



UNIVERSIDAD NACIONAL DE CAÑETE

INFORME FINAL DEL PGCM DEL NEGOCIO BCP

**TRABAJO ELABORADO EN CUMPLIMIENTO
AL CURSO DE AUDITORIA DE SISTEMAS**

DOCENTE: ROSA MENÉNDEZ MUERAS

SAN VICENTE CAÑETE - 2021



UNIVERSIDAD NACIONAL DE CAÑETE



FACULTAD DE INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

AUDITORÍA DE SISTEMAS

INFORME FINAL DEL PGCM DEL NEGOCIO BCP

REALIZADO POR:

**LISETTE GUERRA QUISPE
HUARCAYA DE LA CRUZ LUIS
MATOS ARROYO LUIS
LUDEÑA GUTIÉRREZ RAÚL
PORRAS OROCHE SANDRO**

CAÑETE – LIMA – PERÚ

2021

Contenido

1.	Introducción	4
2.	Objetivo	4
3.	Alcance	5
4.	Bases para el marco del Trabajo	5
4.1.	Generalidades	6
4.1.1.	BCI1 :	6
4.1.2.	DRI INTERNATIONAL2 :	6
4.1.3.	NIST3 :	6
4.1.4.	Norma NTC/ISO 22301	7
4.2.	Base Estratégica	7
4.3.	Base Regulatoria.....	9
4.3.1.	Iso	9
4.3.2.	ISO 22301	10
4.4.	Base Metodológica.....	11
5.	Marco del Trabajo para PGCN.....	14
5.1.	Continuidad del Negocio	14
5.2.	Análisis de Impacto (BIA).....	15
5.3.	Acta de constitución del proyecto	16
5.3.1.	Descripción de la Organización	21
5.3.1.1.	Razón social	21
5.3.1.2.	Localización	21
5.3.1.3.	Breve reseña histórica.....	21
5.4.	Gestión del programa de CN	23
5.4.1.	Gobierno.....	23
5.4.1.1.	Política	23
5.4.1.2.	Estructura	25
5.4.1.3.	Organigrama.....	26
5.4.1.3.1.	División Comercial.....	27
5.4.1.4.	Mapa de Proceso BCP	28

5.4.1.5.	Cadena de Valor	28
5.4.1.6.	Plan Estratégico	29
5.4.1.6.1.	Análisis FODA	29
5.4.1.6.2.	Desarrollo y soporte a los negocios	30
5.5.	Entender de la Organización	37
5.5.1.	Análisis de Impacto (BIA).....	37
5.5.1.1.	Análisis de Riesgos (AR).....	38
5.6.	Establecer de Estrategia de CN	43
5.6.1.1.	Esstrategias pore escenarios	43
5.7.	Desarrollar e implementar la Respuesta de CN	46
5.7.1.	Planes de continuidad del negocio.....	46
5.8.	Probar, Mantener y revisar	47
5.9.	Integrar el PGCN en la cultura de la Organización	49
6.	Anexos	51
6.1.	Glosario de términos.....	51
6.2.	Conclusiones.....	53
6.3.	Recomendaciones	53

1. Introducción

El aumento de las amenazas externas e internas ha llevado a las entidades públicas y empresas privadas como el BCP a considerar la importancia de implementar planes, procedimientos y estructuras que garantizan la continuidad de sus productos y servicios comerciales críticos eventualidades de varias categorías y diferentes niveles de impacto. Estos factores tienen condujo al hecho de que actualmente la presencia de estos planes es un factor común en toda la cadena de suministro de productos y servicios

En el pasado, por supuesto, las amenazas estaban principalmente relacionadas con emergencias. Natural y técnicamente, las amenazas se vuelven cada vez más diferentes en diferentes situaciones. Como terrorismo, huelgas étnicas, globalización y amenazas cibernéticas Muestra la necesidad de incorporar nuevas estrategias para asegurar la continuidad Cara con Los riesgos a los que se enfrenta.

2. Objetivo

El objetivo de esta auditoría es proporcionar seguridad sobre la idoneidad y pertinencia del marco de control de gestión y controles internos establecidos para mantener y poner en funcionamiento el Programa de Planificación de Continuidad en la empresa BCP.

- Proporcionar un enfoque de organización y consolidación dirigidos a la respuesta y recuperación ante una emergencia o interrupción imprevista, evitando confusión y reduciendo la crisis o tensión.

- Reducir el tiempo de recuperación y las probables pérdidas económicas, directas e indirectas, como resultado de una interacción.
- Aumentar la probabilidad de continuar del servicio de presentarse una interrupción

3. Alcance

Gobernanza de la planificación de la continuidad de las operaciones del negocio, controles de gestión del programa BCP, incluidos los controles de gestión diseñados para asegurarse de que los BCP se desarrollen, prueben y actualicen según sea requerido por el banco BCP.

Incluir una evaluación en profundidad de la idoneidad de los BCP para garantizar la continuidad de los servicios en una interrupción.

4. Bases para el marco del Trabajo

Un sistema de gestión se puede entender como una herramienta que ayuda a utilizar los recursos de una empresa en forma eficiente, disminuyendo costos e incrementando su productividad. En ese sentido un sistema de gestión de continuidad del negocio se puede entender como una herramienta que otorga a una empresa la capacidad para seguir brindando los productos y servicios a sus clientes - a un nivel aceptable - luego de haber sufrido un incidente que haya interrumpido sus operaciones. En ese sentido con la presente investigación, se pretende evidenciar que la norma internacional ISO 22301, es la más adecuada para implementar un sistema de Gestión de Continuidad del Negocio.

4.1. Generalidades

4.1.1. BCI1 :

La continuidad del negocio es una colección de procedimientos e información que es desarrollada, compilada y mantenida en preparación para el uso en el evento de una emergencia o desastre.

4.1.2. DRI INTERNATIONAL2 :

La planeación de la continuidad del negocio es el proceso de desarrollar arreglos previos y procedimientos que capaciten a la organización para responder a un evento de tal manera que las funciones críticas del negocio continúen con los niveles planeados de interrupción o cambios esenciales.

4.1.3. NIST3 :

El BCP se enfoca en sostener las funciones de negocio de una organización, durante y después de una interrupción mientras se recupera paralelamente. El BCP se orienta hacia los procesos de negocio. Por su parte, el DRP provee procedimientos detallados para facilitar la recuperación de las capacidades en sitio alternativo. Normalmente está enfocado en Tecnologías de la Información (en adelante TI) y limitado a interrupciones mayores con efectos a largo plazo. Los planes de contingencia representan un amplio espectro de actividades enfocadas a sostener y recuperar servicios críticos de TI después de una emergencia. Debido a que los planes de contingencia deben ser desarrollados para cada

aplicación importante o sistema de soporte, se pueden contar con múltiples planes de contingencia dentro de un BCP.

4.1.4. Norma NTC/ISO 22301

La Gestión de la Continuidad del Negocio (BCM) es un proceso de gestión que identifica amenazas potenciales y riesgos de tipo operacional a la organización y provee una estructura para construir confiabilidad y capacidades para una efectiva respuesta que proteja los intereses de los accionistas, la reputación, la marca y las actividades de creación de valor, también involucra la gestión de la recuperación y continuidad después de un incidente y la gestión de todo el programa por medio de entrenamientos, pruebas, y revisiones para mantener el BCP al día. En la siguiente ilustración se puede observar el ciclo de vida del programa BCM, que inicia en la fase de entendimiento de la organización, luego se definen opciones, se procede a la implementación, se realizan pruebas del plan o planes, su mantenimiento y auditorías tanto internas como externas, y, por último, se debe integrar este ciclo dentro de la cultura organizacional

4.2. Base Estratégica

El plan de continuidad de negocio o BCP está orientado

- a. la protección de las personas, así como al restablecimiento oportuno de los procesos, servicios críticos e infraestructura, frente a eventos de interrupción o desastre.
- b. Todo el personal de la Entidad debe estar entrenado y capacitado en los procedimientos definidos y conocer claramente los roles y responsabilidades que

le competen en el marco de la continuidad del negocio, mediante labores periódicas de formación, divulgación y prueba de los Planes de Continuidad del Negocio.

- c. En caso de presentarse un incidente significativo se deben aplicar los mecanismos de comunicación apropiados, tanto internos como externos
- d. Las etapas del Plan de continuidad deben ser ejecutadas por cada una de las dependencias de la Entidad, con la guía y coordinación de la Oficina de Sistemas e Informática.
- e. Los Jefes de cada dependencia deben designar un Líder de Plan de Continuidad del Negocio, quien es responsable de apoyar las actividades del Programa de Plan de Continuidad de Negocios para la dependencia que representa.
- f. Las diferentes etapas que conforman la fase de Prevención deben ser ejecutadas con la siguiente frecuencia: o El análisis de impacto del negocio debe actualizarse por lo menos una vez al año o cada vez que un Líder de Proceso lo requiera, teniendo en cuenta los cambios de la entidad y sus necesidades. o El monitoreo a los riesgos de continuidad se efectuará de acuerdo a la Guía de Administración de riesgos DC-S-GC-06. o Se debe realizar por lo menos una prueba anual a las estrategias de contingencia definidas.
- g. Los procesos críticos deben ser recuperados dentro de los márgenes de tiempo requeridos en los Planes de Continuidad del Negocio.
- h. Los procesos o servicios de la entidad que sean desarrollados por terceros contratados deben disponer de planes de continuidad, para lo cual el funcionario interventor del contrato debe solicitar este documento y r restablecimiento

oportuno de los procesos, servicios críticos e infraestructura emitirlo a la Oficina de Sistemas e Informática, donde se analizará la cobertura del mismo. Adicionalmente, se debe verificar que los planes, en lo que corresponden a los servicios convenidos, funcionen en las condiciones esperadas, donde la Oficina de Sistemas e Informática debe coordinar con la dependencia responsable del contrato la ejecución de pruebas a dicho plan.

- i. Los planes de contingencia deben mantenerse actualizados, para lo cual se deben desarrollar, probar y de ser necesario mejorar de forma periódica o ante cambios significativos en políticas, personas, proceso, tecnología; siendo necesario que en dicha revisión participen los líderes de los procesos involucrados.

4.3. Base Regulatoria

NORMA	DESCRIPCIÓN
NTC/ISO 22301:2012	Norma Internacional para la gestión de la continuidad del negocio.
Decreto 1078 de 2015	Decreto único Reglamentario del sector TIC en particular las normas atinentes a la estrategia de Gobierno en Línea.

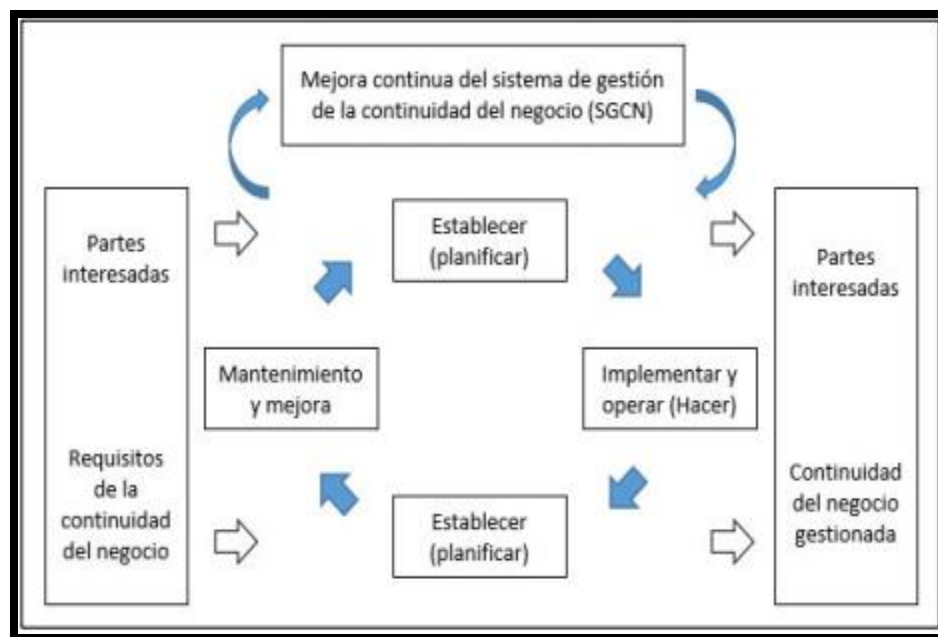
4.3.1. Iso

La ISO, cuya descripción en inglés significa International Organization for Standardization, es una organización que tiene por objetivo la creación de estándares internacionales para las diferentes empresas.

4.3.2. ISO 22301

Se puede describir a la norma ISO 22301, como un estándar que tiene por objetivo describir los requisitos necesarios para la implementación de un sistema de Gestión de Continuidad del Negocio (SGCN). Esta norma toma como referencia el modelo de mejora continua, PDCA por sus siglas en inglés (Plan, Do, Check, Act).

Figure 1 Modelo PDCA aplicado al PGCN



Fuente: Norma Internacional ISO 22301 – Numeral 0.2

Figure 2 Descripción del modelo PDCA aplicado al PGCN

P	Plan (Planificar)	En esta etapa se establece la política de continuidad del negocio, así como sus objetivos, controles, procesos y procedimientos acordes con las políticas y objetivos de la organización.
D	Do (Hacer)	Esta etapa consiste en aplicar la política, controles, procesos y procedimientos de continuidad.
C	Check (Verificar)	Supervisar la efectividad del sistema de gestión considerando los objetivos y política establecidos. Proceder con informar a los niveles correspondientes, y proponer medidas para su corrección y mejora.
A	Act (Actuar)	Mantener y mejorar el SGCN, considerando el resultado de la revisión de la Dirección de la organización.

Fuente: Norma Internacional ISO 22301 – numeral 0.2

Por otra parte, se debe tener en cuenta que cada apartado de la norma ISO 22301, se encuentra relacionado, y en su conjunto conlleva a la implementación del SGCN (ver figura 1). En la figura 2, se puede apreciar que la norma ISO 22301, inicia con identificar el contexto de la organización y las partes interesadas); posteriormente determina los productos y servicios críticos, para luego identificar los procesos asociados a estos productos. Como siguiente paso, se debe realizar el análisis de impacto al negocio, luego realizar la evaluación de riesgos, y posteriormente determinar las estrategias, planes de continuidad, y plan de. Finalmente se debe considerar en la última etapa un sistema de monitoreo como es el caso de auditorías.

4.4. Base Metodológica

La evolución de las compañías en términos de tecnología, sistemas, modelos de estructura, entre tantos otros, ha llevado a generar nuevas maneras de administrar y gestionar sus recursos. Esta evolución también es percibida en los cambios constantes del entorno que traen aparejadas nuevas fuentes de amenazas que

resultan en la ineficacia de algunos procesos que quedan desactualizados en función de los objetivos y misiones de la organización. En la búsqueda de obtener niveles superiores de satisfacción de cliente, es preciso analizar posibles eventos de manera de intentar evitar o al menos minimizar la probabilidad de ocurrencia de estos para asegurar la continuidad del negocio. Para ello, las entidades deben encontrar la manera de responder ante estas anomalías reanudando las actividades en un plazo de tiempo, el cual también será meticulosamente definido, intentando no comprometer la eficiencia y alineado con el objetivo primario de la organización. Se ha hecho referencia a la evolución de los planes de continuidad, haciendo hincapié en los principales referentes del mercado, pero sin dejar de lado los estándares internacionales y recomendaciones de mejores prácticas sobre los cuales se apoya la continuidad del negocio. Se ha descrito la cercanía de las entidades a nivel global, regional y nacional en materia de planes de continuidad aplicados a sus estructuras, tanto para organizaciones en general como para entidades financieras de nuestro país. También se ha desglosado la actualidad de la organización en estudio, mencionando sus características principales, estructura actual y plan de crecimiento, las principales fortalezas y debilidades, como así también las amenazas y oportunidades detectadas en su estructura general y a nivel tecnológico, donde el plan de continuidad hará foco. En otras palabras, con estas herramientas en mano, un marco teórico definido, conociendo y comprendiendo a la organización, buscaremos desarrollar estrategias, elaborar e implementar el plan de continuidad, probarlo y revisarlo con periodicidad.

Como se observará más adelante y tal como lo plantean las mejores prácticas es imprescindible la identificación de las actividades críticas. Aquellas que necesitan restablecerse en periodos cortos de tiempo por su alto impacto en el negocio. Las recomendaciones apuntan a que las organizaciones sean quienes identifiquen y decidan de manera colaborativa qué actividades están consideradas dentro del esquema y estrategia de continuidad y cuáles quedarán excluidas, para luego comunicarlas tanto interna como externamente, de forma de definir el alcance. Así todo, bien definidas las políticas y el alcance, el diagnóstico continúa con la identificación de los recursos claves en la organización, junto con la estructura organizacional presente. Luego, se apunta a detectar los procesos y subprocesos afectados, su relación con los activos, aplicaciones y las dependencias entre sí. Posteriormente, estaremos en condiciones de avanzar en la definición de cuáles de estos son críticos y cuáles deberían no ignorarse en función de la continuidad del negocio, lo cual nos dará pie para analizar el riesgo estableciendo el detalle de amenazas y vulnerabilidades a través de matrices de riesgo. Se hará referencia también a los aspectos analizados dentro del marco normativo, como las observaciones establecidas por el BCRA en el marco de las inspecciones realizadas a la entidad, que atentan contra el BCP. Llegados a este punto, estaremos en condiciones de definir las políticas y el alcance, como así también el objetivo primario del diagnóstico realizado para la elaboración de un plan de continuidad. Expresaremos aquí, las mediciones de nivel de cumplimiento respecto de los estándares incluidos (BCRA A4609 e ISO22301), para cada una de sus secciones. Como parte del tramo final, denominaremos a las dos últimas fases, de desarrollo e implementación, y se caracterizan por la definición de los procedimientos, el lanzamiento del plan, la comunicación hacia todos los sectores involucrados y por último, la verificación y el control de los resultados para luego establecer brechas

existentes. Con base en estos resultados, se podrá establecer un plan de mantenimiento para trabajar sobre las oportunidades de mejora ya sea desde el punto de vista de preventivo o correctivo, intentando sistematizar el proceso, pero teniendo en cuenta las modificaciones o cambios que puedan presentarse en los elementos considerados al origen.

En resumen, considerando los pasos descritos estaremos en condiciones de haber establecido una metodología para el diagnóstico e implementación de un plan de continuidad del negocio, adaptado a la entidad en estudio o entidades financieras afines, considerando el enfoque sistémico y de mejora continua como lo recomienda el estándar ISO 22301:2012 y adaptado a las necesidades críticas y mínimas establecidas en la Comunicación A 4609 de BCRA. La implementación de este permite y requiere de la elaboración de la documentación asociada tal como lo requiere el órgano regulador de entidades financieras (BCRA) y que puede dar pie a saltos de calidad en busca de certificaciones internacionales de calidad y continuidad.

La metodología utilizada para el desarrollo del Plan de Continuidad del Negocio para la Escuela Superior de Administración Pública propone un proceso comprendido desde el inicio del proyecto hasta el mantenimiento del plan. Esta metodología, está apoyada en mejores prácticas a nivel internacional proveniente de reconocidos institutos tales como el BCI, El DRII, NIST, ISO 27001, NFPA 1600, entre otros.

5. Marco del Trabajo para PGCN

5.1. Continuidad del Negocio

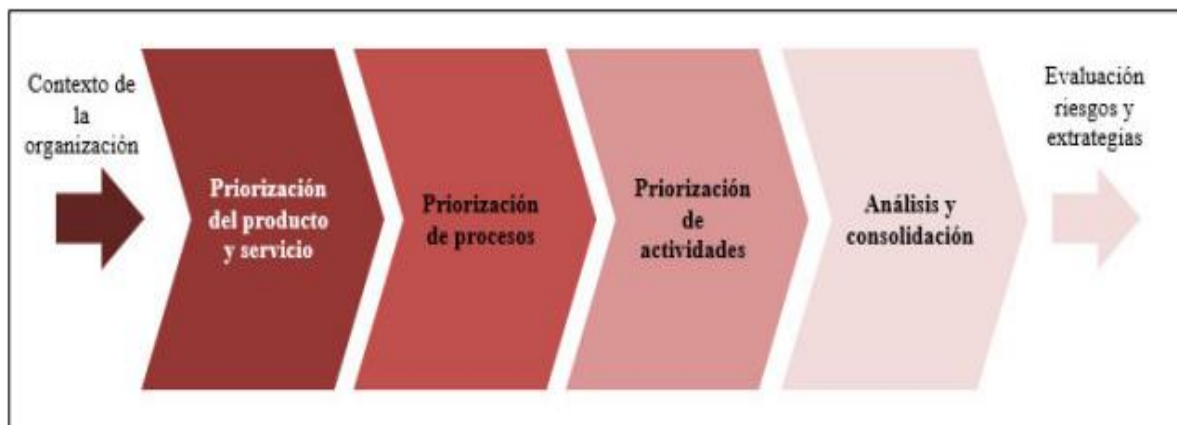
El estándar ISO 22301, define a la continuidad del negocio, como la “capacidad de la organización para continuar realizando la entrega de productos o servicios a niveles

predefinidos aceptables después de un incidente disruptivo”(Iso 22301 2012). Por otra parte, se puede entender que la gestión de continuidad del negocio, es un proceso a través del cual se identifican los riesgos a los cuales está propensa una organización, y el impacto que dichos riesgos podrían ocasionar en caso de interrumpir de forma significativa las operaciones de la empresa; esto a efectos de establecer medidas y lineamientos que permitan aumentar la capacidad de respuesta y resiliencia de la institución a fin de hacer frente a dichos eventos, salvaguardar los intereses de la empresa, así como disminuir posibles pérdidas. Es importante destacar que la continuidad está directamente relacionada al producto o servicio que brinda una organización, para lo cual es crucial identificar los procesos y actividades críticas necesarias para poder brindar dicho producto o servicio; a fin de establecer planes adecuados que permitan reanudar sus procesos y actividades.

5.2. Análisis de Impacto (BIA)

El análisis de impacto al negocio, según describen John W. Rittinghouse, y James F. Ransome en su libro *Business Continuity and Disaster Recovery for Infosec Managers*, es un proceso orientado a identificar funciones críticas para el negocio, y las pérdidas y efectos que se ocasionarían en caso éstos no se encuentren disponibles. En la figura 3 se puede apreciar las etapas de un proceso de análisis de impacto al negocio.

Figure 3 Etapas de un análisis BIA



5.3. Acta de constitución del proyecto

NOMBRE DEL PROYECTO	SIGLAS DEL PROYECTO
Plan de gestión de continuidad de negocio del banco de crédito del Perú	PGCN - BCP
DESCRIPCIÓN DEL PROYECTO:	
<p>El proyecto “Plan de gestión de continuidad del negocio del Banco de Crédito del Perú” Consiste en los procedimientos e instrucciones que una organización debe seguir ante el desastre, ya sea incendios, inundaciones o ciberataques.</p> <p>La implementación ayudará en:</p> <ul style="list-style-type: none"> • Proporcionar un enfoque de organización y consolidación dirigidos a la respuesta y recuperación ante una emergencia o interrupción imprevista, evitando confusión y reduciendo la crisis o tensión. • Reducir el tiempo de recuperación y las probables pérdidas económicas, directas e indirectas, como resultado de una interacción. • Aumentar la probabilidad de continuar del servicio de presentarse una interrupción. <p>El desarrollo del proyecto estará a cargo de:</p> <ul style="list-style-type: none"> • Lisete Guerra Quispe---> Jefe de proyecto • Ludeña Gutierrez • Porras Oroche Sandro • Matos Arroyo Luis • Huarcaya de la Cruz Luis <p>El proyecto iniciará desde el 12-01-2021 hasta el 17-03-2021</p>	

DEFINICIÓN DEL PRODUCTO DEL PROYECTO:

Como producto resultante de este proyecto se obtendrá un plan de gestión para la continuidad del negocio, plan que será implementado en el banco de crédito del Perú.

Este plan contará con:

- El estudio y entendimiento de la organización y su gobierno.
- El análisis de impacto y riesgo.
- Un desarrollo de estrategias por escenario.
- Diversos planes para mitigar los riesgos, recuperar las tecnologías de la información (TI) y restablecer la continuidad del negocio.
- Un seguimiento y evaluación de los indicadores de monitoreo.

DEFINICIÓN DE REQUISITOS DEL PROYECTO:

Información de la estructura organizacional, así como sus procesos, políticas y estrategias.

OBJETIVOS DEL PROYECTO:

CONCEPTO	OBJETIVOS	CRITERIO DE ÉXITO
GOBIERNO	Establece y mantiene actualizado los objetivos y políticas, el alcance, el planeamiento estratégico, la estructura organizacional, el plan operativo y la metodología del programa	Los objetivos y políticas son acordes a la empresa. La estructura organizacional está actualizada.
ENTENDIMIENTO	<ul style="list-style-type: none"> ● Identifica las actividades críticas y sus recursos asociados (personal, equipo, mobiliario, instalaciones, aplicaciones) ● Identifica los riesgos que podrían causar una interrupción de las actividades críticas a fin de mitigarlos mediante la implementación de controles 	<ul style="list-style-type: none"> ● El análisis del impacto de negocio es preciso ● El análisis de riesgo del negocio es preciso

ESTRATEGIAS	<ul style="list-style-type: none"> Define y selecciona las estrategias de respuesta a los eventos que podría causar una interrupción de las actividades críticas y que determinan el enfoque y contenido del Plan de respuesta 	<ul style="list-style-type: none"> Se definen las estrategias para los eventos críticos. Se definen las estrategias para los eventos más probables.
PLANES	<ul style="list-style-type: none"> Desarrolla e implementa los Planes de respuesta específico, que definen las acciones a seguir durante y después de un interrupción de las actividades críticas 	<ul style="list-style-type: none"> Se establece un plan que cumpla el Objetivo del Punto de Recuperación Se establece un plan que cumpla el Objetivo del Tiempo de Recuperación
FINALIDAD DEL PROYECTO:		
Analizar la organización y establecer un plan de gestión para la continuidad del negocio en el banco de credito del Perú		
JUSTIFICACIÓN DEL PROYECTO:		
JUSTIFICACIÓN CUALITATIVA	JUSTIFICACIÓN CUANTITATIVA	
De cara al usuario, cliente y accionista, permite mostrar una empresa planificada ante diversas amenazas.	Permite tener protocolos a seguir en caso de una amenaza.	
	Permite establecer el impacto que ha de tener una amenaza.	

DESIGNACIÓN DEL PROJECT MANAGER DEL PROYECTO		
NOMBRE	Lisette Guerra Quispe	NIVELES DE AUTORIDAD
REPORTA A	Huarcaya de la cruz Luis	Exigir el cumplimiento de entregables del proyecto
SUPERVISA A	Porras Oroche Sandro Ludeña Gutierrez Raul	

CRONOGRAMA DE HITOS DEL PROYECTO	
HITO O EVENTO SIGNIFICATIVO	FECHA PROGRAMADA
Constitucionalización del proyecto	12 - 01 - 2021
Investigación del gobierno de la institución	19 - 01 - 2021
Análisis de impacto del negocio	26 - 01 - 2021
Análisis de riesgo del negocio	03 - 02 - 2021
Desarrollo de estrategias por escenario	10 - 02 - 2021
Desarrollo de planes estratégicos ante diversos eventos	17 - 02 - 2021
Monitoreo y revisión	24 - 02 - 2021
Integración del PCGN en la cultura organizacional	15 - 03 - 2021

ORGANIZACIONES O GRUPOS ORGANIZACIONALES QUE INTERVIENEN EN EL PROYECTO	
ORGANIZACIÓN O GRUPO ORGANIZACIONAL	ROL QUE DESEMPEÑA
Grupo De Auditoría	Brindar la implementación de un plan de continuidad del negocio
Banco de Credito del Peru	Demandante de la implementación de un plan de continuidad del negocio

PRINCIPALES AMENAZAS DEL PROYECTO (RIESGOS NEGATIVOS).

Falta de información y/o acceso a la información organizacional.

Falta de comunicación por el distanciamiento social.

PRINCIPALES OPORTUNIDADES DEL PROYECTO (RIESGOS POSITIVOS).

Asegurar las operaciones ante una situación, interna o externa, que impida el funcionamiento normal de la compañía

LISTA DE INTERESADOS

Banco de crédito del Perú

PRESUPUESTO PRELIMINAR DEL PROYECTO

CONCEPTO	MONTO (US\$)

	Total Línea Base
Reserva de Contingencia	
Reserva de Gestión	
	Total Presupuesto

SPONSOR QUE AUTORIZA EL PROYECTO			
NOMBRE	EMPRESA	CARGO	FECHA
José Esposito	Banco de crédito del Perú	Director de auditoría	12 - 01 - 2021

5.3.1. Descripción de la Organización

5.3.1.1. Razón social

Banco de Crédito del Perú S.A.

5.3.1.2. Localización

Dirección Legal: Calle Centenario N° 156 Urbanización Las Laderas de Melgarejo, La Molina – Lima.

Oficina Principal Lima: Jr. Lampa Esq. Con Ucayali / Mezzanine Op.

5.3.1.3. Breve reseña histórica

Nuestra institución, llamada durante sus primeros 52 años Banco Italiano, inició sus actividades el 9 de abril de 1889, adoptando una política crediticia inspirada en los principios que habrían de guiar su comportamiento institucional en el futuro. El 01 de febrero de 1942, se acordó sustituir la antigua denominación social, por la de Banco de Crédito del Perú. Así, el Banco Italiano, el primero en el país, cerró su eficiente labor después de haber obtenido los más altos resultados de

nuestra institución. Con el propósito de conseguir un mayor peso internacional, instalamos sucursales en Nassau y en Nueva York, hecho que nos convirtió en el único Banco peruano presente en dos de las plazas financieras más importantes del mundo. La expansión de nuestras actividades creó la necesidad de una nueva sede para la dirección central. Con ese fin se construyó un edificio de 30,000 m², aproximadamente, en el distrito de La Molina. Luego, con el objetivo de mejorar nuestros servicios, establecimos la Red Nacional de Tele Proceso, que a fines de 1988 conectaba casi todas las oficinas del país con el computador central de Lima; asimismo, creamos la Cuenta Corriente y Libreta de Ahorro Nacional, e instalamos una extensa red de cajeros automáticos. En 1993, adquirimos el Banco Popular de Bolivia, hoy Banco de Crédito de Bolivia. Un año más tarde, con el fin de brindar una atención aún más especializada, creamos Credifondo, una nueva empresa subsidiaria dedicada a la promoción de los fondos mutuos; al año siguiente establecimos Credileasing, empresa dedicada a la promoción del arrendamiento financiero. Durante los '90, nuestra oficina de representación en Santiago de Chile desarrolló una interesante actividad, dado el notable incremento de los capitales chilenos invertidos en empresas peruanas. La recuperación de los jóvenes talentos que emigraron entre 1970 y 1990 al extranjero, fue otro aspecto importante de esa década. Esos profesionales, sólidamente formados en centros académicos y empresas importantes

de los Estados Unidos y Europa, han contribuido a confirmar la imagen que siempre tuvimos: un Banco con espíritu moderno. Al cumplir 125 años en el mercado local, nuestra institución cuenta con 375 Agencias, más de 1,800 cajeros automáticos, más de 5,600 Agentes BCP y más de 15,000 colaboradores; así como bancos corresponsales en todo el mundo. El BCP es la principal Subsidiaria de Credicorp Ltd. desde su creación en 1995, además participa en el capital de varias empresas que son sus subsidiarias como indica a continuación:

Subsidiaria	País	%
BCP Bolivia y Subsidiarias	Bolivia	95.84
Inversiones BCP	Chile	99.90
Financiera Edyficar	Perú	99.79
Solución EAH	Perú	100.00
Inversiones Credicorp Bolivia	Bolivia	95.84

5.4. Gestión del programa de CN

5.4.1. Gobierno

5.4.1.1. Política

MISIÓN

Promover el éxito de nuestros clientes con soluciones financieras adecuadas para sus necesidades, facilitar el desarrollo de nuestros colaboradores, generar valor para nuestros accionistas y apoyar el desarrollo sostenido del país.

VISIÓN

Ser el banco líder en todos los segmentos y productos que ofrecemos.

Principios BCP

- Satisfacción del Cliente. Ofrecer a nuestros clientes una experiencia de servicio positiva a través de nuestros productos, servicios, procesos y atención.
- Pasión por las Metas. Trabajar con compromiso y dedicación para exceder nuestras metas y resultados, y lograr el desarrollo profesional en el BCP.
- Eficiencia. Cuidar los recursos del BCP como si fueran los propios.
- Gestión al Riesgo. Asumir el riesgo como elemento fundamental en nuestro negocio y tomar la responsabilidad de conocerlo, dimensionarlo y gestionarlo.
- Transparencia. Actuar de manera abierta, honesta y transparente con tus compañeros y clientes, y brindarles información confiable para establecer con ellos relaciones duraderas.
- Disposición al Cambio. Tener una actitud positiva para promover y adoptar los cambios y mejores prácticas.

- **Disciplina.** Ser ordenado y estructurado para aplicar consistentemente los procesos y modelos de trabajo establecidos.

5.4.1.2. Estructura

Directorio, Comité Ejecutivo y Comité de Riesgos.

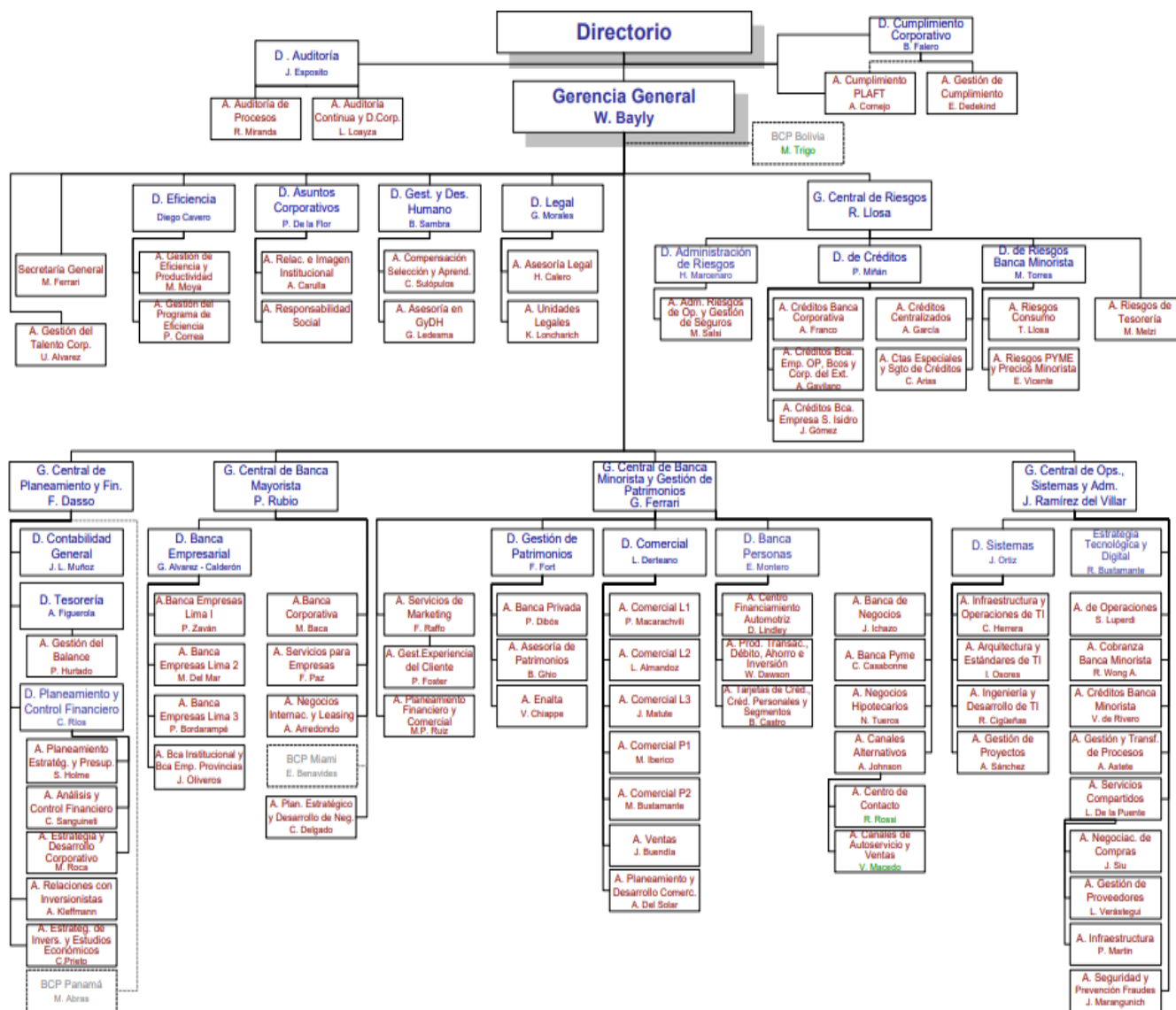
Directorio	
Dionisio Romero P	Presidente
Raimundo Morales	Vicepresidente
Fernando Fort	Director
Benedicto Cigüeñas	Director
Juan Carlos Verme	Director
Eduardo Hochschild	Director
Roque Benavides	Director
Luis Enrique Romero	Director
Irzio Pinasco	Director
Pedro Rubio	Director
Luis Montero	Director
Bárbara Bruce	Director
Patricia Lizárraga	Director
Martín Pérez	Director

Comité Ejecutivo	
Dionisio Romero P.	Presidente
Raimundo Morales	Vicepresidente
Benedicto Cigüeñas	Director
Fernando Fort	Director
Juan Carlos Verme	Director
Martín Pérez	Director
Pedro Rubio	Director

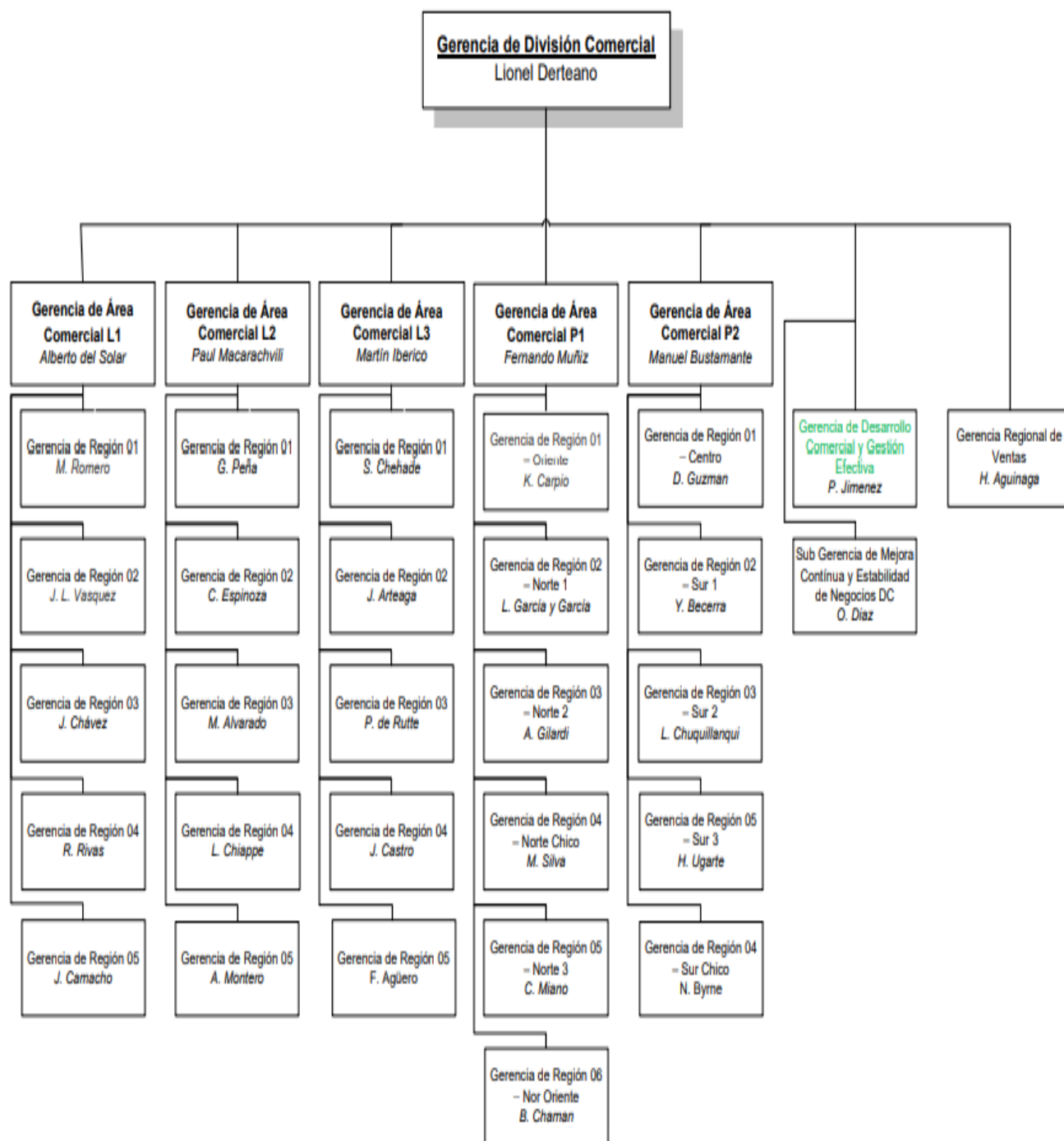
Comité de Riesgos	
Benedicto Cigüeñas	Presidente
Dionisio Romero P.	Director
Raimundo Morales	Director
Pedro Rubio	Director

Gianfranco Ferrari	Gerente General
César Ríos	Gerente Central de Planeamiento y Finanzas
Reynaldo Llosa	Gerente Central de Riesgos
Edgar Vicente	Gerente de División de Administración de Riesgos
José Esposito	Observador permanente

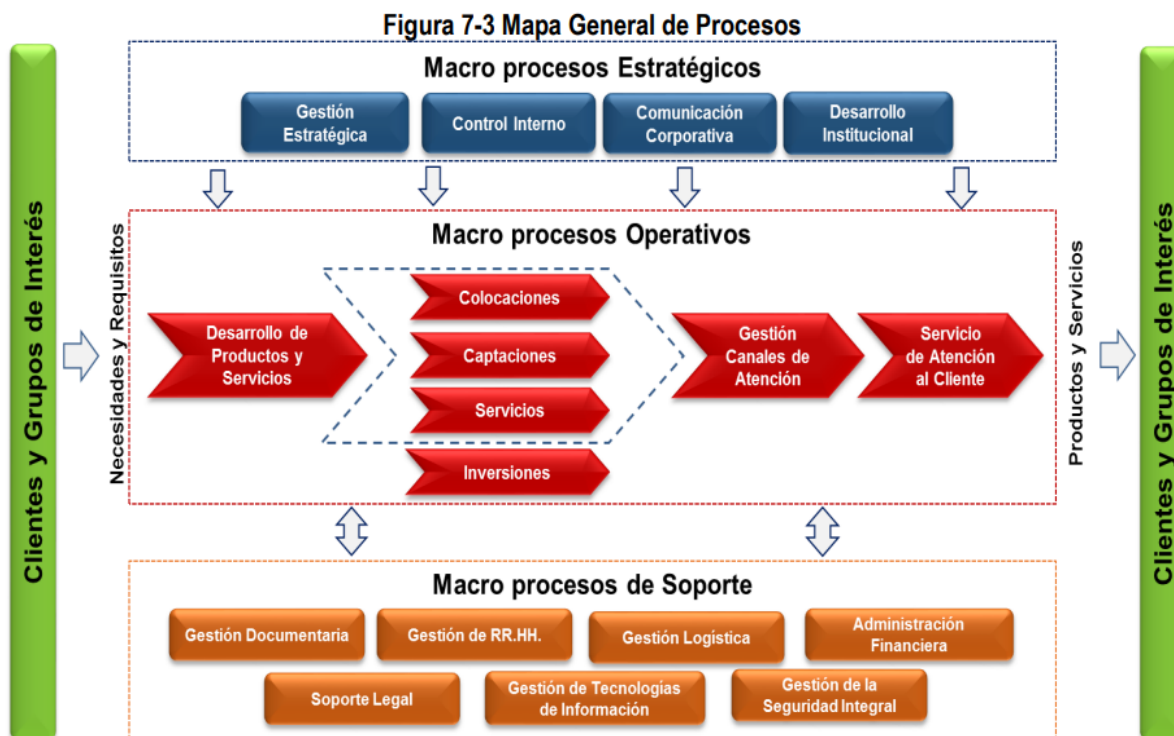
5.4.1.3. Organigrama



5.4.1.3.1. División Comercial



5.4.1.4. Mapa de Proceso BCP



5.4.1.5. Cadena de Valor



5.4.1.6. Plan Estratégico

5.4.1.6.1. Análisis FODA

<p>FODA CRUZADO AGENTE BCP</p>	<p>Fortalezas F1 Valor de marca. F2 Cultura organizacional. F3 Conocimiento del negocio. F4 Capacidad de coordinación con proveedores. F5 Base de datos de comercios con potencial a convertirse en Agentes BCP. F6 Gestión de red de ejecutivos de ventas. F7 Gestión de campañas de marketing para identificar comercios como posibles socios. F8 Capacidad de dar soporte tecnológico a las operaciones del Agente BCP. F9 Gestión de innovaciones tecnológicas.</p>	<p>Debilidades D1 Gestión del riesgo. D2 Inculcar cultura organizacional. D3 Gestión y solución de reclamos D4 Cierre de Agentes BCP. D5 Disponibilidad de comunicaciones.</p>
<p>Oportunidades O1 A pesar de los anuncios de llevar a cabo la "gran transformación", no se realizaron cambios en la política económica instaurada en la década de 1990. O2 Para los años 2014 y 2015 se ha revisado las proyecciones de crecimiento del PBI de 6,2% a 6,0%, y de 6,7% a 6,5%, respectivamente. O3 La proyección de inflación para el periodo 2014-2015 se ubica alrededor de 2,0%, dentro del rango determinado por el Banco Central de Reserva del Perú. O4 De los 1.837 distritos del Perú, solo 847 tienen cobertura del Sistema financiero lo que representa el 46,11%. Aún falta cubrir el 53,9% de distritos. O5 La red dorsal nacional de fibra óptica tendrá una extensión aproximada de 13.500 km de fibra óptica e interconectará a 180 capitales de provincia, brindando servicio de Internet de banda ancha. O6 Agencias, cajeros automáticos o agentes corresponsales disponibles por cada 100.000 habitantes, en el 2008 se contaban con 14.337, llegando a los 45.956 en el 2013. O7 En el 2008, a través de la resolución SBS N°775-2008 se introdujo la regulación de estos cajeros corresponsales, dictando sus requisitos de apertura y operación (SBS 2008b).</p>	<p>Estrategias FO E1 Impulsar el crecimiento de la red de Agentes BCP a nivel nacional (F1, F3, F5, O1, O2, O6, O8). E2 Ampliar los servicios ofrecidos a los clientes (F1, F3, F8, F9, O4, O6). E3 Aumentar visitas a comercios que potencialmente se convertirán en Agentes BCP (F1, F5, F6, F8, O4, O6, O8). E4 Estimular a los socios la utilización de protocolos de atención según lo dicta el BCP (F1, F2, F6, O6, O8). E5 Asegurar la rentabilidad operativa del canal (F3, F4, F6, F9, O2, O3, O6). E6 Robustecer campañas de marketing con el fin de captar más socios (F7, F5, F1, O4, O6).</p>	<p>Estrategias DO E7 Implementar protocolos de contingencia en caso de fallos en la comunicación (D3, O6). E8 Analizar cierre de Agentes BCP cuando aún existen posibilidades de crecimiento (D4, O4, O7).</p>
<p>Amenazas A1 El gobierno de turno fue afectado por escándalos políticos que ocasionaron que su imagen quedara desgastada. A2 Creció la percepción de inseguridad ciudadana, lo cual generó alarma en la sociedad. A3 Se ha incrementado el monto de dinero que ilegalmente se introduce en el circuito económico formal A4 Un problema que limita la profundización y mayor uso del sistema financiero formal es la elevada informalidad existente en la economía que favorece el uso del efectivo. A5 La conciencia de la importancia de desarrollar estrategias de seguridad cibernética está aumentando entre los países de la región de América Latina y del Caribe.</p>	<p>Estrategias FA E9 Preservar la información de los clientes en cada transacción (F8, A5). E10 Detectar y controlar cualquier acción ilícita que se realice a través de los Agentes BCP (F1, F2, A3). E11 Contribuir con la efectiva inclusión financiera haciendo uso de la tecnología (F1, F3, F8, A4).</p>	<p>Estrategias DA E12 Ofrecer a los dueños de comercios afiliados seguros integrales (D2, A2). E13 Impulsar la bancarización en reemplazo del uso del efectivo (D1, A4).</p>

5.4.1.6.2. Desarrollo y soporte a los negocios

La Transformación es una de las iniciativas estratégicas más importantes del BCP, con un amplio alcance que involucra a diferentes equipos de la organización.

La iniciativa nació luego de un análisis exhaustivo para entender cómo la digitalización puede cambiar el negocio y el modelo operativo del BCP. De esta manera, se determinó que la digitalización va más allá de actualizaciones de TI y sistemas, y que la creación de productos y canales digitales. Por este motivo, en el 2015, se creó el Centro de InnovaCXion.

Durante el 2016, se incorporaron al programa los equipos de TI, Experiencia al Cliente, Data y Analítica, y se desarrollaron MVPs (Minimum Viable Products). Por ejemplo, una plataforma para la apertura de cuentas en agencias, una plataforma web para la venta de créditos personales y un aplicativo móvil, Yape, para realizar transferencias de dinero entre cuentas usando números de teléfono.

Hacia el año 2017, se decidió incorporar la iniciativa de Transformación Cultural, donde se unieron al programa los equipos de Riesgo Digital, Digital Operations, Modelo

de Distribución y Gobierno. En este año, se lanzó el primer producto digital para la Banca Mayorista, Carta Fianza Digital, el cual obtuvo un nivel de satisfacción del 90% entre los clientes.

En el 2018, se definió una estrategia adicional con el objetivo de convertirnos en el banco líder en satisfacción al cliente en Perú y el banco más eficiente en la región para el año 2021. Por ello, durante el 2019, la Transformación mantuvo su enfoque en los 10 frentes iniciados en años anteriores, buscando contribuir a estos dos grandes objetivos.

En línea con esto, durante el año hemos trabajado en el desarrollo de habilitadores y puntos de contacto existentes, para brindar a nuestros clientes una experiencia diferenciada. Los habilitadores, y sus logros, se segmentan en los siguientes 3 grupos:

Ciberseguridad

Hemos trabajado en la conciencia del riesgo hacia los colaboradores y en el desarrollo de una cultura de prevención, orientada a la mitigación de riesgos. Asimismo, hemos avanzado en el fortalecimiento de nuestros sistemas de control, monitoreo y seguridad, y en

robustecer nuestra práctica de desarrollo de software y uso de datos.

Tecnología, Data y Ops

Hemos logrado poner a disposición de nuestros clientes más funcionalidades, mejoras y disponibilidades. Esto se evidencia con una reducción del 46% en los tiempos promedio de los pases a producción, a pesar del aumento de 40% en el número de pases a producción respecto al año anterior. Asimismo, el número de incidentes masivos se ha reducido en más del 15% en comparación al 2018 y más de 30% desde el 2017.

Además, estamos utilizando analítica avanzada para detectar oportunidades de optimización y generación de ingresos adicionales. De esta manera, hemos desplegado un Centro de Excelencia de analítica avanzada para poder extender esta capacidad y ser más efectivos en la incorporación de la data para la toma de decisiones de los diferentes equipos.

Las aplicaciones desarrolladas por los laboratorios de data, ParaTi y Manyar, alcanzaron los 500 mil usuarios, lo que nos permite tener mejores datos de contacto e información más actualizada de nuestros clientes y no clientes. Sobre

este último punto, al cierre del 2019 cerramos el año con un incremento de 37% de ofertas pre aprobadas para productos de crédito.

A nivel de operaciones hemos abierto el canal de Whatsapp del BCP para abrir cuentas de ahorro y una nueva plataforma chatbot denominada “Clara” para servir e informar a nuestros clientes. Adicionalmente, hemos puesto en producción soluciones de RPA (Robotic Process Automation) y hemos mejorado procesos en equipos de postventa, lo que va a generarnos ahorros por optimización y permitirnos brindar una experiencia más ágil y efectiva a nuestros clientes.

Agilidad y ser más Clientecéntricos

Durante el año hemos diseñado 16 Tribus y 3 Centros de Excelencia, muchos de los cuales ya se encuentran operando. Con esta forma de organización buscamos mayor flexibilidad y agilidad para llevar valor a los clientes, maximizando la productividad de forma eficiente.

Desde el Centro de InnovaCXion también venimos trabajando en brindar soluciones centradas en el cliente. Al cierre del 2019 tenemos 4 laboratorios en producción, los cuales consisten en: una solución de pago de comercios a

proveedores, un ecosistema inmobiliario, apertura de cuentas por Whatsapp y una plataforma para cambio de moneda.

Por otro lado, además de trabajar en habilitadores, nos hemos enfocado en impactar en el ciclo de vida de un cliente típico. Para esto, hemos identificado cinco etapas claves donde la Transformación ha trabajado, logrando obtener resultados que impactan cómo el cliente experimenta nuestra marca, nuestros servicios y nuestros productos.

La primera etapa consiste en que el cliente nos considere como una opción cuando requiera de algún servicio bancario. Para lograrlo, hemos trabajado en distintos journeys de clientes: 5 de servicios y 2 de productos. De esta forma, hemos logrado mejorar significativamente la experiencia de nuestros clientes, incrementando los niveles de satisfacción top to box en el segmento consumo en 34% respecto al 2018, logrando que nuestros clientes nos reconozcan como el banco #1 en experiencia del cliente.

La segunda etapa consiste en estar presentes durante el proceso de investigación y elección del cliente. Esto nos

ha llevado a reforzar nuestra presencia en canales digitales para brindar toda la información necesaria de manera clara y transparente. Trabajamos en la publicidad digital de los productos y servicios que tenemos digitalizados y en la optimización de las búsquedas de los productos, lo que nos ha llevado a crecer en 30% el número de visitas a la web del banco respecto al 2018.

La tercera etapa son los requerimientos que tenemos como banco para que los clientes puedan realizar sus operaciones con nosotros. En este punto tenemos dos momentos: cuando es un nuevo cliente y cuando es un cliente recurrente. Por un lado, para nuevos clientes trabajamos en la pre aprobación de la PEA, cuyos niveles de cobertura al cierre del 2019 se han incrementado en 37% respecto al cierre del 2018.

Por otro lado, cuando se trata de un cliente recurrente, ponemos a disposición distintos canales digitales para que realice operaciones. Entre estos canales, contamos con Yape, una app para realizar transferencias usando el número de celular o códigos QR, que ha multiplicado por 4 su base de usuarios en el último año, llegando casi a los 2 millones en el 2019. También están los canales digitales del banco: Banca Móvil y Banca por Internet. Estos han

crecido casi en 50% su base de usuarios en el último año, mientras que el número de clientes con token digital se ha más que triplicado en el último año. El token es un requisito para poder hacer transferencias monetarias en las aplicaciones del banco, por lo que la rápida adopción del token digital nos permite incrementar el número de transacciones de los canales digitales, los cuales antes se realizaban a través de canales tradicionales, lo que las hace más costo-eficientes y seguros.

La cuarta etapa es el proceso de contratación de productos. Hemos impulsado los canales digitales para contratación de productos con la ayuda de una estrategia de marketing digital. Esta estrategia, junto con una mayor oferta de productos, nos ha permitido más que duplicar el número de unidades vendidas a través de canales digitales respecto al 2018, siendo estos canales los responsables del 19% del total de unidades vendidas en el mes de diciembre.

Finalmente, la quinta etapa es el paso de nuestros clientes hacia el mundo digital. Hemos ampliado las funcionalidades de nuestros canales digitales por el lado del servicio y la disponibilidad de nuevos productos. También hemos invertido considerablemente en educar a nuestros clientes en los beneficios de ser más digitales

desde nuestras agencias. Esto nos ha permitido aumentar en más de 50% el número de clientes digitales respecto al cierre del 2018 y pasar a tener un ratio de clientes digitales de 40% contra el 30% del cierre del año anterior. Al 2019, más de 8 millones de peruanos eligen transformar sus planes en realidad con el BCP

5.5. Entender de la Organización

5.5.1. Análisis de Impacto (BIA)

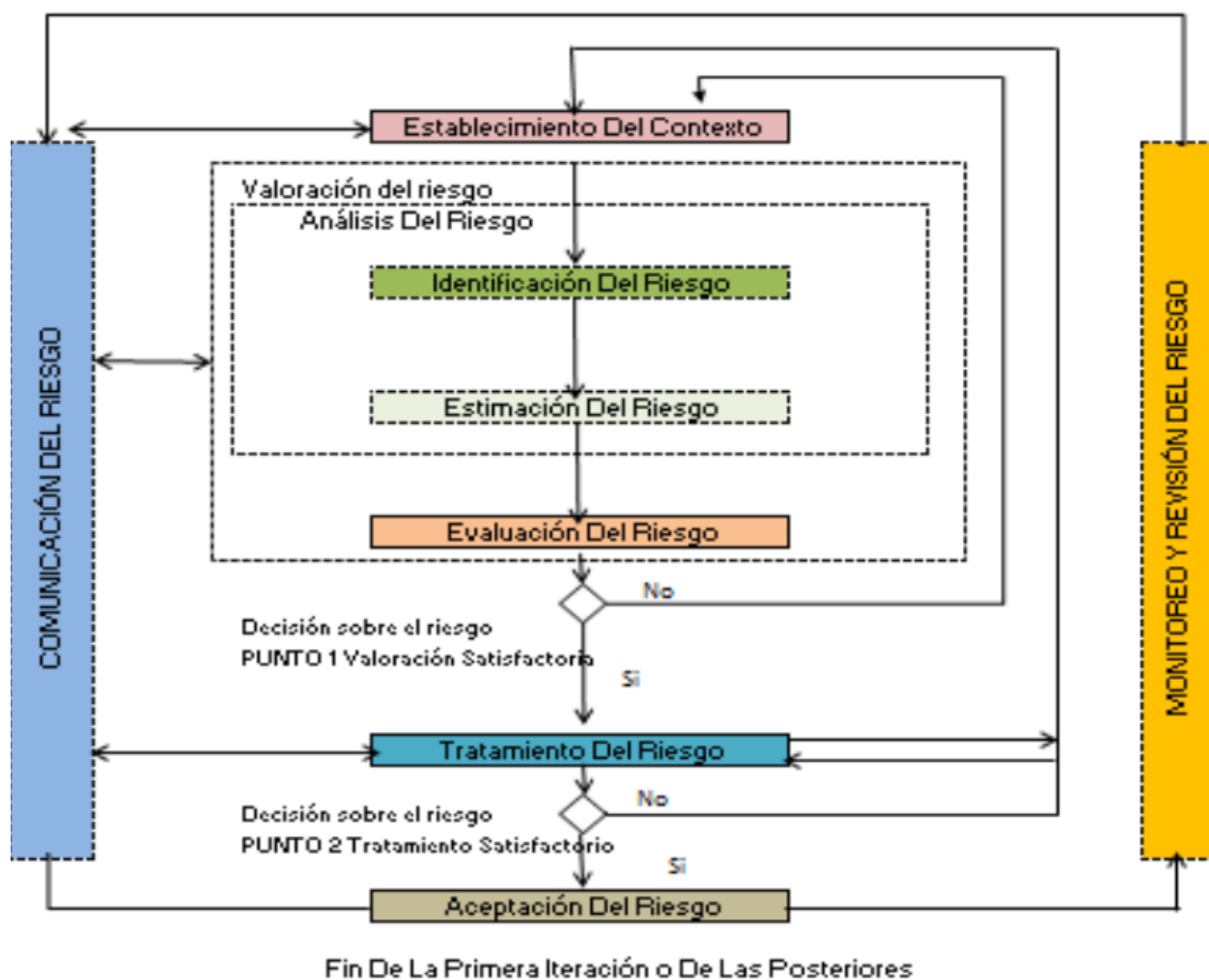
Para realizar el Análisis del Impacto en el Negocio se necesita determinar las labores y los recursos necesarios para asegurar la continuidad del negocio. Además, se debe identificar correctamente los procesos críticos de negocio, las ventanas de tiempo de recuperación y establecer prioridades de recuperación. Por ello, según la ISO 22301 y Luis Rojas, asociado a Isaca Costa Rica Chapter, se deben tener en consideración las siguientes acciones: - Establecer el contexto de la evaluación: Se definen los objetivos, alcance y supuestos del BIA. - Identificar las actividades que soportan los productos y servicios: Se definen e identifican las funciones y los procesos de negocio.

Establecer plazos priorizados para la reanudación de las actividades a un nivel mínimo aceptable especificado: Es decir, tener en cuenta el plazo en que los impactos llegarían a ser inaceptable.

- Establecer para cada actividad el periodo máximo tolerable de interrupción (MTPD), basado en el análisis del impacto.
- Categorizar las actividades de acuerdo con la prioridad de recuperación e identificar las actividades críticas.
- Identificar las dependencias y recursos de apoyo pertinentes a las actividades críticas, incluyendo proveedores, externalizando socios y otras partes interesadas
- Identificar Sistemas y aplicaciones críticos de TI.
- Identificar recursos críticos que no son de TI.
- Determinar el RTO.
- Determinar RPO.
- Definir procedimientos de trabajo.

5.5.1.1. Análisis de Riesgos (AR)

Para el desarrollo del análisis de riesgo se tomó como base la norma técnica Colombiana NTC-ISO/IEC 27005. En la siguiente figura, se visualiza la metodología utilizada, la cual es compatible con los conceptos generales descritos en la norma ISO 27001, permitiendo con su aplicación, un análisis de riesgo estándar implementado en el Banco de crédito del Perú



Para estimar el nivel de exposición de los riesgos de continuidad, se realizó una evaluación de la probabilidad y el impacto que tendrían los riesgos identificados en caso de materializarse. Se debe tener en cuenta que el nivel de riesgo para cada amenaza se calcula considerando el mayor nivel de riesgo resultante de todos los componentes afectados. Para esta evaluación se consideró una matriz de cinco por cinco (05 niveles de probabilidad y 05 niveles de impacto), y cuatro niveles de criticidad:

a. Probabilidad:

Nro.	Probabilidad	Descripción
1	Raro	El evento se presenta cada 05 años o más
10	Improbable	El evento se presenta cada 03 años
50	Posible	El evento se presenta cada año
75	Probable	El evento se presenta cada 06 meses
100	Casi certeza	El evento se presenta cada mes

b. Impacto

1	Bajo	Financiera	Pérdida financiera de hasta S/ 1,22 mil
		Disponibilidad	El efecto es nulo o muy pequeño en la operación de la sede
5	Moderado	Financiera	Pérdida financiera superior a S/ 1,22 mil hasta S/ 6,12 mil
		Disponibilidad	El evento puede afectar hasta 04 horas la operación de la sede
25	Relevante	Financiera	Pérdida financiera superior a S/ 6,12 mil hasta S/ 30,61 mil
		Disponibilidad	El evento puede afectar entre 04 horas y 01 día la operación de la sede
50	Alto	Financiera	Pérdida financiera superior a S/ 30,61 mil hasta S/ 61,23 mil
		Disponibilidad	El evento puede afectar entre 02 y 04 días la operación de la sede
100	Crítico	Financiera	Pérdida financiera superior a S/ 61,23 mil
		Disponibilidad	El evento puede afectar entre una o más semanas la operación de la sede

c. Nivel de Riesgo

MATRIZ DE RIESGOS (Criticidad)							
I M P A C T O	Crítico (Más de S/.122.45M)	100	Moderado	Moderado	Extremo	Extremo	Extremo
	Alto (Hasta S/. 61.23M)	50	Bajo	Moderado	Alto	Alto	Extremo
	Relevante (Hasta S/. 30.61M)	25	Bajo	Moderado	Moderado	Alto	Alto
	Moderado (Hasta S/. 6.12M)	5	Bajo	Bajo	Moderado	Moderado	Moderado
	Bajo (Hasta S/. 1.22M)	1	Bajo	Bajo	Bajo	Moderado	Moderado
			1	10	50	75	100
			Raro (Cada 5 años o más)	Improbable (Cada 3 años)	Posible (Cada año)	Probable (Cada 6 meses)	Casi Certeza (Cada mes)
TASA DE OCURRENCIA (Anualizado)							

La empresa definió los siguientes niveles de riesgo para su medición.

Riesgo	Escenario	Causa	Probabilidad		Impacto		Nivel de Riesgo Inherente
			Descripción	Valor	Descripción	Valor	
Daños en la infraestructura física de la oficina principal y/o agencias de la organización.	Terremoto	Cambios climatológicos constantes	Raro	1	Crítico	100	Moderado
	Incendios	Acciones generadas por personas / Cortocircuitos	Posible	50	Crítico	100	Extremo
Daños en el centro de procesamiento de datos (CPD) (equipos de comunicaciones, servidores, ambientes de desarrollo, calidad y producción).	Incendios	Acciones generadas por personas / Cortocircuitos	Posible	50	Crítico	100	Extremo
	Inundaciones	Fallas en los servicios de agua que generen aniego	Posible	50	Crítico	100	Extremo

Indisponibilidad de los servicios de TI (servicio de base de datos, correo, sistema de créditos, sistema de ahorros).	Ciberataques	Continuos ataques informáticos que deterioran o ponen en riesgo los servicios brindados por la organización	Casi Certeza	100	Alto	50	Extremo
Inaccesibilidad de los trabajadores y clientes a las instalaciones de la organización.	Huelgas / Problemas sociales	Huelgas que ponen riesgo la integridad de las personas y clientes, forzando a cerrar las instalaciones.	Posible	50	Alto	50	Alto
Ausencia de efectivo en las agencias para atención al Riesgo cliente.	Indisponibilidad del Proveedor	Indisponibilidad del proveedor para atender las remesas solicitadas por la agencia con déficit de efectivo	Casi Certeza	100	Relevante	25	Alto
Posibles multas y/o sanciones debido a pérdida de registros vitales tales como contratos de créditos y ahorros, hojas resumen, cartillas informativas, certificados de desgravamente.	Incendio	Acciones generadas por personas / Cortocircuitos	Posible	50	Crítico	100	Extremo
	Inundaciones	Fallas en los servicios de agua que generen aniego	Posible	50	Crítico	100	Extremo
	Errores del personal	Ausencia de personal con el conocimiento y habilidades necesarias para el desarrollo de esta actividad	Casi Certeza	100	Relevante	25	Alto
Posibles multas y/o sanciones debido a incumplimientos de nuevas normas o modificaciones en la regulación que conlleven al cierre de una agencia	Errores del personal	No identificar constantemente la nueva regulación aplicable a la organización	Casi Certeza	100	Moderado	5	Moderado

5.6. Establecer de Estrategia de CN

5.6.1.1. Esstrategias pore escenarios

Riesgo	Escenario	Causa	Probabilidad	Impacto	Nivel de Riesgo inherente	Controles	Nivel de Riesgo Residual
Daños en la infraestructura física de la oficina principal y/o agencias de la organización.	Terremoto	Cambios climatológicos constantes	Raro	Crítico	Moderado	Establecer señalización, rutas de escape, puertas de emergencia, y puntos de encuentro en caso de desastre. Establecer brigadas de emergencia. Programar y ejecutar simulacros de forma periódica. Establecer contratos de seguros contra todo riesgo.	Moderado
	Incendios	Acciones generadas por personas / Cortocircuitos	Posible	Crítico	Extremo	Implementar sistema de alarmas contra incendios, sensores de humo. Distribuir extintores en Riesgo puntos críticos. Establecer brigadas de emergencia. Establecer contratos de seguros contra todo riesgo.	Alto
Daños en el centro de procesamiento de datos (CPD) (equipos de comunicaciones, servidores, ambientes de desarrollo, calidad y producción).	Incendios	Acciones generadas por personas / Cortocircuitos	Posible	Crítico	Extremo	Implementar sistema de alarmas contra incendios, sensores de humo. Distribuir extintores en puntos críticos (Tipo C) Establecer brigadas de emergencia. Implementar un centro de procesamiento de	Alto

						datos alterno. Desarrollar y ejecutar procedimientos de backup para los servidores con información crítica. Establecer contratos de Riesgo seguros contra todo riesgo.	
	Inundaciones	Fallas en los servicios de agua que generen aniego	Posible	Crítico	Extremo	Implementar piso falso/ elevado en todo el ambiente. Implementar un centro de procesamiento de datos alterno. Establecer contratos de seguros contra todo riesgo	Alto
Indisponibilidad de los servicios de TI (servicio de base de datos, correo, sistema de créditos, sistema de ahorros).	Ciberataques	Continuos ataques informáticos que deterioran o ponen en riesgo los servicios brindados por la organización	Casi Certeza	Alto	Extremo	Implementar un software para detectar malware (antivirus) con alcance a todo el parque informático. Configurar Alto correctamente el firewall Configurar correctamente el proxy Instalar herramientas	Alto
Inaccesibilidad de los trabajadores y clientes a las instalaciones de la organización.	Huelgas / Problemas sociales	Huelgas que ponen riesgo la integridad de las personas y clientes, forzando a cerrar las instalaciones.	Posible	Alto	Alto	Establecer planes de comunicaciones (comunicados en página web) Establecer brigadas de emergencia. Establecer alianzas estratégicas con cajeros corresponsales y el Banco de la Nación para poder realizar la atención del proceso de créditos.	Moderado
Ausencia de efectivo en las	Indisponibilidad del Proveedor	Indisponibilidad del proveedor	Casi Certeza	Relevante	Alto	Arqueo diario por parte	Moderado

agencias para atención al Riesgo cliente.		para atender las remesas solicitadas por la agencia con déficit de efectivo				del Coordinador de Operaciones a efectos de identificar los flujos de efectivo. Establecer acuerdos de niveles de servicio (SLA)	
Posibles multas y/o sanciones debido a pérdida de registros vitales tales como contratos de créditos y ahorros, hojas resumen, cartillas informativas, certificados de desgravamente.	Incendio	Acciones generadas por personas / Cortocircuitos	Posible	Crítico	Extremo	Implementar sistema de alarmas contra incendios, sensores de humo. Distribuir extintores en puntos críticos. Establecer brigadas de emergencia. Realizar copias de seguridad sobre la información crítica de la organización. Establecer contratos de seguros contra todo riesgo.	Alto
	Inundaciones	Fallas en los servicios de agua que generen aniego	Posible	Crítico	Extremo	Establecer contratos de seguros contra todo riesgo.	Alto
	Errores del personal	Ausencia de personal con el conocimiento y habilidades necesarias para el desarrollo de esta actividad	Casi Certeza	Relevante	Alto	Implementar evaluaciones técnicas en los procesos de reclutamiento Programas de capacitación periódicos según las funciones de cada puesto de trabajo. Establecer procedimientos disciplinarios y las medidas a adoptar en casos de faltas recurrentes.	Moderado
Posibles multas y/o sanciones debido a incumplimientos de nuevas normas o modificaciones	Errores del personal	No identificar constantemente la nueva regulación aplicable a la organización	Casi Certeza	Moderado	Moderado	Identificar periódicamente la nueva regulación aplicable a la organización. Establecer comités de cumplimiento	Bajo

en la regulación que conlleven al cierre de una agencia						normativo en el cual se expongan las nuevas normas y el estado de los planes de acción a Riesgo adoptar por la organización.	
---	--	--	--	--	--	--	--

5.7. Desarrollar e implementar la Respuesta de CN

5.7.1. Planes de continuidad del negocio

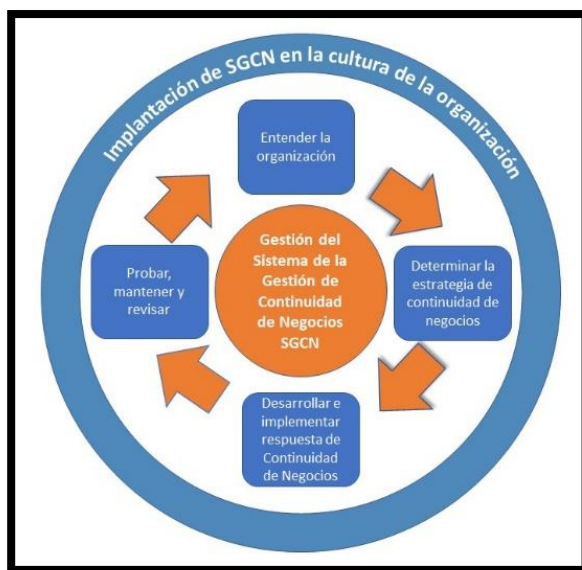
Riesgo	Escenario	Causa	Nivel de Riesgo Residual	Estrategia
Daños en la infraestructura física de la oficina principal y/o agencias de la organización.	Terremoto	Cambios climatológicos constantes	Moderado	<ul style="list-style-type: none"> • Establecer un plan de mantenimiento anual, a efectos de identificar las debilidades en infraestructura e instalaciones, a efectos estos aspectos. • Actualizar anualmente los principales activos que deben ser cubiertos por el seguro contra todo riesgo (SCTR). • Elaborar un mapa de distribución de puestos para el centro de operaciones alterno.
	Incendios	Acciones generadas por personas / Cortocircuitos	Alto	
Daños en el centro de procesamiento de datos (CPD) (equipos de comunicaciones, servidores, ambientes de desarrollo, calidad y producción).	Incendios	Acciones generadas por personas / Cortocircuitos	Alto	<ul style="list-style-type: none"> • Establecer un plan de mantenimiento anual, a efectos de identificar las debilidades en infraestructura e instalaciones, a efectos estos aspectos. • Actualizar anualmente los principales activos que deben ser cubiertos por el seguro contra todo riesgo (SCTR). • Elaborar un mapa de distribución de puestos para el centro de operaciones alterno.
	Inundaciones	Fallas en los servicios de agua que generen aniego	Alto	
Indisponibilidad de los servicios de TI (servicio de base de datos, correo, sistema de créditos, sistema de ahorros).	Ciberataques	Continuos ataques informáticos que deterioran o ponen en riesgo los servicios brindados por la organización	Alto	<ul style="list-style-type: none"> • Establecer un plan de gestión de crisis para los casos en que se presente caída de todos los servicios de TI. • Verificar periódicamente que los sistemas se encuentren actualizados en su última versión. • Establecer planes de respuesta a los incidentes presentados.
Inaccesibilidad de los trabajadores y clientes a las instalaciones de la organización.	Huelgas / Problemas sociales	Huelgas que ponen riesgo la integridad de las personas y clientes, forzando a cerrar las instalaciones.	Moderado	<ul style="list-style-type: none"> • Establecer agencias alternas para atención en caso de cierre de alguna agencia / oficina principal
Ausencia de efectivo en las agencias para atención al Riesgo cliente.	Indisponibilidad del Proveedor	Indisponibilidad del proveedor para atender las remesas solicitadas por la agencia con déficit de	Moderado	<ul style="list-style-type: none"> • Análisis periódico del cumplimiento de los niveles de acuerdo de servicio del proveedor actual. • Analizar y contar con una lista de proveedores alternos que brinden el servicio de remesas en caso de indisponibilidad del actual proveedor.

		efectivo		
Posibles multas y/o sanciones debido a pérdida de registros vitales tales como contratos de créditos y ahorros, hojas resumen, cartillas informativas, certificados de desgravamente.	Incendio	Acciones generadas por personas / Cortocircuitos	Alto	<ul style="list-style-type: none"> • Establecer procesos de digitalización de documentos (registros vitales).
	Inundaciones	Fallas en los servicios de agua que generen aniego	Alto	
	Errores del personal	Ausencia de personal con el conocimiento y habilidades necesarias para el desarrollo de esta actividad	Moderado	
Posibles multas y/o sanciones debido a incumplimientos de nuevas normas o modificaciones en la regulación que conlleven al cierre de una agencia	Errores del personal	No identificar constantemente la nueva regulación aplicable a la organización	Bajo	<ul style="list-style-type: none"> • Establecer planes de capacitación constantes para el personal, y evaluar periódicamente la asimilación de dichas capacitaciones. • Establecer planes de sucesión, identificando claramente a todo el personal clave de cada proceso.

5.8. Probar, Mantener y revisar

Para el banco BCP consideramos La ISO/IEC 22301:2012 aplica un modelo de mejora continua denominado PDCA (Plan, Do, Check, Act) para planificar, establecer, implementar, operar, monitorear, revisar, mantener y mejorar de forma continua la efectividad de un Sistema de Gestión de Continuidad de Negocio. (ISO22301, 2012).

Figure 4 Implantación del PGCN en la cultura de la Organización.



Fuente: Universidad de Chile - 2017

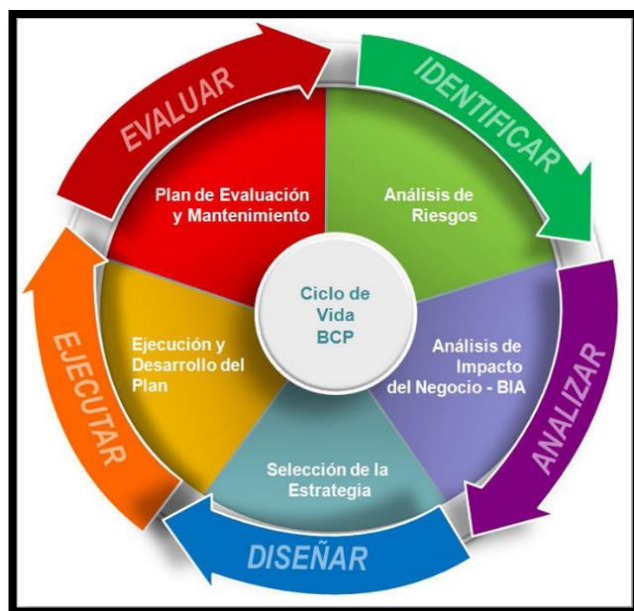
Los componentes del ciclo PDCA según la ISO/IEC 22301:2012 son:

- ✓ Plan (Establecer): En esta fase se construyen las políticas, objetivos, alcance, controles, procesos y procedimientos importantes para la continuidad del negocio.
- ✓ Todos estos documentos tienen que estar alineados a los objetivos y políticas de la organización.
- ✓ Do (Implementar y Operar): En esta fase se implementa y se pone en operación las políticas de continuidad de negocio, controles, procesos y procedimientos involucrados en el SGCN. (Sistema de Gestión de Continuidad de Negocio)
- ✓ Check (Monitorear y Revisar): En esta fase se monitorea y revisa el desempeño contra las políticas de continuidad del negocio y objetivos, reporte de resultados de la revisión de la gestión, y determinar y autorizar acciones para la mejora continua.

- ✓ Act (Mantenimiento y Mejora): En esta fase se toman acciones para mejorar y mantener el SGCN

5.9. Integrar el PGCN en la cultura de la Organización

Para integrar en el programa de gestión de continuidad del negocio (BCM) para el banco BCP. Este debe contar con la participación de las diferentes partes del negocio, incluyendo al Director de Información (CIO), en su elaboración. Luego, se debe elaborar el Plan del Programa donde se especifique paso a paso que se ejecutará, como va a ser financiado y cuándo comenzará su implementación según la criticidad de los procesos de la organización. (Rodriguez, 2016)



Fuente: Ramírez y daza - 2018

La fase de iniciación del proyecto consta de realizar la planificación de todo el proyecto de implementación del BCM especificando los objetivos del proyecto, los resultados esperados y expectativas de los actores claves en el proceso de negocio, las tareas que se realizarán, los roles y sus responsables. Estos objetivos deben ser claros, medibles, alcanzables, relevantes y duraderos en el tiempo para que permitan medir el proyecto durante todo su ciclo de vida.

La fase de análisis del riesgo consta de realizar la identificación de riesgos, su evaluación y análisis del impacto que producirían en el negocio. Esto ayuda a identificar los posibles eventos que pudieran ocurrir, sus causas y consecuencias que traerían consigo. Inicia con la identificación de los riesgos que logra su clasificación de acuerdo a la categorización definida por la organización. Entre los más comunes se encuentran los desastres naturales, artificiales, meteorológicos, geofísicos, accidentales, malintencionados, entre otros. Una vez finalizado, se realiza una evaluación de estos riesgos para estimar y evaluar la probabilidad de ocurrencia, frecuencia y el impacto que generaría. Estas labores se realizan mediante trabajos de análisis estadísticos, datos históricos, revisiones de los activos de tecnologías para conocer sus configuraciones y ubicaciones, etc.

La fase de selección de las estrategias para la mitigación de los riesgos identificados consta de definir aquellos procedimientos que la empresa utilizará para enfrentar los riesgos que identificó. Por ello, la empresa puede optar por transferir el riesgo hacia otra entidad mediante la tercerización de una parte de su empresa, donde fue identificado el riesgo, haciendo responsable a la otra parte de su gestión.

6. Anexos

6.1. Glosario de términos

6.1.1. Tiempo Objetivo de Recuperación (RTO)

El Tiempo Objetivo de Recuperación (RTO en inglés) es el tiempo transcurrido entre la interrupción del proceso y el punto en el cual éste debe estar totalmente operativo.

6.1.2. Tiempo Máximo Permitido de Recuperación (MTD)

El Tiempo Máximo Permitido de Recuperación (MTD en inglés) es el periodo de tiempo medido en minutos, horas, semana o meses, que está asociado a la paralización de una actividad que, una vez superado, la viabilidad de la organización se verá amenazada irrevocablemente.

6.1.3. Amenaza

Eventos que, aprovechando una vulnerabilidad, pueden desencadenar un incidente en la organización, produciendo daños.

6.1.4. Análisis de impacto en el negocio

Proceso de análisis de las actividades de la organización y las consecuencias que una interrupción sobre las mismas pueden provocar en la oficina.

6.1.5. Análisis riesgos

Proceso de identificación, análisis y evaluación de riesgos.

6.1.6. Equipo de Gestión de Crisis (EGC)

El Equipo de Gestión de Crisis (EGC) establece la estrategia de implementación de acuerdo a los pasos sugeridos en esta guía, supervisa la implementación del BCP durante un evento, recopila información para determinar el impacto y sus consecuencias para las operaciones de la oficina, y recomienda la acción de continuidad del negocio al Gerente.

6.1.7. Plan de Continuidad de las operaciones (BCP)

Un Plan de Continuidad de las operaciones (Business Continuity Plan - BCP por sus siglas en inglés) es una serie de procedimientos para restaurar las operaciones normales de oficina después de un desastre y/o un evento importante, dentro de un tiempo predeterminado.

6.1.8. Procesos Críticos

Son los procesos mínimos que deben seguir funcionando para poder entregar cooperación Técnica

6.1.9. Servicios Críticos

Son todos aquellos elementos relacionados con cada uno de los procesos críticos identificados. Entre ellos, los activos de recuperación, personal mínimo que apoyará en ese proceso, sistemas necesarios para ejecutarlos, registros vitales necesarios, proveedores y socios claves, etc.

6.2. Conclusiones

Las empresas de hoy día, esperan siempre estar a la vanguardia de su competencia, por lo que implementar un plan de continuidad del negocio es un pilar importante en el plan de negocios y en la visión empresarial.

En ausencia de un enfoque estratégico, las agencias pueden estar desperdiciando recursos en áreas de riesgo dejando expuestas áreas críticas, ignorando que actualmente se cuenta con una variedad de opciones y aplicaciones informáticas para que las empresas, no importando su tamaño, cuenten con un plan de recuperación ante un desastre

6.3. Recomendaciones

Las agencias deben asegurarse de tener políticas y procedimientos adecuados para áreas clave como gestión de riesgos de TI, seguridad de la información, continuidad del negocio y cambio de control.

Recomendamos el uso de estándares y marcos como referencias para ayudar agencias con implementación de buenas prácticas.

Las agencias deben garantizar que se implementen, actualicen y realicen buenas prácticas de seguridad regularmente para sistemas informáticos.

Todos los cambios deben estar sujetos a una planificación y evaluación de impacto para minimizar la probabilidad de problemas y realizar una documentación de control de cambios la cual debe estar actualizado constantemente.

