UNIVERSIDAD PERUANA DE CIENCIAS APLICADAS

FACULTAD DE INGENIERÍA

PROGRAMA ACADÉMICO DE INGENIERÍA DE SISTEMAS

Mejora al Proceso de Monitoreo Continuo de Vulnerabilidades

TESIS

Para optar el título profesional de Ingeniero de Sistemas

AUTOR(ES)

León Vidalón, Igmarr (0000-0002-2062-2507)

Medina Ampuero, Pablo Jorge (0000-0001-5893-1252)

ASESOR

Subauste Oviden, Daniel Alejandro (0000-0003-1131-1384)

Lima, 05 de Agosto de 2020

DEDICATORIA

Dedicamos el presente trabajo principalmente a Dios, por darnos fuerza para continuar en este proceso de obtener uno de nuestros anhelos más deseados; y a nuestras familias quienes nos brindaron su apoyo incondicional, motivándonos y brindando su confianza a lo largo de nuestra carrera universitaria y a lo largo de nuestra vida.

AGRADECIMIENTOS

A nuestra familia por su apoyo durante el desarrollo toda nuestra carrera.

Mejora al proceso de Monitoreo Continuo de Vulnerabilidades

RESUMEN

El presente trabajo de investigación tiene como objetivo mejorar el proceso de Monitoreo Continuo de Vulnerabilidades de la gerencia de Operaciones de Seguridad Tecnológica lo cual contribuye en gran medida a estar prevenidos y mitigar en gran medida cualquier problema que pueda aprovechar una amenaza externa e interna de Mibanco.

El presente trabajo de investigación contiene seis capítulos entre los principales la definición del Marco Teórico, se desarrollaron los principales conceptos, antecedentes y se definieron las palabras claves relacionadas al tema principal del presente trabajo de investigación; en el capítulo de Desarrollo del Proyecto se evidenciara el problema con más detalle donde se formula el problema principal y el objetivo de mejora el cual estaría enfocado en la reducción sustancial de tiempo con el apoyo de tecnologías de información.

Palabras claves: Vulnerabilidades; Seguridad Tecnológica; Monitoreo.

Improvement in the Continuous Vulnerability Monitoring Process

ABSTRACT

This research work aims to improve the Continuous Vulnerability Monitoring process of Technology Security Operations management, which greatly contributes to being prevented and greatly mitigating any problem that may take advantage of an external and internal threat from Mibanco.

This research work contains six chapters, the main ones being the definition of the Theoretical Framework, the main concepts, antecedents were developed and the key words related to the main topic of this research work were defined; In the Project Development chapter the problem will be shown in more detail where the main problem is formulated and the improvement objective which would be focused on the substantial reduction of time with the support of information technologies.

Key words: Vulnerability; Technology Security; Monitoring.

TABLA DE CONTENIDOS

1	INTRODUCCIÓN.....	1
2	DEFINICIÓN DEL PROYECTO	2
2.1	OBJETO DE ESTUDIO.....	2
2.2	CULTURA.....	4
2.3	PRINCIPIOS	4
2.4	ORGANIGRAMA	5
2.5	DEFINICIÓN DEL PROBLEMA	9
2.6	OBJETIVOS DEL PROYECTO.....	10
2.6.1	Objetivos Específicos	10
3	LOGRO DE LOS STUDENT OUTCOMES	12
3.1	DESARROLLO DE LOS STUDENT OUTCOMES	12
4	MARCO TEÓRICO	15
4.1	ARQUITECTURA EMPRESARIAL.....	15
4.2	TOGAF.....	16
5	DESARROLLO DEL PROYECTO	20
5.1	ANÁLISIS DEL NEGOCIO	20
5.2	INGENIERÍA DE PROCESOS	3
5.2.1	Proceso Actual TISO	3
5.2.2	Proceso Actual TISO09: Monitoreo continuo de Vulnerabilidades.....	5
5.2.3	Nuevo Proceso TISO09: Monitoreo continuo de Vulnerabilidades.....	16
5.3	PROPUESTA DE SOLUCIÓN	18
5.4	GESTIÓN DE REQUERIMIENTOS	19
5.4.1	Especificación de Reglas del Negocio.....	19
5.4.2	Requerimientos Funcionales.....	20
5.4.3	Requerimientos No Funcionales.....	21
5.4.4	Matriz de Trazabilidad entre los Requerimientos Funcionales vs Reglas De Negocio.....	23
5.4.5	Escenarios de Atributos de Calidad.....	25

5.4.6	Matriz de Trazabilidad entre los Requerimientos No Funcionales vs Atributos de Calidad	27
5.4.7	Drivers Arquitectónicos	28
5.4.8	Matriz de Trazabilidad de Requerimientos Funcionales vs Drivers Funcionales	29
5.4.9	Matriz de Trazabilidad de Drivers Funcionales vs Tácticas.....	30
5.4.10	Matriz de Trazabilidad de Drivers de Atributos de Calidad vs Tácticas	30
5.4.11	Matriz de Trazabilidad de Drivers Arquitectónicos vs Casos de Uso de Sistema	31
5.4.12	Diagrama de Paquetes	32
5.4.13	Casos de Uso	33
5.4.14	Matriz de Trazabilidad de Requerimientos Funcionales vs Casos de Uso de Sistema	37
5.4.15	Especificación de Casos de Uso de Sistema.....	38
5.4.16	Conceptos de Diseño	52
5.4.17	Estilos de Arquitectura	53
5.5	DISEÑO DE SOLUCIÓN.....	54
5.5.1	Arquitectura de red TO-BE de la solución propuesta.....	54
5.5.2	Arquitectura Layered de la solución propuesta	54
5.5.3	Arquitectura C4	55
6	GESTIÓN DEL PROYECTO	77
6.1	DESCRIPCIÓN DEL PROYECTO	77
6.2	ALCANCE DEL PROYECTO TESIS	78
6.2.1	Desarrollo de la Propuesta	78
6.2.2	Contexto del Proyecto	79
6.2.3	Estructura de Desglose del Trabajo – EDT	80
6.2.4	Diccionario de la EDT	81
6.3	ORGANIZACIÓN DEL PROYECTO TESIS.....	105
6.3.1	Organigrama	105
6.3.2	Matriz de Asignación de Responsabilidades	105
6.3.3	Descripción de Roles	106
6.4	CONTROL DE CAMBIOS	112

6.5	ASEGURAMIENTO Y CONTROL DE CALIDAD	114
6.6	CRONOGRAMA.....	119
6.6.1	Cronograma de Actividades	119
6.6.2	Diagrama Gantt de Actividades.....	123
6.7	PRESUPUESTO	124
6.7.1	Costo por Recurso	124
6.7.2	Costeo del Proyecto	124
6.7.3	Presupuesto del Proyecto por Fase y Entregable.....	128
6.8	MÉTRICAS DE GESTIÓN	129
6.8.1	Curva S	129
6.8.2	Indicador CPI.....	130
6.8.3	Indicador SPI.....	130
6.9	PLAN DE RESPUESTA A LOS RIESGOS	132
6.9.1	Identificación de Riesgos.....	132
6.9.2	Escala de Valores Numéricos o Cualitativos para la Probabilidad	132
6.9.3	Escala de Valores Numéricos o Cualitativos para el Impacto.....	132
6.9.4	Matriz de Probabilidad por Impacto	133
6.9.5	Análisis Cualitativo de Riesgos	134
6.9.6	Análisis Cuantitativo de Riesgos.....	134
6.9.7	Plan de Respuesta al Riesgo	136
6.10	GESTIÓN DE INTERESADOS.....	145
6.10.1	Matriz de Interesados.....	145
6.10.2	Matriz de Poder / Interés	146
6.10.3	Nivel de Involucramiento	146
6.10.4	Plan de Acción.....	147
6.10.5	Matriz de Comunicaciones	148
6.11	EJECUCIÓN, MONITOREO Y CONTROL.	148
6.12	CIERRE	151
6.12.1	Acta de Cierre	151
6.12.2	Informe de Cierre.....	152
6.12.3	Lecciones Aprendidas.....	155
7	CONCLUSIONES.....	158

8	RECOMENDACIONES	159
9	GLOSARIO DE TERMINOS	160
10	SIGLARIO	162
11	REFERENCIAS	164
12	ANEXOS.....	166
12.1	ANEXO N° 01 PROJECT CHÁRTER	167
12.2	ANEXO N° 02 FORMATO DE INFORME DE AVANCE.....	183
12.3	ANEXO N° 03 FORMATO DE SOLICITUD DE CONTROL DE CAMBIO	186
12.4	ANEXO N° 04 CARTA DE SOLICITUD PARA USO DE INFORMACIÓN DE LA EMPRESA OBJETIVO	187
12.5	ANEXO N° 05 CORREO DE ACEPTACIÓN DE EMPRESA OBJETIVO: CUMPLIMIENTO 188	
12.6	ANEXO N° 06 CORREO DE ACEPTACIÓN DE EMPRESA OBJETIVO: RELACIONES INSTITUCIONALES.	190
12.7	ANEXO N° 07 CARTA DE ACEPTACIÓN DE EMPRESA OBJETIVO: RELACIONES INSTITUCIONALES.	192
12.8	ANEXO N° 08 DECLARACIÓN JURARA IGMAR LEÓN VIDALÓN	193
12.9	ANEXO N° 09 DECLARACIÓN JURADA PABLO JORGE MEDINA AMPUERO.....	194
12.10	ANEXO N° 10 CORREO DE ACEPTACIÓN DE LA SOLUCIÓN: GERENCIAS TISO....	195

ÍNDICE DE TABLAS

Tabla 1 <i>Matriz de Procesos vs Objetivos</i>	2
Tabla 2 <i>Matriz de Procesos vs Áreas</i>	2
Tabla 3 <i>Matriz de Trazabilidad entre los Requerimientos Funcionales vs Reglas De Negocio</i>	23
Tabla 4 <i>Escenarios de atributos de calidad</i>	25
Tabla 5 <i>Matriz de Trazabilidad entre los Requerimientos No Funcionales vs Atributos de Calidad</i>	27
Tabla 6 <i>Matriz de Trazabilidad de Requerimientos Funcionales vs Drivers Funcionales</i> .	29
Tabla 7 <i>Matriz de Trazabilidad de Drivers Funcionales vs Tácticas</i>	30
Tabla 8 <i>Matriz de Trazabilidad de Drivers de Atributos de Calidad vs Tácticas</i>	30
Tabla 9 <i>Matriz de Trazabilidad de Drivers Arquitectónicos vs Casos de Uso de Sistema</i> .	31
Tabla 10 <i>Matriz de Trazabilidad de Requerimientos Funcionales vs Casos de Uso de Sistema</i>	37
Tabla 11 <i>Matriz de Asignación de Responsabilidades</i>	105
Tabla 12 <i>Cronograma de Actividades</i>	119
Tabla 13 <i>Costo por Recurso</i>	124
Tabla 14 <i>Costeo del Proyecto</i>	124
Tabla 15 <i>Presupuesto del Proyecto</i>	128
Tabla 16 <i>Identificación de Riesgos</i>	132
Tabla 17 <i>Escala de Valores Numéricos o Cualitativos de Probabilidad</i>	132
Tabla 18 <i>Escala de Valores Numéricos o Cualitativos de Impacto</i>	132
Tabla 19 <i>Matriz Probabilidad x Impacto</i>	133
Tabla 20 <i>Análisis Cualitativo de Riesgos</i>	134
Tabla 21 <i>Análisis Cuantitativo de Riesgos</i>	134
Tabla 22 <i>Plan de Respuesta al Riesgo</i>	136

Tabla 23 <i>Registro de interesados</i>	145
Tabla 24 <i>Nivel de involucramiento</i>	146
Tabla 25 <i>Matriz de comunicaciones</i>	148

ÍNDICE DE FIGURAS

<i>Figura 1.</i> Captura de pantalla de la Composición del Grupo ACP	2
<i>Figura 2.</i> Captura de pantalla de la Composición del Grupo Credicorp	3
<i>Figura 3.</i> Captura de pantalla del Organigrama de la empresa Mibanco	5
<i>Figura 4.</i> Diagrama de causa y efecto del problema en estudio.....	10
<i>Figura 5.</i> Captura de pantalla de Lista de Frameworks de AE	16
<i>Figura 6.</i> Captura de pantalla de dominios de AE	17
<i>Figura 7.</i> Captura de pantalla del ciclo de desarrollo de la arquitectura.....	18
<i>Figura 8.</i> Captura de pantalla del mapa de procesos de la empresa Mibanco	21
<i>Figura 9.</i> Captura de pantalla de la distribución de oficinas de la empresa Mibanco.....	1
<i>Figura 10.</i> Captura de pantalla de los proceso de la Gerencia de Operaciones de Seguridad Tecnológica	4
<i>Figura 11.</i> Diagrama de red As-Is.....	7
<i>Figura 12.</i> Proceso de monitoreo continuo de vulnerabilidades	11
<i>Figura 13.</i> Sub proceso de analizar vulnerabilidades.....	12
<i>Figura 14.</i> Sub proceso de verificar/actualizar inventario de actividades	12
<i>Figura 15.</i> Proceso de monitoreo continuo de vulnerabilidades To-Be.....	17
<i>Figura 16.</i> Diagrama de paquetes.....	32
<i>Figura 17.</i> Paquete descubrir activos	33
<i>Figura 18.</i> Paquete gestión de vulnerabilidades.....	34
<i>Figura 19.</i> Paquete dashboard	35
<i>Figura 20.</i> Paquete actualización de activos	36
<i>Figura 21.</i> Paquete utilitarios	36
<i>Figura 22.</i> Prototipo detectar activos nuevos.....	39
<i>Figura 23.</i> Prototipo buscar activos	39

<i>Figura 24.</i> Prototipo listado de activos	40
<i>Figura 25.</i> Prototipo escanear vulnerabilidades de activos	42
<i>Figura 26.</i> Prototipo tipo de escaneo	42
<i>Figura 27.</i> Prototipo resultado de escaneo	43
<i>Figura 28.</i> Prototipo información detallada de activo.....	43
<i>Figura 29.</i> Prototipo tipo de escaneo	44
<i>Figura 30.</i> Prototipo ingreso de credenciales para escaneo	44
<i>Figura 31.</i> Prototipo resultado de escaneo	45
<i>Figura 32.</i> Prototipo información detallada de activo.....	45
<i>Figura 33.</i> Prototipo priorizar vulnerabilidades	47
<i>Figura 34.</i> Prototipo priorizar vulnerabilidades de forma manual.....	47
<i>Figura 35.</i> Prototipo programa actualizaciones de equipos	49
<i>Figura 36.</i> Prototipo programación de schedule de actualización	49
<i>Figura 37.</i> Prototipo listado de ejecución de actualizaciones de equipos	50
<i>Figura 38.</i> Prototipo programa manual de actualización de equipos	50
<i>Figura 39.</i> Prototipo ingreso de fecha de actualización de equipo	51
<i>Figura 40.</i> Prototipo ejecución de actualización de equipo	51
<i>Figura 41.</i> Propuesta de diagrama de red To-Be	54
<i>Figura 42.</i> Diagrama Layered	55
<i>Figura 43.</i> Diagrama de Contexto C4	56
<i>Figura 44.</i> Diagrama de Containers – sensores C4	58
<i>Figura 45.</i> Diagrama de Container – análisis de vulnerabilidad C4	60
<i>Figura 46.</i> Diagrama de componentes C4.....	63
<i>Figura 47.</i> Diagrama de código – buscar automáticamente activos.....	65
<i>Figura 48.</i> Diagrama de código – búsqueda manual de activos.....	67
<i>Figura 49.</i> Diagrama de código – escaneo caja negra.....	68

<i>Figura 50.</i> Diagrama de código – escaneo caja blanca	70
<i>Figura 51.</i> Diagrama de código – priorización de vulnerabilidades	72
<i>Figura 52.</i> Diagrama de código – actualización de activo	74
<i>Figura 53.</i> Diagrama de la estructura de desglose de trabajo	80
<i>Figura 54.</i> Organigrama del proyecto	105
<i>Figura 55.</i> Organigrama de calidad del proyecto	117
<i>Figura 56.</i> Diagrama Gantt de Actividades	123
<i>Figura 57.</i> Gráfico de indicador de curva S	130
<i>Figura 58.</i> Gráfico de indicador SPI	131
<i>Figura 59.</i> Gráfico Matriz de poder / Interés	146

1 INTRODUCCIÓN.

Hoy en día la tecnología forma parte de la operatividad de muchas empresas, Mibanco empresa de objeto de estudio es una de ellas, apostando por arquitecturas modernas de cara a la transformación digital, el progresivo uso de la nube por sus diferentes proyectos como Office365, Kusi y (motor de reglas crediticio), app's y su ERP ha demandado generar nuevas capacidades técnicas enfocadas en producir un nuevo modelo de gobierno que permita ampliar sus capacidades de procesamiento más allá de su Data Center y de manera más segura, escalable y rápida, aprovechando tecnologías de cloud computing, convirtiéndose así en una parte fundamental y vital en la organización. En este sentido, también son muy vulnerables a ataques de extraños si no cuentan con la última actualización de su sistema operativo y causar problemas con la operatividad.

Por lo indicado en el punto anterior, el proyecto tiene la finalidad de presentar una propuesta de Arquitectura Empresarial para mejorar el Proceso de Monitoreo Continuo de Vulnerabilidades de los activos tecnológicos (equipos de comunicación, servidores y equipos de usuario) de la organización y disminuir el riesgo de fraudes y otros, estos procesos son:

- Toma de inventario de los activos y clasificación.
- Analizar vulnerabilidades de los activos.
- Priorización de activos.
- Subsanan vulnerabilidades detectadas.
- Tiempo que se toma en detectar una vulnerabilidad y su subsanación.

En el proyecto vamos a usar la metodología de trabajo TOGAF, de esta manera alineamos los procesos de negocio, los objetivos estratégicos, y la tecnología de la organización.

2 DEFINICIÓN DEL PROYECTO

2.1 Objeto de Estudio

Mibanco - Banco de la Microempresa S.A. es una sociedad anónima con número de RUC 20382036655 que fue constituida en Lima - Perú el 02 de marzo de 1998, por escritura pública otorgada ante el Notario Público, Dr. Ricardo Fernandini Barreda, encontrándose inscrita en la Partida N° 11020316 del Registro de Personas Jurídicas de los Registros Públicos de Lima y su funcionamiento fue autorizado por la Superintendencia de Banca Seguros y AFP, mediante Resolución SBS N° 356-98, de fecha 7 de abril de 1998. Es una sociedad anónima de duración indefinida, sujeta a las disposiciones que dicta la Superintendencia de Banca, Seguros y AFP.

Mibanco, inició sus operaciones el 4 de mayo de 1998 en Lima, sobre la base de la experiencia de Acción Comunitaria del Perú (Grupo ACP Inversiones y Desarrollo a partir del año 2007), una sociedad civil sin fines de lucro que opera hace 41 años en el sector de la micro y pequeña empresa, que goza de un excelente prestigio mundial y que mantiene una relación permanente y fluida con la banca nacional e internacional, así como con organismos multilaterales y bilaterales.

Composición Grupo ACP

Figura 1. Captura de pantalla de la Composición del Grupo ACP

Fuente: grupoacp.com.pe, 2020

Mibanco, inició sus operaciones con un total de 13 agencias en Lima, convirtiéndose en el primer banco privado de la pequeña y microempresa, es una institución bancaria dedicada al otorgamiento de productos activos como créditos y operaciones pasivas a

plazo fijo, cuentas de ahorro, cuentas corrientes y cts, trabajando para contribuir a mejorar la calidad de vida de sus clientes a través de la inclusión financiera y a la bancarización.

La adquisición inicial del 60.68% de Mibanco por parte de Financiera Edyficar, a inicios del año 2014, ha sido un evento de alta importancia en el sector micro financiero. Mibanco se convirtió en una subsidiaria del holding Credicorp, quedando el BCP como principal accionista de Mibanco con el 93,6% del total de las acciones a la fecha de la presente valorización.

El Grupo Credicorp está conformado por empresas bancarias y micro financieras, seguros, AFP y Credicorp Capital. Mibanco cuenta, entonces, con el respaldo del Grupo Credicorp, que mantuvo una capitalización bursátil a diciembre del 2014 de US\$ 12,8 billones y activos por US\$ 45,2 billones. Por ello, se mantienen altas expectativas de crecimiento.

Composición Grupo Credicorp

Figura 2. Captura de pantalla de la Composición del Grupo Credicorp

Fuente: www.grupocredicorp.com, 2019

Los esfuerzos de Mibanco están abocados a la concesión de financiamientos para los segmentos de micros y pequeñas empresas. No obstante, su meta no es únicamente la inclusión de estos emprendedores. Su estrategia es más bien la de acompañar a sus clientes en todo el proceso de desarrollo, entablando así una relación a largo plazo.

2.2 Cultura

- Nos centramos en el cliente por vocación de servicio a las personas.
- La confianza es el rasgo distintivo de nuestras relaciones.
- Asumimos un compromiso como contraparte de la confianza entregada.

2.3 Principios

- Asesoramos: Conocemos profundamente a las personas, por eso les damos la mejor asesoría.
- Cuidamos: Nos interesamos de corazón por las personas y, así, construimos confianza.
- Innomejoramos: Innovamos para mejorar, siendo proactivos, adaptables y simples.
- Cooperamos: Logramos resultados que perduran, colaborando unos con otros y asumiendo riesgos responsablemente.
- Jugamos Limpio: Somos un ejemplo de integridad, siempre.

2.4 Organigrama

Figura 3. Captura de pantalla del Organigrama de la empresa Mibanco
Fuente: intranet empresa Mibanco, 2020

Junta de Accionistas: Es el órgano máximo de la Sociedad, está compuesta por todos los accionistas titulares de acciones con derecho a voto, y representa la universalidad de los accionistas. La Junta General se reúne obligatoriamente una vez al año, dentro de los tres meses siguientes a la terminación del ejercicio económico para:

- Pronunciarse sobre la gestión social y los resultados económicos del ejercicio anterior, expuesto en la memoria, y expresados en los correspondientes estados financieros.
- Resolver sobre la aplicación de las utilidades, si las hubiere.
- Elegir, cuando corresponda, a los miembros del Directorio, incluyendo a los directores alternos y suplentes.

- Fijar la retribución de los miembros del Directorio, incluyendo a los directores alternos y suplentes.
- Designar o delegar en el Directorio la designación de los auditores externos y de las empresas clasificadoras de riesgos.
- Tratar cualquier otro asunto que corresponda a la junta general de accionistas, siempre que se hubiese consignado en la agenda de la convocatoria y se cuente con el quórum de ley.

Directorio: Tiene las facultades de gestión y de representación legal necesarias para la administración de la Sociedad dentro de su objeto, dicta las políticas y es responsable conjuntamente con la Gerencia, del control y de la gestión económica - financiera. Al efecto, está investido de los más amplios poderes y tiene todas las facultades y atribuciones para la conducción de las actividades de la empresa. El Directorio, que es el órgano de mayor responsabilidad en la Institución, define la estrategia y las políticas de largo plazo que se concretan a través de la Alta Gerencia. El Directorio está conformado por ocho miembros titulares, de los cuales dos eran independientes.

División de Auditoría: Asegurar la estructura de los controles internos de la organización, tiene la finalidad de verificar en las diversas áreas el cumplimiento del control interno implementado, identifica riesgos y prueba la efectividad de los controles, preserva los intereses de los accionistas y clientes. Informar la importancia del control interno basado en riesgos al resto de áreas de la empresa.

Gerencia General: Es el funcionario de mayor jerarquía en la Institución, encargado de la gestión del Banco en base a las políticas, planes, objetivos y metas establecidas por el Directorio, enmarcado dentro de las regulaciones de los organismos de supervisión. Dispondrá la ejecución de los acuerdos de la Junta de Accionistas y del Comité Ejecutivo de Directorio y tomando las decisiones que considere necesarias, debe asegurar la eficiencia, eficacia y viabilidad empresarial del Banco.

División de Riesgos: Promueve el desarrollo de la gestión integral de riesgos, definiendo las políticas y procedimientos necesarios para ubicarse dentro de las distintas métricas y límites de apetito por riesgo definidos, contando para ello, con los recursos necesarios en términos de infraestructura, herramientas, metodologías y personal debidamente calificado.

División de Finanzas: Apoya a la Gerencia General en el desarrollo e implementación de técnicas de gestión que permitan optimizar los mecanismos de información y medición de resultados para la toma de decisiones oportunas, gestionando el cumplimiento del Planeamiento Estratégico y Presupuesto así como obtener los recursos financieros necesarios que acompañen el crecimiento del negocio. Asimismo, asegura la correcta administración de la liquidez, el fondeo del banco y recursos financieros excedentes para lograr la rentabilidad de los mismos.

División de Soporte: Planifica, conduce y controla los recursos y actividades que dan soporte a las operaciones del negocio, velando por lograr un balance adecuado entre calidad de servicio al cliente y eficiencia en los recursos utilizados. Asimismo, provee todos los servicios de tecnología asegurando la estabilidad operativa y la continuidad de las actividades diarias de la organización.

División de Negocios: Asegura la implementación y seguimiento de las estrategias y políticas comerciales/crediticias de los productos y servicios conforme a los objetivos estratégicos planteados. Impulsa el uso eficiente y rentable de los canales de venta que permitan la mayor cobertura y nivel de servicio a los clientes. Vela y asegura el crecimiento del negocio, la calidad de la cartera y la recuperación o cobranza mediante la coordinación de los esfuerzos de las distintas áreas comerciales.

División de Marketing: Responsable de definir y ejecutar las estrategias, planes y acciones de marketing para la generación de negocios, buscando incrementar los ingresos, la diversificación y reducción del costo de fondeo de clientes pasivos, mediante la innovación, diseño, desarrollo, mejora de productos y servicios.

División de Gestión y Desarrollo Humano: Es un socio estratégico de la Gerencia General, brinda servicios y asesoría integral para el desarrollo de los colaboradores y la mejora continua del desempeño de capital humano. Asimismo, busca estar alineados con las políticas relacionadas a la gestión de personas que se definan a nivel de las empresas del Grupo Credicorp.

División de Administración: Gestiona los bienes y servicios del banco enfocados en la eficiencia y asegurando una adecuada atención de las necesidades del cliente interno alineado a las estrategias de crecimiento de la empresa.

División Legal: Asegura el soporte de asesoría jurídica legal al Banco, gestionando y/o planificando actividades orientadas a prevenir los riesgos legales a los cuales está expuesta la organización, proponiendo soluciones, dirigiendo las actividades y los procesos relacionados con el servicio legal requerido por las diferentes gerencias de la organización dentro del marco de la normativa legal aplicable y la normativa interna establecida por la Gerencia General y los Comités del Directorio.

Área de Inclusión Financiera: Se encarga de brindar el acceso al conocimiento, el cual es fundamental para que las personas logren alcanzar su desarrollo. Por ello, reconoce la capacitación y educación financiera como complementos necesarios para el acceso al capital. Adicionalmente, reconoce el impacto positivo que tienen los créditos en la economía local ya que permiten acercarse a mercados excluidos por la banca tradicional, contribuyendo así con la inclusión financiera.

2.5 Definición del Problema

El proceso de monitoreo continuo de vulnerabilidades se realiza todos los meses por parte del área de TISO, el cual se encarga de velar por la correcta operación de la seguridad informática de Mibanco. El proceso en primera instancia es exigencia por parte del corporativo “Credicorp” basado en la FFIEC la cual cuenta con dos sentencias declarativas para la gestión de vulnerabilidades:

D3.DC.Th.B.1 “Las pruebas independientes (incluidas las pruebas de penetración y el análisis de vulnerabilidades) se realizan de acuerdo con la evaluación de riesgos para los sistemas externos y la red interna.”

D3.CC.Re.B.1 “Los problemas identificados en las evaluaciones se priorizan y resuelven en función de la importancia y dentro de los plazos establecidos en la respuesta al informe de evaluación.”

En adición a las sentencias de la FFIEC sobre vulnerabilidades, es una estrategia interna mantener seguro los activos de información de Mibanco, porque es bien sabido que toda empresa tiene la necesidad de cuidar la ciberseguridad dado que cualquier punto débil de un sistema puede ser aprovechado por amenazas externas. Es por ello que nos centraremos en mitigar las vulnerabilidades de los activos de información, dado que las mismas son el vector de ataque común de los ciberdelincuentes (ruta o camino que utiliza un atacante para tener acceso al activo objetivo).

Para este proceso se deben tener en cuenta varios pasos como son:

- El correcto inventario de activos de la información con su respectiva criticidad.
- El descubrimiento de vulnerabilidades para cada activo del inventario.
- La criticidad de cada vulnerabilidad detectada.
- La remediación y/o el plan de acción.

En nuestro caso varios de los pasos listados se realizan de manera manual, donde la evaluación constante de las vulnerabilidades llega a ser una tarea titánica, la parte del proceso que toma la mayor cantidad de tiempo es el descubrimiento, ya que en este paso se tiene que realizar un proceso de activo por activo tomando cantidad de horas hombre para llegar al objetivo, seguidamente de la priorización de las mismas y su posterior remediación que en muchos de los casos cuando se llega a realizar este, el activo ya tiene nuevas brechas reportadas por el fabricante.

En el siguiente gráfico podemos observar las causas que originan el problema del monitoreo continuo de vulnerabilidades, el cual nos lleva a plantear una posible solución:

Figura 4. Diagrama de causa y efecto del problema en estudio
Fuente: elaboración propia, 2020

2.6 Objetivos del Proyecto

El objetivo general es proponer una solución web que de soporte a la mejora del proceso de gestión de vulnerabilidades de los activos de información para asegurar el cumplimiento de las políticas y normas de seguridad de la empresa, en relación al cumplimiento del corporativo basados en la FFIEC – Cybersecurity Assessment Tool 2015 y la Política General de Seguridad de la información que está alineada a las sentencias FFIEC. Con la mejora propuesta se encaminará al cumplimiento de la sentencias FFIEC.

2.6.1 Objetivos Específicos

- Elaborar un análisis de la situación del proceso actual de Monitoreo Continuo de Vulnerabilidades en la gestión de seguridad informática.
- Elaborar el diseño de una solución Web alojada en un entorno Cloud como un IaaS para resolver los problemas encontrados en el proceso de Monitoreo Continuo de Vulnerabilidades y permita a la organización identificar las oportunidades de mejora, así como poder cumplir con las sentencias del FFIEC.

- Elaborar una arquitectura de acuerdo a las necesidades del proceso que permitan el cumplimiento de los principios del proceso, descubrir, detectar, responder y prevenir.
- Validar que la propuesta de la solución satisfaga las necesidades identificadas del proceso de Monitoreo continuo de vulnerabilidades.

3 LOGRO DE LOS STUDENT OUTCOMES

3.1 Desarrollo de los student outcomes

- La capacidad de identificar, formular y resolver problemas complejos de ingeniería aplicando principios de ingeniería, ciencias y matemáticas.

En nuestro estudio aplicamos diversas herramientas para identificar la arquitectura empresarial mediante el framework de Zachman, así mismo aplicamos una correcta ingeniería de requerimientos, logrando encontrar los principios del proceso objetivo y definiendo adecuadamente los requerimientos funcionales y no funcionales alineados a los requerimientos del proceso, ello se ve reflejado en la gestión de requerimientos.

El cálculo de los indicadores en el proceso nos ha permitido identificar los puntos más álgidos del mismo, permitiendo proponer mejoras en la reducción del tiempo de proceso en 25 días, ello se evidencia en el diferencial del proceso As-Is y el To-Be.

- La capacidad de aplicar diseño de ingeniería para producir soluciones que satisfagan necesidades específicas con consideración de salud pública, seguridad y bienestar, así como factores globales, culturales, sociales, ambientales y económicos.

Al realizar conceptos de diseño, como transparencia, integración y optimización en conjunto con los estilos de arquitectura, se lograron plasmar las diversas capas de solución para su mejor entendimiento y así apoyar con la seguridad informática requerida por la empresa objetivo. La evidencia de ello son los diagramas Layered y la arquitectura C4.

- La capacidad de comunicarse efectivamente con una variedad de audiencias.

La interacción con el área responsable del proyecto ha sido crucial para el levantamiento de información, ello se ve reflejado al poder definir los principales requerimientos críticos para el proceso, la evidencia de ello se encuentra en la gestión de requerimientos.

- La capacidad de reconocer responsabilidades éticas y profesionales en situaciones de ingeniería y hacer juicios informados, que deben considerar el impacto de las soluciones de ingeniería en contextos globales, económicos, ambientales y sociales.

La gestión adecuada de la información ha sido de vital importancia, ya que la empresa objetivo en estudio es una entidad bancaria, donde toman la información como su principal activo, ha llevado a realizar un enmascaramiento de ciertos datos sin vulnerar el corazón del proceso a su vez sin exponer datos críticos de la institución.

Para que la empresa objetivo nos pueda aceptar el proyecto se tuvo que solicitar diversas aprobaciones, que van desde el área de Cumplimiento Normativo, pasando por el área de Seguridad de Información, hasta el área de Marketing quien nos aprobó el uso de los logos y distintivos para fines académicos de la investigación.

- La capacidad de funcionar de manera efectiva en un equipo cuyos miembros juntos brindan liderazgo, crean un entorno colaborativo e inclusivo, establecen metas, planifican tareas y cumplen objetivos.

La interacción entre los miembros de nuestro equipo ha logrado funcionar de acuerdo a lo esperado, como el traspaso de información entre los miembros del equipo ejecutadas en diversas reuniones apoyadas de las videoconferencias, implementado un dinamismo entre nuestras 2 a 3 reuniones semanales para analizar el avance del proyecto.

- La capacidad de desarrollar y llevar a cabo la experimentación adecuada, analizar e interpretar datos, y utilizar el juicio de ingeniería para sacar conclusiones.

Desde el punto de vista de gestión de proyectos, nos ha permitido generar información de indicadores de gestión típicos y su posterior interpretación adecuada nos ha permitido analizar en todo el trayecto de nuestro proyecto donde se han tenido deficiencias y las causantes de las misma, para poder realizar ajustes a nuestros avances y llegar al objetivo, ello se refleja en el cálculo de los indicadores de gestión CPI y SPI.

- La capacidad de adquirir y aplicar nuevos conocimientos según sea necesario, utilizando estrategias de aprendizaje apropiadas.

La ingeniería de sistemas como su nombre etimológico tiene su raíz en ingenio, ello nos lleva al punto que antes de este proyecto no se tenía referencia del modelo de arquitectura C4, el entendimiento rápido del modelo indicado, así como el uso de herramientas para el desarrollo de las diversas capas que van desde identificar el contexto, contenedores, componentes y códigos, se evidencian en la arquitectura propuesta C4.

4 MARCO TEÓRICO

4.1 Arquitectura Empresarial

Se puede puntualizar la Arquitectura Empresarial (AE) como la exhibición de todos los procesos, elementos y políticas de una empresa. Según Gartner, Arquitectura Empresarial es el proceso de trasladar una visión y estrategia de negocio en un cambio efectivo, comunicando las capacidades actuales y repensando los principios y los modelos que describen el estado futuro de la empresa y facilitan su evolución.

La AE nos posibilita tener una visión completa en todas sus dimensiones y complejidades del sistema empresa. Permite determinar los elementos principales de la organización y su correspondencia para adquirir los objetivos del negocio, integrando los aspectos de: planificación, operación y tecnología. Los elementos que se consideran como críticos para su articulación son:

- Los procesos: modelos de negocio y procesos.
- La estructura organizacional: personas, estructuras administrativas.
- Las tecnologías de información: aplicaciones, información, infraestructura tecnológica y seguridad informática.

En la actualidad las empresas son muy complejas que necesitan procesos de negocio muy flexibles sostenidos por sistemas de información tecnológicas (TI). Establecer una arquitectura empresarial inicia de constituir un conjunto de reglas arquitectónicas que posibiliten garantizar un desarrollo acorde con los modelos y necesidades de la empresa, con los procesos de negocio y las tecnologías de información. Estas reglas fundamentales de TI deben iniciar de la misión de la empresa y de la identificación de las estrategias y actividades de negocio que sostienen dicha misión.

La AE permite observar como las estrategias, metas, componentes y tecnologías están relacionadas y mostrar la interdependencia entre ellas, al final de cuentas los proyectos de tecnología debe existir exclusivamente como parte de las estrategias de negocio de la empresa.

El desarrollo de AE debe ser adiestrado como una disciplina que proporciona conceptos, modelos e instrumentos a la organización para desafiar los retos de las áreas estratégicas y los procesos de negocios con las áreas de TI, así poder generar mayor valor, enriquecer el desempeño, la comunicación y la integración en la organización.

El triunfo de una organización y los costos que ello acarrea obedecen cada vez más de sus sistemas de información. En el ámbito de la AE, un ambiente de referencia o framework compete a los elementos especiales que actúan como soporte para la estructuración y ensamblaje de elementos. Un framework de AE resuelve en qué términos se define y documenta la arquitectura.

En la siguiente tabla se precisan los framework de AE más divulgados y empleados por la industria en el mundo empresarial:

ZACHMAN	Zachman Framework for Enterprise Architecture (http://www.zifa.com/)
E2AF	Extended Enterprise Architecture Framework. (http://www.enterprise-architecture.info/)
TOGAF	The Open Group Architecture Framework (http://www.opengroup.org/togaf/)
GEAF	Gartner Enterprise Architecture Framework. (http://www.gartner.com)
FEAF	Federal Enterprise Architecture Framework. US. (http://www.cio.gov)
BTEP	GC Enterprise Architecture and Standards. CANADÁ. (http://www.tbs-sct.gc.ca/inf-inf/index_e.asp)

Figura 5. Captura de pantalla de Lista de Frameworks de AE
Fuente: revistas.udem.edu.co/index.php/ingenierias, 2020

4.2 TOGAF

Es un acrónimo de "The Open Group Architecture Framework" y es un framework de arquitectura. Fue desarrollado en el año 1995, tomando como base a otro marco de trabajo conocido como TAFIM (US Department of Defense Technical Architecture Framework for Information Management), se desarrolla y es mantenido por el "The Open Group Architecture Forum". Es conocido como un estándar global para el diseño, desarrollo y mantenimiento de arquitecturas, considerado como una hoja de ruta para realizar AE, otorga procedimientos y mecanismos para apoyar en la aceptación, producción, uso y mantenimiento de una AE. TOGAF contiene 4 dominios de arquitectura que son aceptados como subdominio de la AE, siendo los siguientes:

Arquitectura de Negocios	Define estrategias de negocios, gobernanza, organización y procesos claves de negocios.
Arquitectura de Aplicación	Provee un plano para sistemas individuales de aplicación que serán desplegados al igual que las interacciones entre estos y los procesos de negocios.
Arquitectura de Datos	Explica la manera en que los datos son ordenados y almacenados por la organización.
Arquitectura Técnica	Describe el componente físico, software y de redes necesario para soportar el núcleo ya especificado.

Figura 6. Captura de pantalla de dominios de AE
Fuente: www.ucipfg.com

TOGAF se basa en un modelo de proceso iterativo, soportado bajo el Modelo de Desarrollo de Arquitectura (Architecture development method-ADM). En ella se menciona las etapas a seguir para poder desarrollar o llevar a cabo una AE en una organización, de tal manera que en la ejecución de cada ciclo de ADM se acrecenté la experiencia de la solución de AE de la organización y el valor que aporta al negocio. El ciclo ADM inicia con la Etapa Preliminar, luego la Etapa A (Visión de Arquitectura) hasta la Etapa H (Gestión de Cambios de Arquitectura). En todo instante, el ciclo ADM se despliega en paralelo a la actividad de gestión de requisitos.

Figura 7. Captura de pantalla del ciclo de desarrollo de la arquitectura
Fuente: www.opengroup.org, 1995-2020

- **Preliminar:** En esta fase se define el entorno de la organización a ser estudiada por la iniciativa de EA, del mismo modo el equipo de EA y los principios de la arquitectura que se puedan aplicar. Por último, se deben poner en marcha las herramientas necesarias que se usarán en el desarrollo de la arquitectura.
- **A – Visión de Arquitectura:** En esta etapa, se debe constituir el alcance de la iniciativa de EA junto con el proyecto de arquitectura. Se debe corroborar los principios de arquitectura y exponer el documento de visión de arquitectura.
- **B – Arquitectura de Negocios | C – Arquitectura de Sistemas de Información | D – Arquitectura de Tecnología:** En estas tres etapas, se elabora la línea base de arquitectura (AS-IS) y la arquitectura final (TO-BE). Luego se debe realizar el análisis gap entre ambas y entregar la hoja de ruta de arquitectura (Roadmap Architecture) para finalmente arribar a la arquitectura objetivo. El entregable principal de esta fase es el documento de definición de arquitectura.

- **E – Oportunidades y Soluciones:** En esta etapa, se determina la planificación inicial para poner en marcha la arquitectura objetivo, se detallan y juntan los paquetes de trabajo principales.
- **F – Planificación de Migración:** En esta etapa, son priorizados los proyectos identificados en la etapa anterior. Para ello, se debe evaluar costo/beneficio, el análisis de riesgo y la distribución del valor para el negocio. También el Roadmap de arquitectura debe ser confirmado y se debe actualizar el documento de definición de arquitectura.
- **G – Gobernanza de la Implementación:** En esta etapa, se ratifica e inspecciona el alcance y las prioridades de los proyectos de implementación. Así mismo se ejecutan las revisiones de cumplimiento de EA, y las revisiones de post-implementación.
- **H – Gestión de Cambios de Arquitectura:** En esta etapa, se inspecciona que la arquitectura final alcance el valor esperado para el objetivo del negocio.
- **Gestión de Requerimientos:** es una labor paralela que se responsabiliza de la identificación, seguimiento y documentación de requerimientos, además se encarga de informar a la etapa oportuna de cualquier modificación o alta de requisitos a tener en cuenta.

5 DESARROLLO DEL PROYECTO

Como parte del proceso de desarrollo del proyecto usaremos el framework de Zachman, para lo cual en los siguientes puntos responderemos las preguntas que el framework lo plantea en la primera fila del resumen ejecutivo del contexto en la empresa en estudio.

5.1 Análisis del negocio

Why: El objetivo de la empresa en estudio se enmarca en la misión y visión:

Misión

Transformar la vida de las personas, comprometidos con su inclusión financiera y progreso, aportando juntos al crecimiento del país.

Visión

Ser el socio más querido de clientes, colaboradores y comunidades, para acompañar su progreso, por la confianza que inspira y el servicio extraordinario que entrega, siendo el principal promotor de evolución de las micro-finanzas de la región.

What: Los elementos importantes que podemos encontrar en la empresa son:

- Clientes: persona natural o jurídica que contrata un producto o servicio que la empresa brinda.
- Colaboradores: personas naturales que laboran en la empresa.
- Accionistas: personas naturales que tienen inversiones en la empresa.
- Proveedores: personas naturales jurídicas que proveen de productos que la empresa necesita.
- Entes reguladores: organismos de control que controlan en representación del Estado a la empresa.

How: Podemos visualizar los siguientes procesos de la empresa:

Figura 8. Captura de pantalla del mapa de procesos de la empresa Mibanco
Fuente: intranet empresa Mibanco, 2020

Where: La empresa se encuentra presente en todas las regiones de nuestro país, con 288 agencias.

Figura 9. Captura de pantalla de la distribución de oficinas de la empresa Mibanco
Fuente: intranet empresa Mibanco, 2020

Who: Como actores más importantes en la empresa tenemos a:

- Clientes: persona natural o jurídica que contrata un producto o servicio que la empresa brinda.
- Entes reguladores: organismos de control que controlan en representación del Estado a la empresa.

When: La empresa en estudio tiene como ámbito de acción a clientes de la micro y pequeña empresa.

MATRIZ DE PROCESOS VS OBJETIVOS

Tabla 1 *Matriz de Procesos vs Objetivos*

Fuente: elaboración propia

Procesos/Objetivos	Experiencia cliente y colaborador	Expansión del negocio		Eficiencia en el modelo de negocio	
	Comprometido con el desarrollo de las personas	Hacer hinchas a los compañeros	Ser referente mundial en microfinanzas	Ser referente de los modelos de negocio digitales	Creer rentablemente y sosteniblemente
Planificación estratégica			X		X
Mercadeo		X		X	
Diseño de productos y servicios		X		X	
Captación de fondos			X		
Colocación de fondos			X	X	X
Servicios	X	X			
Gestión postventa					X
Gestión de Bienes y Servicios					X
Gestión del capital humano y desarrollo organizacional	X				
Gestión tecnológica				X	
Gestión financiera			X		X
Gestión de riesgos			X	X	X
Gestión de la seguridad	X	X	X	X	X
Gestión de procesos				X	

MATRIZ DE PROCESOS VS ÁREAS

Tabla 2 *Matriz de Procesos vs Áreas*

Fuente: elaboración propia

Procesos/Áreas	Accionistas	Directorio	Auditoría Interna	Riesgos	Finanzas	Desarrollo Humano	Administración	Legal	Soporte	Negocios	Marketing
Planificación estratégica	M/R	A		A				A			
Mercadeo							A			A	M/R
Diseño de productos y servicios		A					A			A	M/R
Captación de fondos					M/R	A				A	
Colocación de fondos		M/R		A	A						
Servicios						A			A	M/R	A
Gestión postventa				A						M/R	A
Gestión de Bienes y Servicios							A			M/R	A
Gestión del capital humano y desarrollo organizacional						M/R	A	A	A		
Gestión tecnológica		A			A	A			M/R		
Gestión financiera		A	A	A	M/R			A			
Gestión de riesgos			A	M/R	A						
Gestión de la seguridad		A	M/R	A	A	A	A	A	A	A	A
Gestión de procesos											

5.2 Ingeniería de Procesos

5.2.1 Proceso Actual TISO

5.2.1.1 Objetivo

El objetivo es describir el proceso de la Gerencia de Operaciones de Seguridad Tecnológica, describiendo los procesos internos del área y mejorar la Gestión de Ciberseguridad en Mibanco, en relación al cumplimiento del corporativo basados en la FFIEC – Cybersecurity Assessment Tool 2015, y la Política General de Seguridad de la Información.

5.2.1.2 Consideraciones Generales

El enfoque de Mibanco sobre Ciberseguridad se basa en la pro actividad, en aplicar el conocimiento y la tecnología para alcanzar los niveles de protección requeridos, entendiendo las motivaciones y técnicas empleadas por los atacantes, detectando rápidamente las infracciones o ataques en activo y construyendo las capacidades técnicas y humanas necesarias para responder con eficacia y celeridad ante cualquier brecha o incidente, con el fin de minimizar la ventana de ataques y las consecuencias de los mismos.

En la POL-RIE-017 Política General de Seguridad de la Información establecen los objetivos de control necesarios para alcanzar un nivel de seguridad homogéneo y adecuado a las necesidades del negocio.

Para asegurar el cumplimiento de dichos objetivos, se establecen los siguientes controles de seguridad.

- La Gerencia de Operaciones de Seguridad Tecnológica designa al especialista que elaborará y revisará el Cronograma de Monitoreo, siendo parte de su responsabilidad el seguimiento de cumplimiento de este y la comunicación (al interno del área), y actualización de ser el caso.
- Cada Gerencia que administra algún activo tecnológico designará un responsable para el seguimiento, análisis, para el cumplimiento de este y la comunicación (al interno del área), y actualización de ser el caso.

5.2.1.3 Marco Organizativo

A continuación se describen todos los procesos internos de la Gerencia de Operaciones de seguridad tecnológica (TISO):

Figura 10. Captura de pantalla de los proceso de la Gerencia de Operaciones de Seguridad Tecnológica

Fuente: intranet empresa Mibanco, 2020

TISO00: Proceso General de TISO

TISO01: Análisis de evolución.

TISO02: Aseguramiento de implementación de mecanismos

TISO03: Análisis de Alertas de Seguridad

TISO04: Validación de Políticas

TISO05: Análisis de Monitoreo

TISO06: Análisis de Escenarios de monitoreo

TISO07: Aseguramiento de aplicaciones seguras

TISO08: Ethical Hacking

TISO09: Monitoreo continuo de Vulnerabilidades

TISO10: Asesoría de seguridad.

5.2.2 Proceso Actual TISO09: Monitoreo continuo de Vulnerabilidades

5.2.2.1 Objetivo

El objetivo del presente proceso es definir la forma en cómo se ejecutan los monitoreos de vulnerabilidades, los cuales tienen una determinada frecuencia, de acuerdo al tipo de activo.

5.2.2.2 Alcance

Aplica a todas las áreas que administran activos tecnológicos considerados críticos para las operaciones de Mibanco para los cuales se establecen monitoreos recurrentes enfocados en las vulnerabilidades. Este documento es administrado por la Gerencia de Operaciones de Seguridad Tecnológica, de la División de Soporte Centralizado, e involucra a las siguientes unidades:

- Soporte microinformático.
- Soporte centralizado.
- Recursos Humanos (GDH).
- Seguridad de la Información.
- Producción – Infraestructura.
- Producción – Operaciones Sistemas.

5.2.2.3 Base legal y documentos relacionados

La base legal y los documentos están normados en la Política General de Seguridad de la Información POL-RIE-017.

5.2.2.4 Descripción del proceso

5.2.2.4.1 Monitorización de vulnerabilidades técnicas

Principio	Mibanco debe desarrollar las capacidades necesarias para establecer un proceso de monitorización, identificación y remediación de vulnerabilidades técnicas de los activos tecnológicos (aplicaciones, sistemas, equipos y dispositivos de la organización).
-----------	--

Objetivo	Minimizar el tiempo de exposición de los activos afectados a los riesgos derivados de la posible explotación de las vulnerabilidades técnicas.
Tipo de Control	Fundamental.

5.2.2.4.2 Inventario de Activos

Todas las Unidades de Negocio deben mantener un inventario de activos tecnológicos.

La Gerencia de Seguridad Tecnológica debe estar en conocimiento y tener acceso actualizado a los inventarios de activos existentes en la organización con la información de los activos tecnológicos que tienen exposición a Internet, así como aquellos clasificados como críticos para el negocio.

Para realizar su función de monitorización, identificación y remediación de vulnerabilidades técnicas en los activos, Seguridad Tecnológica gestionará y requerirá la siguiente información de los inventarios de activos:

- Activos tecnológicos gestionados por las áreas técnicas de la organización (áreas de redes y tecnologías de la información).
- Activos gestionados por terceros. Por ejemplo:
 - Servicios y aplicaciones web y/o móviles desarrolladas para la organización, aunque estén alojados en proveedores de hosting ajenos.
 - Servicios en la nube ofrecidos por terceros que utilice la organización.
- Cada activo debe tener registrado, además de sus características técnicas, los datos de contacto del Propietario y del Contacto Técnico (que podrían ser la misma persona).

Los inventarios de activos existentes deberán ser completos y actualizados, como requisito imprescindible para poder realizar una monitorización y gestión eficaz en la identificación y posterior corrección de las vulnerabilidades. La Gerencia de Seguridad Tecnológica podrá realizar chequeos periódicos y/o pruebas aleatorias sobre la completitud y actualización de la información de los inventarios existentes, reportando las posibles discrepancias al propietario del activo para su corrección.

Debe garantizarse la máxima actualización y completitud de la información referente a los dominios y subdominios de la organización. Según la organización interna de cada Gerencia o Gerencias encargadas de la gestión de dominios y subdominios reportarán a la Gerencia de Seguridad Tecnológica las altas, bajas y modificaciones.

La Gerencia de Seguridad de la Información comunicará a la Gerencia de Seguridad Tecnológica el resultado de análisis de riesgos vigente, identificando la criticidad de los activos que vayan a ser monitorizados, atendiendo a criterios de confidencialidad, integridad y disponibilidad de estos identificados durante el Análisis de Impacto al Negocio.

Figura 11. Diagrama de red As-Is
Fuente: elaboración propia, 2020

5.2.2.4.3 Monitorización de vulnerabilidades técnicas en activos

La Gerencia de Seguridad Tecnológica debe identificar las vulnerabilidades técnicas de los activos inventariados mediante un proceso continuo, con análisis de vulnerabilidades manuales.

La Gerencia de Seguridad Tecnológica deberá incluir los siguientes aspectos:

- Información de los activos supervisados (propietarios, contactos técnicos, criticidad del activo, valoración del riesgo, etc.).
- Tiempos máximos de atención de vulnerabilidades, según la criticidad de las mismas será de 4 horas después de detectada la vulnerabilidad y hasta 30 días.
- Periodicidad de la monitorización, se recomienda que como mínimo sea un análisis de los activos críticos indicados por Seguridad de la Información con la periodicidad que ellos designen.
- Procedimiento de actualización del Análisis de Riesgos de un activo, si aplicase por parte de Seguridad de la Información.
- Procedimiento de aceptación del riesgo, caso de incrementarse ante la imposibilidad técnica o económica de resolver una vulnerabilidad sobre un activo.

El proceso de alta, baja o modificación de los activos monitorizados, y la actividad de las mismas (activación/parada) se realizarán por petición de Seguridad de la Información hacia el área de Seguridad Tecnológica.

En el caso de que los análisis puedan generar degradación en el servicio o generar alarmas en la propia monitorización del activo, se acordarán ventanas de operación con Propietario del Activo afectado y se notificará al Contacto Técnico el inicio/fin del análisis.

La Gerencia de Seguridad Tecnológica definirá los parámetros para determinar la criticidad de las vulnerabilidades encontradas, en función de su facilidad de explotación, las implicaciones en el posible ataque, la extensión de la plataforma afectada, las recomendaciones de fuentes externas como CVE o CVSS, etc.

5.2.2.4.4 Alerta temprana de nuevas vulnerabilidades

La Gerencia de Seguridad Tecnológica estará en contacto con los fabricantes de tecnología y organismos externos para la alerta temprana de nuevas vulnerabilidades.

En aquellos casos en que la alerta se catalogue como criticidad alta, debido a la gravedad de esta y/o a la importancia de los activos potencialmente afectados, se establecerán las siguientes obligaciones adicionales de reporte:

- Reporte semanal de los avances en el diagnóstico y remediación de la vulnerabilidad. Este reporte deberá remitirse obligatoriamente al buzón de correo electrónico de Seguridad de la Información, generalmente incluyendo los siguientes aspectos (o aquellos que se soliciten):

- Número de activos potencialmente afectados.
- Contramedidas aplicadas para evitar la explotación de la vulnerabilidad.
- Acciones realizadas para la remediación de la vulnerabilidad.
- Activos parcheados o actualizados según las directrices establecidas.

El resultado del reporte será devuelto con una visión completa a la Gerencia de Seguridad de la Información y las Gerencias afectadas.

5.2.2.4.5 Análisis de activos afectados por vulnerabilidades

La Gerencia de Seguridad Tecnológica, en colaboración con el Centro de Comando de Seguridad, realizará un análisis de los activos afectados por vulnerabilidades para conocer el nivel de exposición de estos, determinar si la vulnerabilidad ha sido explotada y facilitar información adicional para la corrección de estas.

En el caso de que se determine que la vulnerabilidad ha sido explotada, se notificará a la Gerencia de Seguridad de la Información, para iniciar el proceso de gestión de incidentes.

5.2.2.4.6 Corrección de vulnerabilidades técnicas

El Propietario del Activo, junto con el Centro de Comando de Seguridad y Seguridad Tecnológica, debe corregir las vulnerabilidades identificadas.

La Gerencia de Seguridad Tecnológica informará sobre las vulnerabilidades detectadas en los activos de la organización al Propietario del Activo, Seguridad de la Información y al Centro de Comando de Seguridad, incluyendo la criticidad de esta.

El Propietario del Activo y el Centro de Comando de Seguridad, en colaboración con las Gerencias de Seguridad Tecnológica y de Seguridad de la Información, determinarán en función de la criticidad del activo, de la vulnerabilidad encontrada, de la disponibilidad de parches aprobados por el fabricante o de contramedidas adicionales, el plazo de corrección de la vulnerabilidad, que no excederá de 72 horas en el caso de vulnerabilidades criticidad alta que afecten a activos críticos.

Las actividades orientadas a la corrección de la vulnerabilidad podrán tratarse dentro del proceso de gestión de cambios, o requerir de una solución de emergencia.

Los Propietarios de los Activos deben comunicar a la Gerencia de Seguridad Tecnológica la resolución de las vulnerabilidades una vez que han sido solventadas.

La Gerencia de Seguridad Tecnológica reportará periódicamente al área de Seguridad de la Información, las métricas que se definan sobre las vulnerabilidades existentes en función de su criticidad, las que han sido corregidas, etc. con el objetivo de hacer comparaciones y analizar tendencias.

Existe un flujo general a seguir para todos los monitoreos dentro del Cronograma de Monitoreo, el cual tiene como producto final el Informe de Monitoreo.

5.2.2.4.7 Monitoreo recurrente

- Es responsabilidad del Analista de Monitoreo la ejecución de los controles de seguridad descritos en la Ficha de Monitoreo.
- Es responsabilidad del Especialista de Monitoreo el seguimiento de actividades para que los controles de seguridad, descritos en la Ficha de Monitoreo, sean implementados y ejecutados con la periodicidad necesaria.

5.2.2.5 Flujo del proceso

Figura 12. Proceso de monitoreo continuo de vulnerabilidades
Fuente: elaboración propia, 2020

Figura 13. Sub proceso de analizar vulnerabilidades
Fuente: elaboración propia, 2020

Figura 14. Sub proceso de verificar/actualizar inventario de actividades
Fuente: elaboración propia, 2020

5.2.2.5.1 Descripción del Subproceso

NRO.	RESPONSABLE	DESCRIPCIÓN
1.	Auditoria de IT	Cada 1er día de cada mes, el área de auditoria procederá a generar una solicitud de informe de vulnerabilidades de activos tecnológicos. Tiempo de respuesta 30 días.
2.	Gerencia TISO / Analista Senior / Analista TISO	Cada responsable de cada tecnología, debe verificar el cronograma de monitoreo continuo. Procederán a Genera ticket de atención en el sistema de ticket de atención dirigido a cada área que administran activos tecnológicos. Tiempo de respuesta 20 días.
3.	Gerencia que administra activos tecnológicos / Soporte Microinformático /Soporte centralizado/ GDH/Seguridad de la información/ Infraestructura/ Operaciones de sistemas	Revisaran el inventario de activos agrupados y priorizados de acuerdo a procesos Core. No priorizados, procederán a agrupar y priorizar. Analizar Vulnerabilidades. Recopilar la versión del activo tecnológico. Buscar nuevas vulnerabilidades (Microsoft, Owasp, Cisco, marcas del sistema). Comparar las versiones. Genera informe diferencial. Consolidar informes de hallazgos. Genera Ticket, con los hallazgos a cada área que deberá resolver el hallazgo.
4.	Área resolutora	Procederán a Subsanan hallazgos. Deberán elaborar un Plan de acción. Tiempo limitado 10 días. Comunicar a TISO, el Plan de Acción y los hallazgos subsanados.
5.	Gerencia TISO / Analista Senior / Analista TISO	Procederá a elaborar un informe priorizado de vulnerabilidades, con los planes, inventario de activos y hallazgos resueltos. Enviara informe a auditoria interna de IT.

NRO.	RESPONSABLE	DESCRIPCIÓN
6.	Auditoria de IT	Cierre de la solicitud, guardando las evidencias indicadas.

5.2.2.5.2 Indicadores del proceso

PROCESO	MONITOREO CONTINUO DE VULNERABILIDADES			
OBJETIVO	Identificar la brecha de vulnerabilidades actuales de los activos de información (Proceso general, 04.Verificar/Actualizar inventario de activos, 05. Agrupar y priorizar activos, 06. Analizar vulnerabilidades, 09. Subsanan hallazgos)			
META	No superar 2% de equipos no actualizados			
DESCRIPCIÓN	De acuerdo a lo requerido por política corporativa no se debe tener más de 2% de equipos con vulnerabilidades justificadas.			
INDICADOR	Nombre	Activos de información actualizados		
	Expresión Matemática	$\frac{\text{Cantidad de Activos no actualizados}}{\text{Total de equipos identificados}} * 100$		
	Frecuencia de medición:	Mensual	Fuente de medición	Informe de vulnerabilidades
	Responsable de medición	TISO		
	Responsable de tomar acciones	Área resolutora		

PROCESO	MONITOREO CONTINUO DE VULNERABILIDADES			
OBJETIVO	Cantidad de activos de información críticos verificados, en 30 días			
META	100% de activos de información clasificados como críticos en 30 días			
DESCRIPCION	Todo equipo catalogado como critico deberá ser verificado en un plazo no mayor a 30 días (Proceso general)			
INDICADOR	Nombre	Equipos críticos verificados		
	Expresión Matemática	$\frac{\text{Cantidad de equipos críticos Verificados}}{\text{Total de equipos Críticos}} * 100$		
	Frecuencia de medición:	Mensual	Fuente de medición	Informe de vulnerabilidades
	Responsable de medición	TISO		
	Responsable de tomar acciones	TISO		

PROCESO	MONITOREO CONTINUO DE VULNERABILIDADES			
OBJETIVO	Tiempo de resolución de vulnerabilidades (Actividad 09.Subsanar hallazgos)			
META	Equipos clasificados como no críticos deben tener el menor a 4 horas de resolución de vulnerabilidades desde detectada			
DESCRIPCION	Equipos clasificados como no críticos deben tener el menor tiempo de resolución de vulnerabilidades desde detectada			
INDICADOR	Nombre	Equipos no críticos verificados		
	Expresión Matemática	$\frac{\Sigma(\text{Tiempo de resolución en horas de cada equipo})}{\Sigma(\text{cantidad de equipos})}$		
	Frecuencia de medición:	Mensual	Fuente de medición	Informe de vulnerabilidades
	Responsable de medición	TISO		

	Responsable de tomar acciones	TISO
--	-------------------------------	------

5.2.3 Nuevo Proceso TISO09: Monitoreo continuo de Vulnerabilidades

5.2.3.1 Descripción del proceso

El siguiente proceso tiene por misión realizar el proceso de monitorear continuamente las vulnerabilidades de los activos tecnológicos de Mibanco, sin discriminar el área que los administra, ello se logra con la gestión de la herramienta Análisis continuo de vulnerabilidades.

La herramienta Análisis continuo de vulnerabilidades escanea toda la red mediante sondas por puertos de escucha, así como clientes en los diversos sistemas operativos, los cuales continuamente identifican las vulnerabilidades.

5.2.3.2 Flujo del proceso

Figura 15. Proceso de monitoreo continuo de vulnerabilidades To-Be
Fuente: elaboración propia, 2020

5.2.3.2.1 Descripción del proceso

NRO.	RESPONSABLE	DESCRIPCIÓN
1.	Auditoria de IT	Cada 1er día de cada mes el área de auditoria procederá a generar una solicitud de informe de vulnerabilidades de activos tecnológicos.
2.	Gerencia TISO / Analista Senior / Analista TISO	Cada responsable de cada tecnología, verificará el cronograma de monitoreo continuo. Procederá a descargar el último análisis de verificación de vulnerabilidades de la herramienta Análisis continuo de vulnerabilidades . Procederá a generar el informe de hallazgos. Generará un ticket en el sistema de ticket al área resolutora para subsanar los hallazgos.
3.	Área resolutora	Procederán a Subsanar hallazgos, desde el portal de la herramienta Análisis continuo de vulnerabilidades , de los sistemas no críticos. Elaborarán un Plan de acción, para las aplicaciones críticas. Comunicarán a TISO, el Plan de Acción y los hallazgos subsanados.
4.	Gerencia TISO / Analista Senior / Analista TISO	Procederá a Elaborar un informe priorizado de vulnerabilidades, con los planes, inventario de activos y hallazgos resueltos. Enviara informe a auditoria interna de IT.
5.	Auditoria de IT	Cierre de la solicitud, guardando las evidencias indicadas.

5.3 Propuesta de Solución

Desarrollar un diseño de propuesta para implementar un software tipo IaaS que apoye en la mejora sustancial del proceso de monitoreo continuo de vulnerabilidades, basado en los estándares de Mibanco, para así descubrir, detectar, responder y prevenir las brechas de seguridad de los activos de información con mayor eficiencia.

5.4 Gestión de Requerimientos

5.4.1 Especificación de Reglas del Negocio

- **RN001 – Acceso por perfiles**

Ningún usuario deberá tener el usuario administrador global de la herramienta.

- **RN002 – Método de acceso -Usuario y contraseña**

Todo usuario deberá tener contar con una matrícula y contraseña de acuerdo a la políticas vigente POL-RIE-017.

- **RN003 – Método de acceso -Múltiples factores de autenticación**

Todo usuario deberá tener acceso a cualquier aplicación por medio de un MFA autorizado por Mibanco.

- **RN004 – Remediación de vulnerabilidades**

Máximo el 2% de los activos de información podrán estar con vulnerabilidades explotables.

- **RN005 – Tiempo de remediación de equipos no críticos**

El tiempo de remediación de activos de información no críticos deberá ser de máximo 4 horas, desde la detección del mismo.

- **RN006 – Software tipo IaaS**

El sistema deberá ser suministrado en la modalidad Cloud tipo IaaS.

- **RN007 – Certificación**

El sistema debe tener certificación CAS STAR (Basado en ISO/IEC27001).

- **RN008 – Trazabilidad**

Cualquier transacción, cambio y/o modificación deberá mantener la trazabilidad de las acciones.

- **RN009 – Software cliente**

El sistema debe permitir la instalación de clientes en equipos Windows y Linux.

- **RN010 – Gestión de usuarios y perfiles**

El sistema debe permitir el ingreso de múltiples usuarios y perfiles, enlazados al LDAP.

5.4.2 Requerimientos Funcionales

TABLA DE REQUERIMIENTOS FUNCIONALES
RF001_Escanear activos de información con pruebas de Caja Negra
El sistema debe permitir escaneo automático de vulnerabilidades de activos de información, con pruebas de caja negra (sin usuario y password, solo descubrimiento).
RF002_ Escanear activos de información con pruebas de Caja Blanca
El sistema debe permitir escaneo automático de vulnerabilidades de activos de información, con pruebas de caja blanca (con usuario y contraseña).
RF003_Priorización de vulnerabilidades automáticas
El Sistema deberá integrar inteligencia de amenazas, para su priorización.
RF004_Priorización de vulnerabilidades manuales
El Sistema debe permitir modificar manualmente la prioridad de las mismas de acuerdo a los requerimientos del negocio.
RF005_Detección automática de activos de información
El Sistema debe detectar nuevos activos de información en general y por tipo ingresados a la red.
RF006_Detección manual de activos de información
El Sistema permitirá la detección manual de nuevos activos de información en general y por tipo ingresados a la red.
RF007_Clasificación automática de activos de información
El sistema debe clasificar activos de información por tipo y criticidad.
RF008_Clasificación manual de activos de información
El sistema permitirá la clasificación manual de activos de información, de acuerdo a criterios del usuario.
RF009_Actualizaciones automáticas de activos de información no críticos
El Sistema debe permitir la actualización de sistemas catalogados como no críticos.
RF010_Actualizaciones de activos críticos programados
El Sistema debe permitir programar la actualización de sistemas catalogados como críticos.
RF011_Envío de mensajes de alerta de nueva vulnerabilidad

TABLA DE REQUERIMIENTOS FUNCIONALES
El Sistema debe permitir el envío automático de mensajes de nuevas vulnerabilidades detectadas en los activos de información, y también mostrarlas en el dashboard.
RF012_Visualización de la descripción y remediación de vulnerabilidades
El sistema deberá mostrar la descripción de vulnerabilidades y los pasos para su remediación.
RF013_Dashboard general personalizable
El Sistema debe permitir la visualización de reportes dinámicos de alto nivel, el cual debe ser personalizable y también detallado por activo de información.
RF014_Indicadores de madurez
El sistema deberá analizar en base a toda la exposición, el nivel de madurez, basado en el tiempo de respuesta y edad de vulnerabilidad
RF015_Métricas de cyber exposición
El sistema deberá generar métricas de exposición en los análisis de vulnerabilidades.

5.4.3 Requerimientos No Funcionales

TABLA DE REQUERIMIENTOS NO FUNCIONALES
RNF001_Mensajes sistema
El sistema debe implementar mensajes para 3 tipos: Informativo, Error y Confirmación.
RNF002_Almacenamiento Digital
Todos los documentos generados deben ser exportados a excel y pdf.
RNF003_Compatibilidad Navegador
La aplicación web debe ser compatible con Google Chrome.
RNF004_Disponibilidad Sistema
El sistema debe estar disponible los 365 días de año en un 99.99% (indisponibilidad de 52 horas).
RNF005_Persistencia de credenciales
El sistema NO debe guardar el nombre de usuario de acceso al sistema.
RNF006_Tiempo Carga Web

TABLA DE REQUERIMIENTOS NO FUNCIONALES	
	El tiempo de carga de formularios deberá ser de 5 segundos como máximo, sin imágenes.
RNF007_ Tiempo Transacción	
	El tiempo promedio de ejecución de transacciones en línea debe ser de 5 segundos.
RNF008_ Escalabilidad del sistema	
	El sistema debe soportar el incremento de 30% anual de dispositivos.
RNF009_ Tiempo recuperación	
	El sistema debe recuperarse como promedio en 2 horas, desde reportado el incidente.
RNF010_ Mostrar actualización	
	El sistema debe poder mostrar o avisar una actualización disponible de un sistema operativo.
RNF011_ Owasp top ten	
	El sistema deberá escanear mediante Owasp Top Ten, las páginas web monitoreadas.
RNF012_ Gestión de SSO	
	El sistema debe permitir la integración del protocolo SAML.
RNF013_ Gestión de Syslog	
	El sistema debe permitir la descarga de Syslog o envío de log automáticos.

5.4.4 Matriz de Trazabilidad entre los Requerimientos Funcionales vs Reglas De Negocio

Tabla 3 *Matriz de Trazabilidad entre los Requerimientos Funcionales vs Reglas De Negocio*

Fuente: elaboración propia

	RN001-Acceso por perfiles	RN002-Método de acceso - Usuario y contraseña	RN003-Método de acceso - Múltiples factores de autenticación	RN004-Remediación de vulnerabilidades	RN005-Tiempo de remediación de equipos no críticos	RN006-Software tipo SaaS	RN007-Certificación	RN008-Trazabilidad	RN009-Software cliente	RN010-Gestión de usuarios y perfiles
RF001_Escanear activos de información con pruebas de Caja Negra	X	X	X			X	X	X	X	X
RF002_Escanear activos de información con pruebas de Caja Blanca	X	X	X			X	X	X	X	X
RF003_Priorización de vulnerabilidades automáticas				X		X		X		
RF004_Priorización de vulnerabilidades manuales	X	X	X	X		X		X		X
RF005_Detección automática de activos de información						X		X	X	
RF006_Detección manual de activos de información	X	X	X					X	X	X
RF007_Clasificación automática de activos de información						X		X	X	
RF008_Clasificación manual de activos de información	X	X	X			X		X	X	

	RN001-Acceso por perfiles	RN002- Método de acceso - Usuario y contraseña	RN003- Método de acceso - Múltiples factores de autenticación	RN004- Remediación de vulnerabilidad es	RN005-Tiempo de remediación de equipos no críticos	RN006- Software tipo SaaS	RN007- Certificación	RN008- Trazabilidad	RN009- Software cliente	RN010- Gestión de usuarios y perfiles
RF009_Actualizaciones automáticas de activos de información no críticos				X	X			X	X	
RF010_Actualizaciones de activos críticos programadas				X				X		
RF011_Envío de mensajes de alerta de nueva vulnerabilidad						X				
RF012_Visualización de la descripción y remediación de vulnerabilidades						X				
RF013_Dashboard general personalizable						X				
RF014_Indicadores de madurez						X				
RF015_Métricas de cyber exposición						X				

5.4.5 Escenarios de Atributos de Calidad

Tabla 4 *Escenarios de atributos de calidad*

Fuente: elaboración propia

ATRIBUTO	FUENTE	ESTÍMULO	ARTEFACTO	ENTORNO	RESPUESTA	MEDIDA
Desempeño	Casa matriz del software	Enviar una actualización	Aviso	Momento en el que hay mucho tráfico	Debe ser visible para el usuario	10s después de haber sido publicada (t<=10s)
Cuando el sistema detecte una actualización disponible, en los momentos en los que hay mucho tráfico en la red, el aviso se debe hacer visible al usuario tras un máximo de diez (10) segundos de haber sido publicada.						
Disponibilidad	Usuario	Interacción con el sistema	Sistema	Ambiente de uso de sistema	Visualización del sistema o denegación de servicio	Denegar el servicio el menor tiempo posible, 0.01% (24x7)
El sistema deberá ser accesible el 99.99% del tiempo, en algunas ocasiones no será visible y en otras el servicio será denegado al usuario, pidiéndole que trate de acceder más tarde.						
Escalabilidad	Administrador de sistemas	Ampliar activos de información	Sistema	Momento cuando el activo se une a la red	Soportar el incremento del activo	El sistema no se degrada ni ralentiza el tiempo de respuesta
El sistema debe ser capaz de soportar exitosamente el incremento de activos de información cuando la organización decida ampliar, de tal modo que el sistema no se degrade ni se ralentice los tiempos de respuesta.						
Seguridad	Acceso a la información privada	Restringir acceso a los datos	Sistema, servidor, base de datos	Ambiente de uso de sistema	Acceso mediante claves seguras	Acceso de manera ilícita y número de intrusiones debe ser 0
El sistema deberá impedir, en la medida de todo lo posible los fallos de seguridad, como intrusos que puedan acceder al sistema haciéndose pasar por usuarios con determinados permisos, o el acceso a los datos, pudiendo modificarlos, borrarlos o extraerlos.						

ATRIBUTO	FUENTE	ESTÍMULO	ARTEFACTO	ENTORNO	RESPUESTA	MEDIDA
Usabilidad	Usuario	Usar el sistema	Sistema	Sistema operando	El sistema presentará un entorno fácil de utilizar	El usuario debe aprender a usar el sistema en el menor tiempo posible (2 días)
Usuarios nuevos usan por primera vez el sistema.						
Performance	Actualización de la información	Actividad en el sistema	Sistema	Sistema operando	Incremento en el número de accesos e interacción con el sistema	Número de accesos al sistema por mes
El sistema deberá facilitar un mínimo de información al mes, con la finalidad de que los usuarios puedan tener un buen monitoreo.						
Performance	Usuario	Transacciones por minuto	Sistema	Sistema operando	Transacción procesada	Latencia menor a 3 segundos
El usuario solicita 1000 transacciones por minuto bajo condición normal de 9-18 horas, el sistema debe procesarlas en una latencia menor a 3 segundos.						

5.4.6 Matriz de Trazabilidad entre los Requerimientos No Funcionales vs Atributos de Calidad

Tabla 5 *Matriz de Trazabilidad entre los Requerimientos No Funcionales vs Atributos de Calidad*

Fuente: elaboración propia

	Desempeño	Disponibilidad	Escalabilidad	Seguridad	Usabilidad	Performance
RNF001-Mensajes sistema					X	
RNF002-Almacenamiento Digital					X	
RNF003-Compatibilidad Navegador					X	
RNF004-Disponibilidad Sistema		X				
RNF005-Persistencia de credenciales				X		
RNF006-Tiempo Carga Web						X
RNF007-Tiempo Transacción						X
RNF008-Escalabilidad del sistema			X			
RNF009-Tiempo recuperación		X				
RNF010-Mostrar actualización	X					
RNF011-Owasp top ten				X		
RNF012-Gestión de SSO				X		
RNF013-Gestión de Syslog					X	

5.4.7 Drivers Arquitectónicos

DRIVERS FUNCIONALES		JUSTIFICACIÓN
DF001	Escanear activos de información con pruebas de Caja Negra	Son necesarios las escaneo de pruebas de caja negra ya que brindará la visualización desde el exterior de las vulnerabilidades del Activo.
DF002	Escanear activos de información con pruebas de Caja Blanca	Son necesarios las escaneo de pruebas de caja blanca ya que brindará la visualización desde el interior de las vulnerabilidades del Activo.
DF003	Priorización de vulnerabilidades automáticas	Es imperativo la priorización automática de acuerdo a la criticidad de la vulnerabilidad por parte del fabricante.
DF004	Detección automática de activos de información	Es crítica este requerimiento ya que permitirá escanear constantemente la red, el ingreso de nuevos activos, así como encontrar de shadow IT no declarado.
DF005	Actualizaciones automáticas de activos de información no críticos	Es necesario actualizar automáticamente los activos catalogados como no críticos ello descargara bastante el proceso manual actual.
DRIVERS DE ATRIBUTOS DE CALIDAD		JUSTIFICACIÓN
DF006	Disponibilidad del Sistema	Debido a su criticidad el sistema debe tener un alto índice de disponibilidad.
DF007	Tiempo Transacción	La velocidad del sistema es un punto crítico, ya que permitirá un despliegue mucho mayor de funcionalidades simultaneas.
DF008	Escalabilidad del Sistema	Debido a la alta variación de servicios creados cada año, es imperativo que el sistema soporte el crecimiento volumétrico de los activos de información.

5.4.8 Matriz de Trazabilidad de Requerimientos Funcionales vs Drivers Funcionales

Tabla 6 *Matriz de Trazabilidad de Requerimientos Funcionales vs Drivers Funcionales*

Fuente: elaboración propia

	DF001-Escanear activos de información con pruebas de Caja Negra	DF002-Escanear activos de información con pruebas de Caja Blanca	DF003-Priorización de vulnerabilidades automáticas	DF004-Detección automática de activos de información	DF005-Actualizaciones automáticas de activos de información no críticos	DF006-Disponibilidad del Sistema	DF007-Tiempo Transacción	DF008-Escalabilidad del Sistema
RF001_Escanear activos de información con pruebas de Caja Negra	X					X	X	X
RF002_Escanear activos de información con pruebas de Caja Blanca		X				X	X	X
RF003_Priorización de vulnerabilidades automáticas			X			X	X	X
RF004_Priorización de vulnerabilidades manuales						X	X	X
RF005_Detección automática de activos de información				X		X	X	X
RF006_Detección manual de activos de información						X	X	X
RF007_Clasificación automática de activos de información						X	X	X
RF008_Clasificación manual de activos de información						X	X	X
RF009_Actualizaciones automáticas de activos de información no críticos					X	X	X	X
RF010_Actualizaciones de activos críticos programadas						X	X	X
RF011_Envío de mensajes de alerta de nueva vulnerabilidad						X	X	X
RF012_Visualización de la descripción y remediación de vulnerabilidades						X	X	X
RF013_Dashboard general personalizable						X	X	X
RF014_Indicadores de madurez						X	X	X
RF015_Métricas de cyber exposición						X	X	X

5.4.9 Matriz de Trazabilidad de Drivers Funcionales vs Tácticas

Tabla 7 *Matriz de Trazabilidad de Drivers Funcionales vs Tácticas*

Fuente: elaboración propia

	Disponibilidad	Escalabilidad	Performance
	Sistema siempre operativo	Respuesta al incremento de activos	Tiempo de respuesta a un evento
DF001-Escanear activos de información con pruebas de Caja Negra	X	X	
DF002-Escanear activos de información con pruebas de Caja Blanca	X	X	
DF003-Priorización de vulnerabilidades automáticas	X		X
DF004-Detección automática de activos de información	X	X	
DF005-Actualizaciones automáticas de activos de información no críticos	X		

5.4.10 Matriz de Trazabilidad de Drivers de Atributos de Calidad vs Tácticas

Tabla 8 *Matriz de Trazabilidad de Drivers de Atributos de Calidad vs Tácticas*

Fuente: elaboración propia

	Disponibilidad	Escalabilidad	Performance	
	Sistema siempre operativo	Respuesta al incremento de activos	Tiempo de respuesta a un evento	Eventos atendidos en un intervalo de tiempo
DF006_Disponibilidad Sistema	X			
DF007_Tiempo Transacción			X	X
DF008_Escalabilidad del sistema		X		

5.4.11 Matriz de Trazabilidad de Drivers Arquitectónicos vs Casos de Uso de Sistema

Tabla 9 *Matriz de Trazabilidad de Drivers Arquitectónicos vs Casos de Uso de Sistema*

Fuente: elaboración propia

	CUS01: Detectar Activos Nuevos	CUS02: Clasificar Activos de información	CUS03: Buscar activos con parámetros de usuario	CUS04: Buscar activos Automáticamente en la red	CUS05: Clasificar manualmente activos	CUS06: Clasificar automáticamente activos	CUS07: Escanear vulnerabilidades de activos	CUS08: Priorizar vulnerabilidades	CUS09: Escanear con prueba de caja Negra	CUS10: Escanear con prueba de caja Blanca	CUS11: Priorizar manualmente Vulnerabilidades	CUS12: Reportar activos y vulnerabilidades encontradas	CUS13: Priorizar Automáticamente Vulnerabilidades	CUS14: Actualización de nuevas vulnerabilidades	CUS15: Programar actualizaciones de equipos	CUS16: Actualizar equipos no críticos	CUS17: Actualizar equipos críticos	CUS18: Visualizar Dashboard	CUS19: Gestionar Alertas	CUS20: Visualizar Alertas y eventos	CUS21: Procesar indicadores y ciber exposición	CUS22: Listar vulnerabilidades para generar alertas
DF001-Escanear activos de información con pruebas de Caja Negra	X			X			X		X			X		X								
DF002-Escanear activos de información con pruebas de Caja Blanca	X		X	X			X			X		X		X								
DF003-Priorización de vulnerabilidades automáticas								X					X									
DF004-Detección automática de activos de información								X			X											
DF005-Actualizaciones automáticas de activos de información no críticos	X			X																		
DF006-Disponibilidad del Sistema	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
DF007-Tiempo Transaccion	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
DF008-Escalabilidad del Sistema	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

5.4.12 Diagrama de Paquetes

Un diagrama de paquetes en el Lenguaje Unificado de Modelado representa las dependencias entre los paquetes que componen un modelo. Es decir, muestra cómo un sistema está dividido en agrupaciones lógicas y las dependencias entre esas agrupaciones.

Para ello hemos separado paquetes por funcionalidades y su dependencia entre ellos, también hemos identificado un paquete de utilitarios que servirá como soporte a los cuatro procesos funcionales.

Figura 16. Diagrama de paquetes
Fuente: elaboración propia, 2020

5.4.13 Casos de Uso

Figura 17. Paquete descubrir activos
Fuente: elaboración propia, 2020

Figura 18. Paquete gestión de vulnerabilidades
Fuente: elaboración propia, 2020

Figura 19. Paquete dashboard
Fuente: elaboración propia, 2020

Figura 20. Paquete actualización de activos
Fuente: elaboración propia, 2020

Figura 21. Paquete utilitarios
Fuente: elaboración propia, 2020

5.4.14 Matriz de Trazabilidad de Requerimientos Funcionales vs Casos de Uso de Sistema

Tabla 10 *Matriz de Trazabilidad de Requerimientos Funcionales vs Casos de Uso de Sistema*

Fuente: elaboración propia

	CUS01: Detectar Activos Nuevos	CUS02: Clasificar Activos de Información	CUS03: Buscar activos con parámetros de usuario	CUS04: Buscar activos Automáticamente en la red	CUS05: Clasificar manualmente activos	CUS06: Clasificar automáticamente activos	CUS07: Escanear vulnerabilidades de activos	CUS08: Priorizar vulnerabilidades	CUS09: Escanear con prueba de caja Negra	CUS10: Escanear con prueba de caja Blanca	CUS11: Priorizar manualmente Vulnerabilidades	CUS12: Reportar activos y vulnerabilidades encontradas	CUS13: Priorizar Automáticamente Vulnerabilidades	CUS14: Actualización de nuevas vulnerabilidades	CUS15: Programar actualizaciones de equipos	CUS16: Actualizar equipos no críticos	CUS17: Actualizar equipos críticos	CUS18: Visualizar Dashboard	CUS19: Gestionar Alertas	CUS20: Visualizar Alertas y eventos	CUS21: Procesar Indicadores y ciber exposición	CUS22: Listar vulnerabilidades para generar alertas
RF001_Escanear activos de información con pruebas de Caja Negra	X			X			X		X			X		X								
RF002_Escanear activos de información con pruebas de Caja Blanca	X		X	X			X			X		X		X								
RF003_Priorización de vulnerabilidades automáticas								X					X									
RF004_Priorización de vulnerabilidades manuales								X			X											
RF005_Detección automática de activos de información	X			X																		
RF006_Detección manual de activos de información			X																			
RF007_Clasificación automática de activos de información		X				X																
RF008_Clasificación manual de activos de información		X			X																	
RF009_Actualizaciones automáticas de activos de información no críticos															X	X						
RF010_Actualizaciones de activos críticos programadas															X		X					
RF011_Envío de mensajes de alerta de nueva vulnerabilidad																		X				
RF012_Visualización de la descripción y remediación de vulnerabilidades																			X			X
RF013_Dashboard general personalizable																		X				
RF014_Indicadores de madurez																					X	
RF015_Métricas de cyber exposición																					X	

5.4.15 Especificación de Casos de Uso de Sistema

Caso de Uso	
Nombre	CUS01: Detectar activos nuevos
Actor(es)	Administrador, SW-HW-Sonda
Propósito:	Detectar activos nuevos
Caso(s) de uso asociado(s):	CUS03: Buscar Activos con parámetro de usuarios CUS04: Buscar Activos Automáticamente en la red
Descripción:	El propósito del caso de uso es iniciar el proceso de detección de activos de información
Precondiciones:	El administrador autenticado en el sistema
Clasificación:	Primario
<p>Flujo Normal:</p> <ol style="list-style-type: none"> 1. El sistema muestra una pantalla con los últimos activos de información detectados automáticamente por el sistema, específicamente por el actor SW-HW-Sonda. 2. El administrador presiona el botón “Buscar Activo de Información”. 3. El sistema muestra los últimos activos encontrados. <p>Flujo Altern01:</p> <ol style="list-style-type: none"> 1. El sistema muestra una pantalla, con opciones de búsqueda de activos de información (IP, Rango IP, SO, etc.). 2. El administrador presiona el botón “Buscar”. 3. El sistema muestra los resultados de los activos detectados, en la pantalla inicial. 	
Post Condiciones:	Se actualiza la lista de activos detectados con parámetros de usuario.

Flujo Normal:

Figura 22. Prototipo detectar activos nuevos
Fuente: elaboración propia, 2020

Flujo Alternol:

Figura 23. Prototipo buscar activos

Fuente: elaboración propia, 2020

Figura 24. Prototipo listado de activos

Fuente: elaboración propia, 2020

Caso de Uso	
Nombre	CUS07: Escanear Vulnerabilidades de activos
Actor(es)	Administrador, SW-HW-Sonda, SW-Cliente
Propósito:	Buscar las vulnerabilidades de los activos de información
Caso(s) de uso asociado(s):	CUS09: Escanear con pruebas de caja negra CUS10: Escanear con pruebas de caja blanca
Descripción:	El propósito del caso de uso es buscar las vulnerabilidades de forma manual, con parámetros de usuario
Precondiciones:	El administrador autenticado en el sistema El sistema, realizó pruebas de caja negra
Clasificación:	Primario
<p>Flujo Normal:</p> <ol style="list-style-type: none"> 1. El sistema muestra una pantalla con los activos de información y las últimas vulnerabilidades detectadas automáticamente por el actor del sistema SW-HW-Sonda y SW-Cliente. 2. El administrador, selecciona el activo que desea escanear. 3. El administrador, presiona el botón “Escanear”. 	

Caso de Uso	
	<p>4. El sistema muestra opciones de tipos de escaneo.</p> <p>5. El administrador selecciona el tipo de escaneo “Búsqueda Básica” de acuerdo al activo de información.</p> <p>6. El administrador presiona el botón “Analizar”, y el sistema realizará pruebas de caja negra.</p> <p>7. El sistema muestra el resultado del análisis priorizados automáticamente.</p> <p>8. El administrador selecciona la vulnerabilidad y presiona el botón de “Detalle”.</p> <p>9. El sistema muestra el detalle de la vulnerabilidad elegida.</p> <p>Flujo Alternol:</p> <p>1. El administrador en el punto 5, selecciona la opción “Búsqueda Avanzada” y el sistema le solicitará que ingrese un usuario y contraseña de activo de información, debe elegir el tipo de categoría y luego presiona el botón “Analizar”.</p> <p>2. El sistema realizará pruebas de caja blanca, validando las credenciales ingresadas previamente por el administrador en el punto anterior.</p> <p>3. El sistema muestra el resultado del análisis priorizado automáticamente.</p> <p>4. El administrador selecciona una de las vulnerabilidades y presiona el botón de “Detalle”.</p> <p>5. El sistema muestra el detalle de la vulnerabilidad elegida.</p>
Post Condiciones:	<p>Se actualiza la lista de vulnerabilidades detectadas por el proceso.</p> <p>Se actualiza el usuario y contraseña del activo de información.</p>

Flujo Normal:

Figura 25. Prototipo escanear vulnerabilidades de activos
Fuente: elaboración propia, 2020

Figura 26. Prototipo tipo de escaneo
Fuente: elaboración propia, 2020

Figura 27. Prototipo resultado de escaneo
Fuente: elaboración propia, 2020

Figura 28. Prototipo información detallada de activo
Fuente: elaboración propia, 2020

Flujo Alternol:

Figura 29. Prototipo tipo de escaneo
Fuente: elaboración propia, 2020

Figura 30. Prototipo ingreso de credenciales para escaneo
Fuente: elaboración propia, 2020

Figura 31. Prototipo resultado de escaneo
Fuente: elaboración propia, 2020

Figura 32. Prototipo información detallada de activo
Fuente: elaboración propia, 2020

Caso de Uso	
Nombre	CUS08: Priorizar Vulnerabilidades
Actor(es)	Administrador, SW-Core-IaaS
Propósito:	Priorizar las vulnerabilidades detectadas de forma automática
Caso(s) de uso asociado(s):	CUS03: Priorizar manualmente vulnerabilidades CUS13: Priorizar automáticamente vulnerabilidades
Descripción:	El propósito del caso de uso es Priorizar las vulnerabilidades detectadas de forma automática por el sistema, para moldearlas de acuerdo a las necesidades del negocio.
Precondiciones:	El administrador autenticado en el sistema. El sistema, realizó pruebas de caja negra o pruebas de caja blanca.
Clasificación:	Primario
<p>Flujo Normal:</p> <ol style="list-style-type: none"> 1. El sistema muestra una pantalla con los últimos activos de información detectados por el sistema. 2. El sistema muestra en la pantalla las columnas de consolidado de vulnerabilidades por activo de información, agrupadas en Críticos, Alto, Medio y Bajo, catalogadas por el administrador de sistema SW-Core-IaaS. 3. El administrador selecciona la vulnerabilidad que desea priorizar y presiona el botón “Priorización Manual”. 4. El sistema muestra la pantalla de priorización manual de vulnerabilidades. 5. El administrador selecciona una vulnerabilidad y le cambia de nivel de prioridad. 6. El administrador presiona el botón “Guardar”. 	
Post Condiciones:	Se actualiza la lista de vulnerabilidades priorizadas con el check de priorización manual.

Flujo Normal:

Figura 33. Prototipo priorizar vulnerabilidades
Fuente: elaboración propia, 2020

Figura 34. Prototipo priorizar vulnerabilidades de forma manual
Fuente: elaboración propia, 2020

Caso de Uso	
Nombre	CUS15: Programa actualizaciones de equipos
Actor(es)	Administrador, SW-Core-IaaS
Propósito:	Realizar una programación de actualización de activos de información
Caso(s) de uso asociado(s):	CUS16: Actualizar equipos no críticos CUS17: Actualizar equipos críticos
Descripción:	El propósito del caso de uso, es realizar el proceso de actualización de activos de información
Precondiciones:	El administrador autenticado en el sistema El sistema, debe tener catalogado los activos de información como críticos y no críticos
Clasificación:	Primario
<p>Flujo Normal:</p> <ol style="list-style-type: none"> 1. El sistema muestra una pantalla donde se debe seleccionar el activo de información o grupo de activos de información para realizar la programación. 2. El Administrador selecciona el grupo y presiona el botón “Programar actualización”. 3. El Administrador selecciona la fecha de actualización para los equipos. 4. El Administrador selecciona el check de actualización inmediata y presiona el botón “Ejecutar Actualización”. 5. El sistema muestra la lista de activos a actualizar. 6. El sistema ejecuta la actualización de los activos. 7. El sistema genera eventos y alertas de actualización. <p>Flujo Alternol:</p> <ol style="list-style-type: none"> 1. En el punto 2 del flujo normal el administrador selecciona un solo activo de información para actualizar. 2. El administrador presiona el botón “Programar Actualización” para el activo. 3. El administrador selecciona una fecha y hora para la actualización. 4. El administrador presiona el botón “Ejecutar Actualización”. 6. El sistema genera eventos y alertas de actualización. 	
Post Condiciones:	Ejecución de actualizaciones de acuerdo al programa.

Flujo Normal:

Figura 35. Prototipo programa actualizaciones de equipos
Fuente: elaboración propia, 2020

Figura 36. Prototipo programación de schedule de actualización
Fuente: elaboración propia, 2020

Figura 37. Prototipo listado de ejecución de actualizaciones de equipos
Fuente: elaboración propia, 2020

Flujo Alternol:

Figura 38. Prototipo programa manual de actualización de equipos
Fuente: elaboración propia, 2020

Figura 39. Prototipo ingreso de fecha de actualización de equipo
Fuente: elaboración propia, 2020

Figura 40. Prototipo ejecución de actualización de equipo
Fuente: elaboración propia, 2020

5.4.16 Conceptos de Diseño

Transparencia

Asociamos este concepto, porque el sistema debe ser percibido como un todo, en vez de una colección de componentes independientes. La transparencia la aplicamos en:

Acceso: Permitiendo el acceso remoto de la misma forma como si fuera local.

Concurrencia: Permitiendo que varios procesos del sistema operen concurrentemente utilizando objetos compartidos y de forma que no exista interferencia entre ellos.

Replicación: Permitiendo utilizar múltiples instancias del sistema incrementando la fiabilidad y las prestaciones sin que los usuarios tengan que conocer la existencia de las réplicas.

Fallos: Permitiendo al sistema completar sus tareas a pesar de la ocurrencia de fallos en el hardware o en el software.

Migración: Permitiendo el movimiento del sistema sin afectar a los usuarios o a otros sistemas.

Prestaciones: Permitiendo que el sistema sea reconfigurado para mejorar las prestaciones mientras la carga varia.

Escalado: Permitiendo la expansión del sistema sin cambiar su estructura.

Integración

Asociamos este concepto, porque el sistema debe conectarse a nuestras aplicaciones unas con otras así poder intercambiar información operativa. Cuando los sistemas no pueden compartir su información, se crean cuellos de botella que requieren de la intervención humana en la forma de toma de decisiones o en el ingreso mismo de la información. Con una arquitectura de integración correctamente implementada, nuestra organización puede enfocar la mayoría de sus esfuerzos en la creación de competencias que generen valor, en lugar de enfocarse en la coordinación de labores operativas y crear ventajas competitivas futuras.

Optimización

Asociamos este concepto, porque al software se le pueda realizar cualquier modificación y que algún aspecto del mismo funcione de manera más eficiente y/o utilice menos recursos (mayor rendimiento). En general, el software puede ser optimizado para que se ejecute más rápidamente, o sea capaz de operar con menos memoria u otros recursos, o consuman menos energía.

5.4.17 Estilos de Arquitectura

N-Tier/3-Tier

Por el presente trabajaremos con este estilo, porque tenemos la necesidad de visualizar las diferentes capas de la arquitectura de red actual, donde nuestra herramienta requiere interactuar con los diversos equipos de red y seguridad, ello mostrara el panorama de ubicación de los diversos sensores (Sonda y clientes).

Layered

Usaremos este estilo, para visualizar la interacción de las diferentes capas de la solución, desde el activo de información, pasando por los diversos sensores, módulos del sistema hasta llegar a la capa de dashboard de reportes y alertas.

Así mismo en el grafico se muestra los principios requeridos del proceso de una manera alineada, desde descubrir, detectar, responder hasta prevenir ataques.

Figura 42. Diagrama Layered
Fuente: elaboración propia, 2020

5.5.3 Arquitectura C4

5.5.3.1 Diagrama de Contexto

Es el primer nivel del modelo 4C, donde se puede visualizar la estructura general del sistema de Análisis Continuo de Vulnerabilidades y la interacción a alto nivel entre ellos, se muestra a las usuarios que utilizaran (Administrador y Visualizador) el sistema, así como la interacción con el otro sistema, quienes forman parte de la solución propuesta.

El otro sistema es el de Sensores, quien se encarga de recopilar la información de campo de los activos de información, y enviar la información al sistema superior para su procesamiento y presentación al usuario. El diagrama evidencia la independencia de los dos sistemas, donde el sistemas principal (Sistema de Análisis Continuo de vulnerabilidades-“SACV”) será alojado en un entorno cloud, el cual asegura la disponibilidad y crecimiento de la solución. Por otro lado el sistema de los sensores, al ser una gran cantidad desplegados en la red física

y en los activos de información de la institución, podrán relevar su funcionalidad en caso se presente problemas en alguno de ellos.

El sistema encaja en el entorno actual del proceso de TISO, automatizando la tarea de la detección de activos de información con los sensores y el procesamiento de la información con el sistema de Análisis Continuo de Vulnerabilidades.

Figura 43. Diagrama de Contexto C4
Fuente: elaboración propia, 2020

5.5.3.2 Diagrama de Contenedores – Sensores

El segundo nivel del modelo 4C diagrama de contenedores, aquí podemos observar el detalle del sistema de sensores en los dos contenedores.

La forma como trabaja este sistema, es la de cliente servidor, se tiene el cliente instalado en todos los activos de información y un servidor a donde envían la información los clientes.

En primera instancia se puede observar la Sonda, el cual es un elemento encargado de descubrir todos los activos de su alcance mediante la captura de información a través del puerto SPAN en la red donde se aloja. Así mismo realiza la pasarela para poder ejecutar las pruebas de caja negra y caja blanca, estas sondas serán tantas como se requiere en la red física, virtual y cloud, garantizando la escalabilidad de la solución.

La Sonda al detectar cada activo de información que trate de comunicarse en la red escuchada, enviará la información al SACV, para su procesamiento y clasificación, también realizara un análisis preliminar de caja negra al sistema del activo detectado; cuando se cuente con el usuario y contraseña del activo de información se procederá a realizar el escaneo de caja blanca.

El contenedor SW-Cliente, es una aplicación que se instala del lado del Sistema Operativo (Windows o Linux) que lo pueda soportar, ellos reportarán al sistema principal las pruebas de caja blanca que se soliciten.

Esta capa interactúa con el SACV quien se encuentra en cloud, mediante protocolo https a través de archivos JSON y desde la capa superior hacia las sondas deberá estar abierto el puerto 443 para temas de comunicación y control. La descarga de actualizaciones es controlada por la capa superior del SACV y enviada al SW-Cliente mediante protocolo SFTP por un puerto personalizado 888.

La distribución de sensores en interacción con el sistema así como su diversidad garantizará en gran medida la detección oportuna de activos de información así como su análisis correspondiente.

Figura 44. Diagrama de Containers – sensores C4
Fuente: elaboración propia, 2020

5.5.3.3 Diagrama de Contenedores - Análisis de Vulnerabilidad

El segundo nivel del modelo 4C diagrama de contenedores, vemos el detalle del Sistema de Análisis Continuo de vulnerabilidades –“SACV”, donde se evidencia cuatro tipos de contenedores: elípticos son los sistemas Core, rectangular los complementarios, hexagonales los de apoyo y la base de datos.

Los contenedores de forma de elipse (Core) son los que se encuentran alineados a los drivers funcionales, los cuales son críticos:

- Inventario: se encarga de la recolección de inventario de activos por medio de los sensores.
- Monitoreo continuo: se encarga de las pruebas de caja negra y caja blanca en conjunto con el sistema de sensores.
- Gestión de vulnerabilidades: encargado de orquestar todo el proceso y donde se encuentra el proceso automatizado de análisis continuo, los otros dos contenedores se comunican con este.
- Actualización de activos: es el encargado de la actualización del sistema operativo soportado en interacción con los otros contenedores Core.

Los contenedores de forma rectangular son los complementarios, aquellos encargados de mostrar alertas y eventos hacia la capa de usuarios, también es un utilitario que se encarga de la administración de usuarios, configuración de conexiones, gestión de log entre otros.

El contenedor hexagonal, será utilizado para garantizar el correcto funcionamiento del sistema, apoyando a diversos contenedores con el manejo de excepciones, con ello se logrará mantener la estabilidad y disponibilidad del sistema.

Contenedor	Descripción
Administrador	Administrador de la plataforma IaaS
Visualizador	Usuario con propiedades de solo visualización
Sistema de Análisis continuo de vulnerabilidades	Software System
Actualización de activos	Realiza el proceso de actualizar un activo de información
Alertas	Muestras alertas de nuevos activos detectados y vulnerabilidades nuevas detectadas
Dashboard	Panel de visualización interactivo, donde se muestran los activos críticos con las vulnerabilidades críticas detectadas
Database	Base de datos del sistema
Gestión de eventos	Proceso de gestión de eventos detectados
Gestión de excepciones	Gestión de errores
Gestión de vulnerabilidades	Proceso que recibe la lista de activos de información clasificada, solicita los diversos tipos de escaneo, generar alertas, eventos y carga la información para el dashboard
Inventario	Proceso de descubrimiento de activos de información, mediante las sondas desplegadas
Monitoreo Continuo	Proceso critico de análisis de vulnerabilidades ello se lleva de forma automática como parte del descubrimiento inicialmente como caja negra y cuando se suministre usuario y contraseña serán pruebas de caja blanca
Sonda	App que se encarga de escuchar el tráfico de la red para detectar y monitorear activos de información
SW-Cliente	Software instalado en equipos windows y linux
Utilitarios	Diversos utilitarios de gestión

5.5.3.4 Diagrama de Componentes

El tercer nivel del modelo 4C diagrama de componentes, aquí podemos observar más detalle de los contenedores, los cuales detallaremos a continuación.

Desde la parte inferior se evidencian los diferentes tipo de sensores, estos pueden ser de tipo virtual, hardware y para instancias cloud, garantizando la escalabilidad de la solución. Para garantizar una correcta performance de estos componentes de SW-Cliente, están formados por dos tipos de componentes, los cuales son uno de método pasivo y activo, configurables para obtener una adecuada performance de los activos de información. El método activo está

en constante búsqueda de vulnerabilidades ello puede generar consumo de CPU y RAM, con respecto al método pasivo que es a demanda de la configuración del usuario.

Los componente principales, son paquetes de software automatizados que van desde la búsqueda automática de activos de información, pasando por la clasificación automática, pruebas de caja negra, pruebas de caja blanca, el procesamiento de estas mismas en el componente Priorizar Automáticamente Vulnerabilidades y la remediación con la actualización automática de activos no críticos, mediante el Sw-Cliente.

Los componentes complementarios son los de apoyo al proceso automático donde el administrador interviene con parámetros personalizados, como búsquedas de activos personalizados, sus clasificación es manual.

El bajo acoplamiento de sus componentes asegura un buen diseño del software, dado que si llegara a fallar un proceso automático, esta se puede realizar de forma manual a demanda del usuario, hasta que se pueda solucionar el funcionamiento del componente.

Así mismo se tienen componentes de gestión de errores, de time out y sincronización los cuales aseguran la operatividad del sistema, así no lleguen a la capa de usuario, ello asegura la disponibilidad y mensajes correctos del sistema al usuarios dando consistencia al mismo.

Componente	Descripción
Actualizar equipos críticos	Proceso de actualizar equipos críticos programados
Actualizar equipos no críticos	Proceso automático de parchado de equipos que pueden actualizar
Programar Actualización de Activos	Calendario de actualización con fechas y horas para activos críticos
Gestionar alertas	Modificación de alertas solo usuarios con perfiles de administrador
Proceso de indicadores	Procesar indicadores y ciber-exposición
Visualizar Dashboard	Panel personalizable donde se muestran los activos de información con sus respectivas vulnerabilidades, permite navegabilidad
Database	Base de datos del sistema
Modificar Eventos	Permite modificar los eventos, como actualizaciones realizadas
Visualizar eventos	Muestra los eventos, desde el más actual hasta el más antiguo
Gestión de errores	Gestión de errores del sistema
Gestión de Time Out	Gestión de Time Out
Sincronización	Sincronización de conexiones.
Priorizar automáticamente Vulnerabilidades	Prioriza de acuerdo a las recomendaciones del fabricante
Priorizar manualmente Vulnerabilidades	Módulo de personalización de vulnerabilidades, se deberá realizar de acuerdo a las necesidades de la organización
Búsqueda manual con parámetros de usuario	Módulo de búsqueda de activos, donde el usuario ingresara parámetros de búsqueda como el segmentos de red y la ip
Búsqueda automática de Activos	Proceso Daemon que busca mediante escucha del puerto SPAN, nuevos activos de información
Clasificación de activos automática	Clasifica el activo de acuerdo a los parámetros detectados en el SYNC y ACK del entorno de red
Clasificación de activos manual	Módulo de clasificación manual de activos, donde el usuario modifica parámetros detectados
Escanear con prueba de caja Negra	Las pruebas de caja negra, es una técnica de pruebas de software en la cual la funcionalidad se verifica sin tomar en cuenta la estructura interna de código, detalles de implementación o escenarios de ejecución internos en el software
Escanear con prueba de caja Blanca	Las técnicas de caja blanca o estructural, que se basan en un minucioso examen de los detalles procedimentales del código a evaluar, por lo que es necesario conocer la lógica del

Componente	Descripción
	programa. A este tipo de técnicas se le conoce también como Técnicas de Caja Transparente o de Cristal.
Comp.Cache	Memoria intermedia del software, guarda datos para rápido acceso
Comp.logging	Librería de inicio de sesión al sistema.
Comp.Seguridad	Componente de seguridad del sistema, encriptación, certificados
Descargar Syslog	Proceso de envío y descarga de log
Gestionar usuarios	Módulo de gestión de usuario, para enlazar a un LDAP

5.5.3.5 Diagrama de Código

5.5.3.5.1 Diagrama de Código Buscar Automáticamente Activos

La finalidad de este proceso es la búsqueda y detección automática de activos de información por medio de la sonda, la sonda se comunica con el software SACV, si la sonda no se encuentra registrada se crea en el sistema y procede al envío de los activos detectados, seguidamente el proceso clasifica los activos de información de acuerdo a su base.

Figura 47. Diagrama de código – buscar automáticamente activos

Fuente: elaboración propia, 2020

Detalle de elementos de Buscar Automáticamente Activos:

1. Clase DetOrigSonda

Método	Descripción
CrearSonda	El sistema detecta una nueva sonda y el sistema la crea
BuscarSonda	Búsqueda de sonda ya creada
ActualizarSonda	Actualiza datos de la sonda como IP/Ubicación, nombre

2. Clase Activo

Método	Descripción
CrearActivo	El sistema crea un nuevo activo detectado por la sonda
BuscarActivo	Búsqueda de activo ya creado
ActualizarActivo	Actualiza datos del activo como IP/Ubicación, nombre, entre otros

3. Clase Sonda

Método	Descripción
BuscarActivo	Búsqueda de activos en la red mediante el puerto SPAN

4. Clase Clasificación de activos

Método	Descripción
ValidaClasificación	Valida la existencia de la clasificación en la base de datos

5. Componentes de seguridad

Componente	Descripción
ISync.Comp	Componentes de sincronización utilizado por la clase Activo, para asegurar del envío de datos desde la sonda
ISeg.Com	Validación de la sonda origen, mediante un intercambio de certificados de autenticación mutua

5.5.3.5.2 Diagrama de Código Búsqueda Manual de Activos

La finalidad de este proceso es la búsqueda manual de activos de información por medio de parámetros de usuarios, las cuales se envían a la sonda y el Sw-cliente, estos al detectar se comunican con el software SACV y procede al envío de los activos detectados, seguidamente el proceso clasifica el activo de información de acuerdo a su base.

Figura 48. Diagrama de código – búsqueda manual de activos
Fuente: elaboración propia, 2020

Detalle de elementos de Búsqueda Manual de Activos:

1. Interfaces

Interface	Descripción
IBusquedaActivos	Encargada de mostrar al usuario parámetros de búsqueda y ejecutar la búsqueda de activos de información

2. Clase BusquedaActivos

Método	Descripción
CrearBusqueda	Generar búsqueda de activos
ParametrosBusqueda	Detalle de la búsqueda personalizada del usuario
EjecutarBusqueda	Realiza el proceso de búsqueda, envía los parámetros de búsqueda a la sonda y al SW-Cliente

3. Clase Sonda

Método	Descripción
BuscarActivo	Búsqueda de activos en la red mediante el puerto SPAN

4. Clase Sw-Cliente

Método	Descripción
BuscarActivo	Búsqueda de activos en la red.

5. Clase Clasificación de activos

Método	Descripción
ValidaClasificación	Valida la existencia de la clasificación en la base de datos

6. Clase Activo

Método	Descripción
CrearActivo	El sistema crea un nuevo activo detectado por la sonda
BuscarActivo	Búsqueda de activo ya creado
ActualizarActivo	Actualiza datos del activo como IP/Ubicación, nombre, entre otros

7. Componentes de seguridad

Componente	Descripción
ISync.Comp	Componentes de sincronización utilizado por la clase Activo, para asegurar del envío de datos desde la sonda
ISeg.Com	Validación de la sonda origen, mediante un intercambio de certificados de autenticación mutua

5.5.3.5.3 Diagrama de Código Escaneo de caja negra

Proceso de escaneo de caja negra automático, después de detectar un activo de información y clasificarlo en el SACV, busca en la base si la vulnerabilidad ya ha sido detectada en anteriores procesos y procede a actualizarla, caso contrario buscar nuevas vulnerabilidades para el activo de información.

Figura 49. Diagrama de código – escaneo caja negra

Fuente: elaboración propia, 2020

Detalle de elementos de Escaneo de Caja Negra

1. Clase Activo

Método	Descripción
EscaneaActivo	El sistema procede a realizar el escaneo del activo en la búsqueda de vulnerabilidades
BuscarActivo	Búsqueda de activo ya creado
ListarActivo	Lista de activo para el escaneo

2. Clase ActivoVulnerabilidad

Método	Descripción
ComparaVulnerabilidad	Realiza la comparación de acuerdo a la versión de SO, firmware de activo, con el proceso anterior
CreaVulnerabilidad	Ingresa una nueva vulnerabilidad detectada de acuerdo al SO, firmware de activo enviada por la Sonda
ActualizaVulnerabilidadActivo	Actualiza la vulnerabilidad detectada o remediada
ListarVulnerabilidadActivo	Lista la vulnerabilidad del activo

3. Clase Sonda

Método	Descripción
EscaneoVulnerabilidad	Búsqueda de nuevas vulnerabilidades

4. Clase Clasificación de activos

Método	Descripción
ValidaClasificación	Valida la existencia de la clasificación en la base de datos
BusquedaClasificación	Busca la clasificación del activo

5. Clase VulnerabilidadesUpdate

Método	Descripción
DescargaVulnerabilidades	Descarga la lista de vulnerabilidades solicitada por la sonda
ActualizaVulnerabilidades	Actualiza la lista de vulnerabilidades

6. Clase SyncVulnerabilidades

Método	Descripción
ActualizaNuevas Vulnerabilidades	Envía nuevas vulnerabilidades detectadas

7. Componentes de seguridad

Componente	Descripción
ICache.Comp	Componentes de Cache que almacena la información de activos en escaneo activo, para garantizar su disponibilidad

5.5.3.5.4 Diagrama de Código Escaneo de caja blanca

Proceso de escaneo de caja blanca, puede ser automático o a demanda del usuario, después de ingresar las credenciales del activo de información se procede a realizar el escaneo con privilegios obteniendo mayor detalle de las vulnerabilidades.

Figura 50. Diagrama de código – escaneo caja blanca

Fuente: elaboración propia, 2020

Detalle de elementos de Escaneo de Caja Blanca

1. Interfaces

Interface	Descripción
IActivo	Encargada de mostrar al usuario parámetros de ingreso para realizar la búsqueda de caja blanca así como el método de Búsqueda de vulnerabilidades a demanda

2. Clase Activo

Método	Descripción
EscaneaActivo	El sistema procede a realizar el escaneo del activo en la búsqueda de vulnerabilidades
BuscarActivo	Búsqueda de activo ya creado
ListarActivo	Lista de activo para el escaneo
BuscarVulnerabilidad Activo	Proceso para usuario de búsqueda de vulnerabilidades de caja blanca a demanda

3. Clase ActivoVulnerabilidad

Método	Descripción
ComparaVulnerabilidad	Realiza la comparación de acuerdo a la versión de SO, firmware de activo, con el proceso anterior
CreaVulnerabilidad	Ingresa una nueva vulnerabilidad detectada de acuerdo al SO, firmware de activo enviada por la Sonda
ActualizaVulnerabilidadActivo	Actualiza la vulnerabilidad detectada o remediada
ListarVulnerabilidadActivo	Lista la vulnerabilidad del activo

4. Clase Sonda

Método	Descripción
EscaneoVulnerabilidad	Búsqueda de nuevas vulnerabilidades

5. Clase SW-Cliente

Método	Descripción
EscaneoVulnerabilidad	Búsqueda de nuevas vulnerabilidades

6. Clase UserPassword

Método	Descripción
BuscarCredenciales	Búsqueda de credenciales para al activo de información

7. Clase Clasificación de activos

Método	Descripción
ValidaClasificación	Valida la existencia de la clasificación en la base de datos
BusquedaClasificación	Busca la clasificación del activo

8. Clase VulnerabilidadesUpdate

Método	Descripción
DescargaVulnerabilidades	Descarga la lista de vulnerabilidades solicitada por la sonda
ActualizaVulnerabilidades	Actualiza la lista de vulnerabilidades

9. Clase SyncVulnerabilidades

Método	Descripción
ActualizaNuevasVulnerabilidades	Envía nuevas vulnerabilidades detectadas

10. Componentes de seguridad

Componente	Descripción
ICache.Comp	Componentes de Cache que almacena la información de activos en escaneo activo, para garantizar su disponibilidad
ILogging.Com	Componente de validación de inicio de sesión en el activo

5.5.3.5.5 Diagrama de Código Priorización de vulnerabilidades

El proceso de priorización de vulnerabilidades es el principal de todos, ya que procesa la información de los activos contra sus vulnerabilidades detectadas, con la clasificación de activos, así como la categorización del vendedor del software o sistema operativo, se puede lograr una priorización automática, o con la interface hacia el usuario se puede lograr un priorización manual, ello generará eventos, alertas e indicadores.

Figura 51. Diagrama de código – priorización de vulnerabilidades
Fuente: elaboración propia, 2020

Detalle de elementos de Priorización de vulnerabilidades

1. Interfaces

Interface	Descripción
IPriorización Vulnerabilidades	Encargada de mostrar al usuario la priorización de vulnerabilidades, realizada en forma automática por el sistema, también tendrá la opción de realizar la priorización de forma manual

2. Clase PriorizaciónVulnerabilidades

Método	Descripción
CreaPriorizaciónVulAuto	Crea proceso de búsqueda de vulnerabilidades automática
ActualizaPriorizaciónVulAuto	Actualiza el proceso de Priorización

3. Clase PriorizaciónVulnerabilidadesActivo

Método	Descripción
CreaPriorizaciónVulActivo	Crea Priorización de vulnerabilidad por activo
ActualizaPriorizaciónVulActivo	Actualiza Priorización de vulnerabilidad por activo
ProcesaPriorizaciónVulActivo	Proceso continuo de generación de alertas, eventos e indicadores de Priorización de vulnerabilidad por activo

4. Clase Alertas

Método	Descripción
CreaAlertaVulActivo	Crea alerta detectada, específicamente para el activo de información

5. Clase Eventos

Método	Descripción
CreaEventosVulActivo	Crea eventos de alertas no atendidas

6. Clase Indicadores

Método	Descripción
CreaIndicadoresVulActivo	Crea indicadores de atención de las alertas y la remediación de las mismas

7. Clase SyncVulnerabilidades

Método	Descripción
ActualizaNuevaVulnerabilidades	Actualiza nuevas vulnerabilidades
DescargaNuevaVulnerabilidades	Descarga nuevas vulnerabilidades desde el vendedor mediante el uso de internet

8. Clase Activo

Método	Descripción
EscaneoVulnerabilidad	El sistema procede a realizar el escaneo del activo en la búsqueda de vulnerabilidades

9. Clase ActivoVulnerabilidad

Método	Descripción
BuscarVulnerabilidadActivo	Proceso de búsqueda de Vulnerabilidades

10. Clase PriorizaciónVulnerabilidadesManuales

Método	Descripción
BuscarPriorizaciónManual	Búsqueda de priorizaciones hechas por el usuario para el tipo de vulnerabilidad detectada, esta sobre-escribirá en la priorización a la catalogada por el sistema

11. Clase Clasificación de activos

Método	Descripción
ValidaClasificación	Valida la existencia de la clasificación en la base de datos
BusquedaClasificación	Busca la clasificación del activo

12. Componentes de seguridad

Componente	Descripción
ILogging.Com	Componente de validación de inicio de sesión en el activo

5.5.3.5.6 Diagrama de Código Actualización de activos

Este componente tiene por finalidad que el usuario pueda generar un programa de actualización de activos no críticos, ello después de detectar sus vulnerabilidades, el proceso generara un Script que enviará al SW-Cliente, también el proceso descargará las actualizaciones que serán enviadas al SW-Cliente, para actualizarlas en los activos de información.

Figura 52. Diagrama de código – actualización de activo

Fuente: elaboración propia, 2020

Detalle de elementos de Actualización de activos:

1. Interfaces

Interface	Descripción
IProgramaciónActivos	Encargada de mostrar los controles necesarios para actualizar un activo de información crítico y no crítico

2. Clase ProgramaActualización

Método	Descripción
CreaPrograma	Crea programa de actualización de activos
ActualizaPrograma	Actualiza el programa de actualización de activos
GeneraPrograma	Genera un programa automático de actualización de activos

3. Clase VulnerabilidadesActualizar

Método	Descripción
ListarVulnerabilidadesPorActivo	Genera una lista de vulnerabilidades por activo a actualizar

4. Clase ActualizaciónActivosNoCriticos

Método	Descripción
GenerarScripDeActualización	Genera un script de acuerdo a cada SO y firmware con la lista de vulnerabilidades a actualizar.

5. Clase DescargasDeActualización

Método	Descripción
DescargaActualización	Con la lista de vulnerabilidades a actualizar descarga las actualizaciones de acuerdo al SO y firmware a actualizar

6. Clase PriorizaciónVulnerabilidadesActivo

Método	Descripción
BuscaPriorizaciónVulActivo	Buscar la lista de vulnerabilidades por activo que no han sido remediadas

7. Clase Eventos

Método	Descripción
CreaEventosVulActivo	Crea de alertas de actualización

8. Clase Activo

Método	Descripción
ListarActivos	Lista activos de información

9. Clase Clasificación de activos

Método	Descripción
ValidaClasificación	Valida la existencia de la clasificación en la base de datos
BusquedaClasificación	Busca la clasificación del activo

10. Clase SW-Cliente

Método	Descripción
EjecutaScrip	Ejecuta script con las actualizaciones para la vulnerabilidad del activo de información programado

6 GESTIÓN DEL PROYECTO

6.1 Descripción del Proyecto

La empresa Mibanco debe realizar todos los meses el proceso de monitoreo continuo de vulnerabilidades a exigencia del corporativo por estar alineado a las sentencias de la FFIEC, este proceso a la fecha es un problema para la empresa porque es realizado manualmente. Así mismo el proceso es tomado por la empresa como una estrategia interna para mantener seguros los activos de información, para la ejecución del proceso se deben tener en cuenta los siguientes pasos:

- El correcto inventario de activos de la información con su respectiva criticidad.
- El descubrimiento de vulnerabilidades para cada activo del inventario.
- La criticidad de cada vulnerabilidad detectada.
- La remediación y/o el plan de acción.

Como se indicó en el párrafo anterior, varios de los pasos listados se realizan de manera manual, tomando muchas horas hombre en completar el proceso, y la parte del proceso que toma la mayor cantidad de tiempo es el descubrimiento, ya que en este paso se tiene que realizar activo por activo, y cuando se llega al paso de remediación el activo ya tiene nuevas brechas reportadas por el fabricante.

La propuesta de solución que proponemos en el presente proyecto, es automatizar varios de los pasos del proceso en estudio, de esta manera se obtendrá las siguientes mejoras:

- Contar con un inventario automatizado y en línea.
- Descubrimiento de vulnerabilidades de manera automática.
- Priorización de los activos para su remediación posterior.
- Remediación inmediata o programada al descubrimiento de la vulnerabilidad.
- Dashboard con información importante (reportes dinámicos de alto nivel) para la Gerencia de Operaciones de Seguridad Tecnológica.

El acta del proyecto se encuentra en el Anexo N° 01 Project Chárter.

6.2 Alcance del Proyecto Tesis

6.2.1 Desarrollo de la Propuesta

DESCRIPCIÓN DEL PRODUCTO DEL PROYECTO	
El alcance del proyecto será desarrollar un diseño para la propuesta de implementación de un software tipo IaaS que apoye en la mejora sustancial al proceso de monitoreo continuo de vulnerabilidades para la empresa Mibanco, basado en los estándares de la empresa, para así descubrir, detectar, responder y prevenir las brechas de seguridad de los activos de información con mayor eficiencia.	
DESCRIPCIÓN DE LOS ENTREGABLES DEL PROYECTO	
ENTREGABLE	DESCRIPCIÓN
Project Chárter	Definición y alcance del proyecto a alto nivel
Cronograma	Cronograma de análisis y diseño del proceso de mejora
Análisis de arquitectura empresarial Zachman	Análisis de Zachman nivel I
Análisis de requerimientos	Recopilación de requerimientos funcionales y no funcionales (lista de entregables)
Diagramas de caso de uso	Especificación de los casos de uso de los drivers funcionales
To-Be del proceso de monitoreo de vulnerabilidades	Diagrama BPM de mejora del proceso de mejora
Diagrama de arquitectura TO-BE de RED	Arquitectura de red donde se desplegará la herramienta
Diagrama de arquitectura Layered	Diagrama de capas de interacción de la solución propuesta

Diagrama de arquitectura usando C4	Diagrama de cuatro capas de la solución propuesta.
CRITERIOS DE ACEPTACIÓN DE ENTREGABLES	
Análisis de arquitectura empresarial Zachman	Juicio de expertos en arquitectura empresarial, el documento de tesis debe contener el análisis de Zachman Nivel I y II.
Análisis de requerimientos, Diagramas de caso de uso, To-Be del proceso de mejora, Diagrama de arquitectura TO-BE de RED, Diagrama de arquitectura Layered, Diagrama de arquitectura C4	Juicio de expertos con conocimiento en arquitectura de software. El documento de tesis debe contener todos los diagramas, requeridos.

6.2.2 Contexto del Proyecto

EXCLUSIONES DEL PROYECTO
El proyecto no considera entregable de desarrollo de software, <i>no se incluye la fase de implementación del software.</i>
RESTRICCIONES
<ul style="list-style-type: none"> • Políticas internas de Mibanco • Restricciones presupuestales • Tiempo de duración de desarrollo del PAP
ASUNCIONES
Afectación al proyecto por extensión de Covid-19

6.2.3 Estructura de Desglose del Trabajo – EDT

Figura 53. Diagrama de la estructura de desglose de trabajo

Fuente: elaboración propia, 2020

6.2.4 Diccionario de la EDT

PAQUETE DE TRABAJO	DICCIONARIO
Nombre:	Fase Análisis
Código:	1.1
Objetivo:	Análisis de la situación actual
Descripción	Analizar la arquitectura desde el punto de vista empresarial hasta el proceso y sus requerimientos de mejora
Responsables	<p>Responsable: Jefe de Proyecto</p> <p>Participa:</p> <p>Revisa: Líder Técnico Arquitectónico</p> <p>Aprueba: Experto Empresarial</p> <p>Da información: Área de TISO-Mibanco</p>
Fechas programadas	<p>Fecha de inicio: 22/05/2020</p> <p>Fecha de fin: 18/06/2020</p> <p>Hito: Aprobación Arquitectura empresarial Zachman</p> <p>Hito: Análisis de requerimientos</p>
Criterios de aceptación	<p>Stakeholder que acepta: Experto Empresarial</p> <p>Forma que se aceptara: Reunión del equipo de proyecto</p> <p>Requisitos que deben cumplirse: Debe entregarse documento con los entregables de la fase de análisis completados, Arquitectura empresarial, análisis del proceso objetivo, gestión de requerimientos.</p>

PAQUETE DE TRABAJO	DICCIONARIO
Supuestos	Recibir toda la información necesaria para elaborar el análisis de la arquitectura empresarial, aprobación del proyecto por parte de Mibanco
Riesgos	Que la fase de análisis sea aprobada por el experto
Recursos asignados y costos	Personal: Jefe de proyectos
Dependencias	Antes del paquete de trabajo (pdt) Después del pdt: Descripción de arquitectura empresarial

PAQUETE DE TRABAJO	DICCIONARIO
Nombre:	Análisis de arquitectura empresarial
Código:	1.1.1
Objetivo:	Análisis de la situación actual
Descripción	Analizar la arquitectura empresarial con el framework de Zachman
Responsables	Responsable: Jefe de Proyecto Participa: Revisa: Líder Técnico Arquitectónico Aprueba: Experto Empresarial Da información: Área de TISO-Mibanco
Fechas programadas	Fecha de inicio: 22/05/2020 Fecha de fin: 26/05/2020 Hito: Aprobación Arquitectura empresarial Zachman

PAQUETE DE TRABAJO	DICCIONARIO
Criterios de aceptación	<p>Stakeholder que acepta: Experto Empresarial</p> <p>Forma que se aceptara: Reunión del equipo de proyecto</p> <p>Requisitos que deben cumplirse: Documento que debe contar con la arquitectura nivel 1 y 2 Zachman.</p>
Supuestos	Recibir toda la información necesaria para elaborar el análisis de la arquitectura empresarial.
Riesgos	Que la arquitectura no sea aprobada por el experto
Recursos asignados y costos	Personal: Jefe de proyectos
Dependencias	<p>Antes del pdt :Fase Análisis</p> <p>Después del pdt: Descripción del proceso objetivo AS-IS</p>

PAQUETE DE TRABAJO	DICCIONARIO
Nombre:	Análisis del Proceso Objetivo
Código:	1.1.2
Objetivo:	Análisis del proceso objetivo
Descripción	Analizar el proceso del TISO con respecto al proceso de Análisis continuo de vulnerabilidades
Responsables	<p>Responsable: Jefe de Proyecto</p> <p>Participa:</p> <p>Revisa: Líder Técnico Arquitectónico</p> <p>Aprueba: Experto Empresarial</p>

PAQUETE DE TRABAJO	DICCIONARIO
	Da información: Área de TISO-Mibanco
Fechas programadas	Fecha de inicio: 27/05/2020 Fecha de fin: 29/05/2020
Criterios de aceptación	Stakeholder que acepta: Experto Empresarial Forma que se aceptara: Reunión del equipo de proyecto donde se expondrá. Requisitos que deben cumplirse: Deberá tener el documento con el proceso AS-IS el mismo debe contar con BPMN y detalle del proceso.
Supuestos	Recibir el proceso del área TISO
Riesgos	-
Recursos asignados y costos	Personal: Jefe de proyectos
Dependencias	Antes del pdt :Descripción de la arquitectura empresarial Después del pdt: Requerimientos funcionales

PAQUETE DE TRABAJO	DICCIONARIO
Nombre:	Especificaciones de reglas de negocio.
Código:	1.1.3
Objetivo:	Recopilar las reglas del negocio.
Descripción	Recopilar normas, políticas, restricciones presentes en la organización
Responsables	Responsable: Jefe de Proyecto

PAQUETE DE TRABAJO	DICCIONARIO
	Participa: Revisa: Líder Técnico Arquitectónico Aprueba: Experto en Arquitectura Da información: Área de TISO-Mibanco
Fechas programadas	Fecha de inicio:01/06/2020 Fecha de fin: 04/06/2020
Criterios de aceptación	Stakeholder que acepta: Experto en Arquitectura Forma que se aceptara: Reunión del equipo de proyecto Requisitos que deben cumplirse: Presentara documento con las reglas de negocio codificadas.
Supuestos	Recibir las normas, políticas de la empresa
Riesgos	-
Recursos asignados y costos	Personal: Jefe de proyectos
Dependencias	Antes del pdt :Descripción del Proceso AS-IS Después del pdt: Requerimientos No funcionales

PAQUETE DE TRABAJO	DICCIONARIO
Nombre:	Requerimientos funcionales
Código:	1.1.4
Objetivo:	Levantamiento de requerimientos que se puedan automatizar del proceso del TISO

PAQUETE DE TRABAJO	DICCIONARIO
Descripción	Analizar los requerimientos del TISO sobre el análisis continuo de vulnerabilidades
Responsables	Responsable: Jefe de Proyecto Participa: Revisa: Líder Técnico Arquitectónico Aprueba: Experto en Arquitectura Da información: Área de TISO-Mibanco
Fechas programadas	Fecha de inicio:05/06/2020 Fecha de fin: 11/06/2020
Criterios de aceptación	Stakeholder que acepta: Experto en Arquitectura Forma que se aceptara: Reunión del equipo de proyecto Requisitos que deben cumplirse: Presentara documento donde se expondrá la tabla de requerimientos funcionales debidamente codificada
Supuestos	Recibir los requerimientos de TISO
Riesgos	-
Recursos asignados y costos	Personal: Jefe de proyectos
Dependencias	Antes del pdt :Descripción del Proceso AS-IS Después del pdt: Requerimientos No funcionales

PAQUETE DE TRABAJO	DICCIONARIO
Nombre:	Requerimientos no funcionales

PAQUETE DE TRABAJO	DICCIONARIO
Código:	1.1.5
Objetivo:	Levantamiento de requerimientos no funcionales del proceso del TISO
Descripción	Analizar los requerimientos no funcionales del TISO sobre el análisis continuo de vulnerabilidades
Responsables	Responsable: Jefe de Proyecto Participa: Revisa: Líder Técnico Arquitectónico Aprueba: Experto en Arquitectura Da información: Área de TISO-Mibanco
Fechas programadas	Fecha de inicio: 12/06/2020 Fecha de fin: 12/06/2020
Criterios de aceptación	Stakeholder que acepta: Experto en Arquitectura Forma que se aceptara: Reunión del equipo de proyecto. Requisitos que deben cumplirse: Presentara documento donde se expondrá la tabla de requerimientos no funcionales debidamente codificada
Supuestos	Recibir los requerimientos de TISO
Riesgos	-
Recursos asignados y costos	Personal: Jefe de proyectos
Dependencias	Antes del pdt : Requerimientos funcionales

PAQUETE DE TRABAJO	DICCIONARIO
	Después del pdt: Especificación de atributos de calidad

PAQUETE DE TRABAJO	DICCIONARIO
Nombre:	Especificación de atributos de calidad
Código:	1.1.6
Objetivo:	Especificación de atributos de calidad
Descripción	Analizar los atributos de calidad del software los cuales debería cumplir
Responsables	Responsable: Jefe de Proyecto Participa: Revisa: Líder Técnico Arquitectónico Aprueba: Experto en Arquitectura Da información: Área de TISO-Mibanco
Fechas programadas	Fecha de inicio:15/06/2020 Fecha de fin: 16/06/2020
Criterios de aceptación	Stakeholder que acepta: Experto en Arquitectura Forma que se aceptara: Reunión del equipo de proyecto donde se expondrá. Requisitos que deben cumplirse: Presentara documento con los escenarios de atributos de calidad y la matriz de Trazabilidad entre los Requerimientos No Funcionales vs Atributos de Calidad.
Supuestos	Recibir los requerimientos de TISO

PAQUETE DE TRABAJO	DICCIONARIO
Riesgos	-
Recursos asignados y costos	Personal: Jefe de proyectos
Dependencias	Antes del pdt : Requerimientos no funcionales Después del pdt: Especificación de driver arquitectónicos

PAQUETE DE TRABAJO	DICCIONARIO
Nombre:	Especificación de driver arquitectónicos
Código:	1.1.7
Objetivo:	Especificación de driver arquitectónicos
Descripción	Seleccionar los requerimientos funcionales más relevantes y necesarios del proceso, para que funcionen como pilares de la fase de diseño.
Responsables	Responsable: Jefe de Proyecto Participa: Revisa: Líder Técnico Arquitectónico Aprueba: Experto en Arquitectura Da información: Área de TISO-Mibanco
Fechas programadas	Fecha de inicio: 17/06/2020 Fecha de fin: 18/06/2020
Criterios de aceptación	Stakeholder que acepta: Experto en Arquitectura Forma que se aceptara: Reunión del equipo de proyecto donde se expondrá.

PAQUETE DE TRABAJO	DICCIONARIO
	Requisitos que deben cumplirse: Presentara documento con driver arquitectónicos, mínimo deberá contener 5 drivers debidamente codificados, Matrices de Trazabilidad de Requerimientos Funcionales vs Drivers Funcionales, Drivers Funcionales vs Tácticas, Drivers de Atributos de Calidad vs Tácticas, Drivers Arquitectónicos vs Casos de Uso de Sistema.
Supuestos	-
Riesgos	-
Recursos asignados y costos	Personal: Jefe de proyectos
Dependencias	Antes del pdt : Requerimientos no funcionales Después del pdt:

PAQUETE DE TRABAJO	DICCIONARIO
Nombre:	Fase Diseño
Código:	1.2
Objetivo:	Desarrollo del diseño propuesto
Descripción	Realizar un diseño funcional y técnico de la propuesta
Responsables	Responsable: Jefe de Proyecto Participa: Revisa: Líder Técnico Arquitectónico Aprueba: Experto en Arquitectura Da información: Área de TISO-Mibanco
Fechas programadas	Fecha de inicio:16/06/2020

PAQUETE DE TRABAJO	DICCIONARIO
	<p>Fecha de fin: 29/07/2020</p> <p>Hito: Diagrama de casos de uso</p> <p>Hito: Diagramas de arquitectura</p>
Criterios de aceptación	<p>Stakeholder que acepta: Experto en Arquitectura</p> <p>Forma que se aceptara: Reunión del equipo de proyecto donde se expondrá el diseño.</p> <p>Requisitos que deben cumplirse: Documento con diagramas de casos de uso y diagramas de arquitectura de la solución.</p>
Supuestos	La fase de análisis aprobada
Riesgos	Cambio de alcance del proyecto, la no identificación de todos los entregables del diseño.
Recursos asignados y costos	Personal: Jefe de proyectos, Arquitecto de TI
Dependencias	<p>Antes pdt:</p> <p>Después del pdt: Descripción del proceso To-Be</p>

PAQUETE DE TRABAJO	DICCIONARIO
Nombre:	Caracterización del Proceso Objetivo To-Be
Código:	1.2.1
Objetivo:	Mejora del proceso actual
Descripción	Realizar mejoras al proceso actual y realizar un proceso propuesto con mejoras de automatización
Responsables	Responsable: Líder Técnico Arquitectónico

PAQUETE DE TRABAJO	DICCIONARIO
	Participa: Revisa: Jefe de Proyecto Aprueba: Experto en Arquitectura Da información: Área de TISO-Mibanco
Fechas programadas	Fecha de inicio: 16/06/2020 Fecha de fin: 17/06/2020
Criterios de aceptación	Stakeholder que acepta: Experto en Arquitectura Forma que se aceptara: Reunión del equipo de proyecto donde se expondrá el proceso. Requisitos que deben cumplirse: Documento con el BMNP mejorado y evidenciar las mejoras.
Supuestos	Tener el proceso AS-IS
Riesgos	-
Recursos asignados y costos	Personal: Jefe de proyectos
Dependencias	Antes del pdt : Después del pdt: Definición de casos de uso

PAQUETE DE TRABAJO	DICCIONARIO
Nombre:	Definición de casos de uso
Código:	1.2.2
Objetivo:	Especificar los casos de uso del sistema

PAQUETE DE TRABAJO	DICCIONARIO
Descripción	Realizar gráficos de los casos de uso del proceso, donde se reflejen los requerimientos funcionales
Responsables	Responsable: Líder Técnico Arquitectónico Participa: Revisa: Jefe de Proyecto Aprueba: Experto en Arquitectura Da información: Área de TISO-Mibanco
Fechas programadas	Fecha de inicio: 18/06/2020 Fecha de fin: 22/06/2020
Criterios de aceptación	Stakeholder que acepta: Experto en Arquitectura Forma que se aceptara: Reunión del equipo de proyecto. Requisitos que deben cumplirse: Documento con los paquetes de casos de uso, de acuerdo a los requerimientos funcionales, diagramas de los casos de uso.
Supuestos	Tener los requerimientos funcionales y los drivers arquitectónicos definidos y aprobados
Riesgos	-
Recursos asignados y costos	Personal: Jefe de proyectos, Analista funcional
Dependencias	Antes del pdt : Descripción del proceso To-Be, Especificación de drivers arquitectónicos Después del pdt: Diagrama Layered

PAQUETE DE TRABAJO	DICCIONARIO
Nombre:	Especificación del Diagrama Layered
Código:	1.2.3
Objetivo:	Esquematizar el proceso del sistema, por capas
Descripción	Realizar un diagrama donde se explique la interacción de las diversas capas del sistema
Responsables	<p>Responsable: Líder Técnico Arquitectónico</p> <p>Participa:</p> <p>Revisa: Jefe de Proyecto</p> <p>Aprueba: Experto en Arquitectura</p> <p>Da información: Área de TISO-Mibanco</p>
Fechas programadas	<p>Fecha de inicio: 24/06/2020</p> <p>Fecha de fin: 25/06/2020</p>
Criterios de aceptación	<p>Stakeholder que acepta: Experto en Arquitectura</p> <p>Forma que se aceptara: Reunión del equipo de proyecto.</p> <p>Requisitos que deben cumplirse: Documento con el diagrama de requerimientos, con relación a los módulos del sistema, estratificado en diversas capas para su mejor entendimiento.</p>
Supuestos	Tener la definición de los casos de uso verificada
Riesgos	-
Recursos asignados y costos	Personal: Jefe de proyectos, Analista funcional
Dependencias	Antes del pdt : definición de los casos de uso

PAQUETE DE TRABAJO	DICCIONARIO
	Después del pdt: Diagrama C4

PAQUETE DE TRABAJO	DICCIONARIO
Nombre:	Especificación del Diagrama C4
Código:	1.2.4
Objetivo:	Esquematizar el proceso por niveles
Descripción	Detallar los contenedores y componentes del sistema
Responsables	<p>Responsable: Líder Técnico Arquitectónico</p> <p>Participa:</p> <p>Revisa: Jefe de Proyecto</p> <p>Aprueba: Experto en Arquitectura</p> <p>Da información: Área de TISO-Mibanco</p>
Fechas programadas	<p>Fecha de inicio: 25/06/2020</p> <p>Fecha de fin: 01/07/2020</p>
Criterios de aceptación	<p>Stakeholder que acepta: Experto en Arquitectura</p> <p>Forma que se aceptara: Reunión del equipo de proyecto.</p> <p>Requisitos que deben cumplirse: Documento con el diagrama C4 y sus niveles: contexto, contenedor, componente y código (Solo de los procesos Core), con la especificación de cada componente de los diagramas.</p>
Supuestos	-

PAQUETE DE TRABAJO	DICCIONARIO
Riesgos	-
Recursos asignados y costos	Personal: Jefe de proyectos, Analista funcional
Dependencias	Antes del pdt : Diagrama Layered Después del pdt: Matrices de trazabilidad

PAQUETE DE TRABAJO	DICCIONARIO
Nombre:	Matrices de trazabilidad
Código:	1.2.5
Objetivo:	Realizar la trazabilidad de la solución
Descripción	Detallar la trazabilidad desde los requerimientos, casos de uso versus la solución del sistema
Responsables	Responsable: Líder Técnico Arquitectónico Participa: Revisa: Jefe de Proyecto Aprueba: Experto en Arquitectura Da información: Área de TISO-Mibanco
Fechas programadas	Fecha de inicio: 01/07/2020 Fecha de fin: 06/07/2020
Criterios de aceptación	Stakeholder que acepta: Experto en Arquitectura Forma que se aceptara: Reunión del equipo de proyecto. Requisitos que deben cumplirse: Documento con la

PAQUETE DE TRABAJO	DICCIONARIO
	Matriz de Trazabilidad de Requerimientos Funcionales vs Casos de Uso de Sistema
Supuestos	-
Riesgos	-
Recursos asignados y costos	Personal: Jefe de proyectos, Analista funcional
Dependencias	Antes del pdt : Diagrama C4 Después del pdt:

PAQUETE DE TRABAJO	DICCIONARIO
Nombre:	Especificación de Mockups
Código:	1.2.6
Objetivo:	Realizar la especificación de los casos de uso del sistema, con los respectivos Mockups
Descripción	Detallar la especificación de los casos de uso del sistema solo de los que están alineados a los drivers funcionales, con los respectivos Mockups.
Responsables	Responsable: Líder Técnico Arquitectónico Participa: Revisa: Jefe de Proyecto Aprueba: Experto en Arquitectura Da información: Área de TISO-Mibanco
Fechas programadas	Fecha de inicio: 02/07/2020 Fecha de fin: 15/07/2020

PAQUETE DE TRABAJO	DICCIONARIO
Criterios de aceptación	<p>Stakeholder que acepta: Experto en Arquitectura</p> <p>Forma que se aceptara: Reunión del equipo de proyecto.</p> <p>Requisitos que deben cumplirse: Documento con la especificación de los casos de uso drivers del sistema, con los respectivo Mockups.</p>
Supuestos	-
Riesgos	-
Recursos asignados y costos	Personal: Jefe de proyectos, Analista funcional
Dependencias	<p>Antes del pdt : Diagrama C4</p> <p>Después del pdt:</p>

PAQUETE DE TRABAJO	DICCIONARIO
Nombre:	Gestión del proyecto
Código:	1.3
Objetivo:	Gestionar el proyecto
Descripción	Seguimiento y gestión de la salud del proyecto
Responsables	<p>Responsable PM: Jefe de Proyecto</p> <p>Participa: Líder Técnico Arquitectónico</p> <p>Revisa:</p> <p>Aprueba: Experto en Gestión de Proyectos</p> <p>Da información: Project Manager Mibanco</p>
Fechas programadas	Fecha de inicio:08/05/2020

PAQUETE DE TRABAJO	DICCIONARIO
	<p>Fecha de fin: 31/07/2020</p> <p>Hito: Aprobación Plan de proyecto</p> <p>Hito: Cronograma</p> <p>Hito: Entrega de la EDT</p>
Criterios de aceptación	<p>Stakeholder que acepta: Experto en Gestión de Proyectos</p> <p>Forma que se aceptara: Reunión del equipo de proyecto y envío del documento.</p> <p>Requisitos que deben cumplirse: Documento con Acta de proyecto, Plan de Proyecto, Análisis de riesgos.</p>
Supuestos	El Sponsor brindará la información necesaria para elaborar el proyecto
Riesgos	Que el Acta de proyecto no sea aprobado
Recursos asignados y costos	Personal: Sponsor, PM
Dependencias	<p>Antes del pdt:</p> <p>Después del pdt: Acta de proyecto</p>

PAQUETE DE TRABAJO	DICCIONARIO
Nombre:	Acta de Proyecto
Código:	1.3.1
Objetivo:	Conocer el proyecto
Descripción	Mostrar el proceso del proyecto a alto nivel.
Responsables	Responsable PM: Jefe de Proyecto

PAQUETE DE TRABAJO	DICCIONARIO
	Participa: Revisa: Experto en Gestión de Proyectos Aprueba: Patrocinador Da información: Project Manager Mibanco
Fechas programadas	Fecha de inicio: 08/05/2020 Fecha de fin: 19/05/2020 Hito: Aprobación de acta de proyecto
Criterios de aceptación	Stakeholder que acepta: PM Forma que se aceptara: Reunión del equipo de proyecto y envío del documento. Requisitos que deben cumplirse: Documento con Acta de proyecto y envío del documento para aprobación de PM.
Supuestos	El Sponsor brindará la información necesaria para elaborar el Acta de proyecto El Sponsor conoce el objetivo del proyecto.
Riesgos	Que el Acta de proyecto no sea aprobado. El alcance no se define claramente los criterios necesarios para la planificación y desarrollo del proyecto.
Recursos asignados y costos	Personal: Sponsor, PM
Dependencias	Antes del pdt: Después del pdt: Plan de Proyecto

PAQUETE DE TRABAJO	DICCIONARIO
Nombre:	Plan de Proyecto
Código:	1.3.2
Objetivo:	Planificar el proyecto.
Descripción	Documento formalmente aprobado que define cómo se ejecuta, supervisa y controla el proyecto.
Responsables	<p>Responsable PM: Jefe de Proyecto</p> <p>Participa:</p> <p>Revisa:</p> <p>Aprueba: Experto en Gestión de Proyectos</p> <p>Da información: Project Manager Mibanco</p>
Fechas programadas	<p>Fecha de inicio: 20/05/2020</p> <p>Fecha de fin: 03/06/2020</p> <p>Hito: Aprobación Plan de proyecto</p> <p>Hito: Cronograma</p>
Criterios de aceptación	<p>Stakeholder que acepta: Experto en Gestión de Proyectos</p> <p>Forma que se aceptara: Reunión del equipo de proyecto.</p> <p>Requisitos que deben cumplirse: El plan debe ser factible.</p>
Supuestos	<p>El Sponsor brindará la información necesaria para elaborar la planificación</p> <p>El Alcance ha sido aprobado.</p>

PAQUETE DE TRABAJO	DICCIONARIO
Riesgos	Cambio de alcance del proyecto. La no identificación de los entregables necesarios para elaborar el proyecto.
Recursos asignados y costos	Personal: Sponsor, PM
Dependencias	Antes del pdt: Acta de proyecto Después del pdt: Análisis de Riesgos

PAQUETE DE TRABAJO	DICCIONARIO
Nombre:	Análisis de Riesgos
Código:	1.3.3
Objetivo:	Identificar y analizar los riesgos del proyecto
Descripción	Tener mapeado los riesgos que se pueda tener durante el desarrollo del proyecto, así como los
Responsables	Responsable PM: Jefe de Proyecto Participa: Revisa: Aprueba: Experto en Gestión de Proyectos Da información: Project Manager Mibanco
Fechas programadas	Fecha de inicio:04/06/2020 Fecha de fin: 08/06/2020 Hito: Aprobación Plan de riesgos
Criterios de aceptación	Stakeholder que acepta: Experto en Gestión de Proyectos

PAQUETE DE TRABAJO	DICCIONARIO
	<p>Forma que se aceptara: Reunión del equipo de proyecto.</p> <p>Requisitos que deben cumplirse: Riesgos identificados y plan de respuesta completados.</p>
Supuestos	El PM debe detallar los riesgos que se puede presentar en el proyecto
Riesgos	Se presente un riesgo que no fue identificado
Recursos asignados y costos	Personal: Sponsor, PM
Dependencias	<p>Antes del pdt: Plan de Proyecto</p> <p>Después del pdt: Cierre</p>

PAQUETE DE TRABAJO	DICCIONARIO
Nombre:	Cierre
Código:	1.3.4
Objetivo:	Cerrar el proyecto
Descripción	Dar por terminado el proyecto validando todos los entregables solicitados
Responsables	<p>Responsable PM: Jefe de Proyecto</p> <p>Participa:</p> <p>Revisa: Experto en Gestión de Proyectos</p> <p>Aprueba: Patrocinador</p> <p>Da información: Project Manager Mibanco</p>
Fechas programadas	Fecha de inicio:31/07/2020

PAQUETE DE TRABAJO	DICCIONARIO
	<p>Fecha de fin: 31/07/2020</p> <p>Hito: Aprobación el cierre del proyecto</p>
Criterios de aceptación	<p>Stakeholder que acepta: Experto en Gestión de Proyectos</p> <p>Forma que se aceptara: Reunión del equipo de proyecto.</p> <p>Requisitos que deben cumplirse: Documento final con la aprobación por los tres expertos.</p>
Supuestos	
Riesgos	Que no se cierre el proyecto
Recursos asignados y costos	Personal: Sponsor, PM
Dependencias	<p>Antes del pdt: Análisis de Riesgos</p> <p>Después del pdt:</p>

6.3 Organización del proyecto tesis

6.3.1 Organigrama

Figura 54. Organigrama del proyecto
Fuente: elaboración propia, 2020

6.3.2 Matriz de Asignación de Responsabilidades

Tabla 11 Matriz de Asignación de Responsabilidades
Fuente: elaboración propia

MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES						
ENTREGABLE	ROLES					
	<i>PA</i>	<i>JP</i>	<i>LT</i>	<i>EE</i>	<i>EA</i>	<i>EP</i>
1. <i>Gestión del Proyecto</i>						
a. <i>Acta de Proyecto</i>	A	RP				V
b. <i>Plan de Proyecto</i>		RV	P			A
c. <i>Análisis de Riesgos</i>		RV	P			A
d. <i>Acta de Cierre</i>	A	RP				V
2. <i>Fase Análisis</i>						
a. <i>Análisis de Arquitectura Empresarial</i>		R	VP	A		
b. <i>Análisis del Proceso Objetivo</i>		R	VP	A		
c. <i>Especificaciones de Reglas de Negocio</i>		R	VP		A	
d. <i>Requerimientos Funcionales</i>		R	VP		A	
e. <i>Requerimientos No Funcionales</i>		R	VP		A	

MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES						
f. Especificación de Atributos de Calidad		R	VP		A	
g. Especificación de Driver Arquitectónicos		R	VP		A	
3. Fase Diseño						
a. Caracterización del Proceso Objetivo To-Be		R	VP		A	
b. Definición de Casos de Uso		R	VP		A	
c. Especificación del Diagrama Layered		R	VP		A	
d. Especificación del Diagrama C4		R	VP		A	
e. Matrices de Trazabilidad		R	VP		A	
f. Especificación de Mockups		R	VP		A	
<p>R: Responsable de entrega A: Aprueba P: Participa V: Verifica</p> <p>PA: Patrocinador JP: Jefe de Proyecto LT: Líder Técnico Arquitectónico EE: Experto Empresarial EA: Experto en Arquitectura EP: Experto en Gestión de Proyectos</p>						

6.3.3 Descripción de Roles

NOMBRE DEL ROL	PATROCINADOR
OBJETIVOS DEL ROL:	
Proporcionar apoyo y recursos para el proyecto, toma las decisiones importantes y comunicar a la organización la importancia del proyecto.	
RESPONSABILIDADES:	
<ul style="list-style-type: none"> Aprobar el Acta de Constitución Aprobar el cierre del proyecto. 	
FUNCIONES:	
<ul style="list-style-type: none"> Obtener el presupuesto para el proyecto Defender el proyecto 	
NIVELES DE AUTORIDAD:	
Debe contar con gran autoridad para poder tomar decisiones importantes para el desarrollo del proyecto en la organización	
Reporta a:	Gerencia
REQUISITOS DEL ROL:	

CONOCIMIENTOS:	Conocer el negocio funcionalmente y la tecnologías de información
HABILIDADES:	Debe ser un líder y transmitir confianza y credibilidad en el proyecto
EXPERIENCIA:	Experiencia en tecnologías de información y capacidad de negociación y comunicación
OTROS:	

NOMBRE DEL ROL	JEFE DE PROYECTO
OBJETIVOS DEL ROL:	
Encargado de planificar, ejecutar y monitorizar el proyecto, así como tomar las decisiones de los requerimientos de cada situación que se presente en el proyecto.	
RESPONSABILIDADES:	
<ul style="list-style-type: none"> • Gestionar el buen desarrollo del proyecto desde la fase de inicio hasta el cierre • Entregar todos los entregables resultado de la fase de análisis del proyecto • Entregar todos los entregables resultado de la fase del diseño del proyecto 	
FUNCIONES:	
<ul style="list-style-type: none"> • Planificar el proyecto • Liderar el equipo del proyecto • Dirigir y coordinar con los recursos disponibles • Identificar problemas y proponer soluciones • Responder por los resultados • Gestionar las restricciones del proyecto en tiempo, alcance y costo 	
NIVELES DE AUTORIDAD:	
Autoridad para poder tomar decisiones importantes en la gestión del proyecto	
Reporta a:	Patrocinador

REQUISITOS DEL ROL:	
CONOCIMIENTOS:	Conocer de tecnologías de información y de la gestión de proyectos
HABILIDADES:	Debe ser un buen comunicador para llevar buenas relaciones con el patrocinador, cliente, proveedor y los recursos del proyecto
EXPERIENCIA:	Experiencia en proyectos de tecnologías de información capacidad de negociación y comunicación
OTROS:	

NOMBRE DEL ROL	LÍDER TÉCNICO ARQUITECTÓNICO
OBJETIVOS DEL ROL:	
Proporcionar apoyo con la propuesta de desarrollo de la arquitectura de software del proyecto de Proceso de Monitoreo Continuo de Vulnerabilidades	
RESPONSABILIDADES:	
<ul style="list-style-type: none"> • Participar y verificar los entregables resultado de la fase de análisis • Participar y verificar los entregables resultado de la fase de diseño • Participar en toda la gestión del proyecto 	
FUNCIONES:	
<ul style="list-style-type: none"> • Revisar el proceso del proyecto y definir el TO BE • Elaborar la propuesta de arquitectura de software del proyecto 	
NIVELES DE AUTORIDAD:	

Contar con autoridad para con los recursos del proyecto	
Reporta a:	Jefe de Proyecto
REQUISITOS DEL ROL:	
CONOCIMIENTOS:	Conocer el proceso de negocio y de arquitectura de software
HABILIDADES:	Ser un buen comunicador
EXPERIENCIA:	Experiencia en tecnologías de información, especialmente en desarrollo de arquitecturas de software
OTROS:	

NOMBRE DEL ROL	EXPERTO EMPRESARIAL
OBJETIVOS DEL ROL:	
Proporcionar apoyo en la fase de análisis del proyecto y de aprobar el entregable resultado de esta fase.	
RESPONSABILIDADES:	
<ul style="list-style-type: none"> Aprobar los entregables de la fase de análisis 	
FUNCIONES:	
<ul style="list-style-type: none"> Brindar el apoyo en el uso correcto de las herramientas a usarse en la fase de análisis Aprobar los entregables resultado de la fase de análisis 	
NIVELES DE AUTORIDAD:	

Debe contar con la suficiente autoridad para poder tomar decisiones con el equipo durante el desarrollo de la fase de análisis del proyecto	
Reporta a:	Jefe de Proyecto
REQUISITOS DEL ROL:	
CONOCIMIENTOS:	Conocer de tecnologías de información y las herramientas a usarse durante la fase de análisis del proyecto
HABILIDADES:	Debe ser un buen comunicador, transmitir confianza y credibilidad en el proyecto
EXPERIENCIA:	Experiencia en tecnologías de información y la aplicación de arquitectura empresarial en los proyectos
OTROS:	

NOMBRE DEL ROL	EXPERTO EN ARQUITECTURA
OBJETIVOS DEL ROL:	
Proporcionar apoyo en la fase de análisis y diseño del proyecto y de aprobar los entregables.	
RESPONSABILIDADES:	
<ul style="list-style-type: none"> • Aprobar los entregables de la fase de análisis • Aprobar los entregables de la fase de diseño 	
FUNCIONES:	
<ul style="list-style-type: none"> • Brindar el apoyo en el uso correcto de las herramientas a usarse en las fases de análisis y diseño • Aprobar los entregables resultado de las fases de análisis y diseño 	

NIVELES DE AUTORIDAD:	
Debe contar con la suficiente autoridad para poder tomar decisiones con el equipo durante el desarrollo de las fases de análisis y diseño del proyecto	
Reporta a:	Jefe de Proyecto
REQUISITOS DEL ROL:	
CONOCIMIENTOS:	Conocer de tecnologías de información y de las herramientas a usarse durante las fases de análisis y diseño del proyecto
HABILIDADES:	Debe ser un buen comunicador, transmitir confianza y credibilidad en el proyecto
EXPERIENCIA:	Experiencia en tecnologías de información y la aplicación de arquitectura empresarial en los proyectos
OTROS:	

NOMBRE DEL ROL	EXPERTO EN GESTIÓN DE PROYECTOS
OBJETIVOS DEL ROL:	
Proporcionar apoyo en la fase de gestión del proyecto y de aprobar el entregable resultado de esta fase.	
RESPONSABILIDADES:	
<ul style="list-style-type: none"> Aprobar los entregables de la fase de gestión del proyecto 	
FUNCIONES:	

<ul style="list-style-type: none"> • Brindar el apoyo con el uso correcto de las herramientas a usarse en la fase de gestión del proyecto • Aprobar los entregables resultado de la fase de gestión de proyectos 	
NIVELES DE AUTORIDAD:	
Debe contar con la suficiente autoridad para poder tomar decisiones con el equipo durante el desarrollo de la fase de gestión del proyecto	
Reporta a:	Jefe de Proyecto
REQUISITOS DEL ROL:	
CONOCIMIENTOS:	Conocer de tecnologías de información y de gestión de proyectos
HABILIDADES:	Debe ser un buen comunicador y transmitir confianza y credibilidad en el proyecto
EXPERIENCIA:	Experiencia en tecnologías de información y en la gestión de proyectos
OTROS:	

6.4 Control de cambios

GESTIÓN DE CAMBIO		
<i>Nombre</i>	<i>Nombre del Rol</i>	<i>Responsabilidades</i>
Igmar León	Jefe de Proyecto	Verificar el impacto en el cronograma. Comunica a los interesados los cambios del proyecto

GESTIÓN DE CAMBIO		
Pablo Medina	Líder Técnico Arquitectónico	Revisa el cambio propuesto, determina su nivel de criticidad, para determinar si aceptar o no el cambio.
Equipo Evaluador	Equipo Evaluador	Equipo de personas encargadas de evaluar la gestión del cambio
Cualquier interesado del proyecto <i>(Asesores del Proyecto, usuarios de negocio)</i>	Interesado	Genera la solicitud del cambio definiendo la necesidad y detalle las razones por la cual se debe realizar el cambio.
Tipos de Cambio para Admitir: Se detalla los tipos de cambios a ser admitidos y define su alcance.		
a) Cambio de Costos: Justificación de cambio de costos ya establecidos, con referencia a mano de obra. b) Cambio de Alcance: Justificación de cambio de alcance, que impacte directamente en el proyecto, como cambio de una herramienta, que pueda interesar a algún stakeholder. c) Cambio de tiempo: Justificación de cambio de cronograma, establecido por la línea base, ya sea solo por la mitigación de un riesgo, no se aceptara retrasos por riesgos no indicados previamente.		
PROCESO GENERAL DE GESTIÓN DE CAMBIOS: Describe los procesos que se realiza durante la ejecución de la gestión del cambio.		
Solicitante	Es aquel que registra el cambio en el formato solicitado, detallando de forma clara las causas y consecuencias del cambio, el formato se encuentra en el Anexo N° 03 Formato de Solicitud de Control de Cambio.	
Jefe de proyecto	Cumple la función de comunicador del resultado de la evaluación	

GESTIÓN DE CAMBIO	
Equipo evaluador	En una reunión analizan el cambio solicitado y deliberan sobre el impacto en costos, alcance y tiempo del proyecto indicando las observaciones en el formato del Anexo N° 03 Formato de Solicitud de Control de Cambio. Si la respuesta es positiva será comunicada al jefe de proyecto, caso contrario, debe proponer la alternativa de solución y el plazo de implementación.

6.5 Aseguramiento y Control de Calidad

POLÍTICA DE CALIDAD DEL PROYECTO
<p>CONTROL DE LA CALIDAD</p> <p>Este aspecto de la Gerencia de la Calidad será cubierto, con las pruebas y correcciones de los errores que se puedan presentar durante el proceso de desarrollo de la propuesta.</p>
<p>ASEGURAMIENTO DE LA CALIDAD</p> <p>Para poder cumplir este aspecto de la Gerencia de la Calidad, durante todo el proceso de desarrollo de la propuesta se verificará el cumplimiento de los requerimientos definidos en el alcance del proyecto, realizando auditorías en cada entregable.</p>
<p>MEJORAMIENTO CONTINUO</p> <p>El aspecto de la Mejora Continua será aplicado usando el ciclo de Deming, definiendo un plan de mejora, luego se aplicará un cambio a pequeña escala, se comprobará si los cambios fueron positivos y finalmente se estandarizará la mejora propuesta.</p>

LÍNEA BASE DE CALIDAD DEL PROYECTO				
FACTOR DE CALIDAD RELEVANTE	OBJETIVO DE CALIDAD	MÉTRICA A UTILIZAR	FRECUENCIA Y MOMENTO DE MEDICIÓN	FRECUENCIA Y MOMENTO DE REPORTE
Rendimiento del proyecto	CPI $\geq$ 0.95	Indicador de costos	Semanal Todos los lunes	Semanal Los lunes por la tarde
	SPI $\geq$ 0.96	Indicador de cronograma	Semanal Todos los lunes	Semanal Los lunes por la tarde
Satisfacción de los usuarios	Nivel de satisfacción $\geq$ 4	Indicador de satisfacción	2 días después de un entregable	2 días después de un entregable

Nivel de Satisfacción				
Muy Insatisfecho	Poco Insatisfecho	Neutro	Poco Satisfecho	Muy Satisfecho
1	2	3	4	5

MATRIZ DE ACTIVIDADES DE CALIDAD			
Paquete de Trabajo	Estándar o norma de calidad aplicable	Actividades de Prevención	Actividades de Control
Project Chárter	PMI		Aprobación de Patrocinador
Cronograma	PMI		Aprobación de Jefe de Proyectos
Análisis de arquitectura	ZACHMAN	Revisión de modelo estándar	Aprobación de Experto Empresarial

MATRIZ DE ACTIVIDADES DE CALIDAD			
Paquete de Trabajo	Estándar o norma de calidad aplicable	Actividades de Prevención	Actividades de Control
empresarial Zachman			
Análisis de requerimientos	RUP		Aprobación de Experto en Arquitectura
Diagramas de caso de uso	RUP	Revisión de diagrama estándar	Aprobación de Experto en Arquitectura
To-Be del proceso de monitoreo de vulnerabilidades	BPMN	Revisión de diagrama estándar	Aprobación de Experto en Arquitectura
Diagrama de arquitectura TO-BE de RED	RUP	Revisión de diagrama estándar	Aprobación de Experto en Arquitectura
Diagrama de arquitectura Layered	LAYERED	Revisión de diagrama estándar	Aprobación de Experto en Arquitectura
Diagrama de arquitectura usando C4	4C	Revisión de diagrama estándar	Aprobación de Experto en Arquitectura
Diseño de Mockups	RUP	Revisión de modelo estándar	Aprobación de Experto en Arquitectura
Documento del proyecto de tesis	APA	Revisión de modelo estándar	Aprobación de Experto Empresarial

ORGANIGRAMA PARA LA CALIDAD DEL PROYECTO

Figura 55. Organigrama de calidad del proyecto
Fuente: elaboración propia, 2020

ROLES PARA LA GESTIÓN DE LA CALIDAD

ROL Nro. 1 Jefe de Proyecto	<i>Objetivos del rol:</i> Gestionar operativamente la calidad
	<i>Funciones del rol:</i> Revisar estándares, revisar entregables, aceptar entregables o disponer su reproceso, deliberar para generar acciones correctivas, aplicar acciones correctivas
	<i>Niveles de autoridad :</i> Exigir cumplimiento de entregables al equipo de proyecto
	<i>Reporta a:</i> <i>Patrocinador</i>
	<i>Supervisa a:</i> <i>Equipo de Proyecto</i>

	<i>Requisitos de conocimientos:</i> Conocimiento de la Gestión de Proyectos
	<i>Requisitos de habilidades:</i> Liderazgo, Comunicación, Negociación, Motivación, y Solución de Conflictos
	<i>Requisitos de experiencia:</i> 3 años de experiencia en el cargo

ROL Nro. 2 Líder Técnico Arquitectónico	<i>Objetivos del rol:</i> Apoyar en la gestión operativa de la calidad
	<i>Funciones del rol:</i> Analizar los requerimientos y revisar que se usen los estándares en los entregables, apoyar en la aplicación de las acciones correctivas
	<i>Niveles de autoridad :</i> Exigir cumplimiento de entregables al equipo de proyecto
	<i>Reporta a:</i> <i>Jefe Proyectos</i>
	<i>Supervisa a:</i> -
	<i>Requisitos de conocimientos:</i> Tecnologías de información, conceptos de proyectos
	<i>Requisitos de habilidades:</i> Liderazgo, Comunicación, Motivación
	<i>Requisitos de experiencia:</i> 3 años de experiencia en el cargo

6.6 Cronograma

Para el cronograma elaborado se ha utilizado el juicio de expertos, la cual ha sido tomado como referencia de proyectos anteriores. Así como una planificación en cascada especificando las tareas de cada entregable.

6.6.1 Cronograma de Actividades

Tabla 12 *Cronograma de Actividades*

Fuente: elaboración propia

Tareas		Duración	Comienzo	Fin	Predecesora
Análisis Continuo de vulnerabilidades		62 días	vie 08/05/20	vie 31/07/20	
1.1	Fase Análisis	20 días	vie 22/05/20	jue 18/06/20	
	1.1.1 Análisis de arquitectura empresarial	3 días	vie 22/05/20	mar 26/05/20	
	Realizar análisis de arquitectura	2 días	vie 22/05/20	lun 25/05/20	
	Validar Arquitectura empresarial	1 día	mar 26/05/20	mar 26/05/20	4
	Hito: Arquitectura empresarial Zachman	0 días	vie 29/05/20	vie 29/05/20	3
	1.1.2 Análisis del Proceso objetivo	3 días	mié 27/05/20	vie 29/05/20	3
	Realizar análisis del proceso objetivo	2 días	mié 27/05/20	jue 28/05/20	3
	Validar el proceso objetivo	1 día	vie 29/05/20	vie 29/05/20	8
	1.1.3 Especificaciones de reglas de negocio	4 días	lun 01/06/20	jue 04/06/20	9
	Recopilar necesidades	3 días	lun 01/06/20	mié 03/06/20	9
	Describir funcionalidades	1 día	mar 02/06/20	mar 02/06/20	11
	Validar funcionalidades	1 día	jue 04/06/20	jue 04/06/20	11
	1.1.4 Requerimientos funcionales	5 días	vie 05/06/20	jue 11/06/20	10
	Recopilar Requerimientos	2 días	vie 05/06/20	lun 08/06/20	10
	Especificar Requerimientos	2 días	mar 09/06/20	mié 10/06/20	15
	Validar Requerimientos	1 día	jue 11/06/20	jue 11/06/20	16

Tareas		Duración	Comienzo	Fin	Predecesora
	1.1.5 Requerimientos no funcionales	1 día	vie 12/06/20	vie 12/06/20	14
	Recopilar Requerimientos	1 día	vie 12/06/20	vie 12/06/20	14
	Especificar Requerimientos	1 día	vie 12/06/20	vie 12/06/20	14
	Validar Requerimientos	1 día	vie 12/06/20	vie 12/06/20	14
	1.1.6 Especificación de atributos de calidad	2 días	lun 15/06/20	mar 16/06/20	18
	Especificar Atributos	1 día	lun 15/06/20	lun 15/06/20	18
	Verificar Atributos	1 día	mar 16/06/20	mar 16/06/20	23
	1.1.7 Especificación de drivers arquitectónicos	2 días	mié 17/06/20	jue 18/06/20	22
	Identificación de drivers	1 día	jue 18/06/20	jue 18/06/20	22
	Verificar Drivers	1 día	jue 18/06/20	jue 18/06/20	26
	Hito: Análisis de requerimientos	0 días	jue 18/06/20	jue 18/06/20	
	1.2 Fase Diseño	33 días	mar 16/06/20	mié 29/07/20	18
	1.2.1 Caracterización del Proceso Objetivo To-Be	2 días	mar 16/06/20	mié 17/06/20	18
	1.2.2 Definición de casos de uso	3 días	jue 18/06/20	lun 22/06/20	30
	Hito: Diagrama de casos de uso	0 días	mié 24/06/20	mié 24/06/20	
	1.2.3 Especificación del Diagrama Layered	2 días	mié 24/06/20	jue 25/06/20	32
	Definir diagrama	1 día	mié 24/06/20	mié 24/06/20	32
	Verificar diagrama	1 día	jue 25/06/20	jue 25/06/20	34
	1.2.4 Especificación del Diagrama C4	5 días	jue 25/06/20	mié 01/07/20	34
	Realizar diagrama	2 días	jue 25/06/20	vie 26/06/20	34
	Realizar diagrama	2 días	sáb 27/06/20	lun 29/06/20	37
	Verificar diagrama	2 días	mar 30/06/20	mié 01/07/20	38

Tareas		Duración	Comienzo	Fin	Predecesora
	Hito: Diagramas de arquitectura	0 días	mié 01/07/20	mié 01/07/20	
	1.2.5 Matrices de trazabilidad	5 días	mié 01/07/20	lun 06/07/20	38
	Realizar matriz de trazabilidad	4 días	mié 01/07/20	sáb 04/07/20	38
	Verificar matriz de trazabilidad	1 día	lun 06/07/20	lun 06/07/20	42
	1.2.6 Especificación de Mockups	11 días	jue 02/07/20	mié 15/07/20	38
	Especificar Mockups	10 días	jue 02/07/20	mar 14/07/20	38
	Verificar Mockups	1 día	mié 15/07/20	mié 15/07/20	45
	1.3 Gestión de proyecto	62 días	vie 08/05/20	vie 31/07/20	
	1.3.1 Acta de proyecto	8 días	vie 08/05/20	mar 19/05/20	
	Realizar acta de proyecto	1 día	vie 08/05/20	vie 08/05/20	
	verificar acta de proyecto	1 día	vie 08/05/20	vie 08/05/20	
	Hito: Entrega de Project Chárter	1 día	mar 19/05/20	mar 19/05/20	
	1.3.2 Plan de proyecto	11 días	mié 20/05/20	mié 03/06/20	48
	Gestión de recursos	4 días	mié 20/05/20	lun 25/05/20	48
	Gestión de Costos	8 días	lun 25/05/20	mié 03/06/20	53
	Identificar costos de recursos	4 días	lun 25/05/20	jue 28/05/20	53
	Verificar costos de recursos	4 días	vie 29/05/20	mié 03/06/20	55
	Métricas de gestión	3 días	jue 04/06/20	lun 08/06/20	54
	Definir métricas	1 día	vie 08/05/20	vie 08/05/20	49
	Identificar Métricas	1 día	vie 08/05/20	vie 08/05/20	49
	Verificar Métricas	1 día	vie 08/05/20	vie 08/05/20	49
	Analizar métricas	1 día	vie 08/05/20	vie 08/05/20	49
	1.3.3 Análisis de Riesgos	3 días	jue 04/06/20	lun 08/06/20	
	Identificación de riesgos	3 días	jue 04/06/20	lun 08/06/20	54
	Análisis de riesgos	3 días	jue 04/06/20	lun 08/06/20	54

Tareas			Duración	Comienzo	Fin	Predecesora
		1.3.4 Cierre	1 día	vie 31/07/20	vie 31/07/20	

6.6.2 Diagrama Gantt de Actividades

Figura 56. Diagrama Gantt de Actividades
Fuente: elaboración propia, 2020

6.7 Presupuesto

6.7.1 Costo por Recurso

Tabla 13 *Costo por Recurso*

Fuente: elaboración propia

Nombre del Recurso	Tipo	Iniciales	Costo por Hora
Jefe de Proyecto	Trabajo	JP	S/. 30.00/h
Líder Técnico Arquitectónico	Trabajo	LT	S/. 25.00/h
Experto Empresarial	Trabajo	EA	S/. 30.00/h
Experto de Arquitectura	Trabajo	EE	S/. 30.00/h
Experto en Gestión de Proyectos	Trabajo	EG	S/. 25.00/h

6.7.2 Costeo del Proyecto

Tabla 14 *Costeo del Proyecto*

Fuente: elaboración propia

Entregable	Actividad	Tipo Recurso: Personal				
		Recurso	Unid.	QTY.	Costo Unitario x Hora	Costo Total
Análisis de arquitectura empresarial	Realizar análisis de arquitectura	Jefe de Proyecto	Horas	12	S/30.00	S/360.00
	Validar Arquitectura empresarial	Experto Empresarial	Horas	0.48	S/30.00	S/14.40
Análisis del Proceso objetivo	Realizar análisis del proceso objetivo	Jefe de Proyecto	Horas	24	S/30.00	S/720.00
	Validar el proceso objetivo	Experto Empresarial	Horas	24	S/30.00	S/720.00
Especificaciones funcionales	Recopilar necesidades	Jefe de Proyecto	Horas	32	S/30.00	S/960.00

Entregable	Actividad	Tipo Recurso: Personal				
		Recurso	Unid.	QTY.	Costo Unitario x Hora	Costo Total
	Describir funcionalidades	Líder Técnico Arquitectónico	Horas	32	S/25.00	S/800.00
	Validar funcionalidades	Experto en Arquitectura	Horas	32	S/30.00	S/960.00
Requerimientos funcionales	Recopilar Requerimientos	Jefe de Proyecto	Horas	40	S/30.00	S/1,200.00
	Especificar Requerimientos	Líder Técnico Arquitectónico	Horas	40	S/25.00	S/1,000.00
	Validar Requerimientos	Experto en Arquitectura	Horas	40	S/30.00	S/1,200.00
Requerimientos no funcionales	Recopilar Requerimientos	Jefe de Proyecto	Horas	8	S/30.00	S/240.00
	Especificar Requerimientos	Líder Técnico Arquitectónico	Horas	8	S/25.00	S/200.00
	Validar Requerimientos	Experto en Arquitectura	Horas	8	S/30.00	S/240.00
Especificación de atributos de calidad	Especificar Atributos	Líder Técnico Arquitectónico	Horas	16	S/25.00	S/400.00
	Verificar Atributos	Experto en Arquitectura	Horas	16	S/30.00	S/480.00
Especificación de drivers arquitectónicos	Identificación de drivers	Líder Técnico Arquitectónico	Horas	16	S/25.00	S/400.00
	Verificar Drivers	Experto en Arquitectura	Horas	16	S/30.00	S/480.00
Fase Diseño						

Entregable	Actividad	Tipo Recurso: Personal				
		Recurso	Unid.	QTY.	Costo Unitario x Hora	Costo Total
Descripción del Proceso Objetivo To-Be	Caracterización de To-Be	Líder Técnico Arquitectónico	Horas	16	S/25.00	S/400.00
Definición de casos de uso	Definir casos de uso	Líder Técnico Arquitectónico	Horas	24	S/25.00	S/600.00
Diagrama Layered	Definir diagrama	Líder Técnico Arquitectónico	Horas	16	S/25.00	S/400.00
	Verificar diagrama	Experto en Arquitectura	Horas	16	S/30.00	S/480.00
Diagrama C4	Realizar diagrama	Jefe de Proyecto	Horas	32	S/30.00	S/960.00
	Realizar diagrama	Líder Técnico Arquitectónico	Horas	32	S/25.00	S/800.00
	Verificar diagrama	Experto en Arquitectura	Horas	24.32	S/30.00	S/729.60
Matrices de trazabilidad	Realizar matriz de trazabilidad	Líder Técnico Arquitectónico	Horas	17.6	S/25.00	S/440.00
	Verificar matriz de trazabilidad	Experto en Arquitectura	Horas	17.6	S/30.00	S/528.00
Especificación de Mockups	Especificar Mockups	Jefe de Proyecto	Horas	48	S/30.00	S/1,440.00
	Verificar Mockups	Líder Técnico Arquitectónico	Horas	71.68	S/25.00	S/1,792.00
Gestión de proyecto						
Acta de proyecto	verificar acta de proyecto	Jefe de Proyecto	Horas	64	S/30.00	S/900.00

Entregable	Actividad	Tipo Recurso: Personal				
		Recurso	Unid.	QTY.	Costo Unitario x Hora	Costo Total
	Realizar acta de proyecto	Líder Técnico Arquitectónico	Horas	64	S/25.00	S/1,600.00
Plan de proyecto						
Gestión de recursos	Definir recursos	Jefe de Proyecto	Horas	32	S/30.00	S/960.00
Gestión de Costos	Identificar costos de recursos	Jefe de Proyecto	Horas	28	S/30.00	S/840.00
	Identificar costos de recursos	Líder Técnico Arquitectónico	Horas		S/25.00	S/0.00
Métricas de gestión	Definir métricas	Jefe de Proyecto	Horas	24	S/30.00	S/720.00
	Analizar métricas	Experto en Gestión de Proyectos	Horas	24	S/30.00	S/720.00
Riesgos						
Identificación de riesgos	Identificar riesgos	Jefe de Proyecto	Horas	12	S/30.00	S/360.00
	Verificar riesgos	Experto en Gestión de Proyectos	Horas	12	S/30.00	S/360.00
Análisis de riesgos	Plan de mitigación de riesgos	Jefe de Proyecto	Horas	24	S/30.00	S/720.00
	Verificar plan	Experto en Gestión de Proyectos	Horas	24	S/30.00	S/720.00

6.7.3 Presupuesto del Proyecto por Fase y Entregable

Tabla 15 *Presupuesto del Proyecto*

Fuente: elaboración propia

Proyecto	Fase	Entregable	Monto
PROYECTO PROPUESTA PARA LA GESTIÓN CONTINUA DE VULNERABI LIDADES	1. Fase Análisis	Análisis de arquitectura empresarial	S/. 374.40
		Análisis del Proceso objetivo	S/. 1,440.00
		Especificaciones funcionales	S/. 2,720.00
		Requerimientos funcionales	S/. 3,400.00
		Requerimientos no funcionales	S/. 680.00
		Especificación de atributos de calidad	S/. 880.00
		Especificación de drivers arquitectónicos	S/. 880.00
		Total Fase	S/. 10,374.40
	2. Fase Diseño	Descripción del Proceso Objetivo To-Be	S/. 400.00
		Definición de casos de uso	S/. 600.00
		Diagrama Layered	S/. 880.00
		Diagrama C4	S/. 2,040.00
		Matrices de trazabilidad	S/. 440.00
		Especificación de Mockups	S/. 2,200.00
		Total Fase	S/. 6,560.00
	3. Gestión de proyecto	Acta de proyecto	S/. 3,344.00
		Plan de proyecto	S/. 1,680.00
		Gestión de recursos	S/. 720.00
		Gestión de Costos	S/. 960.00
		Métricas de gestión	S/. 1,320.00
		Riegos	S/. 1,980.00
		Identificación de riesgos	S/. 660.00
		Análisis de riesgos	S/. 1,320.00

Proyecto	Fase	Entregable	Monto
		Total Fase	S/. 8,324.00
		Total Fases	S/25,258.40
		Reserva contingencia	S/2,119.18
		Líneas Base del Costo	S/27,377.58
		Reserva de Gestión	S/1,368.88
		Presupuesto del Proyecto	S/28,746.46

Para calcular el valor de Reserva de Contingencia se sumó el resultado de la matriz de Probabilidad x Impacto de cada riesgo (Tabla 21 Análisis Cuantitativo de Riesgos), el valor de estos costos se sumó al total de fases (Tabla 15 Presupuesto del Proyecto) dando como resultado el costo de la línea base.

Para el cálculo de la Reserva de Gestión se tomó un 5% del Costo de Línea Base, como estimación de juicio de expertos además se tomó este porcentaje por ser un proyecto de pocos meses, donde no deberían pasar imprevistos mayores.

6.8 Métricas de Gestión

6.8.1 Curva S

El presente grafico representa el costo acumulado en el tiempo. En la gráfica se muestra el Costo presupuestado del trabajo planificado (CPTP) en comparación con Costo real del trabajo realizado (CRTR).

Figura 57. Gráfico de indicador de curva S
Fuente: elaboración propia, 2020

6.8.2 Indicador CPI

Costo proyectado S/ 25,258.40	Realmente cuesta S/ 27,091.00	CPI=0.93
----------------------------------	----------------------------------	----------

Según el indicador de CPI, el proyecto estaría por encima del 7% sobre el presupuesto estimado proyectado, la razón de ello es debido a que en el alcance inicial no se considera la reserva de contingencia ni la reserva de gestión.

6.8.3 Indicador SPI

SPI (Schedule Performance Index), también se denomina en español al Índice de rendimiento de la programación (IRP), se calcula de la siguiente manera:

CPTR (Costo presupuestado del trabajo realizado)

CPTP (Costo presupuestado del trabajo planificado)

$$IRP = CPTR / CPTP$$

En el largo de todo el proyecto, se puede concluir que siempre se ha tenido un desempeño por debajo de lo estimado, como se puede apreciar en el siguiente gráfico:

Figura 58. Gráfico de indicador SPI

Fuente: elaboración propia, 2020

En el gráfico se puede apreciar que el 24 de mayo el indicador de SPI es de 0.85, fue por la baja eficiencia de avance real de trabajo, gastamos muchas horas de trabajo y varias iteraciones en el análisis de la arquitectura empresarial en contraste con el valor ganado.

En las siguientes semanas se realizó ajustes y optimizaciones, pero nuestro desempeño no ha sido el mejor y se ha tenido que realizar varias horas extras para terminar los entregables en las fechas indicadas

6.9 Plan de respuesta a los riesgos

6.9.1 Identificación de Riesgos

Tabla 16 *Identificación de Riesgos*

Fuente: elaboración propia

ID	Riesgo	Descripción de Riesgo
R001	Ausencia de uno de los integrantes	Debido a la coyuntura que se viene pasando, es posible que uno de los integrantes del equipo de proyectos se pueda enfermar con el virus de Covid19.
R002	Falta de energía eléctrica	Debido a la coyuntura, el trabajo se viene realizando desde los hogares de los integrantes, es posible que en el lugar donde se encuentre la empresa de servicios realice un mantenimiento al servicio de energía eléctrica.
R003	Reestructuración en la organización	Debido a la coyuntura, muchas organizaciones vienen reestructurando al personal, es posible que esta reestructuración se presente en la organización propuesta.
R004	Cambio inesperado en el alcance del proyecto	Cambio que se pueda presentar luego de haber presentado el plan del proyecto, pero este cambio sería muy importante para la empresa el cual afectaría el costo, tiempo y alcance.

6.9.2 Escala de Valores Numéricos o Cualitativos para la Probabilidad

Tabla 17 *Escala de Valores Numéricos o Cualitativos de Probabilidad*

Fuente: elaboración propia

	Muy Baja / 0.10	Baja / 0.30	Moderada / 0.50	Alta / 0.70	Muy Alta / 0.90
PROBABILIDAD	Ocurrencia muy poco probable	Ocurrencia poco probable	Ocurrencia probable	Ocurrencia muy probable	Ocurrencia casi segura

6.9.3 Escala de Valores Numéricos o Cualitativos para el Impacto

Tabla 18 *Escala de Valores Numéricos o Cualitativos de Impacto*

Fuente: elaboración propia

		Muy Bajo / 0.05	Bajo / 0.10	Moderado / 0.20	Alto / 0.40	Muy Alto / 0.80
IMPACTO	COSTO	Aumento de costo insignificante	Aumento de costo menor 10%	Aumento de costo entre 10-20%	Aumento de costo entre 20-40%	Aumento de costo mayor a 40%
	PLAZOS	Aumento de plazo insignificante	Aumento de plazo menor 5%	Aumento de plazo entre 5-10%	Aumento de plazo entre 10-20%	Aumento de plazo mayor a 20%
	ALCANCE	Reducción de alcance apenas perceptible	Áreas secundarias afectadas	Áreas principales afectadas	Reducción de alcance no aceptable por patrocinador	Resultado final inservible

6.9.4 Matriz de Probabilidad por Impacto

Tabla 19 *Matriz Probabilidad x Impacto*

Fuente: elaboración propia

PROBABILIDAD	Matriz Probabilidad x Impacto				
0.90	0.05	0.09	0.18	0.36	0.72
0.70	0.04	0.07	0.14	0.28	0.56
0.50	0.03	0.05	0.10	0.20	0.40
0.30	0.02	0.03	0.06	0.12	0.24
0.10	0.01	0.01	0.02	0.04	0.08
	0.05	0.10	0.20	0.40	0.80
	IMPACTO				

UMBRALES		
Amenaza		Oportunidad
Aceptable		Aceptable
Moderado		Moderado
Inaceptable		Recomendable

6.9.5 Análisis Cualitativo de Riesgos

Para obtener este análisis se hizo uso de la matriz de probabilidad por impacto, otorgando los valores de probabilidad e impacto para cada riesgo, dando como resultado un porcentaje para cada uno de ellos.

Tabla 20 *Análisis Cualitativo de Riesgos*

Fuente: elaboración propia

ID	Riesgo	Probabilidad	Impacto	Probabilidad x Impacto	Requiere Respuesta Inmediata	Nivel
R001	Ausencia de uno de los integrantes	0.50	0.20	0.10	Sí	Moderado
R002	Falta de energía eléctrica	0.10	0.10	0.01	No	Aceptable
R003	Reestructuración en la organización	0.30	0.40	0.12	Sí	Moderado
R004	Cambio inesperado en el alcance del proyecto	0.10	0.80	0.08	Sí	Moderado

6.9.6 Análisis Cuantitativo de Riesgos

El resultado de este análisis es calcular el Costo del Proyecto por cada rango de valor del Impacto, luego este se multiplicó por la probabilidad obteniendo otro rango de valor y el promedio se obtuvo en la reserva de contingencia.

Tabla 21 *Análisis Cuantitativo de Riesgos*

Fuente: elaboración propia

ID	Riesgo	Probabilidad	Impacto (S/)	Probabilidad x Impacto (S/)	Reserva de Contingencia (S/)	Nivel
R001	Ausencia de uno de los integrantes	0.50	2,525.84 ; 5,051.68	252.58 ; 505.17	378.88	Moderado
R002	Falta de energía eléctrica	0.10	2,273.26	22.73	22.73	Aceptable
R003	Reestructuración en la organización	0.30	5,051.68 ; 10,103.36	606.20 ; 1,212.40	909.30	Moderado
R004	Cambio inesperado en el alcance del proyecto	0.10	10,103.36	808.27	808.27	Moderado

6.9.7 Plan de Respuesta al Riesgo

Tabla 22 *Plan de Respuesta al Riesgo*

Fuente: elaboración propia

ID	Amenaza / oportunidad	Descripción Riesgo	Causa Raíz	Disparador	Entregables afectados	Probabilidad x Impacto total	Tipo de riesgo	Responsable del riesgo	Respuestas planificadas	Estrategia	Responsable de la respuesta	Fecha planificada	Acciones
R001	Amenaza	Ausencia de uno de los integrantes	Integrante enfermo	Retraso en entregables	Indistinto	0.10	Moderado	Jefe Proyecto	Otro integrante debe asumir el trabajo	Mitigar	Jefe Proyecto	No se tiene una fecha	Contar con un repositorio centralizado, para ser usado por cualquier integrante del equipo
R002	Amenaza	Falta de energía eléctrica	Mantenimiento del servicio	Retraso en entregables	Indistinto	0.01	Aceptable	Jefe Proyecto	Informar al equipo para solicitar apoyo con otro integrante	Mitigar	Jefe Proyecto	No se tiene una fecha	Reprogramar reuniones virtuales, usar horas extras para ponerse a fecha
R003	Amenaza	Reestructuración en la organización	Rotación o renuncia del patrocinador	Se detiene el proyecto	Indistinto	0.12	Moderado	Organización	Solicitar una reunión con el nuevo equipo	Mitigar	Organización	No se tiene una fecha	Reunión con el nuevo equipo y presentar el proyecto y el avance en el que se encuentra
R004	Amenaza	Cambio inesperado en el alcance del proyecto	Usuario olvidó incluir un requerimiento importante	Retraso en entregables	Indistinto	0.08	Moderado	Patrocinador	Ejecutar una gestión de cambio	Aceptar	Patrocinador	No se tiene una fecha	Dar a conocer al Patrocinador que el cambio moverá el cronograma

6.10 Gestión de interesados.

6.10.1 Matriz de Interesados

Tabla 23 *Registro de interesados*

Fuente: elaboración propia

ID	Nombre	Posición	Rol	Expectativas	Influencia	Clasificación
PR	Pedro Roque	Gerente de TISO	Sponsor	Proyecto exitoso	Alta	Alta Prioridad
RS	Rodolfo Suarez	Gerente de CISO	Comité	Proyecto exitoso	Alta	Alta Prioridad
AF	Alfredo Flores	Gerente de arquitectura	Comité	Hacer cumplir el proceso de arquitectura	Alta	Alta Prioridad
RV	Roger Velázquez	Gerente de soluciones	Comité	Proyecto exitoso	Alta	Alta Prioridad
TS	Tania Silva	PMO	PMO	Informar avance del proyecto	Media	Media Prioridad
JR	Javier Rojas	Supervisor de operaciones informáticas	Usuario final	Ninguna	Media	Alta Prioridad
PM	Igmar León	Jefe de proyecto	Jefe de proyecto	Proyecto exitoso	Media	Media Prioridad
IL	Pablo Medina	Analista funcional	Analista funcional	Proyecto exitoso	Media	Media Prioridad
FDL	Fiorella De los Santos	Analista funcional	Supervisora del proceso	Proyecto exitoso	Baja	Media Prioridad
OR	Omar Roca	Divisional de soporte	Líder comité	Cumplir las sentencias de FFIEC	Alta	Alta Prioridad

6.10.2 Matriz de Poder / Interés

Se ha elaborado una Matriz de Gardner la cual orienta a clasificar a los stakeholders de acuerdo a las variables de “poder que poseen” y el “grado de interés” que demuestran por las estrategias de la empresa.

Figura 59. Gráfico Matriz de poder / Interés
Fuente: elaboración propia, 2020

6.10.3 Nivel de Involucramiento

Tabla 24 Nivel de involucramiento

Fuente: elaboración propia

ID	Nombre	Posición	Desinformado	Resistente	Neutral	Promotor	Impulsador
PR	Pedro Roque	Gerente de TISO					A / D
RS	Rodolfo Suarez	Gerente de CISO				A	D
AF	Alfredo Flores	Gerente de arquitectura			A	D	
RV	Roger Velázquez	Gerente de soluciones					A / D
TS	Tania Silva	PMO			A	D	

ID	Nombre	Posición	Desinformado	Resistente	Neutral	Promotor	Impulsador
JR	Javier Rojas	Supervisor de operaciones informáticas			A	D	
PM	Igmar León	Jefe de proyecto					A / D
IL	Pablo Medina	Analista funcional				A / D	
FDL	Fiorella De los Santos	Analista funcional				A / D	
OR	Omar Roca	Divisional de Soporte			A	D	

A: Nivel Actual de compromiso D: Nivel deseado de compromiso

6.10.4 Plan de Acción

- Como resultado de la identificación de interesados se encuentran como posibles detractores a “Divisional de Soporte y Gerente de arquitectura”, para los cuales se debería plantear una estrategia, para cambiarlos de ser neutrales a deseable y que lleguen a ser promotores, ya que el gran poder y bajo interés puede afectar al proyecto, para lo cual se plantea lo siguientes puntos a través de una gestión adecuada:
 - Hacerles participe en las reuniones del proyecto para que compartan los objetivos que se definen para el beneficio de la empresa.
 - Remitir informes personalizados semanales sobre el avance del proyecto, que satisfagan los intereses de ellos.
- Con respecto al “Supervisor de operaciones informáticas y PMO”, se tienen que estar monitoreando constantemente y mantenerlos informados de los avances del proyecto.
- Con respecto al “Jefe de proyecto y los Analistas funcionales”, mantenerlos informados y nunca ignorarlos.
- Con respecto al “Gerente de TISO, Gerente de CISO y Gerente de soluciones”, trabajar directamente con ellos, para que no pierdan el interés en el proyecto.

6.10.5 Matriz de Comunicaciones

Tabla 25 *Matriz de comunicaciones*

Fuente: elaboración propia

¿Qué se comunica?	Documento	¿Quién lo comunica?	¿A quién le comunica?	¿Cuándo lo comunica?	¿Cómo lo comunica?
Inicio del Proyecto	Project Charter	Jefe de Proyecto	Todos los interesados	Una sola vez al inicio del proyecto	Reunión Kick off
Planificación del proyecto	Plan de Proyecto	Jefe de Proyecto	Sponsor / Equipo de proyecto	En la reunión de avance de proyecto con el sponsor.	Reunión
Cambios	Solicitud de cambios	Sponsor	Jefe de Proyecto	Cuando se requiera el cambio	Reunión
Informe de avance	Informe de Avance del Proyecto	Jefe de Proyecto	Equipo de proyecto	Semanalmente	Envío de informe semanal
Fin del proyecto	Informe de Cierre	Jefe de Proyecto	Todos los interesados	Una sola vez al finalizar el proyecto	Reunión

6.11 Ejecución, Monitoreo y Control.

En el siguiente apartado se procederá a presentar el avance del proyecto a fecha de corte 18/07/2020, el formato se encuentra en Anexo N° 02 Formato de Informe de Avance:

INFORME DE AVANCE SEMANA N° 11

SECCIÓN 1. INFORMACIÓN GENERAL

Código y Nombre del Proyecto	Fecha del Reporte
Mejora en el Proceso de Monitoreo Continuo de Vulnerabilidades	18/07/2020
Elaborado por:	
Jefe de Proyecto	

SECCIÓN 2. RESUMEN

1. TIEMPO

2. PRESUPUESTO

Aprobado (S/.)	Comprometido (S/.)	Ejecutado (S/.)	Disponible (S/.)
25 k	25 k	26 K	0 M

3. RECURSOS

4. PROBLEMAS Y RIESGOS

P	0	0	0
R	0	0	1

SECCIÓN 3. AVANCES Y PENDIENTES

Fase	% Avance	Inicio	Fin
	Real	Planificado	Planificado
Fase Análisis	100%	22/05/2020	26/05/2020
Hito: Arquitectura Empresarial	100%	29/05/2020	29/05/2020

Fase	% Avance Real	Inicio Planificado	Fin Planificado
Hito: Análisis de requerimientos	100%	18/06/2020	18/06/2020
Fase Diseño	89%	16/06/2020	29/07/2020
Hito: Diagrama de casos de uso	100%	24/06/2020	24/06/2020
Hito: Diagrama de arquitectura	100%	01/07/2020	01/07/2020
Gestión de Proyecto	88%	08/05/2020	31/07/2020
Hito: Entrega de Project Charter	100%	19/05/2020	19/05/2020
Hito: Entrega de Tesis	0	31/05/2020	22/05/2020

Indicadores

CPI 0.940

SPI 0.961

Actividades relevantes / Hitos de la semana

Dom 12/07/2020 al Termino de Mockups

Sab 18/07/2020 Seguimiento semanal

Gestión de costos

Próximos Pasos (La siguiente semana)

Dom 19/06/2020 al Validación de Mockups

Sab 25/07/2020 Elaboración de métricas de gestión del proyecto

SECCIÓN 5. RIESGOS E INCIDENTES

Riesgo o Incidente	Acciones	Responsable	Fecha	Estado
Riesgo: Cambio de alcance, no se tenía considerado realizar Mockups	Realizar Mockups de los Drivers principales	Jefe de Proyecto	01/07/2020	En proceso
Riesgo: Retraso en la especificación de los casos de uso.	Realizar sobre trabajo para cumplir el entregable	Líder Técnico Arquitectónico	07/07/2020	En proceso
Riesgo: Retraso en la realización de los Mockups	Realizar sobre trabajo para cumplir el entregable	Líder Técnico Arquitectónico	10/07/2020	En proceso
Riesgo: Sobrecosto por el sobre tiempo al realizar la especificación de los casos de uso y los Mockups	Se utiliza la reserva de contingencia.	Jefe de Proyecto	10/07/2020	En Proceso
Incidente: Falla de equipo del Líder Técnico Arquitectónico, retraso en terminar los Mockups	Se utilizará equipo de cómputo de respaldo para terminar el entregable	Líder Técnico Arquitectónico	12/07/2020	Cerrado
Riesgo: Término de la licencia de prueba de la herramienta que apoya en la realización de Mockups	Importar el proyecto en formato JSON, crear nueva cuenta y continuar el trabajo.	Líder Técnico Arquitectónico	15/07/2020	Cerrado

6.12 Cierre

6.12.1 Acta de Cierre

Con el Acta de Cierre se da por concluida todas las actividades del proceso de la gestión o fase de proyecto, el Jefe de Proyectos revisa toda la documentación a ser entregada. En la fase del cierre se pueden dar las siguientes situaciones: con entrega de todos componentes del proyecto, con entrega de algunos y otros componentes cancelados, o se cancelan todos los componentes. Para este proyecto, estamos realizando el cierre con la entrega de todos los componentes definidos en el alcance y su aceptación. Finalmente se solicita la firma del patrocinador y del jefe de proyectos para dar por aprobado el cierre del proyecto o fase.

6.12.2 Informe de Cierre

En esta sección presentamos el informe de cierre del proyecto, se podrá observar una evaluación y algunos indicadores.

Sección 1. Información General

Código y Nombre del Proyecto	Fecha del Reporte
Mejora en el Proceso de Monitoreo Continuo de Vulnerabilidades	31/07/2020
Elaborado por:	
León Vidalón, Igmar Medina Ampuero, Pablo Jorge	

Sección 2. Resumen

De acuerdo a lo revisado el 31 de julio del presente año, se ha podido identificar que el proyecto se ha ejecutado de forma normal, es decir no ha presentado incidentes que afecten de manera sustancial al desarrollo del proyecto.

Tema	Estado Actual (Semáforo)
Alcance
Costo
Cronograma
Riesgos
Incidentes

Sección 3. Avances y Pendientes

El proyecto se desarrolló de forma normal como se mencionó en el punto anterior, con eventos de tipo incidente y riesgos que fueron controlados dentro del plan de repuesta al riesgo y control de cambios del plan del proyecto. A continuación se muestra un resumen:

Tema	Detalle
Entregables completados	Project Chárter Cronograma Análisis de arquitectura empresarial Zachman Análisis de requerimientos Diagramas de caso de uso To-Be del proceso de monitoreo de vulnerabilidades Diagrama de arquitectura TO-BE de RED Diagrama de arquitectura Layered Diagrama de arquitectura usando C4 Diseño de Mockups
Pendientes	Acta de cierre de Proyecto

Sección 4. Planificado versus Ejecutado

En la siguiente sección mostramos una evaluación financiera del proyecto, se considera el presupuesto planificado y el costo real ejecutado.

Tema	Planificado	Ejecutado
Presupuesto	S/25,258.40	S/25,258.40
Reserva de Contingencia	S/2,119.18	S/808.27
Total, Línea Base (Presupuestado + reserva de contingencia)	S/27,377.58	S/26,066.67
Reserva de Gestión (5% Línea Base)	S/1,368.88	S/1,024.33
Costo Total del Proyecto	S/28,746.46	S/27,091.00
Plazo entrega	31/07/2020	31/07/2020

Como se puede observar en el cuadro, al finalizar el proyecto se ejecutó el 100% del presupuesto. En la semana 9 se presentó una variación en el costo del presupuesto, ocasionando un ligero incremento del costo real, al cierre del proyecto quedó el siguiente valor:

Planificado (PV)	Ejecutado (EV)	Real (AC)
S/25,258.40	S/25,258.40	S/27,091.00

Nombre	Fórmula	Valor Obtenido	Estado
Varianza del Cronograma (SV)	EV - PV	0.00	Bien
Varianza de Costo (CV)	EV - AC	1,832.60	Sobre costo
Rendimiento de Costo (CSI)	EV / AC	0.932	Sobre costo

En la semana 9 se empleó recursos económicos de la reserva de contingencia, esto debido a que se presentó un requerimiento nuevo en el proyecto (riesgo R004 del plan de respuesta al riesgo), por lo que se tuvo que realizar un trabajo de horas extras y no afectar el cronograma.

Sección 5. Riesgos e Incidentes

A continuación se detallan los siguientes riesgos e incidentes presentados en el proyecto:

Riesgo (R) o Incidente (I)	Acciones	Responsable	Fecha	Estado
(R) Corte de energía eléctrica en la ubicación del Líder Técnico Arquitectónico	Se reprograma las reuniones y se avanza los pendientes en sobre hora	Líder Técnico Arquitectónico	05/06/2020	Cerrado

Riesgo (R) o Incidente (I)	Acciones	Responsable	Fecha	Estado
(R) Cambio en el alcance, no se tenía considerado realizar Mockups.	Realizar Mockups de los drivers principales	Jefe de Proyectos	01/07/2020	Cerrado
(I) Falla de equipo del Líder Técnico Arquitectónico.	Se utiliza equipo de cómputo de respaldo	Líder Técnico Arquitectónico	12/07/2020	Cerrado
(I) Término de la licencia de prueba de la herramienta para elaborar los Mockups	Importar el proyecto en formato JSON, crear nueva cuenta y continuar el trabajo.	Líder Técnico Arquitectónico	15/07/2020	Cerrado

6.12.3 Lecciones Aprendidas

Durante todo el desarrollo del proyecto se presentaron diversos eventos, que en un futuro nos ayudarán con una correcta toma de decisiones y nos sirven como un aprendizaje en la gestión de proyectos.

REGISTRO DE LECCIONES APRENDIDAS	
Identificación de Lección Aprendida: LA01	
Nombre Propuesto para la Lección Aprendida:	Contar con el Alcance claro y detallado.
Grupo de procesos:	Inicio
Proceso Específico de la Gerencia de Proyecto que está siendo utilizado:	
Desarrollo del Acta de Constitución del Proyecto.	
Práctica específica, herramienta o técnica que está siendo utilizada:	
Reuniones y recopilación de datos.	
¿Cuál fue la acción sucedida, que pasó?	
Durante la ejecución del proyecto, a más de la mitad del avance, solicitaron se agregue nuevos entregables que no estuvieron contemplados en el alcance.	

REGISTRO DE LECCIONES APRENDIDAS			
¿Cuál fue el resultado o impacto de la incidencia? Afecto el presupuesto y el cronograma del proyecto.			
¿Cuál es la lección aprendida? Cualquier cambio significativo y a un tiempo avanzado del proyecto, ocasiona cambios en el cronograma y presupuesto del proyecto.			
¿Qué acción se tomó? Se tuvo que trabajar horas extras en la fase de diseño de la arquitectura y no se vea afectado el cronograma de entrega.			
¿Qué comportamiento se recomienda para el futuro? Una mayor comunicación con los interesados, y también involucrar a los usuarios que harán uso del sistema, con la finalidad de tener mayor claro el alcance.			
¿Dónde y cómo este conocimiento, puede ser utilizado más adelante en el proyecto actual? Si se presentase la solicitud de nuevos entregables.			
¿Dónde y cómo este conocimiento, se puede utilizar en un proyecto futuro? En la acta de constitución del proyecto y el alcance del mismo.			
¿Quién debe ser informado sobre esta lección aprendida?: (marcar una)			
☐	Empleados	☒	Sponsor del proyecto
☐		☒	Equipo del Proyecto
☐			Todo el
¿Cómo debe ser distribuida esta lección aprendida? (marcar todas las que apliquen)			
☐	e-mail	☒	Intranet/pagina Web
☐		☒	Preguntas Frecuentes
☐			Bibliot
¿Ha anexado referencia(s), ejemplo(s) y/o material(es) adicional(es)?			☐ si ☒ no
Nombre(s) de anexo(s): 1. No Existen			

REGISTRO DE LECCIONES APRENDIDAS	
Identificación de Lección Aprendida: LA02	
Nombre Propuesto para la Lección Aprendida:	Uso de herramientas gratuitas.
Grupo de procesos:	Ejecución
Proceso Específico de la Gerencia de Proyecto que está siendo utilizado:	

REGISTRO DE LECCIONES APRENDIDAS									
Gestión de adquisiciones									
Práctica específica, herramienta o técnica que está siendo utilizada: Herramienta de software.									
¿Cuál fue la acción sucedida, que pasó? Durante la ejecución del proyecto, se hizo uso de herramientas gratuitas para el diseño de diagramas y prototipos, estas vencieron y en el momento no se pudieron editar los archivos.									
¿Cuál fue el resultado o impacto de la incidencia? Afectó en el tiempo del desarrollo del proyecto.									
¿Cuál es la lección aprendida? El uso de herramientas gratuitas no puede ser usado por un periodo largo, sólo para un trabajo específico y corto.									
¿Qué acción se tomó? Se tuvo que volver a registrar con otro usuario para usarlo por otro tiempo corto.									
¿Qué comportamiento se recomienda para el futuro? Definir las herramientas a usarse en el proyecto y mejor si cuenta con licencia.									
¿Dónde y cómo este conocimiento, puede ser utilizado más adelante en el proyecto actual? En el uso de herramientas si se presentase más adelante									
¿Dónde y cómo este conocimiento, se puede utilizar en un proyecto futuro? En la gestión de adquisiciones del proyecto.									
¿Quién debe ser informado sobre esta lección aprendida?: (marcar una)									
☐	☐	Empleados	☒	Sponsor del proyecto	☒	Equipo del Proyecto	☐	Todo	el
¿Cómo debe ser distribuida esta lección aprendida? (marcar todas las que apliquen)									
☐	☐	e-mail	☒	Intranet/pagina Web	☒	Preguntas Frecuentes	☐	Bibliot	
¿Ha anexado referencia(s), ejemplo(s) y/o material(es) adicional(es)?							☐	si	☒
Nombre(s) de anexo(s): 1. No Existen									

7 CONCLUSIONES

Luego de realizar el presente trabajo podemos concluir lo siguiente:

La evaluación realizada a la arquitectura empresarial de Mibanco basada en Zachman, nos ha ayudado a identificar la necesidad del negocio con respecto a una gestión adecuada de la seguridad informática.

El análisis realizado al proceso de monitoreo continuo de vulnerabilidades en conjunto con el modelado con BPMN nos ha permitido encontrar los puntos críticos del proceso, siendo el más resaltante las tareas manuales que llevan gran tiempo en realizar, las cuales fueron centro de nuestra propuesta de mejora.

El análisis de requerimientos de la investigación se ha podido observar la gran importancia de la comunicación con el área responsable del proceso, para llegar a sintetizar los principios del proceso los cuales son descubrir, detectar, responder, prevenir.

Al aplicar diversos estilos de arquitectura, alineados a los principios requeridos del proceso, nos ha permitido generar un marco de referencia para el entendimiento y la trazabilidad entre los requerimientos de negocio y las funcionalidades.

La disciplina de gestión de proyectos ha beneficiado al proyecto, en determinar una adecuada planificación y determinación de riesgos principalmente, para ser proactivos y tomar acción en el momento adecuado, apoyado de los diferentes indicadores calculados.

8 RECOMENDACIONES

En el presente proyecto se detectaron las siguientes recomendaciones:

- Para poder implementar un modelo de arquitectura empresarial se debe tener claro los objetivos de la organización.
- Es necesario que se tenga infraestructura necesaria para poder lograr los resultados planteados en el modelo de solución.
- Para el diseño de diagramas detectamos la herramienta Draw.io el cual es un reemplazo práctico para el reemplazo del Visio.
- Durante el diseño de la solución C4 encontramos a Structurizr, que es una herramienta que permite el diseño desde el Contexto, Contenedor, Componente y Código.

9 GLOSARIO DE TERMINOS

Zero-day: tipo de ciberataque contra una aplicación o sistema que tiene como objetivo la ejecución de código malicioso gracias al conocimiento de vulnerabilidades que el fabricante del producto y los usuarios desconocen.

Alerta: notificación o aviso sobre alguna amenaza o vulnerabilidad que podría llegar a afectar a alguno de los activos.

Amenaza: una causa potencial de un incidente inesperado, que puede resultar en un daño a un activo o a la organización.

APT: Acrónimo de Amenaza Persistente Avanzada. Amenaza que agrupa diferentes técnicas y software malicioso para explotar vulnerabilidades en los sistemas.

Contacto técnico: es el empleado o cargo que, por cuenta del Propietario del activo, siguiendo sus indicaciones y de acuerdo con los controles de seguridad aplicables según el Análisis de Riesgos vigente, se encarga del desarrollo y mantenimiento del activo.

Evento de seguridad: ocurrencia que indica una posible brecha de seguridad o un fallo de los controles de seguridad. También se conoce como incidencia de seguridad.

Firewall: Tecnología empleada para la protección de sistemas de información y comunicaciones que limitan o impiden las conexiones de red. En castellano se denomina “cortafuegos”.

IDS o IPS: Acrónimos de Sistema de Detección de Intrusiones y Sistema de Protección de Intrusiones, respectivamente. Tecnologías empleadas para la protección de sistemas de información y comunicaciones que limitan o impiden los accesos no autorizados.

Incidente de seguridad: uno o una serie de eventos o incidencias de seguridad, que pueden dañar uno o varios activos de la organización, o pueden comprometer su operación.

SIEM: Acrónimo de Gestión de Eventos y Seguridad de la Información. Tecnologías que proporcionan análisis en tiempo real de alertas y eventos de seguridad generadas por el hardware y el software de una organización.

Vulnerabilidad: debilidad de un activo o de un control de seguridad, que puede ser explotada por una o más amenazas.

Cronograma de monitoreo: Se refiere al documento (Excel) donde se especifica la programación y responsable de cada monitoreo para el año en curso.

Manual de Monitoreo: Se refiere a cada manual específico por cada monitoreo, en dicho manual se especifica el procedimiento a seguir para la ejecución de un monitoreo en particular. Formato adjunto en Anexos.

Informe de Monitoreo: Documento producto de la ejecución de un monitoreo en específico, en él se sintetiza los hallazgos, evidencias y recomendaciones que surjan del proceso.

10 SIGLARIO

- ERP (enterprise resource planning): Los sistemas de planificación de recursos empresariales son los sistemas de información gerenciales que integran y manejan muchos de los negocios asociados con las operaciones de producción y de los aspectos de distribución de una compañía en la producción de bienes o servicios.
- FFIEC (Federal Financial Institutions Examination Council's): Es un organismo formal interinstitucional del gobierno de los Estados Unidos compuesto por cinco reguladores bancarios que está "facultado para prescribir principios, estándares y formularios de informe uniformes para promover la uniformidad en la supervisión de las instituciones financieras.
- CAT (Cybersecurity Assessment Tool) Herramienta de evaluación de ciberseguridad de FFIEC.
- TISO Gerencia de Operaciones de Seguridad Tecnológica.
- CVE (Common Vulnerabilities and Exposures) es una lista de información registrada sobre vulnerabilidades de seguridad conocidas, en la que cada referencia tiene un número de identificación CVE-ID, descripción de la vulnerabilidad, que versiones del software están afectadas, posible solución al fall (si existe) o como configurar para mitigar la vulnerabilidad y referencias a publicaciones o entradas de foros o blog donde se ha hecho pública la vulnerabilidad o se demuestra su explotación.
- CVSS (Common Vulnerability Score System) El Sistema de puntuación de vulnerabilidad común es un estándar de la industria gratuito y abierto para evaluar la gravedad de las vulnerabilidades de seguridad del sistema informático.
- Owasp (Open Web Application Security Project) es un proyecto de código abierto dedicado a determinar y combatir las causas que hacen que el software sea inseguro.
- IaaS (Infraestructure as a Service) es un modelo de distribución de software donde el soporte lógico y los datos que maneja se alojan en servidores de una compañía de tecnologías de información y comunicación (TIC), a los que se accede vía Internet desde un cliente.
- CAS STAR (Cloud Security Alliance Security Trust Assurance and Risk) es una evaluación independiente rigurosa de terceros de la seguridad de un proveedor de servicios en la nube.

- SSO (Single Sign-On, SSO) es un procedimiento de autenticación que habilita a un usuario determinado para acceder a varios sistemas con una sola instancia de identificación.
- SAML (Security Assertion Markup Language) es un estándar de código abierto basado en XML que permite el intercambio de información, tanto de autenticación como de autorización entre diferentes partes: un identity provider (proveedor de identidad) y un service provider (proveedor de servicios).

11 REFERENCIAS

Consejo Federal de Examen de Instituciones Financieras (FFIEC). (Mayo 2017) Appendix A: Mapping Baseline Statements to FFIEC IT Examination Handbook. USA. Recuperado de https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_Appendix_A_May_2017.pdf [Consulta: 15 de Junio de 2020].

Consejo Federal de Examen de Instituciones Financieras (FFIEC). (Mayo 2017) Appendix B: Mapping Cybersecurity Assessment Tool to NIST CybersecurityFramework. USA. Recuperado de https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_App_B_Map_to_NIST_CSF_June_2015_PDF4.pdf [Consulta: 15 de Junio de 2020].

Common Vulnerabilities and Exposures (CVE). (05 Marzo 2020) CVE Numbering Authority (CNA) Rules V3.0 Recuperado de <https://cve.mitre.org/cve/cna/rules.html> [Consulta: 20 de Junio de 2020].

Forum of Incident Response and Security Teams (First) (2019) Common Vulnerability Scoring System version 3.1, Specification Document, Revision 1. Recuperado de https://www.first.org/cvss/v3-1/cvss-v31-specification_r1.pdf [Consulta: 20 de Junio de 2020].

Open Web Application Security Project (Owasp) (2017) OWASP Top Ten. Recuperado de <https://owasp.org/www-project-top-ten/> [Consulta: 20 de Junio de 2020].

David R. Kuhn, Mohammad Raunak, Raghu N. Kacker (2017).It Doesn't Have to Be Like This: Cybersecurity Vulnerability Trends. Recuperado <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7047612/> [Consulta: 20 de Junio de 2020].

Instituto Nacional de Estándares y Tecnología (16 Abril 2018). Framework for Improving Critical Infrastructure Cybersecurity. V1.1. Recuperado <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf> [Consulta: 20 de Junio de 2020].

Martín Darío Arango Serna, Jesús Enrique Londoño Salazar, Julián Andrés Zapata Cortés (junio, 2010). Arquitectura empresarial - una visión general. *Revista Ingenierías Universidad de Medellín*, 9 (16), 101-111, doi: 10.22395/rium [Consulta: 8 de Junio de 2020].

J.Zachman, "A Framework for Information Systems Architecture," the IBSM Systems Journal vol. 26, no.3, pp.454-470, 1987.

12 ANEXOS

Anexo N° 01 Project Chárter

Anexo N° 02 Formato de Informe de Avance

Anexo N° 03 Formato de Solicitud de Control de Cambio

Anexo N° 04 Carta de Solicitud para Uso de Información de la Empresa Objetivo

Anexo N° 05 Correo de Aceptación de Empresa Objetivo: Cumplimiento

Anexo N° 06 Correo de Aceptación de Empresa Objetivo: Relaciones Institucionales

Anexo N° 07 Correo de Aceptación de Empresa Objetivo: Relaciones Institucionales

Anexo N° 08 Declaración Jurada Igmarr León Vidalón

Anexo N° 09 Declaración Jurada Pablo Jorge Medina Ampuero

Anexo N° 10 Correo de aceptación de la solución: Gerencia TISO

12.1 Anexo N° 01 Project Chárter

PROPUESTA DE SOLUCIÓN PARA LA MEJORA DEL PROCESO DE MONITOREO CONTINUO DE VULNERABILIDADES EN LA EMPRESA MIBANCO

PROJECT CHARTER V4.0

Preparado por:

Jefe de Proyecto:	Pablo Jorge Medina Ampuero	Igmar León Vidalón
Especialidad:	Ingeniería de Sistemas	
Empresa:	Mibanco	
Línea de tesis:	Programa de Actualización Profesional (PAP)	

Historial de Revisiones

Versión	Fecha	Autor		Descripción
1.0	04/07/2020	Igmar L.		Creación de documento
1.1	10/07/2020	Pablo M.		Modificación del alcance, miembros, interesados
1.2	17/07/2020	Igmar L.		Modificación de documento
1.3	22/07/2020	Igmar L.		Modificación de documento
1.4	27/07/2020	Igmar L.		Modificación de documento

• RESUMEN EJECUTIVO

En el presente Project Chárter damos a conocer el problema con el proceso de monitoreo continuo de vulnerabilidades de la empresa Mibanco, el cual se debe realizar todos los meses como una exigencia por parte del corporativo, pero más aún como estrategia interna para mantener seguros los activo de información de Mibanco, porque es bien sabido que toda empresa tiene la necesidad de cuidar la ciberseguridad, dado que cualquier punto débil de un sistemas puede ser aprovechado por amenazas externas. Es por ello que nos centraremos en mitigar uno, el más común vector de ataque (ruta o camino que utiliza un atacante para tener acceso al activo objetivo).

Para este proceso se deben tener en cuenta varios pasos como son:

- El correcto inventario de activos de la información con su respectiva criticidad.
- El descubrimiento de vulnerabilidades para cada activo del inventario.
- La criticidad de cada vulnerabilidad detectada.
- La remediación y/o el plan de acción.

En nuestro caso varios de los pasos listados se realizan de manera manual, donde la evaluación constante de las vulnerabilidades llega a ser una tarea titánica, la parte del proceso que toma la mayor cantidad de tiempo es el descubrimiento, ya que en este paso se tiene que realizar un proceso de activo por activo tomando cantidad de horas hombre para llegar al objetivo, luego se tiene que priorizar los activos para su posterior remediación que en muchos de los casos cuando se llega a realizar este, el activo ya tiene nuevas brechas reportadas por el fabricante.

La propuesta de solución que proponemos en el presente proyecto, es automatizar varios de los pasos del proceso en estudio, de esta manera se obtendrá las siguientes mejoras:

- Contar con un inventario automatizado y en línea.
- Descubrimiento de vulnerabilidades de manera automática.
- Priorización de los activos para su remediación posterior.
- Remediación inmediata o programada al descubrimiento de la vulnerabilidad.
- Dashboard con información importante (reportes dinámicos de alto nivel) para la Gerencia de Operaciones de Seguridad Tecnológica.

• POSICIONAMIENTO

• PLANTEAMIENTO DEL PROBLEMA

El campo de acción se da en el proceso de Monitoreo Continuo de Vulnerabilidades de la empresa Mibanco, en la Gerencia de Operaciones de Seguridad Tecnológica. La finalidad es la de alcanzar los niveles de protección requeridos haciendo uso del conocimiento y la tecnología, entendiendo las motivaciones y técnicas empleadas por los atacantes, detectando rápidamente las infracciones o ataques en activo y construyendo las capacidades técnicas y humanas necesarias para responder con eficacia y celeridad ante cualquier brecha o incidente, con el fin de minimizar la ventana de ataques y las consecuencias de los mismos.

Problema en el proceso de Monitoreo Continuo de Vulnerabilidades de la empresa Mibanco, se encontraron los siguientes problemas:

- Inventario de activos, actualmente se toma muchos días en tener un inventario de los activos de información.
- Monitoreo de vulnerabilidades, esta actividad a la fecha se realiza de manera manual causando demora en la detección de vulnerabilidades, del mismo modo el análisis de los activos afectados por las vulnerabilidades y su corrección futura.
- Corrección de vulnerabilidades, esta actividad se realiza de manera manual luego de haber realizado un previo análisis, disponibilidad del parche y la criticidad asociada a la vulnerabilidad

Causas, las causas que originan los problemas encontrados en el proceso de Monitoreo Continuo de Vulnerabilidades de la empresa Mibanco, son las siguientes:

- Activos de información dispersos en muchas oficinas a nivel nacional, no se encuentra centralizado en un solo ambiente físico.
- Constante incremento de intrusos que tratan de encontrar vulnerabilidades en los sistemas para poder ingresar y extraer información.

- FLUJO DEL PROCESO

Ilustración 60 – Proceso Monitoreo continuo de vulnerabilidades

Ilustración 61 – Sub Proceso Analizar vulnerabilidades

Ilustración 62 – Sub Proceso Verificar/Actualizar Inventario de Actividades

Problema	Causas
Inventario de activos	<ul style="list-style-type: none"> • Grandes cantidades de activos de información • Ubicación de los activos de información • Acceso físico a los activos de información
Monitoreo de vulnerabilidades	<ul style="list-style-type: none"> • Proceso manual • Incremento de intrusos que buscan vulnerabilidades en los sistemas
Corrección de vulnerabilidades	<ul style="list-style-type: none"> • Proceso manual <ul style="list-style-type: none"> ○ Priorización de activos para su revisión ○ Criticidad de la vulnerabilidad • Búsqueda de disponibilidad de parche

• OBJETIVOS

• OBJETIVO GENERAL

El objetivo general es proponer una solución web que de soporte a la mejora del proceso de gestión de vulnerabilidades de los activos de información para asegurar el cumplimiento de las políticas y normas de seguridad de la empresa, en relación al cumplimiento del corporativo basados en la FFIEC – Cybersecurity Assessment Tool 2015 y la Política General de Seguridad de la información que está alineada a las sentencias FFIEC. Con la mejora propuesta se encaminará al cumplimiento de la sentencias FFIEC.

• OBJETIVOS ESPECÍFICOS

- Elaborar un análisis de la situación del proceso actual de Monitoreo Continuo de Vulnerabilidades en la gestión de seguridad informática.
- Elaborar el diseño de una solución Web alojada en un entorno Cloud como un IaaS para resolver los problemas encontrados en el proceso de Monitoreo Continuo de Vulnerabilidades y permita a la organización identificar las oportunidades de mejora, así como poder cumplir con las sentencias del FFIEC.
- Elaborar una arquitectura de acuerdo a las necesidades del proceso que permitan el cumplimiento de los principios del proceso, descubrir, detectar, responder y prevenir.

- Validar que la propuesta de la solución satisfaga las necesidades identificadas del proceso de Monitoreo continuo de vulnerabilidades.

• INDICADORES DE ÉXITO

El cumplimiento de los objetivos del proyecto se mide a través de los siguientes indicadores de logro:

Indicador de éxito		Objetivo
01	Acta de aprobación sobre el resultado del análisis de la situación actual del proceso de Monitoreo Continuo de Vulnerabilidades, por el experto empresarial	Aprobado
02	Acta de aprobación por el diseño planteado para la solución a los problemas del proceso de Monitoreo Continuo de Vulnerabilidades, por el experto de arquitectura	Aprobado
03	Acta de aprobación sobre la propuesta de solución para la mejora del proceso de Monitoreo Continuo de Vulnerabilidades, por el patrocinador	Aprobado

• ALCANCE DEL PROYECTO

El alcance del proyecto se basa en el desarrollo de un diseño para la propuesta de implementación de un software tipo IaaS (Infrastructure as a Service) que apoye en la mejora sustancial al proceso de monitoreo continuo de vulnerabilidades, basado en los estándares de Mibanco para así descubrir, detectar, responder y prevenir las brechas de seguridad de los activos de información con mayor eficiencia. Como parte del proyecto se realizará los siguientes entregables:

- Análisis de arquitectura empresarial Zachman
- Análisis de requerimientos
- Diagramas de caso de uso
- To-Be del proceso de monitoreo de vulnerabilidades
- Diagrama de arquitectura TO-BE de RED
- Diagrama de arquitectura Layered
- Diagrama de arquitectura usando C4
- Diseño de Mockups

- No se desarrollará la puesta en marcha del proyecto

- **IMPACTO EN LA ORGANIZACIÓN**

- **BENEFICIO TANGIBLE**

- Contar con un inventario de activos de información en línea y clasificado por tipo de activo.
- Detección automática de vulnerabilidades en los sistemas de los activos de información de manera inmediata.
- Actualización automática e inmediata de vulnerabilidades detectadas en los activos de información.
- Reducción de 83% en el tiempo de revisión de vulnerabilidad del total de activos críticos.

- **BENEFICIO INTANGIBLE**

- Contar con información oportuna que ayudará en la toma de decisiones y mejorar la planificación estratégica de la Gerencia.

- **ORGANIZACIÓN DEL PROYECTO**

- **EQUIPO DEL PROYECTO**

El organigrama del proyecto es:

El equipo del proyecto estará conformado por:

Rol	Miembro	Responsabilidades
Patrocinador	Gerente de la empresa	Aprobar el Acta de Constitución Aprobar el cierre del proyecto
Jefe de proyecto	Igmar León	Gestionar el buen desarrollo del proyecto desde la fase de inicio hasta el cierre Entregar todos los entregables resultado de la fase de análisis del proyecto Entregar todos los entregables resultado de la fase del diseño del proyecto
Líder Técnico Arquitectónico	Pablo Medina	Participar y verificar los entregables resultado de la fase de análisis Participar y verificar los entregables resultado de la fase de diseño Participar en toda la gestión del proyecto
Experto Empresarial	Asesor arquitectura empresarial	Aprobar los entregables de la fase de análisis
Experto de Arquitectura	Asesor arquitectura	Aprobar los entregables de la fase de análisis Aprobar los entregables de la fase de diseño
Experto en Gestión de Proyectos	Asesor en Gestión de proyectos	Aprobar los entregables de la fase de gestión del proyecto

• INTERESADOS

Stakeholders	Necesidades	Entregables
Gerente de arquitectura de TI de Mibanco	Analizar la propuesta de la arquitectura de la mejora del proceso	Arquitectura To-Be
Gerente de operaciones de seguridad tecnológica de Mibanco	Mejorar la eficiencia en el proceso de monitoreo de vulnerabilidades	To-Be del proceso

• FASES E HITOS DEL PROYECTO

Las Fases e Hitos de control de entregables, las fases deben estar alineadas a la metodología de desarrollo y/o implementación, de preferencia considerar el PMBOK.

FASE		HITO	ENTREGABLE
Inicio		Aprobación Project Chárter	Project Chárter
Planificación		Aprobación del alcance del proyecto	Plan de proyecto
Ejecución	Análisis de la situación actual	Aprobación del análisis de la situación actual del proceso y propuesta de mejora	Análisis Zachman nivel 1 Diagrama y características de procesos (AS-IS) Diagrama y características de procesos (TO-BE)
	Diseño de la arquitectura a desarrollar	Aprobación del diseño de la arquitectura	Lista de requerimientos Diagrama de Casos de Uso de Sistema Modelo C4: - Diagrama de Contexto de

			<ul style="list-style-type: none"> - Diagrama de Contenedores - Diagrama de Componentes - Diagrama de Código
	Elaboración de Especificaciones de Casos de Uso de Sistema y prototipos	Aprobación de los ECUS y Prototipos	ECUS Prototipo de pantallas
Cierre		Aprobación de sustentación	Documento de Tesis

• ENFOQUES DEL TRABAJO

El presente trabajo para su fase de Análisis usará los frameworks TOGAF Y ZACHMAN, así incrementar la madurez de la solución de la arquitectura empresarial de la organización y el valor que aporta al negocio. Del mismo modo se hará uso de BPMN para el modelado del proceso a mejorar.

Usaremos la metodología RUP para el análisis y diseño de la propuesta de mejora del proceso en estudio.

Para el diseño de la arquitectura haremos uso del modelo C4, el cual nos permitirá describir la arquitectura de software a proponer.

Finalmente usaremos la guía del PMBOK para la gestión de proyectos.

La gestión de este proyecto será basado bajo el enfoque predictivo o en cascada, los entregables se elaborarán de manera secuencial y en un orden específico.

• RIESGOS

Se ha mapeado los siguientes riesgos que pueden impactar el éxito del proyecto:

ID	Fecha Registro	Riesgo	Descripción Riesgo	Probabilidad	Impacto	Probabilidad x Impacto	Respuesta	Estrategia	Estado
R001	15/05/2020	Ausencia de uno de los integrantes	Debido a la coyuntura que se viene pasando, es posible que uno de los integrantes del equipo de proyectos se pueda enfermar con el virus de Covid19	0.50	0.20	0.10	Mitigar	Se debe contar con un repositorio centralizado, para que cualquier integrante del equipo pueda continuar	Activo
R001	15/05/2020	Falta de energía eléctrica	Debido a la coyuntura, el trabajo se viene realizando desde los hogares de los integrantes, es posible que en el lugar donde se encuentre la empresa de servicios realice un mantenimiento al servicio de energía eléctrica	0.10	0.10	0.01	Mitigar	Reprogramar reuniones virtuales, usar horas extras para ponerse a fecha	Activo
R001	15/05/2020	Reestructuración en la organización	Debido a la coyuntura, muchas organizaciones vienen reestructurando al personal, es posible que esta reestructuración se presente en la organización propuesta	0.30	0.40	0.12	Mitigar	Reunión con el nuevo equipo y presentar el proyecto y el avance en el que se encuentra	Activo

ID	Fecha Registro	Riesgo	Descripción Riesgo	Probabilidad	Impacto	Probabilidad x Impacto	Respuesta	Estrategia	Estado
R001	15/05/2020	Cambio inesperado en el alcance del proyecto	Cambio que se pueda presentar luego de haber presentado el plan del proyecto, pero este cambio sería muy importante para la empresa el cual afectaría el costo, tiempo y alcance	0.10	0.40	0.04	Aceptar	Dar a conocer al Patrocinador que el cambio moverá el cronograma	Activo

• REFERENCIAS

Guía del PMBOK

• APROBACIÓN

Nombre	Cargo	Firma
Patrocinador	Gerente de operaciones de seguridad tecnológica de Mibanco	

12.2 Anexo N° 02 Formato de Informe de Avance

INFORME DE AVANCE SEMANA N° X

SECCIÓN 1. INFORMACIÓN GENERAL

Código y Nombre del Proyecto	Fecha del Reporte
NONBRE DEL PROYECTO	DD/MM/YYYY
Elaborado por:	
Jefe de Proyecto	

SECCIÓN 2. RESUMEN

1. TIEMPO

2. PRESUPUESTO

Aprobado (S/.)	Comprometido (S/.)	Ejecutado (S/.)	Disponible (S/.)
25 k	25 k	26 K	0 M

3. RECURSOS

100%

4/4 Miembros

4. PROBLEMAS Y RIESGOS

P

R

0	0	0
0	0	1

SECCIÓN 3. AVANCES Y PENDIENTES

Cronograma

Fase	% Avance Real	Inicio Planificado	Fin Planificado
Fase XX	100%	DD/MM/YYYY	DD/MM/YYYY
Hito: 1	100%	DD/MM/YYYY	DD/MM/YYYY
Hito: 2	100%	DD/MM/YYYY	DD/MM/YYYY
Fase XX	0%	DD/MM/YYYY	DD/MM/YYYY
Hito: 2	0%	DD/MM/YYYY	DD/MM/YYYY

Indicadores

CPI	-
SPI	-

Actividades relevantes / Hitos de la semana

Dom Indicar las actividades de las semana

DD/MM/YYYY al

Sab

DD/MM/YYYY

Próximos Pasos (La siguiente semana)

Dom Indicar las actividades de la próxima semana

DD/MM/YYYY

al Sab

DD/MM/YYYY

SECCIÓN 5. RIESGOS E INCIDENTES

Riesgo o Incidente	Acciones	Responsable	Fecha	Estado
Indicar el riesgo o incidentes	Acciones realizadas	Jefe de Proyecto	DD/MM/YYYY	Identificado/En proceso/Cerrado

12.3 Anexo N° 03 Formato de Solicitud de Control de Cambio

SOLICITUD DE CONTROL DE CAMBIOS N° X

SECCIÓN 1. INFORMACIÓN GENERAL

Código y Nombre del Proyecto	Fecha de Solicitud
Propuesta de mejora del proceso de Monitoreo Continuo de Vulnerabilidades	29/06/2020
Promotor de cambio:	
Solicitante: Líder Técnico Arquitectónico	
Equipo Evaluador:	
Equipo de Proyecto "Propuesta de mejorar del proceso Análisis continuo de vulnerabilidades"	
Comunicador:	
Jefe de Proyectos	

SECCIÓN 2. TIPOS DE CAMBIOS

Cambio de Costos
Justificación de cambio de costos ya establecidos, con referente a mano de obra
Cambio de Alcance
Justificación de cambio de alcance, que impacte directamente en el proyecto, como cambio de una herramienta, que pueda interesar a algún Stakeholder
Cambio de Tiempo
Justificación de cambio de cronograma, establecido por la línea base, ya sea solo por la mitigación de un riesgo, no se aceptara retrasos por riesgos no indicados previamente.

SECCIÓN 3. EVALUACIÓN

Observaciones del Equipo evaluador
1.- Observación 1..... 2.- Observación 1..... 3.- Observación 1..... 4.- Observación 1.....
Resultado
Rechazado/En revisión(Se debe levantar las observaciones)/Aprobado

12.4 Anexo N° 04 Carta de Solicitud para Uso de Información de la Empresa Objetivo

Lima 15 de Junio 2020

Señores
MiBanco
Av. República de Panamá 4575 – Surquillo

Presente.-

SOLICITUD: DE USO DE INFORMACIÓN PARA DESARROLLO DE TESIS

Por medio de la presente, tengo a bien comunicarle que me encuentro cursando el programa de actualización profesional 22 de la carrera de Ingeniería Sistemas de Universidad Peruana de Ciencias Aplicadas - UPC, para optar al título de Ingeniería de Sistemas por medio de la cual solicito a su autoridad poner en consideración la aprobación del uso de información corporativa para el desarrollo de la tesis, que tiene como finalidad mejorar un proceso interno de Mibanco.

La información a utilizar sería desde información pública (nombre, imagen, logo) información privada (objetivos empresariales de alto nivel, organigrama, mapa de proceso de alto nivel, proceso objetivo), no se utilizarán ninguna base de datos, IP y cualquier información que pueda afectar la seguridad y confidencialidad de Mibanco, si se requiere alguna información adicional se solicitará a la gerencia respectiva donde se indicará el uso y si requiere algún tipo de enmascaramiento se aplicará, caso contrario se asumirán datos públicos teóricos.

"Mejora del proceso de monitoreo continuo de vulnerabilidades "

Autor: Medina Ampuero, Pablo Jorge

DNI: 40581200

Coautor: León Vidalón, Igmarr

DNI: 29718456

La tesis tiene los siguientes objetivos:

Objetivo General.

Desarrollar mejoras al proceso de monitoreo de vulnerabilidades a cargo de la Gerencia de Operaciones de Seguridad Tecnológica bajo metodologías de gestión de procesos de negocio, tendencias en arquitectura de software con el soporte de metodologías ágiles de gestión de proyectos TI. Con el objetivo de analizar el proceso y proponer mejoras soportadas en sistemas de información para la recopilación y validación de vulnerabilidades y así otorgar visibilidad del status actual, para garantizar el cumplimiento de lineamientos y políticas.

Objetivos Específicos.

Análisis del contexto empresarial

Análisis del proceso actual

Propuesta de solución para mejora de proceso

Propuesta de software de Automatización de monitoreo de vulnerabilidades

Por lo expuesto, Ruego a usted pueda acceder a mi solicitud.

Pablo Jorge Medina Ampuero
Arquitecto de seguridad
DNI:40581200

12.5 Anexo N° 05 Correo de Aceptación de Empresa Objetivo: Cumplimiento

Saturday, August 1, 2020 at 11:58:40 Peru Standard Time

Asunto: RE: Solicitud de Aprobación de uso de información para Tesis de ingeniería de Sistemas UPC
Fecha: lunes, 22 de junio de 2020, 12:34:27 hora estándar de Perú
De: Cumplimiento
A: Pablo Jorge Medina Ampuero
CC: [REDACTED]
Datos adjuntos: image001.jpg, image002.jpg

Estimad@:

A su solicitud, se evaluó el alcance de la información requerida para llevar a cabo el proyecto de tesis que se indica en la referencia, encontrando viable el pedido.

En ese sentido, conforme por el frente de Cumplimiento.

Para mayor información puede consultar en la intranet la Política Corporativa de Protección de Datos Personales y las políticas del Sistema de Gestión de Seguridad de la Información.

Para cualquier consulta adicional, por favor comunicarse con Diana Binasco.

Saludos,

Cumplimiento
Sede Principal | Av. República de Panamá 4575 – Surquillo

De: Pablo Jorge Medina Ampuero <pablo.medina.a@mibanco.com.pe>

Enviado el: lunes, 15 de junio de 2020 11:04

Para: Cumplimiento <cumplimiento@mibanco.com.pe>

Asunto: Solicitud de Aprobación de uso de información para Tesis de ingeniería de Sistemas UPC

Estimados

Por medio de la presente, tengo a bien comunicarle que me encuentro cursando el programa de actualización profesional 22 de la carrera de Ingeniería Sistemas de Universidad Peruana de Ciencias Aplicadas - UPC, para optar al título de Ingeniería de Sistemas por medio de la cual solicito a su autoridad poner en consideración la aprobación del uso de información corporativa para el desarrollo de la tesis, que tiene como finalidad mejorar un proceso interno de Mibanco.

La información a utilizar sería desde información pública (nombre, imagen, logo) información privada (objetivos empresariales de alto nivel, organigrama, mapa de proceso de alto nivel, proceso objetivo), no se utilizarán ninguna base de datos, IP y cualquier información que pueda afectar la seguridad y confidencialidad de Mibanco, si se requiere alguna información adicional se solicitará a la gerencia respectiva donde se indicará el uso y si requiere algún tipo de enmascaramiento se aplicará, caso

Page 1 of 2

contrario se asuman datos publicos teoricos.

Tema:

“Mejora del proceso de monitoreo continuo de vulnerabilidades ”

Empresa: Mibanco.

Autor: Medina Ampuero, Pablo Jorge

DNI: 40581200

Codigo UPC: U611967

Coautor: León Vidalón, Igmar

DNI: 29718456

Codigo UPC: U412747

Objetivo General.

Desarrollar mejoras al proceso de monitoreo de vulnerabilidades a cargo de la Gerencia de Operaciones de Seguridad Tecnológica (TISO) bajo metodologías de gestión de procesos de negocio, tendencias en arquitectura de software con el soporte de metodologías ágiles de gestión de proyectos TI. Con el objetivo de analizar el proceso y proponer mejoras soportadas en sistemas de información para la recopilación y validación de vulnerabilidades y así otorgar visibilidad del status actual, para garantizar el cumplimiento de lineamientos y políticas.

Objetivos Específicos.

Análisis del contexto empresarial

Análisis del proceso actual

Propuesta de solución para mejora de proceso

Propuesta de software de Automatización de monitoreo de vulnerabilidades

Espero pueda acceder a nuestra solicitud

Por lo expuesto, Ruego a usted pueda acceder a mi solicitud.

Adjunto Documentos

Solicitud dirigida a Mibanco. : Solicitud Firmada.pdf

Solicitud dirigida a Gerente TISO: Correo_Solicitud_TISO_ [REDACTED]

Solicitud dirigida a Gerente Arquitectura Tecnológica:

Correo_Solicitud_Arquitectura_Tecnologica_ [REDACTED]

Aprobación de coordinador de Ingeniería de Sistemas UPC: Solicitud UPC de aprobación de Tema de Tesis PAP.pdf

Estare atento a su comentarios

Saludos,

Pablo Medina Ampuero

Arquitecto de Seguridad

Cel: 987 307 400

www.mibanco.com.pe

12.6 Anexo N° 06 Correo de Aceptación de Empresa Objetivo: Relaciones institucionales.

De: Alvaro Daniel Marcos Mauricio alvaro.marcos.m@mibanco.com.pe
Asunto: RE: Solicitud de Aprobación de uso de información para Tesis de Ingeniería de Sistemas UPC
Fecha: 10 de agosto de 2020, 20:32
Para: Pablo Jorge Medina Ampuero pablo.medina.a@mibanco.com.pe

Estimado Pablo,
De acuerdo con tu solicitud, adjuntamos la autorización.
Slds

De: Pablo Jorge Medina Ampuero <pablo.medina.a@mibanco.com.pe>
Enviado el: lunes, 10 de agosto de 2020 12:43
Para: Alvaro Daniel Marcos Mauricio <alvaro.marcos.m@mibanco.com.pe>
Asunto: FW: Solicitud de Aprobación de uso de información para Tesis de Ingeniería de Sistemas UPC

Estimado Alvaro

Por medio de la presente, tengo a bien comunicarle que me encuentro cursando el programa de actualización profesional 22 de la carrera de Ingeniería Sistemas de Universidad Peruana de Ciencias Aplicadas - UPC, para optar al título de Ingeniería de Sistemas por medio de la cual solicito a su autoridad poner en consideración la aprobación del uso de información corporativa para el desarrollo de la tesis, que tiene como finalidad mejorar un proceso interno de Mibanco.

La información a utilizar sería desde información pública (nombre, imagen, logo) información privada (objetivos empresariales de alto nivel, organigrama, mapa de proceso de alto nivel, proceso objetivo), no se utilizarán ninguna base de datos, IP y cualquier información que pueda afectar la seguridad y confidencialidad de Mibanco, si se requiere alguna información adicional se solicitará a la gerencia respectiva donde se indicará el uso y si requiere algún tipo de enmascaramiento se aplicará, caso contrario se asumirán datos públicos teóricos.

Al respecto, de manera expresa por favor podríamos autorizar que dicha información pase a ser de carácter pública dentro de los fines académicos que son propios de la naturaleza de este tipo de trabajos, entre los cuales está su publicación, una vez concluido el mismo, en el repositorio de la Universidad Peruana de Ciencias Aplicadas.

Tema:
"Mejora del proceso de monitoreo continuo de vulnerabilidades "
Empresa: Mibanco.

Autor: Medina Ampuero, Pablo Jorge
DNI: 40581200 Código UPC: U611967
Coautor: León Vidalón, Igmar
DNI: 29718456 Código UPC: U412747

Objetivo General.

Desarrollar mejoras al proceso de monitoreo de vulnerabilidades a cargo de la Gerencia de Operaciones de Seguridad Tecnológica (TISO) bajo metodologías de gestión de procesos de negocio, tendencias en arquitectura de software con el soporte de metodologías ágiles de gestión de proyectos TI. Con el objetivo de analizar el proceso y proponer mejoras soportadas en sistemas de información para la recopilación y validación de vulnerabilidades y así otorgar visibilidad del status actual, para garantizar el cumplimiento de lineamientos y políticas.

Objetivos Específicos.

Análisis del contexto organizacional

Análisis del contexto empresarial
Análisis del proceso actual
Propuesta de solución para mejora de proceso
Propuesta de software de Automatización de monitoreo de vulnerabilidades
Publicación de la tesis en el repositorio de la UPC
Por lo expuesto, Ruego a usted pueda acceder a mi solicitud.

Saludos,

Pablo Medina Ampuero
Arquitecto de Seguridad
Cel: 987 307 400
www.mibanco.com.pe

De: Cumplimiento <cumplimiento@mibanco.com.pe>

Fecha: lunes, 22 de junio de 2020, 12:34

Para: Pablo Jorge Medina Ampuero <pablo.medina.a@mibanco.com.pe>

Asunto: RE: Solicitud de Aprobación de uso de información para Tesis de ingeniería de Sistemas UPC

Estimad@:

A su solicitud, se evaluó el alcance de la información requerida para llevar a cabo el proyecto de tesis que se indica en la referencia, encontrando viable el pedido.

En ese sentido, conforme por el frente de Cumplimiento.

Para mayor información puede consultar en la intranet la Política Corporativa de Protección de Datos Personales y las políticas del Sistema de Gestión de Seguridad de la Información.

Para cualquier consulta adicional, por favor comunicarse con Diana Binasco.

Saludos,

Cumplimiento
Sede Principal | Av. República de Panamá 4575 – Surquillo

12.7 Anexo N° 07 Carta de Aceptación de Empresa Objetivo: Relaciones institucionales.

Lima, 10 de agosto de 2020

Señor,
Pablo Jorge Medina Ampuero
Presente,

Estimado Jorge,

Hemos recibido la solicitud para la publicación de tu tesis de grado “Mejora del proceso de monitoreo continuo de vulnerabilidades” en el repositorio de la Universidad Peruana de Ciencias Aplicadas, donde vienes cursando el programa de actualización profesional 22 de la carrera de Ingeniería de Sistemas para optar por el título de Ingeniero de Sistemas.

En la misma solicitud, nos indicas que no se utilizará información que pueda afectar la seguridad y confidencialidad de Mibanco, y en caso lo requieras, esta nos las solicitaras, indicando su uso y fines.

Al respecto y luego de las evaluaciones que hemos realizado, consideramos viable autorizar la publicación de tu tesis con carácter público, siempre que su uso sea únicamente con fines académicos.

Atentamente,

Alvaro Marcos Mauricio
Gerente de Relaciones Institucionales

12.8 Anexo N° 08 Declaración Jurada Igmarr León Vidalón

DECLARACIÓN JURADA

Yo, Igmarr León Vidalón, con
código de alumno U412747, de la Carrera de Ingeniería de Sistemas,
de la Facultad de Ingeniería, autor ☒ coautor ☐ de la Tesis ☐ del Trabajo
de Suficiencia Profesional ☐ Trabajo de Investigación ☐, titulada:

MEJORA AL PROCESO DE MONITOREO CONTINUO DE

VULNERABILIDADES

DECLARO BAJO JURAMENTO QUE:

1. El título y contenido del trabajo desarrollado, es auténtico y las citas mencionan de forma clara y exacta su origen o autor, tanto en el cuerpo del texto, ilustraciones, cuadros, tablas u otros elementos que estén protegidos por el Derecho de Autor o Propiedad Intelectual, habiendo tenido la diligencia debida para su uso.
2. El trabajo se basa en información de una persona jurídica pública o privada:

SI ☒

NO ☐

La persona jurídica pública o privada tiene conocimiento de la información a ser utilizada en la elaboración del trabajo que motiva la presente Declaración y ha autorizado expresamente, de acuerdo a la carta que se adjunta en original, que la información pase a ser de carácter pública dentro de los fines académicos que son propios de la naturaleza de este tipo de trabajos, dentro de los cuales está su publicación, una vez concluido el trabajo, en el repositorio de la Universidad Peruana de Ciencias Aplicadas.

En este sentido, soy consciente de que el hecho de no respetar los derechos de autor, no tener el consentimiento de la empresa objeto de estudio y/o consignar información falsa, me sujeta a los alcances de lo establecido en el artículo 411° del Código Penal, concordante con el artículo 32° de la Ley N° 27444, Ley del Procedimiento Administrativo General, Política de Protección de la Propiedad Intelectual de la Universidad y demás normas internas aplicables.

Lima, 10 de Agosto de 2020.

Nombre: Igmarr León Vidalón
DNI: 29718456

12.9 Anexo N° 09 Declaración Jurada Pablo Jorge Medina Ampuero

DECLARACIÓN JURADA

Yo, Pablo Jorge Medina Ampuero, con
código de alumno u611967, de la Carrera de Ingeniería de Sistemas,
de la Facultad de Ingeniería, autor ☒ coautor ☐ de la Tesis ☒ del Trabajo
de Suficiencia Profesional ☐ Trabajo de Investigación ☐, titulada:
MEJORA AL PROCESO DE MONITOREO CONTINUO DE VULNERABILIDADES

DECLARO BAJO JURAMENTO QUE:

1. El título y contenido del trabajo desarrollado, es auténtico y las citas mencionan de forma clara y exacta su origen o autor, tanto en el cuerpo del texto, ilustraciones, cuadros, tablas u otros elementos que estén protegidos por el Derecho de Autor o Propiedad Intelectual, habiendo tenido la diligencia debida para su uso.
2. El trabajo se basa en información de una persona jurídica pública o privada:

SI ☒

NO ☐

La persona jurídica pública o privada tiene conocimiento de la información a ser utilizada en la elaboración del trabajo que motiva la presente Declaración y ha autorizado expresamente, de acuerdo a la carta que se adjunta en original, que la información pase a ser de carácter pública dentro de los fines académicos que son propios de la naturaleza de este tipo de trabajos, dentro de los cuales está su publicación, una vez concluido el trabajo, en el repositorio de la Universidad Peruana de Ciencias Aplicadas.

En este sentido, soy consciente de que el hecho de no respetar los derechos de autor, no tener el consentimiento de la empresa objeto de estudio y/o consignar información falsa, me sujeta a los alcances de lo establecido en el artículo 411° del Código Penal, concordante con el artículo 32° de la Ley N° 27444, Ley del Procedimiento Administrativo General, Política de Protección de la Propiedad Intelectual de la Universidad y demás normas internas aplicables.

Lima, 04 de Agosto de 2020.

Nombre: Pablo Jorge Medina Ampuero
DNI: 40581200

12.10 Anexo N° 10 Correo de Aceptación de la Solución: Gerencias TISO.

Tuesday, August 11, 2020 at 12:37:43 Peru Standard Time

Asunto: Re: Solicitud de Aprobación de mejora al proceso Monitoreo recurrente de vulnerabilidades.
Fecha: lunes, 10 de agosto de 2020, 12:03:12 hora estándar de Perú
De: Guiuliana Krystal Roca Chunga
A: Pablo Jorge Medina Ampuero
Datos adjuntos: image001.png, image002.png, image003.png, image004.jpg

De acuerdo

Obtener [Outlook para iOS](#)

De: Pablo Jorge Medina Ampuero <pablo.medina.a@mibanco.com.pe>
Enviado: Monday, August 10, 2020 11:44:03 AM
Para: Guiuliana Krystal Roca Chunga <guiuliana.roca.c@mibanco.com.pe>
Asunto: Solicitud de Aprobación de mejora al proceso Monitoreo recurrente de vulnerabilidades.

Estimada Guiuliana

A continuación envío para su aprobación, los requerimientos del proceso levantado en el proceso de Monitoreo recurrente de vulnerabilidades así como la propuesta de Solución de mejora y la arquitectura propuesta.

Propuesta de Solución

Desarrollar un diseño de propuesta para implementar un software tipo IaaS que apoye en la mejora sustancial del proceso de monitoreo recurrente de vulnerabilidades, basado en los estándares de Mibanco, para así descubrir, detectar, responder y prevenir las brechas de seguridad de los activos de información con mayor eficiencia.

TABLA DE REQUERIMIENTOS FUNCIONALES
RF001_ Escanear activos de información con pruebas de Caja Negra
El sistema debe permitir escaneo automático de vulnerabilidades de activos de información, con pruebas de caja negra (sin usuario y password, solo descubrimiento).
RF002_ Escanear activos de información con pruebas de Caja Blanca
El sistema debe permitir escaneo automático de vulnerabilidades de activos de información, con pruebas de caja blanca (con usuario y contraseña).
RF003_ Priorización de vulnerabilidades automáticas
El Sistema deberá integrar inteligencia de amenazas, para su priorización.
RF004_ Priorización de vulnerabilidades manuales
El Sistema debe permitir modificar manualmente la prioridad de las mismas de acuerdo a los requerimientos del negocio.
RF005_ Detección automática de activos de información

El Sistema debe detectar nuevos activos de información en general y por tipo ingresados a la red.
RF006_Detección manual de activos de información
El Sistema permitirá la detección manual de nuevos activos de información en general y por tipo ingresados a la red.
RF007_Clasificación automática de activos de información
El sistema debe clasificar activos de información por tipo y criticidad.
RF008_Clasificación manual de activos de información
El sistema permitirá la clasificación manual de activos de información, de acuerdo a criterios del usuario.
RF009_Actualizaciones automáticas de activos de información no críticos
El Sistema debe permitir la actualización de sistemas catalogados como no críticos.
RF010_Actualizaciones de activos críticos programados
El Sistema debe permitir programar la actualización de sistemas catalogados como críticos.
RF011_Envío de mensajes de alerta de nueva vulnerabilidad
El Sistema debe permitir el envío automático de mensajes de nuevas vulnerabilidades detectadas en los activos de información, y también mostrarlas en el dashboard.
RF012_Visualización de la descripción y remediación de vulnerabilidades
El sistema deberá mostrar la descripción de vulnerabilidades y los pasos para su remediación.
RF013_Dashboard general personalizable
El Sistema debe permitir la visualización de reportes dinámicos de alto nivel, el cual debe ser personalizable y también detallado por activo de información.
RF014_Indicadores de madurez
El sistema deberá analizar en base a toda la exposición, el nivel de madurez, basado en el tiempo de respuesta y edad de vulnerabilidad
RF015_Métricas de cyber exposición
El sistema deberá generar métricas de exposición en los análisis de vulnerabilidades.

Diagrama de Red propuesto

Diagrama de Contexto 4C

El segundo nivel del modelo 4C diagrama de contenedores, vemos el detalle del Sistema de Análisis Continuo de vulnerabilidades –“SACV”, donde se evidencia cuatro tipos de contenedores: elípticos son los sistemas Core, rectangular los complementarios, hexagonales los de apoyo y la base de datos.

Los contenedores de forma de elipse (Core) son los que se encuentran alineados a los drivers funcionales, los cuales son críticos:

- Inventario: se encarga de la recolección de inventario de activos por medio de los sensores.
- Monitoreo continuo: se encarga de las pruebas de caja negra y caja blanca en conjunto con el sistema de sensores.
- Gestión de vulnerabilidades: encargado de orquestar todo el proceso y donde se encuentra el proceso automatizado de análisis continuo, los otros dos contenedores se comunican con este.
- Actualización de activos: es el encargado de la actualización del sistema operativo soportado en interacción con los otros contenedores Core.

Los contenedores de forma rectangular son los complementarios, aquellos encargados de mostrar alertas y eventos hacia la capa de usuarios, también es un utilitario que se encarga de la administración de usuarios, configuración de conexiones, gestión de log entre otros.

El contenedor hexagonal, será utilizado para garantizar el correcto funcionamiento del sistema, apoyando a diversos contenedores con el manejo de excepciones, con ello se logrará mantener la estabilidad y disponibilidad del sistema.

Saludos,

Pablo Medina Ampuero

Arquitecto de Seguridad

Cel: 987 307 400

www.mibanco.com.pe