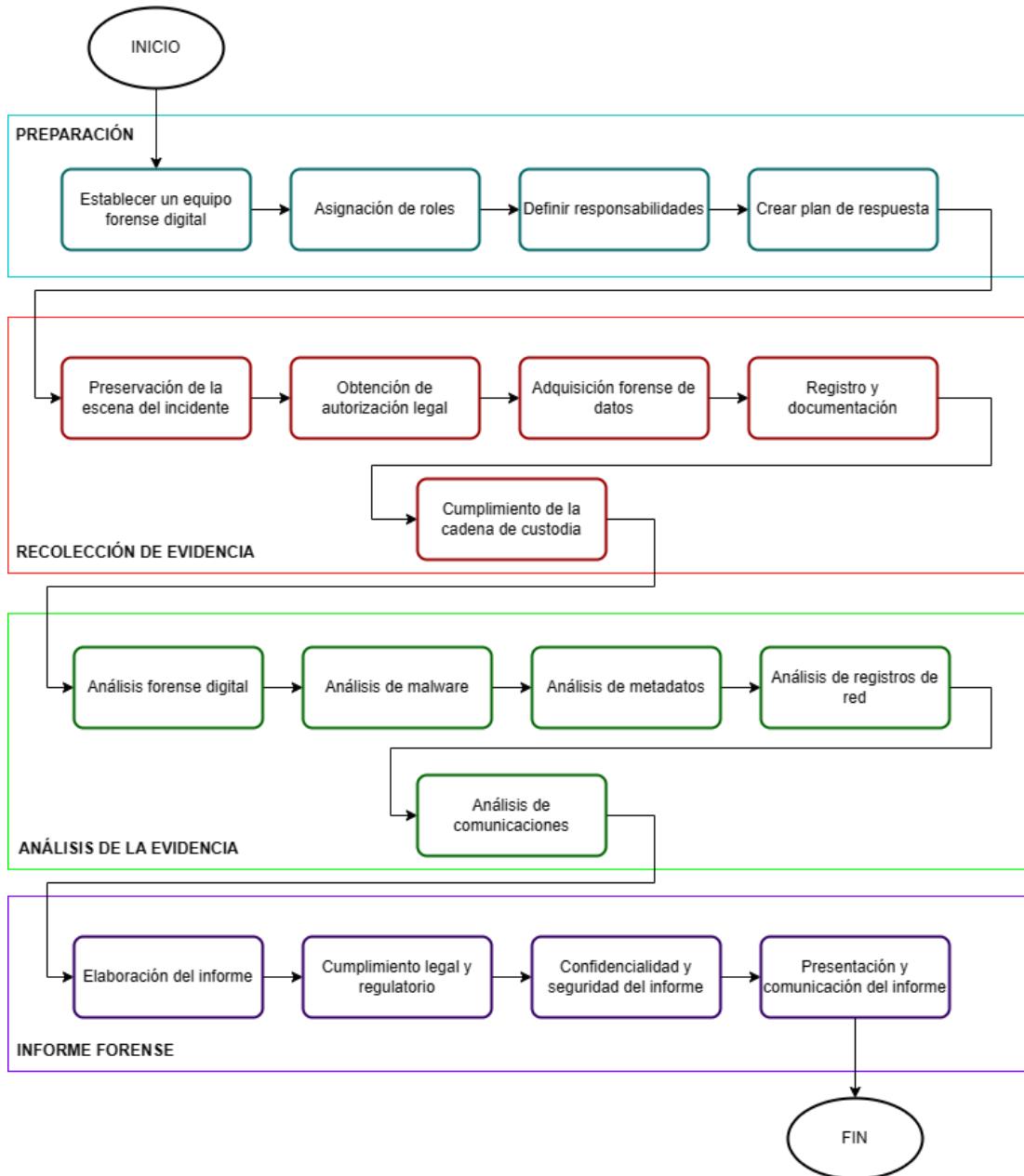
b. Cumplimiento legal y regulatorio: Durante la redacción del informe forense, es fundamental asegurarse de que todas las acciones y recomendaciones estén en pleno cumplimiento de las leyes y regulaciones bancarias de Guatemala. Esto implica respetar las normas de protección de datos personales, cumplir con las regulaciones de notificación de incidentes ciberneticos y cumplir con las disposiciones legales aplicables. El informe forense debe ser redactado teniendo en cuenta estas obligaciones legales y regulatorias, y debe ser presentado de acuerdo con los procedimientos establecidos por las autoridades competentes en Guatemala.

c. Confidencialidad y seguridad del informe: El informe forense debe tratarse como un documento confidencial y estar sujeto a medidas de seguridad adecuadas. Se deben establecer controles de acceso y distribución para garantizar que solo las partes autorizadas tengan acceso al informe. Además, se debe tener en cuenta cualquier restricción legal o contractual en relación con la divulgación de la información contenida en el informe. Es importante que el equipo forense trabaje en estrecha colaboración con el departamento legal del banco para garantizar que se cumplan todas las medidas de confidencialidad y seguridad establecidas por las leyes y regulaciones bancarias de Guatemala.

d. Presentación y comunicación del informe: El informe forense debe presentarse de manera clara y comprensible para las partes interesadas, incluyendo la alta dirección del banco, el departamento legal y los responsables de la seguridad de la información. El equipo forense debe preparar una presentación verbal del informe, destacando los aspectos clave y respondiendo a cualquier pregunta o inquietud. Es importante transmitir de manera efectiva los hallazgos y

recomendaciones del informe, enfatizando la importancia de tomar medidas correctivas y preventivas para fortalecer la seguridad cibernética del banco.

**Figura 7.** Procedimiento para el análisis forense digital de incidentes cibernéticos



Nota: Dentro de este diagrama de flujo se describe detalladamente cada paso que se debe de realizar para la realización del informe forense. Fuente: elaboración propia.

## **Sanciones y/o penalizaciones por parte de la SIB ante el incumplimiento de dichas resoluciones**

Actualmente la SIB no tiene sanciones relacionadas a las resoluciones JM-102-2011, JM-42-2020 y JM-104-2021. Sin embargo, la Superintendencia de Bancos se toma muy en serio el cumplimiento de la legislación y regulaciones vigentes en Guatemala es por lo cual que luego de realizar una investigación y análisis exhaustivo se plantea las siguientes multas, sanciones y medidas adicionales para el cumplimiento de estas:

### **Multas económicas**

- Se impondrán multas proporcionales basadas en la gravedad del incumplimiento y la magnitud de las consecuencias causadas (Congreso de la República de Guatemala, 2002).
- Las multas varían en función de diferentes factores, como el tamaño de la entidad financiera, el volumen de transacciones afectadas, el número de clientes perjudicados y la duración del incumplimiento (Congreso de la República de Guatemala, 2002).
- Se impondrán multas adicionales por cada día que persista el incumplimiento después de la notificación oficial de la Superintendencia de Bancos (Congreso de la República de Guatemala, 2002).
- Las multas serán aplicadas en concordancia con la Ley de Bancos y Grupos Financieros de Guatemala y las regulaciones emitidas por la Superintendencia de Banco (Congreso de la República de Guatemala, 2002).

### **Suspensión temporal de operaciones**

- La Superintendencia de Bancos podrá ordenar la suspensión temporal de las operaciones en su totalidad o actividades específicas de la entidad financiera, como la suspensión de determinados servicios, productos o líneas de negocio que se encuentren en incumplimiento (Decreto 18-2002).

- Durante el periodo de suspensión, la entidad financiera deberá cesar inmediatamente las actividades afectadas y tomar medidas correctivas para rectificar las deficiencias identificadas (Decreto 18-2002).

- La duración de la suspensión varía dependiendo de la gravedad del incumplimiento y de los esfuerzos demostrados por la entidad financiera para corregir las deficiencias y cumplir con los requisitos establecidos en la resolución (Decreto 18-2002).

- Esta medida se encuentra respaldada por la Ley de Supervisión Financiera de Guatemala (Decreto 18-2002).

### **Prohibición de actividades específicas**

- La Superintendencia de Bancos podría prohibir a la entidad financiera llevar a cabo ciertas actividades o servicios específicos que estén directamente relacionados con los incumplimientos detectados. Por ejemplo, se podría prohibir la implementación de nuevos sistemas tecnológicos hasta que se demuestre el cumplimiento de los estándares de seguridad establecidos en la resolución (Superintendencia de Bancos de Guatemala, s.f.).

- La prohibición podría levantarse una vez que la entidad financiera haya implementado las medidas correctivas necesarias y haya demostrado su capacidad para cumplir con los requisitos de la resolución (Superintendencia de Bancos de Guatemala, s.f.).

### **Responsabilidad penal**

- En casos de incumplimientos graves que involucren delitos financieros o afecten la integridad y confianza del sistema financiero, la Superintendencia de Bancos puede remitir el caso a las autoridades judiciales competentes (Superintendencia de Bancos de Guatemala, s.f.).

- Las autoridades judiciales podrán iniciar un proceso penal contra los responsables del incumplimiento, lo que podría resultar en penas de prisión, multas adicionales y otras sanciones legales establecidas en la legislación vigente, como la Ley contra el Lavado de Dinero u otros delitos financieros (Superintendencia de Bancos de Guatemala, s.f.).

## Sanciones administrativas

- La Superintendencia de Bancos podrá imponer sanciones administrativas adicionales, como la suspensión o destitución de los directivos o funcionarios responsables del incumplimiento (Superintendencia de Bancos de Guatemala, s.f.).
- Estas sanciones se basarán en la Ley de Bancos y Grupos Financieros de Guatemala y otras regulaciones aplicables.

## Retirada de licencia

- En casos extremos de incumplimiento persistente o incumplimientos graves que representen un riesgo significativo para la estabilidad financiera o la seguridad de los clientes, la Superintendencia de Bancos podría revocar la licencia de operación de la entidad financiera (Superintendencia de Bancos de Guatemala, s.f.).
- La revocación de la licencia implicaría el cese completo de las operaciones de la entidad financiera y la prohibición de continuar realizando actividades bancarias en el país (Superintendencia de Bancos de Guatemala, s.f.).
- Esta medida se tomaría como último recurso, cuando otras sanciones no hayan sido efectivas para corregir los incumplimientos y proteger los intereses de los clientes y del sistema financiero (Superintendencia de Bancos de Guatemala, s.f.).

Es fundamental tener en cuenta que las multas, sanciones y medidas adicionales mencionadas están sujetas a la legislación y regulaciones vigentes en Guatemala. La Superintendencia de Bancos tiene la facultad y el deber de aplicar las sanciones correspondientes, en cumplimiento de dichas normativas, con el objetivo de proteger la estabilidad y solidez del sistema financiero y garantizar la confianza y protección de los clientes (Superintendencia de Bancos de Guatemala, s.f.).

## Casos de sanciones en Guatemala

Con base a las sanciones mencionadas anteriormente se detallan algunos casos de su aplicabilidad en el territorio nacional en el siguiente listado:

• Para la entidad financiera nombrada Financiera Consolidados. S. A., se emitió en el mes de marzo del año 2023 una infracción con la cantidad de \$5,200, debido a que en su manual de riesgo tecnológico y plan de recuperación ante desastres no incluye los aspectos necesarios y requeridos dentro del reglamento para la administración del riesgo tecnológico poniendo en riesgo tanto su cómputo principal como el alterno (Superintendencia de Bancos, 2023).

• A la entidad de Banco Agromercantil de Guatemala S. A., se emitió en el mes de febrero del año 2023 una infracción con la cantidad de \$1,300 por la razón de incumplir con el reglamento para la administración del riesgo tecnológico, debido a que no posee políticas y procedimientos sobre una administración adecuada de riesgos permanentemente dentro de su manual (Superintendencia de Bancos, 2023).

• A la institución del Crédito Hipotecario nacional de Guatemala se emitió en el mes de diciembre del año 2022 una infracción con el monto de \$1,300 por el motivo de no enviar el manual de administración del riesgo tecnológico actualizado y su plan de recuperación ante desastres en el tiempo establecido incumpliendo con el reglamento de la administración del riesgo tecnológico (Superintendencia de Bancos, 2022).

• Para la entidad financiera conocida como Banco de Desarrollo Rural S. A., se emitió en el mes de mayo del año 2022 una infracción con el monto de \$1,300 por no cumplir con lo mínimo sobre el plan de recuperación ante desastre que rige el reglamento de administración del riesgo tecnológico (Superintendencia de Bancos, 2022).

• Al Banco de Desarrollo Rural S. A. en el mes de diciembre del año 2016 se le infraccionó debido a que su centro de cómputo alterno no cuenta con lo necesario para alguna emergencia, es decir no cumple con lo mínimo física y lógicamente de sistemas necesarios para otorgar la continuidad de procesos críticos por lo que se le sancionó con \$1,300, todo esto de acuerdo con el reglamento de administración del riesgo tecnológico (Superintendencia de Bancos, 2016).

- Al banco Bac Banck. Inc. en el mes de marzo del año 2016 se le infraccionó debido a que no tenía un centro de cómputo alterno dentro del territorio guatemalteco, no obstante, se realizó fuera del territorio nacional incumpliendo con el reglamento para la administración de riesgos tecnológicos por lo cual se le sancionó con \$10,100 (Superintendencia de Bancos, 2016).
- Banco Americano, S. A., se emitió en el mes de junio del año 2011 una infracción por el monto de \$3,100 por no tener implementado en el tiempo estipulado un sitio alterno de operaciones críticas de acuerdo con el mismo plan que ellos proveyeron (Superintendencia de Bancos, 2011).

## Conclusiones

• A medida que las tecnologías avanzan, se generan constantemente nuevas formas de procesamiento y almacenamiento de datos. Sin embargo, este progreso también conlleva un incremento en los ataques ciberneticos, ya que los actores malintencionados buscan obtener información sensible con fines perjudiciales. Es imperativo estar al tanto de estas nuevas amenazas y contar con medidas de seguridad actualizadas para salvaguardar de manera efectiva la información confidencial. Solo a través de una comprensión profunda de las últimas tendencias en ciberseguridad y una implementación proactiva de las mejores prácticas se puede mitigar el riesgo y asegurar la integridad de los datos.

• Es crucial gestionar de manera adecuada los riesgos asociados a la tecnología con el fin de proteger la información confidencial, salvaguardar la reputación de la organización y cumplir con los reglamentos y normativas establecidas. La correcta gestión de los riesgos tecnológicos implica la implementación de medidas preventivas y de mitigación, así como la adopción de prácticas de seguridad sólidas. Al hacerlo, se fortalece la protección de la información sensible, se preserva la confianza de los clientes y se evitan posibles repercusiones legales o sanciones regulatorias. La gestión adecuada de los riesgos tecnológicos se convierte en una prioridad estratégica para las organizaciones, permitiéndoles mantener una postura segura y resiliente en un entorno digital en constante evolución.

• La implementación y el cumplimiento de los reglamentos y resoluciones relacionados con el riesgo tecnológico tienen múltiples beneficios. Estas acciones permiten identificar y evaluar los posibles riesgos de manera efectiva, respaldan la toma de decisiones informadas y basadas en análisis sólidos. Además, contribuyen a la protección de la información, refuerzan la seguridad de los sistemas y aseguran la continuidad del negocio frente a posibles interrupciones tecnológicas. Al cumplir con estos reglamentos, las organizaciones establecen una base sólida para gestionar y mitigar los riesgos tecnológicos, lo que resulta fundamental en un entorno empresarial cada vez más dependiente de la tecnología.

## Recomendaciones

- Buscar asesoramiento de expertos en gestión de riesgos y tecnología, y formar un equipo con personas altamente capacitadas en el tema, para contar con conocimientos técnicos y de cumplimiento adecuados.
- Realizar un análisis exhaustivo de los sistemas, tecnologías y procesos existentes con el objetivo de identificar riesgos, vulnerabilidades y posibles amenazas. Este análisis debe ser integral y considerar tanto aspectos técnicos como normativos y legales.
- Establecer controles y llevar a cabo un monitoreo constante para garantizar el cumplimiento de los requisitos, reglas y normas establecidos en las resoluciones vigentes de la junta monetaria de Guatemala. Esto incluye la implementación de medidas de seguridad, auditorías periódicas y revisiones internas para asegurar el cumplimiento continuo.
- Brindar capacitaciones regulares, implementar mejoras y mantenerse actualizado sobre las resoluciones y la información relevante. Esto permitirá fortalecer los procesos, tener un mayor control y rendimiento, y desarrollar planes de contingencia efectivos en caso de que ocurra algún evento inesperado en la institución. La capacitación y la actualización constante son fundamentales para mantenerse al día con las mejores prácticas y las últimas tendencias en gestión de riesgos y tecnología.

## Referencias bibliográficas

- Azucena Portillo, 12 diciembre 2022. "Guía para hacer una Política de Seguridad de la Información". Recuperado de: <https://www.piranirisk.com/es/academia/especiales/guia-politica-de-seguridad-de-la-informacion#:~:text=Realizar%20la%20gesti%C3%B3n%20de%20riesgos%20sobre%20activos%20de,activos%20de%20informaci%C3%B3n%20que%20est%C3%A1n%20bajo%20su%20administraci%C3%B3n>.
- Carlos Villamizar. 19 mayo 2022. "¿Qué es COBIT y para qué sirve?". Recuperado de: <https://www.globalsuitesolutions.com/es/que-es-cobit/>
- Conexión Esan, 01 de junio 2016. Cinco Principios de COBIT 5. Recuperado de: <https://www.esan.edu.pe/conexion-esan/los-cinco-principios-de-cobit-5#:~:text=COBIT%205%20es%20un%20marco,las%20TI%20en%20la%20empresa>
- Congreso de la República de Guatemala. (2002). Ley de Bancos y Grupos Financieros (Decreto Número 19-2002). Recuperado de: [https://www.banguat.gob.gt/sites/default/files/banguat/leyes/2021/ley\\_bancos\\_y\\_grupos\\_financieros.pdf](https://www.banguat.gob.gt/sites/default/files/banguat/leyes/2021/ley_bancos_y_grupos_financieros.pdf)
- CyberSecurity Información y Privacidad, 31 diciembre 2020. Análisis de la normativa JM 42-2020. Recuperado de: <https://csecmagazine.com/2020/12/31/ley-de-proteccion-de-datos/>
- Decreto 18-2002 Ley de supervisión financiera, Guatemala.
- Desafíos del Riesgo Cibernético, Recuperado de: <https://www.oas.org/es/sms/cicte/docs/Desafios-del-riesgo-cibernetico-en-el-sector-financiero-para-Colombia-y-America-Latina.pdf>
- GlobalSuite Solutions. 20 marzo 2023. "¿Qué es la norma ISO 27001 y para qué sirve?". Recuperado de: <https://www.globalsuitesolutions.com/es/que-es-la-norma-iso-27001-y-para-que-sirve/>

Investigador de informática forense: Guía profesional 2023. (s.f.). Coursera.  
<https://www.coursera.org/mx/articles/computer-forensic-investigator>

Jiménez, M. M. (s.f.). Rol del analista forense digital en la ciberseguridad.  
<https://www.piranirisk.com/es/blog/rol-analista-forense-digital-ciberseguridad>

Josue Theissen. 18 de enero 2022. "Reglamento para la Administración del Riesgo Tecnológico en Guatemala." Recuperado de:  
<https://www.bdvanguardia.com/reglamento-para-la-administracion-del-riesgo-tecnologico-en-guatemala/>

Julia Martins, 1 de febrero 2023. ¿Qué es la gestión de riesgos? Recuperado de:  
<https://asana.com/es/resources/project-risk-management-process>

Luis Vilalobos. 28 de febrero 2023. "Resolución JM-47 2022: Objetivos, principales retos, importancia de una implementación con visión integral del riesgo." Recuperado de: <https://www.bdvanguardia.com/resolucion-jm-47-2022-objetivos-principales-retos-importancia-de-una-implementacion-con-vision-integral-del-riesgo/>

Superintendencia de Bancos de Guatemala. (s.f.). Inicio. Recuperado de  
<https://www.sib.gob.gt/>

Superintendencia de Bancos, 2023. Leyes y Normativas. Recuperado de:<https://www.sib.gob.gt/web/sib/superintendencia>

Superintendencia de Bancos. (2011). Suplemento con información de instituciones sujetas a la vigilancia e inspección de la SIB.  
[https://www.sib.gob.gt/web/sib/informacion\\_sistema\\_financiero/suplemento-mensual?p\\_p\\_id=110\\_INSTANCE\\_n1HH&p\\_p\\_action=0&p\\_p\\_state=maximized&p\\_p\\_mode=view&p\\_p\\_col\\_id=&p\\_p\\_col\\_pos=0&p\\_p\\_col\\_count=0&\\_110\\_INSTANCE\\_n1HH\\_struts\\_action=%2Fdocument\\_library\\_display%2Fview&\\_110\\_INSTANCE\\_n1HH\\_folderId=369724](https://www.sib.gob.gt/web/sib/informacion_sistema_financiero/suplemento-mensual?p_p_id=110_INSTANCE_n1HH&p_p_action=0&p_p_state=maximized&p_p_mode=view&p_p_col_id=&p_p_col_pos=0&p_p_col_count=0&_110_INSTANCE_n1HH_struts_action=%2Fdocument_library_display%2Fview&_110_INSTANCE_n1HH_folderId=369724)

Superintendencia de Bancos. (2016). Suplemento con información de instituciones sujetas a la vigilancia e inspección de la SIB.  
[https://www.sib.gob.gt/web/sib/informacion\\_sistema\\_financiero/suplemento-mensual?p\\_p\\_id=110\\_INSTANCE\\_n1HH&p\\_p\\_action=0&p\\_p\\_state=maximized&p\\_p\\_mode=view&p\\_p\\_col\\_id=&p\\_p\\_col\\_pos=0&p\\_p\\_col\\_count=0&\\_110\\_INSTANCE\\_n1HH\\_struts\\_action=%2Fdocument\\_library\\_display%2Fview&\\_110\\_INSTANCE\\_n1HH\\_folderId=369724](https://www.sib.gob.gt/web/sib/informacion_sistema_financiero/suplemento-mensual?p_p_id=110_INSTANCE_n1HH&p_p_action=0&p_p_state=maximized&p_p_mode=view&p_p_col_id=&p_p_col_pos=0&p_p_col_count=0&_110_INSTANCE_n1HH_struts_action=%2Fdocument_library_display%2Fview&_110_INSTANCE_n1HH_folderId=369724)

zed&p\_p\_mode=view&p\_p\_col\_id=&p\_p\_col\_pos=0&p\_p\_col\_count=0&\_110\_INSTANCE\_n1HH\_struts\_action=%2Fdocument\_library\_display%2Fview&\_110\_INSTANCE\_n1HH\_folderId=2991446

Superintendencia de Bancos. (2022). Suplemento con información de instituciones sujetas a la vigilancia e inspección de la SIB.  
[https://www.sib.gob.gt/web/sib/informacion\\_sistema\\_financiero/suplemento-mensual?p\\_p\\_id=110\\_INSTANCE\\_n1HH&p\\_p\\_action=0&p\\_p\\_state=maximized&p\\_p\\_mode=view&p\\_p\\_col\\_id=&p\\_p\\_col\\_pos=0&p\\_p\\_col\\_count=0&\\_110\\_INSTANCE\\_n1HH\\_struts\\_action=%2Fdocument\\_library\\_display%2Fview&\\_110\\_INSTANCE\\_n1HH\\_folderId=9760495](https://www.sib.gob.gt/web/sib/informacion_sistema_financiero/suplemento-mensual?p_p_id=110_INSTANCE_n1HH&p_p_action=0&p_p_state=maximized&p_p_mode=view&p_p_col_id=&p_p_col_pos=0&p_p_col_count=0&_110_INSTANCE_n1HH_struts_action=%2Fdocument_library_display%2Fview&_110_INSTANCE_n1HH_folderId=9760495)

Superintendencia de Bancos. (2023). Suplemento con información de instituciones sujetas a la vigilancia e inspección de la SIB.  
[https://www.sib.gob.gt/web/sib/informacion\\_sistema\\_financiero/suplemento-mensual?p\\_p\\_id=110\\_INSTANCE\\_n1HH&p\\_p\\_action=0&p\\_p\\_state=maximized&p\\_p\\_mode=view&p\\_p\\_col\\_id=column-2&p\\_p\\_col\\_pos=1&p\\_p\\_col\\_count=3&\\_110\\_INSTANCE\\_n1HH\\_struts\\_action=%2Fdocument\\_library\\_display%2Fview&\\_110\\_INSTANCE\\_n1HH\\_folderId=9817723](https://www.sib.gob.gt/web/sib/informacion_sistema_financiero/suplemento-mensual?p_p_id=110_INSTANCE_n1HH&p_p_action=0&p_p_state=maximized&p_p_mode=view&p_p_col_id=column-2&p_p_col_pos=1&p_p_col_count=3&_110_INSTANCE_n1HH_struts_action=%2Fdocument_library_display%2Fview&_110_INSTANCE_n1HH_folderId=9817723)

## Anexos

### Anexo 1. Entrevista gestión de riesgos tecnológico y ciberseguridad.

Link de entrevista con el experto de la entidad financiera de Guatemala:  
<https://drive.google.com/file/d/12Fx2kYRi-sFJUnn0vfvojQBkV-B1QQaK/view?usp=sharing>

### Anexo 2. Instrumento de evaluación.

**Figura 8.** Encuesta para la obtención de resultados del nivel de madurez COBIT del dominio planear y organizar en la entidad financiera.

COBIT	PREGUNTA	Escala				
		0	1	2	3	4
PLANEAR Y ORGANIZAR (PO)						
PO1	¿Involucra a la gerencia general para diseñar los ANS de los servicios contratados alineando tecnología con procesos de negocio?	X				
PO4	¿El proveedor se integra adecuadamente a los procesos de la organización?				X	
PO4	¿Cuenta con una clasificación de sus proveedores, catalogados de acuerdo con el tipo de proveedor, la importancia y la criticidad de los servicios que prestan?			X		
PO7	¿Durante la entrega de los servicios contratados, realiza validación y prueba de servicios?			X		
PO8	¿Tiene un plan de acción cuando los servicios no van a estar operando por cambios programados?		X			
PO4	¿Tienen políticas de seguridad de la información aplicables a toda la organización?				X	
PO4	¿Tiene un proceso establecido para que las demás áreas de la empresa puedan crear incidentes de seguridad?		X			
PO6	¿Lleva a cabo campañas de concientización de la seguridad de la información?			X		
PO6	¿Tiene un programa de capacitación de seguridad de la información a las demás áreas de la empresa?			X		
PO4	¿Tiene procedimientos para coordinar esfuerzos para incorporar el tema de la seguridad de la información con las demás áreas que gestionan datos que no son unidades de TI?	X				
PO3	¿Tiene establecidas políticas para garantizar la seguridad de la información en la navegación en internet?		X			
PO8	¿La empresa ha realizado alguna vez las evaluaciones post-incidente para identificar las causas subyacentes de una interrupción del servicio y para desarrollar medidas de prevención?		X			
PO6	¿Se cuenta con capacitación y concienciación del personal encargado de la gestión de los servidores?	X				
PO6	¿Los altos mandos de la organización entienden claramente los riesgos informáticos?	X				
PO6	¿Se ha establecido un plan de comunicación y notificación que incluya procedimientos específicos para alertar al personal, clientes y proveedores en caso de interrupciones del servicio?			X		
PO3	¿Tiene un proceso establecido para darle seguimiento a las solicitudes de los incidentes de seguridad?			X		

Nota: Se describen las preguntas sobre los procesos de la organización que correspondan al grupo planear y organizar del marco de referencia COBIT.

**Figura 9.** Encuesta para la obtención de resultados del nivel de madurez COBIT del dominio entregar y dar soporte en la entidad financiera.

COBIT	PREGUNTA	Escala				
		0	1	2	3	4
<b>ENTREGAR Y DAR SOPORTE (DS)</b>						
DS2	¿Ha evaluado el riesgo asociado a desastres naturales y causados por el hombre a las instalaciones de sus proveedores de servicio?		X			
DS2	¿Ha identificado y realizado un plan para mitigar los riesgos relacionados con la habilidad de los proveedores para mantener una efectiva entrega de servicios de forma segura y eficiente sobre una base de continuidad?	X				
DS2	¿Realiza una verificación de antecedentes en el proceso de selección de proveedores?					X
DS12	¿Cuenta con un procedimiento estándar para establecer, modificar y concluir contratos de servicios de conectividad?	X				
DS2	¿Involucra al departamento legal durante el proceso de contratación de servicios de conectividad?					X
DS2	¿Cuenta con un proceso para la documentación de las bases de datos de los nuevos servicios?					X
DS8	¿Internamente se realizan informes de seguimiento de los incidentes encontrados?					X
DS1	Realiza un desglose de incidentes por categoría de seguridad de la información	X				
DS8	Lleva un control de número incidentes de seguridad de la información acumulados					X
DS8	Lleva un control de número y porcentaje incidentes de seguridad de la información graves					X
DS8	¿Cuenta con un formato estándar y entendible para informar los incidentes de seguridad a todos los interesados?	X				
DS8	¿Las estadísticas de monitoreo son analizadas para identificar tendencias positivas y negativas de cada uno de los servicios?		X			
DS8	¿La empresa cuenta con planes de continuidad con respecto al área de telecomunicaciones?					X
DS9	¿En algún momento se ha probado el plan de contingencia y logrado identificar algún área deficiente en este?		X			
DS12	¿Tiene un proceso definido para la actualización de las bases de datos luego de un cambio?					X

Nota: Se describen las preguntas sobre los procesos de la organización que correspondan al grupo entregar y dar soporte del marco de referencia COBIT.

**Figura 10.** Encuesta para la obtención de resultados del nivel de madurez COBIT del dominio adquirir e implementar en la entidad financiera.

COBIT	PREGUNTA	Escala				
		0	1	2	3	4
<b>ADQUIRIR E IMPLEMENTAR (AI)</b>						
AI7	¿Tiene un plan para detectar riesgos de seguridad de la información en conexiones remotas?	X				
AI7	¿Tiene un plan para detectar riesgos de seguridad de la información en sistemas que gestionan datos?					X
AI5	¿Tiene un plan para supervisar la instalación y mantenimiento de firewall en los servidores de la empresa?					X
AI6	¿Tiene establecidos lineamientos generales para las configuraciones de conexión a internet?					X
AI6	¿Tiene políticas de seguridad de la información para el proceso de instalación de hardware?					X
AI5	¿Ha realizado una verificación física de las condiciones de los centros de datos de sus proveedores?	X				
AI6	¿Cuenta con una estructura de enlace, comunicación y coordinación con los proveedores?					X
AI6	¿Cuenta con un marco de trabajo con roles y responsabilidades que brinde un proceso formal de administración de niveles de servicio entre la organización y el proveedor?		X			
AI2, DS1	¿Cuenta con un proceso para hacer cumplir los derechos y obligaciones de sus proveedores y la organización en los términos contractuales, que comprendan los criterios de aceptación, para la adquisición de infraestructura, instalaciones y servicios de conectividad?					X
AI5	¿Cuenta con un proceso formal de administración de relaciones con proveedores por cada proveedor?					X
AI3	¿Se han instalado sistemas de detección y extinción de incendios, como detectores de humo y rociadores automáticos?					X
AI1	Cuando de aplican cambios nuevos en los sistemas, ¿se tiene en cuenta los riesgos que pueden ocurrir?	X				
AI6	¿Se cuenta con algún archivo de identificación y documentación de los servidores?					X
AI6	¿Se tiene un documento con la versión de los sistemas operativos instalados en los servidores?					X
AI6	¿Se tiene un documento con los parches de seguridad y actualizaciones instaladas en los servidores?					X
AI6	¿Se cuenta con un documento sobre los permisos y accesos autorizados a los servidores?					X
AI6	¿Se cuenta con política de contraseñas en los servidores?					X
AI3	¿Se cuenta con un documento con los firewalls instalados y su configuración?					X
AI6	¿Se cuenta con la documentación sobre la evaluación de la configuración de los servicios de red en los servidores?	X				
AI6	¿Se cuenta con documentación sobre la revisión de los sistemas de copias de seguridad y su correcto funcionamiento?		X			
AI2	¿Se cuenta con documentación sobre la evaluación de las aplicaciones instaladas en los servidores y su seguridad?					X
AI6	¿Se cuenta con documentación sobre la verificación de la presencia de malware o virus en los servidores?					X
AI6	¿Se cuenta con documentación de la revisión de los protocolos de acceso remoto a los servidores?		X			
AI6	¿Se cuenta con documentación sobre la verificación de la protección física de los servidores?					X
AI6	¿Se cuenta con documentación sobre la evaluación de los sistemas de monitorización y detección de intrusiones en los servidores?	X				
AI6	¿Se cuenta con documentación sobre las pruebas a los sistemas de detección y extinción de incendios?		X			

Nota: Se describen las preguntas sobre los procesos de la organización que correspondan al grupo adquirir e implementar del marco de referencia COBIT.

**Figura 11.** Encuesta para la obtención de resultados del nivel de madurez COBIT del dominio monitorear y evaluar en la entidad financiera.

COBIT	PREGUNTA	Escala				
		0	1	2	3	4
<b>MONITOREAR Y EVALUAR (ME)</b>						
ME2	¿Se encuentra implementado las medidas correspondientes de de backup y redundancia adecuadas para los sistemas de telecomunicaciones, como la copia de seguridad de los datos críticos y la disponibilidad de sistemas de respaldo?					X
ME1	¿Se ha probado alguna vez la capacidad de recuperación de los backups y sistemas redundantes?	X				
ME2	¿Se tiene identificado los riesgos asociados a las telecomunicaciones, como interrupciones del servicio, fallos de hardware o software, y errores humanos dentro del plan de continuidad?			X		
ME2	¿Se tienen establecidos procedimientos para la revisión y respuesta a las alertas de monitoreo?	X				
ME3	¿Se cuenta con políticas de gestión de riesgos y contingencias en los servidores?		X			
ME2	¿Se cuenta con documentación sobre la verificación de la existencia de políticas de gestión de riesgos y contingencias en los servidores?			X		
ME1	¿Se cuenta con protocolos de acceso remoto a los servidores?					X
ME1	¿Los servidores se encuentran en una ubicación segura y de acceso restringido?				X	
ME4	¿El acceso a los servidores está controlado mediante cámaras de vigilancia?	X				
ME4	¿El acceso a los servidores está controlado mediante sistemas de alarma?		X			
ME4	¿Los servidores se encuentran en una sala con acceso restringido mediante cerraduras, tarjetas de acceso o sistemas biométricos?					X
ME4	¿Existe un registro de los ingresos a los servidores físicos?	X				

Nota: Se describen las preguntas sobre los procesos de la organización que correspondan al grupo monitorear y evaluar del marco de referencia COBIT.

Universidad Mariano Gálvez de Guatemala  
Facultad de Ingeniería de Sistemas de Información  
Maestría en Seguridad de Informática  
Proyecto de Investigación II  
50/50 Pts. 100/100 Pts.  
Ing. Juan Pedro Cáceres López



Juan  
Pedro  
Cáceres  
López

Firmado  
digitalmente  
por Juan Pedro  
Cáceres López  
Fecha:  
2023.12.05  
00:51:02 -06'00'

## PRINCIPALES ATAQUES INFORMÁTICOS Y VULNERABILIDADES QUE SE PRESENTAN DENTRO DE UNA ENTIDAD DEL GOBIERNO DE GUATEMALA

<i>Nombre</i>	<i>Carnet</i>
Bryan Orlando Aguirre Sagastume	1293-17-646
Ricardo Alejandro Pérez Rodríguez	1293-17-1255
Jonathan Renato del Cid Juárez	1293-15-10369

Guatemala, 30 de noviembre 2023.

# PRINCIPALES ATAQUES INFORMÁTICOS Y VULNERABILIDADES QUE SE PRESENTAN DENTRO DE UNA ENTIDAD DEL GOBIERNO DE GUATEMALA

¿Cuál es la mejor manera de evitar los ataques informáticos?

**Bryan Orlando, Aguirre Sagastume**  
baguirres@miumg.edu.gt  
Universidad Mariano Gálvez de Guatemala  
Guatemala, Guatemala

**Ricardo Alejandro, Pérez Rodríguez**  
rpererzr8@miumg.edu.gt  
Universidad Mariano Gálvez de Guatemala  
Guatemala, Guatemala

**Jonathan Renato, del Cid Juárez**  
jdelcidj@miumg.edu.gt  
Universidad Mariano Gálvez de Guatemala  
Guatemala, Guatemala

## **Resumen.**

*Las entidades gubernamentales de Guatemala, siendo los rectores primordiales de la administración pública, se enfrentan a los diferentes cambios tecnológicos y al incremento mundial de ataques ciberneticos. Muchas veces estos cambios digitales y tecnológicos, con base a las nuevas tecnologías que día a día juegan un papel importante en los procesos y a la continuidad del giro del negocio. Estas tecnologías les permiten brindar un mejor servicio a los ciudadanos que requieren la información precisa y confiable. Los cambios tecnológicos dentro de la administración pública son necesarios para poder afrontar a las nuevas amenazas y procesos que requieren una mejor infraestructura, concientización y modernización para que se resguarden los datos importantes y el activo primordial.*

**Palabras claves:** Antivirus, ataque informático, Entidad de gobierno de Guatemala, sistemas de información, políticas, ataques frecuentes en organizaciones.

***Abstract.***

*Technological innovation is experiencing constant growth globally, especially in the context of information security. In this sense, we observe an adaptation gap in organizations, particularly in government sectors that are carrying out the adoption and awareness of cyber-attacks that they face every day on their local infrastructure to a totally different and abstract environment, which in turn offers numerous benefits. Through the surveys carried out, it has been confirmed that 67% of the attacks that the Ministry of Economy suffered during 2022 were phishing, as well as 100% of the time the information backup procedure is carried out. but in comparison to the 70% in which it is indicated that the main problem of vulnerabilities is the human factor. The data collected reveals the existence of a gap, motivated by poor information and adaptation of technological processes and a lack of awareness of cyber dangers.*

***Keywords.***

*Cyber-attacks, phishing, vulnerabilidades, backup data*

## **1 Materiales y Métodos**

### **1.1 Materiales**

Las técnicas de recolección de datos y materiales utilizados durante la investigación y proceso del artículo fueron de tipo electrónico, tanto como para las entrevistas y también de igual manera la recolección de datos, esto se realizó con la herramienta Google Forms, luego se compartió dicha encuesta al personal responsable de responderla por medio de correo electrónico o WhatsApp, después se unificó, analizó y luego se presentaron los resultados de las encuesta con el uso de software tales como Excel, Power BI y Power Point.

### **1.2 Métodos**

La metodología utilizada fue la de investigación descriptiva, debido a que únicamente se desea recopilar y comprobar información sobre los ataques y vulnerabilidades dentro de la entidad gubernamental.

Las investigaciones van dirigidas a ciertos grupos de estudio, es decir, personas, objetos, casos, entre otros, con la finalidad de obtener respuestas, para este caso se detalla el siguiente grupo de estudio: La investigación se realizará en una entidad del gobierno de Guatemala la cual es la encargada de hacer cumplir el régimen jurídico al desarrollo de

actividades productivas del comercio interno, externo, la protección del consumidor y del fomento de la competencia. Haciendo uso del tipo de estudio descriptivo y el diseño de investigación no experimental transeccional para obtener la información del tema

#### **1.2.1 Diseño no experimental**

Se utilizó el diseño no experimental debido a que es un enfoque de investigación en el cual el investigador no manipula directamente las variables independientes, sino que observa y analiza las relaciones entre las variables y en este caso los ataques que se realizan a la entidad del gobierno.

#### **1.2.2 Árbol de Marco Metodológico**

- Tipo de investigación
- Descripción del ámbito de la investigación
- Población y muestra
- Técnicas e instrumentos para la recolección de datos
- Validez y confiabilidad del instrumento
- Plan de recolección y procesamiento de datos.

## 2 Resultados

### 2.1 Población y Muestra

Se determina que la población de interés comprende a los miembros del departamento de Tecnologías de la Información (IT), así como de sus organismos dependientes. Respecto a la muestra, se incluye a la totalidad de los individuos. Teniendo en cuenta el número de empleados del departamento de IT asciende a 30 colaboradores.

La población del estudio será todo el personal que pertenece al departamento de IT de la entidad de gobierno. La muestra es todo personal que pertenece al departamento de IT de la entidad de gobierno y todas sus dependencias. Dada la cantidad de personal dentro de la entidad se toma la elección de no hacer muestreo sino un censo de 30 trabajadores.

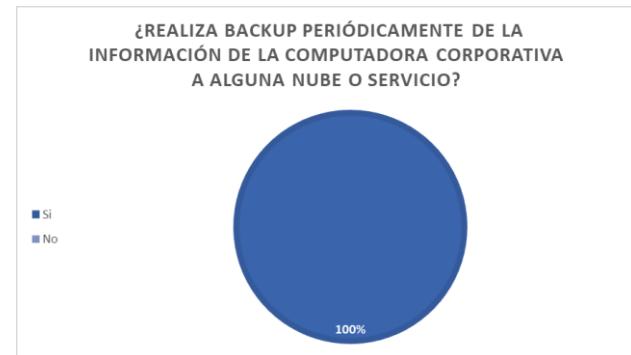
### 2.2 Encuestas

Luego de realizar la encuesta a los empleados de la entidad, se tabularon los datos para analizarlos con herramientas de análisis de datos que permitan graficar los datos e interpretarlos de una manera sencilla.



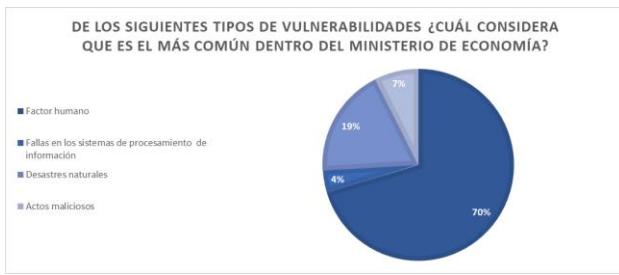
*Fuente: Elaboración propia*

El 67% de encuestados indicaron que el ataque más frecuente es Phishing y el 33% indicó que el otro ataque más frecuente es Malware.



*Fuente: Elaboración propia*

El 100% de los encuestados indicó que, sí se realizan backups periódicamente, es un resultado bastante satisfactorio ya que con esto se asegura que existe integridad en la información y que al momento que suceda algún incidente la información puede ser recuperada con rapidez.



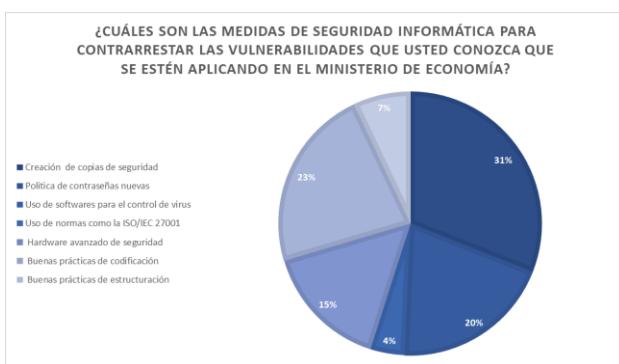
*Fuente: Elaboración propia*

El factor humano fue el tipo de vulnerabilidad más común y alto que indicaron los encuestados con un 70%, en segundo lugar, los desastres naturales y en tercer lugar los actos maliciosos. En este caso existe una brecha de mejora para reducir el 70% de vulnerabilidad de factor humano, realizando planes de concientización, capacitaciones, entre otros.



*Fuente: Elaboración propia*

El 72% de encuestados indicó que el área que debe de mejorar en el aspecto de seguridad informática es la de Desarrollo, como segundo lugar a mejorar es el área de Operaciones con el 20% y por último el área de Soporte con un 8%.



*Fuente: Elaboración propia*

Los encuestados indicaron que una de las medidas para contrarrestar las vulnerabilidades en la entidad es la creación de copias de seguridad con un 31%, buenas prácticas de codificación al momento de desarrollar con un 23% y creación de políticas de contraseñas nuevas con un 20%.

### 3 Marco Teórico.

#### 3.1 Entidad de Gobierno

La entidad de gobierno es la entidad gubernamental responsable de implementar la legislación relacionada con el desarrollo de actividades productivas no agrícolas, comercio interno y externo y protección al consumidor. También se ocupa de promover la inversión y la competitividad en el desarrollo industrial y comercial.

Por medio del acuerdo gubernativo No. 182-2000, se considera la creación y distribución orgánica de la estructura de la entidad de gobierno. Por lo tanto, se descentralizan tres viceministerios. Viceministerio de inversión y competencia, Viceministerio de integración y

comercio exterior y el Viceministerio de desarrollo a la MIPYME.

En el artículo 18 se crea la subgerencia de informática la cual tiene como principales funciones la supervisión de adquisición, creación, instalación, administración y mantenimiento de sistemas y equipos informáticos y de comunicación, así como la introducción y resguardo de la información de la entidad. Seguridad operativa y de infraestructura.

### **3.2 Vulnerabilidades**

Con el constante aumento de los ataques informáticos a través de medios digitales y de servicios tecnológicos. La seguridad se ha convertido en un punto fundamental para los procesos complejos. La implementación de tecnologías da un gran beneficio a las labores y transformación digital.

Los sistemas de información son propensos a la manipulación y hackeo por parte de personas con intenciones no favorables para las organizaciones, así mismo las vulnerabilidades no existen únicamente en la infraestructura de redes hiperconvergentes, si no que en los sistemas desarrollados con el fin de poder sistematizar los procesos.

Para la OWASP (Open Web Application Security Project), categoriza las vulnerabilidades en 10 categorías, las cuales son:

- Control de Acceso Deficiente
- Fallas Criptográficas
- Inyecciones SQL
- Diseño Inseguro
- Configuraciones Incorrectas
- Componentes Vulnerables
- Fallas de Identificación
- Fallas de Integridad
- Fallas de Registro y Monitoreo
- Falsificación de Peticiones

Para Guatemala se clasifican los ataques más frecuentes, como los ataques de publicaciones falsas, robos de identidad, ciberacoso, ciberestafas, phishing por correos. Así como estos tipos de vulnerabilidades aumentaron durante la pandemia del COVID 19 teniendo un 42% de aumento en comparación con el año 2019.

### **3.3 Ataques informáticos**

Un ataque informático es conocido como el intentar ingresar a un sistema o equipo de computación con el objetivo de provocar daños al propietario, consiste en identificar una falla o brecha de seguridad para penetrar con algún método con el fin de obtener un beneficio o

simplemente producir una consecuencia perjudicial entre las cuales suelen ser: sustraer información importante o íntima de la persona o empresa atacada, detener total o parcialmente las operaciones de una organización, divulgar datos sensibles, conseguir una remuneración económica por revertir el perjuicio.

Durante el primer trimestre del año dos mil veintidós los ataques con mayor frecuencia, son los siguiente, que se mencionan por orden de concurrencia fueron: publicidad falsa (consiste en colocar información engañosa sobre un producto o servicio en páginas web), robo de identidad (es usar intencionalmente el nombre o usuarios de una persona para realizar actividades sin su consentimiento para obtener ganancias personales), ciberacoso (trata de un hostigamiento que se realiza por medio de redes sociales o cualquier cana digital) y ciberestafas, residen en invitar a la persona a realizar una acción y a cambio el delincuente tiene algo a cambio sin el consentimiento real de la persona afectada.

Los ataques que consisten en obtener información de la persona o empresa se realizan con diferentes objetivos que podrían ser divulgar información comprometedora para la reputación de una organización de sus clientes, proveedores o de la misma entidad, solicitar una extorsión a

cambio de recuperar los datos o bien de que no se publiquen o simplemente eliminarlos.

### 3.4 Prevención

Es importante contar tanto con tecnología como con un equipo humano que también realice un análisis en tiempo real de transacciones o anomalías en los servicios o equipos de la empresa o dispositivos propios para tener mayor seguridad y protección.

Una recomendación efectiva y fácil de realizar es mantener un antivirus de suscripción anual o mensual de licencia original con sus actualizaciones al día, que no sea pirata o una marca no reconocida, ya que es el que se encarga de identificar y eliminar software que considere peligroso del dispositivo incluso antes de que ingrese al sistema y haya hecho algún daño. El antivirus constantemente está realizando un análisis y una comparación de los archivos que se encuentran en el dispositivo contra una base de datos que tiene la compañía de varios modelos de malwares reconocidos.

Para las empresas es altamente recomendable establecer políticas a los empleados para prevenir el mal uso del equipo informático brindado por la corporación, es importante añadir controles como bloquear puertos USB, prohibir la navegación libre en

internet, colocar doble factor de autenticación para ingresar a los sistemas de la organización, crear un estándar para tener contraseñas seguras, cambiar contraseñas mensualmente, no registrar el correo electrónico corporativo en ningún sitio para motivos personales o de estudio, no utilizar el equipo para realizar tareas o investigaciones que no sean atribución del puesto, obligarlos a realizar copias de seguridad de la información periódicamente y velar por que estas normas sean cumplidas a través de auditorías anual o mensualmente.

## 5 Conclusiones

La entidad de gobierno cuenta con muy buenas prácticas de seguridad informática dentro de las cuales se puede destacar el respaldo periódico que se realizan en las diferentes instalaciones asegurando la integridad de la información de esta entidad, además del correcto uso de dispositivos de firewall y programas informáticos como antivirus para garantizar la seguridad dentro de su infraestructura, destacando que el 56% de las encuestas tienen como primer barrera un antivirus y seguido de firewall y antivirus en conjunto.

Dentro de las encuestas, los encuestados destacaron la importancia de implementar en su plenitud las normas ISO como un régimen

obligatorio que debiera de utilizarse en la organización para poder proveer de una mayor seguridad en los sistemas informáticos, esto resaltado en las encuestas en donde el 45% de las respuestas indican que las vulnerabilidades son debido a faltas de las normas y otro 17% a políticas seguido de un 18% por falta de concientización hacia el personal.

Conforme lo anterior, las encuestas también revelaron que el tipo de vulnerabilidad más destacado que se tiene dentro de esta entidad es el factor humano, siendo mencionado en el 70% de las encuestas, seguido de desastres naturales y actos maliciosos, por lo que resulta realmente preocupante debido a que de acuerdo con las encuestas el 67% de los ataques se centra en phishing que ataca a su factor más vulnerable de esta entidad, seguido de un 33% de malware identificado por los sistemas de seguridad.

Como recomendación y anotaciones encontradas dentro de las encuestas se insta a todas las organizaciones el uso completo de alguna norma ISO que provea de buena seguridad a sus sistemas, haciendo gran enfoque en la concientización y capacitación de los usuarios o empleados, además de enfocar varios parámetros de seguridad en el área de desarrollo, operaciones y soporte para garantizar en la

organización una buena integridad de información y seguridad en sus sistemas.

## Referencias

- Alsina Rodríguez, J. M. (2015). Recomendaciones para prevenir ciberataques (Bachelor's thesis, Universidad Piloto de Colombia). Recuperado de: <http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2922/Trabajo%20de%20grado.pdf?sequence=1&isAllowed=y>
- Anónimo (s.f.). Historia del Mineco en Guatemala. Recuperado de: [https://www.mineco.gob.gt/sites/default/files/informacion%20publica/historia\\_mineco\\_.pdf](https://www.mineco.gob.gt/sites/default/files/informacion%20publica/historia_mineco_.pdf)
- Armas Vega, E. A. (2016). Herramientas de análisis dinámico de vulnerabilidades en aplicaciones web.
- Cando-Segovia, M. R., & Chicaiza, R. P. M. (2021). Prevención en ciberseguridad: enfocada a los procesos de infraestructura tecnológica. 3 c TIC: cuadernos de desarrollo aplicados a las TIC, 10(1), 17-41. Recuperado de: <https://dialnet.unirioja.es/servlet/articulo?codigo=7888164>
- Castro, M. I. R., Morán, G. L. F., Navarrete, D. S. V., Cruzatty, J. E. Á., Anzáles, G. R. P., Mero, C. J. Á., ... & Merino, M. A. C. (2018). Introducción a la seguridad informática y el análisis de vulnerabilidades (Vol. 46). 3Ciencias.
- Centro estadístico de observación y monitoreo de ciberdelitos en Guatemala. (2022). Estadísticas de ciberdelitos en el año 2022. Recuperado de: <https://ogdi.org/estadisticas>
- Corbino, M. (2022). La importancia de capacitar a sus empleados sobre los riesgos de un ciberataque. Boletín del Departamento de Seguridad Internacional y Defensa. Recuperado de: [http://sedici.unlp.edu.ar/bitstream/handle/10915/141816/Documento\\_completo.pdf?sequence=1&isAllowed=y](http://sedici.unlp.edu.ar/bitstream/handle/10915/141816/Documento_completo.pdf?sequence=1&isAllowed=y)
- Daniel Valero (2014). Los diez principales riesgos informáticos. Recuperado de: <https://www.lasprovincias.es/economia/empresas/201409/30/principales-riesgosinformaticos-20140930162144.html>
- Dragonjar. (s.f.). Vulnerabilidades y Amenazas informáticas. Dragonjar. Recuperado de: <https://www.dragonjar.org/vulnerabilidades-y-amenazas-informaticas.xhtml>
- Fernández Yubal. (2017). La historia de Creeper, el primer virus informático jamás programado. Recuperado de: <https://www.xataka.com/historia-tecnologica/la-historia-de-creeper-el-primer-virus-informatico-jamas-programado>
- Fernando Sevillano. (2017). Infografía: Las 7 causas más habituales de un ciberataque a empresas. Recuperado de: <https://willistowerswatsonupdate.es/ciberseguridad/infografia-las-7-causas-mashabituales-de-los-ciberataques-a-empresas/>
- Figueroa-Suárez, J. A., Rodríguez-Andrade, R. F., Bone-Obando, C. C., & Saltos-Gómez, J. A. (2018). La seguridad informática y la seguridad de la información. Polo del conocimiento, 2(12), 145-155.
- Hernández Suarez, J. H., & Peña Lévano, S. F. (2019). Análisis y diseño de controles informáticos críticos en la ética informática para minimizar las vulnerabilidades en el acceso de las historias clínicas electrónicas.
- Incibe. (2017). Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian? INCIBE. Recuperado de: <https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian>
- Instituto Nacional de Ciberseguridad de España. (2021). Glosario de términos de Ciberseguridad. Recuperado de: [https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia\\_glossario\\_ciberseguridad\\_2021.pdf](https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glossario_ciberseguridad_2021.pdf)
- Iván Belcic. (2022). ¿Qué es el malware? Recuperado de: <https://www.avast.com/es-es/c-malware>
- Izquierdo Cabrera, J., & Tafur Callirgos, T. E. (2017). Mecanismos de seguridad para contrarrestar ataques informáticos en servidores web y base de datos. Recuperado de: <https://repositorio.uss.edu.pe/handle/20.500.12802/4062>
- Jorge Mieres. (2009). Ataques informáticos, debilidades de seguridad comúnmente explotadas. Recuperado de: [https://www.evilfingers.net/publications/white\\_AR/01\\_Ataques\\_informaticos.pdf](https://www.evilfingers.net/publications/white_AR/01_Ataques_informaticos.pdf)
- Kaspersky Lab. (2022). Daños causados por el malware. Recuperado de: <https://encyclopedia.kaspersky.es/knowledge/damage-caused-by-malware/>
- Marta Romero. (2021). Los principales tipos de ataques informáticos y cómo protegernos ante ellos. Recuperado de: <https://computerhoy.com/reportajes/tecnologia/malware-que-es-tipos-840271>
- Olmedo, J. I., & Gavilánez, F. L. (2018). Análisis de los ciberataques realizados en América Latina. INNOVA Research Journal, 3(9), 172-181. Recuperado de: <http://201.159.222.115/index.php/innova/article/view/837>
- Programa MIPYMES y Cooperativas (2022). Sistema Nacional de Calidad. Recuperado de: <https://programamipymesycooperativas.gob.gt/sistema-nacional-de-calidad>
- Romero Castro, M. I., Figueroa Morán, G. L., Vera Navarrete, D. S., Álava Cruzatty, J. E., Parrales Anzáles, G. R., Álava Mero, C. J., Murillo Quimiz, Á. L. y Castillo Merino, M. A. (2018). Introducción a la seguridad informática y el análisis de vulnerabilidades. Editorial Científica 3Ciencias. Recuperado de: <https://doi.org/10.17993/ingytec.2018.46>
- Temperini, M. G. (2014). Delitos Informáticos en Latinoamérica: Un estudio de derecho comparado. In XLIII Jornadas Argentinas de Informática e Investigación Operativa (43JAIIO)-XIV Simposio Argentino de Informática y Derecho (SID) (Buenos Aires, 2014).
- Villacís, G. V., & Morocho, R. A. R. (2017). Vulnerabilidades y amenazas a los servicios web de la intranet de la universidad técnica de Babahoyo. 3c Tecnología: glosas de innovación aplicadas a la pyme, 6(1), 53-66.
- WordPress. (2022). WordPress Vulnerabilities. WSCAN. Recuperado de: <https://wpscan.com/>

Zambrano, S. M. Q., & Valencia, D. G. M. (2017).  
*Seguridad en informática: consideraciones. Dominio de las Ciencias*,  
3(3), 676-688