PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

FACULTAD DE CIENCIAS E INGENIERÍA

DISEÑO DE UN SISTEMA DE GESTIÓN DE CONTINUIDAD DE NEGOCIOS (SGCN) PARA LA RENIEC BAJO LA ÓPTICA DE LA NORMA ISO/IEC 22301

Tesis para optar por el Título de **Ingeniero Informático**, que presenta el bachiller:

Laura Daiana Castro Marquina

ASESOR: Moisés Antonio Villena Aguilar

Lima, setiembredel 2013

TABLA DE CONTENIDO

Índice de Figuras

Introducción

En la actualidad, el incremento de competitividad dentro de las organizaciones empresariales y a su vez de la demanda más exigente de los clientes, logra que las mismas se exijan brindar servicios y/o productos con una mayor rapidez y confiabilidad. Por otro lado, la tecnología viene incrementándose a pasos agigantados y por ello, las organizaciones dependen cada vez más de las Tecnología de InformaciónEs por ello que, habitualmente las empresas se ven obligadas a mantener operativas las actividades diarias de forma ininterrumpida, con la preparación adecuada y la capacidad de restablecer las operaciones de TI en caso ocurra algún incidente y/o desastre que afecte negativamente los procesos claves del negocio o interrumpa la consecución de los objetivos estratégicos marcados, para así lograr mantener o mejorar la posición competitiva.

En el sector público peruano, las entidades del Estado juegan un papel fundamental de acuerdo a los servicios que se brindan a los ciudadanos. Un claro ejemplo es el Registro Nacional de Identificación y Estado Civil (RENIEC), que es una institución que registra la identificación de las personas y garantiza la seguridad técnica y jurídica de todos los actos civiles. Para este tipo de instituciones la continuidad de negocios no es un tema ajeno, pues existe normativa legal que recomiendan se implemente y desarrolle de forma adecuada en las mismas.

El SGCN diseñado en el presente proyecto para el RENIEC, tiene como finalidad facilitar la identificación de impactos ante posibles amenazas o desastres que pueden poner en peligro la continuidad de los niveles y estándares de los procesos manejados por RENIEC y además, contar con una respuesta efectiva que asegure mantener operando dichos procesos críticos y lograr así, estar preparada para afrontar situaciones de urgencia específicas.

A continuación se especificará a detalle cada uno de las actividades realizadas con sus entregables específicos en cada uno de los capítulos relacionados para un mayor entendimiento de la misma.

Capítulo 1. Generalidades

En el presente capítulo, se explica la importancia de la gestión de continuidad de negocios en toda organización y el impacto al no manejarla; el papel que desempeña en el país y en sectores específicos. Asimismo, la relevancia de la labor del Registro Nacional de Identificación y Estado Civil (RENIEC) como entidad pública y la necesidad de que cuente con un Sistema de Gestión de Continuidad de Negocios (SGCN).

Para estructurar de manera adecuada el proyecto, se definen el objetivo general, los objetivos específicos y los resultados esperados que lo conforman; así como las metodologías y procedimientos para cada resultado esperado; los alcances y limitaciones a los cuales estará afecto el proyecto.Finalmente, se presenta la justificativa y viabilidad de la realización de este.

1.1 Definición del Problema

Actualmente la tecnología viene cambiando y avanzando a pasos agigantados de la mano con el incremento de competitividad dentro de las organizaciones empresariales y a su vez de la demanda más exigente de los clientes [Hiles, 2007].

De acuerdo a la administración de empresas modernas, las organizaciones dependen fuertemente de las tareas que día a día son ejecutadas con el fin de mantener los beneficios y la estabilidad. La mayoría posee bienes tangibles, empleados, sistemas y tecnologías de información. Si alguno de estos componentes es dañado o deja de ser accesible por cualquier razón, la organización puede paralizarse. Cuanto mayor sea el tiempo de inactividad, mayor será el impacto económico[BCI, 2012].Es por ello que, habitualmente las empresas se ven obligadas a mantener operativas las actividades diarias de forma ininterrumpida –que pueden provocar desde una pérdida importante de información hasta la destrucción de la infraestructura tecnológica de la organización– existiendo algunas que no se encuentran preparadas para dichos acontecimientos e incluso, existen muchas organizaciones que no han sido capaces de recuperarse después de ser víctimas de algún incidente o desastres [DisasterRecoveryJournal, 2012].

Según el Lead Auditor Dejan Kosutic en un artículo: *"Continuidad de Negocios ¿Es necesaria o no?"* [2011], indica que cuando se habla de continuidad de negocio y de posibles amenazas que pueden poner en peligro la supervivencia y estabilidad de una organización, muchas de las respuestas coinciden en –lo que él nombra como un síndrome– "A nosotros no nos pasará", ya que muchas organizaciones consideran que por el hecho de no haber sufrido ningún incidente en el pasado, el futuro será igual o mejor y evidentemente, es un gran error. La realidad es que cualquier organización pequeña o grande– puede ser víctima de un incidente o desastre que afecte a su continuidad y, dependiendo de la forma en que se gestione dicho incidente, las consecuencias pueden ser más o menos graves.

Según Stephen Flynn– experto en seguridad y comercio [RandomHouse, 2007]: *"Los desastres no siempre se pueden evitar, pero pueden anticiparse y tomar medidas prácticas para prevenir las consecuencias en cascada que probablemente se derivan de ellas".*

En un informe de investigación–efectuado por *MarshRiskConsulting*a lo largo de diez años a todo Latinoamérica– [2011], se indicó que el 33% de las causas para la interrupción de negocios es atribuible a fallas operacionales y que el software; es decir, la tecnología de la información y la comunicación, es el 13% del mismo.
Por lo imprescindible que es mantener operando todos los procesos de una organización –para ofrecer a sus clientes productos de calidad o brindar servicios con eficiencia y eficacia– son cada vez más los inversionistas y clientes que buscan el resguardo de organizaciones que estén preparadas para afrontar

cualquier situación de urgencia, con respuestas eficientes e inmediatas, que manejen Planes de Continuidad que garanticen la continuidad de la actividad del Negocio.

En Junio del 2012 se publicó un informe elaborado por el EconomistIntelligenceUnit y producido por IBM [IBM,2012], donde se muestran resultados de encuestas en línea y entrevistas a más de 427 altos ejecutivos de 23 industrias diferentes en todo el mundo, el estudio detallado investiga cómo organizaciones de todo el mundo están gestionando su reputación y cómo se manejan las operaciones de TI y del negocio ante eventos que puedan interrumpir la habilidad de lograr sus objetivos estratégicos.

Dentro de los resultados más resaltantes del estudio, se indica que respecto al año pasado menos empresas tienen un plan de gestión de riesgos formal y que un 64% de ejecutivos optarían por una planificación y ejecución de un plan de continuidad del negocio como una prioridad para sus empresas y organizaciones.

Por otro lado, AT&T, realizó este año un estudio sobre continuidad de negocios en Estados Unidos que indicó que el 86% de las empresas ya cuentan con un plan de continuidad de negocio en caso de un desastre o incidente- hasta un 8% de aumento en los últimos cinco años [AT&T, 2012]. Los resultados del informe de IBM se muestran en el **ANEXO A.**

A partir de los estudios mencionados, se puede llegar a la conclusión que la continuidad de negocios complementa la Gestión de Riesgos, mostrando la real magnitud del impacto de algunos desastres, ya que analiza el efecto originado por el riesgo.

Por otro lado, el Perú es una de las regiones de más alta actividad sísmica por encontrarse dentro del Cinturón de Fuego del Pacífico, lo que conlleva a encontrarse expuesto permanentemente a sismos y/o terremotos, que al materializarse tienen como resultado altos índices de pérdidas humanas y materiales [INDECI, 2012]. Asimismo, los incendios no son ajenos a organizaciones en el Perú, en el 2011 se reportaron 1387 incendios en el país, de los cuales 473 son de organizaciones administrativas e industriales [INEI, 2012].

Es por ello que en el Perú, la continuidad de negocios no es un tema ajeno, en especial en el sector financiero, la circular G -139-2009-SBS [SBS, 2009] –emitida por la Superintendencia de Banca, Seguros y AFP– indica que se debe manejar

una colaboración integrada de administración de riesgos y continuidad de negocios para dicho sector. Es por ello que cuentan con sistema de contingencia y planificación en caso de cualquier incidente o desastre. Por otro lado, la Norma Técnica Peruana 27001 [INDECOPI, 2008], incluye un dominio de continuidad de negocios, direccionado a empresas públicas para reducir las interrupciones a causa de factores internos o externos.

En el sector público, las entidades del Estado juegan un papel fundamental de acuerdo a los servicios que se brindan a los ciudadanos. El Registro Nacional de Identificación y Estado Civil (RENIEC), es una institución que registra la identificación de las personas y garantiza la seguridad técnica y jurídica de todos los actos civiles. Dentro de los servicios más relevantes que brinda a los ciudadanos se encuentran:Generación y emisión del Documento Nacional de Identidad (DNI), Registros Civiles (RRCC), Padrón Electoral y Certificados Digitales.

A partir de lo mencionado, aparece la necesidad de que dicha organización pública peruana cuente con un Sistema de Gestión de Continuidad de Negocios (SGCN), el cual le permita preservar y proteger la información de todos los peruanos y de los servicios que esta brinda. Además que facilite la identificación de los principales impactos ante posibles amenazas a su organización y tener la habilidad de contar con una respuesta efectiva que permita mantener su prestigio y afianzar la satisfacción de los ciudadanos.

En el presente proyecto de tesis, se diseñará un SGCN para RENIEC para escenarios de Sismos e Incendio, que permita cumplir con los requisitos mínimos recomendados por la Norma Técnica Peruana 27001 y que utilice como base el estándar internacional ISO/IEC 22301.

1.2 Objetivo General

Diseñar un modelo de Sistema de Gestión de Continuidad de Negocios (SGCN) para el Registro Nacional de Identificación y Estado Civil (RENIEC)bajo la óptica de la norma ISO/ IEC 22301.

1.3 Objetivos Específicos

OE1. Modelar los procesos del negocio establecidos como alcance de la gestión de continuidad de negocios.
OE2. Elaborar el Análisis de Riesgos de la Organización.
OE3. Elaborar un Análisis de Impacto al Negocio (BIA).
OE4. Elaborar un Plan de Manejo de Crisis.
OE5. Realizar un Plan de Emergencia bajo escenarios de desastres específicos.
OE6. Elaborar un Plan de Recuperación de Desastres (DRP).
OE7. Elaborar un Plan de Continuidad de Negocios (BCP).
OE8. Desarrollar un Plan de Pruebas que sea consistente con el alcance del Plan de Continuidad de Negocios y permita manejarlo de forma precisa.

1.4 ResultadosEsperados

- **Resultado 1 para el OE1:** Documento con modelamiento de procesos de negocio usando la notación BPMN.
- **Resultado 2 para el OE2:** Mapa de Riesgos de la Organización.
- **Resultado 3 para el OE3:** Análisis de Impacto de Negocio (BIA).
- **Resultado 4 para el OE4:** Plan de Comunicación y Gestión de Crisis.
- **Resultado 5 para el OE5:** Plan de Respuesta a Emergencias
- **Resultado 6 para el OE6**: Plan de Recuperación de Desastres (DRP).
- **Resultado 7 para el OE7:** Planes de Continuidad de Negocios (BCP) de acuerdo a los desastres específicos.
- **Resultado 8 para el OE8:** Planes de Pruebas para cada BCP realizado.

1.5 Métodos, metodologías y procedimientos

1.5.1 Relacionadosa la gestión del proyecto

Para el desarrollo del proyecto se empleará algunos principios metodológicos del Project Management Body of Knowledge (PMBOK), ya que es un marco estándar que permite manejar el ciclo de un proyecto a través de sus procesos(Iniciación, Planificación, Ejecución, Control, Cierre) integrados con sus 9 áreas del conocimiento (Gestión de la Integración del Proyecto, Gestión del Alcance del Proyecto, Gestión del Tiempo del Proyecto, Gestión de los Costes del Proyecto,

Gestión de la Calidad del Proyecto, Gestión de los Recursos Humanos del Proyecto, Gestión de las Comunicaciones del Proyecto, Gestión de los Riesgos del Proyecto, Gestión de las Adquisiciones del Proyecto)[PMI,2008].

El presente Proyecto de Tesis se enfocará sólo en ciertos puntos a considerar:

- **Gestión de la Integración del Proyecto:**Permite la integración efectiva de los procesos a realizar en el proyecto, así como supervisar y controlar las tareas a realizar, minimizar riesgos y cerrar el proyecto.

- **Gestión del Alcance del Proyecto:** Permite establecer los procesos necesarios para asegurar que se incluya todas las actividades necesarias para lograr un adecuado monitoreo y control del cumplimiento de los objetivos y alcances del presente proyecto.

- **Gestión del Tiempo del Proyecto:**Permite especificar las actividades a realizar, secuenciarlas, estimar una duración por cada una de ellas, desarrollar un cronograma que las compacte con restricciones de dependencia y tiempo, y controlar cualquier cambio realizado.

- **Gestión de Calidad del Proyecto:**El SGCN está enfocado bajo la óptica de una norma ISO, para lo cual es necesario asegurar que el proyecto utilice todos los procesos para cumplir con los requisitos y así asegurar su calidad.

- **Gestión de las Comunicaciones del Proyecto:**Permite asegurar la generación, recopilación, almacenamiento y control de la información del proyecto así como la gestión adecuada de la comunicación con los interesados (Empresa, Asesor) de forma que se verifica el adecuado avance del proyecto.

- **Gestión de los Riesgos del Proyecto:**Permite no solo identificar y gestionar los riesgos del proyecto, sino priorizarlos y realizar una planificación de respuesta y un plan de contingencia para reducir cualquier amenaza.

No se consideran la gestión de costos, pues al tratarse de un proyecto de tesis no se realizará la implementación a la empresa, por lo que no se planifica ni estima costos; gestión de recursos humanos, pues es realizado por una sola persona, por lo que no hay asignación de roles y responsabilidades; y gestión de adquisiciones del proyecto, pues no se incurre en adquisiciones de productos o servicios ni se maneja contratos ni vendedores.

1.5.2 Relacionados a los resultados esperados

- **Metodología 1 para el RE1:**

BPMN (Business Process Modeling Notation) 2.0

BPMN es una notación gráfica estandarizada diseñada por el Object Management Group (OMG) para normalizar y facilitar el modelado de flujo de procesos. El objetivo principal es ser un estándar que facilite la elaboración e interpretación de diagramas de procesos de negocio, ya que antes de BPMN, no existía una técnica de modelamiento estándar desarrollada, mientras que ahora los usuarios se beneficiarán de esta notación al igual que el mundo de la ingeniería de software lo hace con UML (UnifiedModelingLanguage); es decir, este modelo se basa en el UML y tiene la ventaja de ser compatible con XML. [OMG, 2011].

Cabe recalcar que una de las directrices para el desarrollo de BPMN es crear un mecanismo simple para diagramar flujos de proceso y que a su vez maneje la complejidad inherente a los procesos del negocio, con el fin de organizar los aspectos gráficos de la notación en categorías específicas. Esto proporciona un sistema de categorías que ayuda al lector de un diagrama de BPMN a reconocer fácilmente los tipos básicos de elementos y entender el diagrama.

Las cuatro categorías básicas de estos elementos son [OMG, 2011]:

- **Elementos de Flujo (FlowObjects):** Son los principales elementos gráficos que definen el comportamiento de los procesos. Pueden ser eventos o actividades.
- **Conectores (ConnectingObjects):** Representan el esqueleto de la estructura del proceso de negocio, asociaciones, secuencias, relaciones, etc.
- **Canales (Swimlanes):** Son mecanismos de organización de las actividades en categorías visuales separadas para representan un sector del flujo.
- **Artefactos (Artifacts):** Son grupos o anotaciones en el diagrama, usados para proveer información adicional sobre el proceso. Otorgan flexibilidad a la notación para expresar diferentes contextos en forma apropiada.
- **Data:** Representan a los datos de los procesos (entrada y salida).

La razón para emplearlo en el presente proyecto es debido a la familiaridad de sus elementos y el fácil entendimiento de su notación.

- **Metodología 2 para el RE2:**

ISO 31000:2009

La Norma ISO 31000:2009, es un estándar que proporciona principios y directrices sobre la gestión de riesgos. Una norma aplicable a todas las organizaciones independientemente del sector, de su actividad o del tamaño de la empresa. Proporciona las orientaciones para la implantación de un sistema de gestión del riesgo que sea compatible con los estándares en su sector. [ISACA, 2012].

El enfoque está estructurado en tres elementos claves para una efectiva gestión de riesgos [ISO: 2009]:Los principios de gestión de Riesgo, el Marco Teórico (Framework) para la gestión de Riesgo y, el proceso de gestión de Riesgo.

Beneficios de la ISO 31000

- Ayuda a concienciar de la importancia de identificar y tratar los riesgos de toda la organización.
- Establece una base de confianza que mejora la toma de decisiones y la planificación.
- Facilita el reconocimiento y utilización de los recursos para la gestión de riesgos.
- Ayuda a detectar las oportunidades y amenazas a la vez que se reducen al mínimo las pérdidas de la organización.
- Mejora la continuidad y la capacidad de recuperación de la organización.
- Mejora la eficacia y la eficiencia operativa.

La razón para basar el mapa de riesgos a realizar en esta metodología, se debe a que es un estándar internacional que actualmente, tiene más puntos en común con la ISO/IEC 22301, ya que ambas hablan de que los riesgos y la continuidad de negocio pueden y **deben afectar a toda la organización,** a todas sus áreas y niveles y a todas sus actividades y productos[AUDISEC, 2012].

- **Metodología 3 para RE3-RE8:**

Para la elaboración de entregables como: BIA, Plan de Crisis, Plan de Emergencia, Plan de Recuperación de Desastres , Plan(es) de Continuidad de Negocios y Plan(es) de Prueba correspondientes, se empleará el modelo **PDCA (Plan-Do-**

Check-Act) mencionado y definido previamente; la elección de este método se debe a que la norma en la que está basada el proyecto (ISO/IEC 22301) menciona la utilización de este modelo para la adecuada realización de un SGCN, además implica la autoevaluación, monitoreo y control de cada uno de los resultados esperados mencionados.

Cabe mencionar que también se tomará en cuenta para la elaboración de dichos entregables las prácticas profesionales manejadas y aprobadas por entidades internacionales como son el BCI de Inglaterra y el DRI de Estados Unidos.

1.6 Alcance y Limitaciones

1.6.1 Alcance

El presente trabajo de tesis de diseño de un SGCN se enfocará en los siguientes procesos críticos de negocio:

- **Proceso de Registro de Identificación:** Este proceso se encarga del servicio de digitalización de Formulario para el DNI y la emisión del mismo, tiene como objetivo conducir los procesos de evaluación, depuración y actualización del Registro Único de Identificación de las Personas Naturales (RUIPN), para ello cuenta con un archivo registral físico y una base de datos que permite brindar seguridad de información de identidad de los peruanos.

- **Proceso de Registros Civiles:** Este proceso se encarga de consolidar y procesar las actas registrales de hechos vitales, tiene como objetivo emitir las actas de Hechos Vitales de forma inmediata y descentralizada, para asegurar la información, cuenta con base de datos de Registro civiles y la información se encuentra almacenada en archivo físico y lógico.

Cabe mencionar, que debido a la complejidad y tiempo de diseño de un SGCN, para cada incidente o desastre propenso al perfil de la organización mencionada, se tomarán como escenarios preliminares: Incendios y Sismos.

1.6.2 Limitaciones

- La elaboración de las pruebas para el BCP desarrollado no implica llevarla a cabo, puesto que ello significa inversión en personal, tiempo y presupuesto, lo cual no aplica al presente proyecto de tesis.

- El trabajo de campo que se debe realizar para relevar la información, es limitado, pues de realizarlo, se requiere del personal clave de la empresa, y éste puede no contar con disponibilidad para atención.
- Los procesos tomados en cuenta pueden ser cambiados a lo largo del desarrollo de la tesis, lo cual implica un alto riesgo y limitación del proyecto.
- Al tratarse de un Proyecto Académico, el tiempo de realización del presente proyecto está limitado y propenso a reducción de alcance de ser necesario.
- No disponibilidad del personal durante la ejecución de pruebas de escritorio.

1.7 Viabilidad y Justificativa del Proyecto

El SGCN a diseñar en el presente proyecto para el RENIEC, tiene como finalidad facilitar la identificación de impactos ante posibles amenazas o desastres que pueden poner en peligro la continuidad y además, contar con una respuesta efectiva que asegure mantener operando dichos procesos críticos y lograr así, estar preparada para afrontar situaciones de urgencia específicas.

A partir de lo mencionado, con el diseño de un SGCN a desarrollar en el presente proyecto de Tesis se lograrán otros beneficios relevantes en el rubro de empresas en la que está enfocada, tales como:

- Al estar enfocado bajo la óptica de la norma ISO/IEC 22301, se asegura a través de un estándar internacional lograr una adecuada y efectiva respuesta ante situaciones de emergencia específicas; es decir que en caso ocurra un incidente o desastre ocasione los daños mínimos, asegurando así la continuidad de la organización.
- La continuidad de negocio no será un tema ajeno para la organización, pues se logrará que sus integrantes se encuentren preparados ante cualquier incidente o desastre, logrando así una adecuada cultura organizacional.
- Cabe mencionar que, si en el futuro se evalúa la posibilidad de realizar la implementación y la certificación del SGCN a diseñar en la presente tesis, la organización en cuestión ganará una ventaja respecto a otras entidades públicas, pues al asegurar la continuidad de sus operaciones y actividades, incrementa su reputación, prestigio e imagen frente a los ciudadanos.

Nota: Como parte de la viabilidad es relevante y necesario tomar en cuenta la gestión de cambios en caso el presente proyecto de Tesis se llegue a implementar.

Capítulo 2. Marco Teóricoy Estado del Arte

Para todo proyecto, es esencial tener como base ciertos conceptos con el fin de poder entender el contexto sobre el cual se está trabajando; motivo por el cual en el presente capitulo, se busca definir los conceptos necesarios para abarcarse en este proyecto. Asimismo, también se da una descripción de los productos y metodologías actuales que satisfacen la solución al problema planteado; buscando así, obtener las ventajas y desventajas que serán consideradas para el desarrollo del producto final.

2.1 Marco Teórico

2.1.1 Conceptos relacionados al problema

- **Amenaza**

Una causa potencial de un incidente[1] no-deseado, el cual puede resultar en daño a un sistema u organización [ISO 27005].

[1] Es la interrupción no planeada de un servicio o la reducción en la calidad de un servicio. También, es un incidente la falla de un elemento de configuración que aún no impacta el servicio.[Hiles, 2007].

NIST de los Estados Unidos de América [2008] lo define como : "*Cualquier circunstancia o hecho que pueda afectar negativamente a las operaciones de la organización, sus activos de información*[2] *o individuos a través del acceso no autorizado, destrucción, acceso, modificación de la información, y/o negación de servicio. Además, la posibilidad de una amenaza de fuente de explotar con éxito una vulnerabilidad de la información del sistema en particular.*En otra acepción, "*son todas las actividades, eventos o circunstancias que pueden afectar el buen uso de un activo de información dañando el soporte a un proceso, perjudicando el logro de los objetivos de negocio*"[Tupia, 2010].

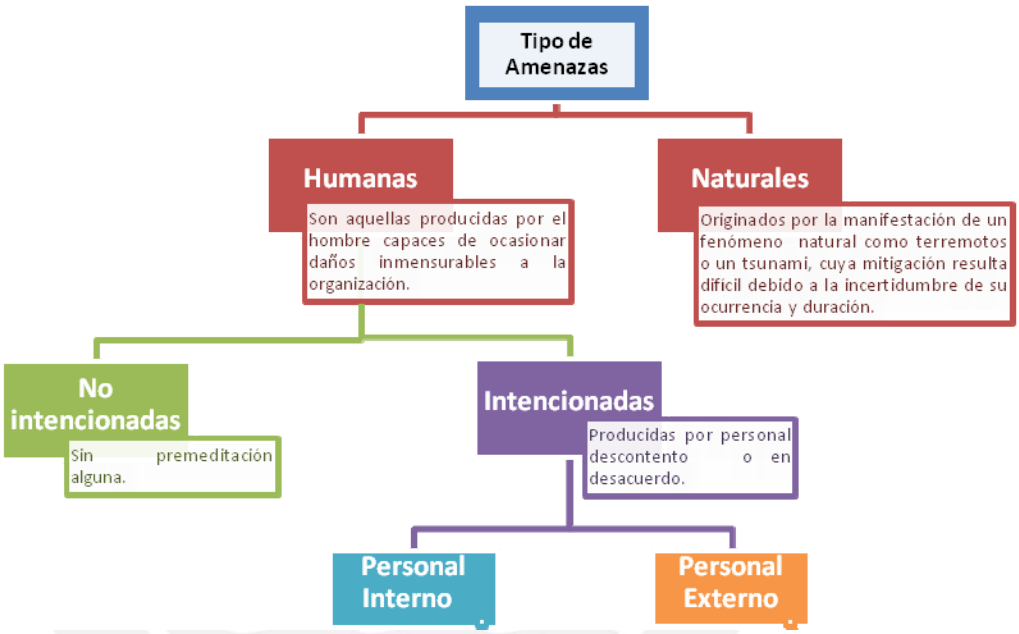


Figura 2.1. Tipos de amenazas [Del Pino, 2007]

- **Vulnerabilidad**

La debilidad de un activo o grupo de activos que puede ser explotada y perjudicada por una o más amenazas. [ISO 27002, 2005]. Son debilidades que pueden ser explotadas para convertir una amenaza en un riesgo real que puede causar daños graves en una organización. Las vulnerabilidades son una o más condiciones que pueden permitir a una amenaza afectar a un activo.Según el BCI [2010]: "*Las vulnerabilidades en el negocio y en el modelo de operación de una organización pueden considerarse en siete áreas: reputación, cadena de suministro, información y comunicaciones, sedes e instalaciones, personas, finanzas y clientes*".

[2]Elemento impreso o digital que contenga información, así como todo sistema --conformado por software, hardware y su documentación pertinente-- que cree, maneje, procese información y tiene valor para una organización; también se puede incluir a la infraestructura tecnológica donde se desenvuelven dichos sistemas. Se considera activo esté o no registrado contablemente [Tupia 2010].

Se puede imputar a la ausencia de controles o a su deficiente establecimiento como las principales causas de vulnerabilidad sobre los activos de una organización [Tupia, 2010].

- **Riesgo**

Potencial de que una amenaza –externa o interna– explote una vulnerabilidad de uno o varios activos ocasionando daño a la organización. Su naturaleza puede depender de aspectos operativos, financieros, regulatorios y administrativos [ISO 27005, 2008].

Según COSO en su "Marco de Gestión Integral de Riesgo" [2008]: *"Los riesgos son futuros eventos inciertos, los cuales pueden influir el cumplimiento de los objetivos estratégicos, operacionales, financieros y de cumplimiento".*

Causas de los Riesgos:

- **Personal:**Fallas cometidas por el personal. Ejemplo: Por falta de conocimiento.
- **Procesos:**Fallas causadas por debilidades en el diseño y/o ejecución de procesos de la organización como por ejemplo controles inadecuados.
- **Sistemas:**Fallas causadas por vulnerabilidades en los sistemas, como fallas de red o caídas de sistemas.
- **Eventos externos:** Fallas que resultan por cambios adversos en el entorno de la organización, por situaciones causadas por terceros o por desastres naturales.

Figura 2.2. Tipo de Riesgos [ISACA, 2011]

Identificar riesgos implica analizar causas de aparición, consecuencias, magnitud e impacto; así como definir criterios de aceptación y la implementación de controles.

- **Impacto**

El Business ContinuityInstitute [2010] lo define como un "*Evento que tiene la capacidad de provocar la pérdida de o la interrupción*[3] *de las operaciones, servicios o funciones de la organización, el cual, si no se administra, puede escalar y convertirse en una emergencia, crisis o desastre".*Su identificación y cuantificación es relevante en el proceso de la Gestión de Riesgos, que es el conjunto de actividades que permite analizar, tratar y evaluar los riesgos en las organizaciones. Cabe mencionar que la valoración del impacto puede ser expresado de forma cuantitativa, es decir estimando las pérdidas económicas, o de forma cualitativa, asignando un valor dentro de una escala (p. e. alto, bajo, medio), también se recurre al análisis de grado de pérdida o daño que causaría una interrupción en un activo de información mediante el manejo de probabilidades[4] de ocurrencia, ya que se utiliza para determinar si se invertirá en medidas para evitar dicha interrupción.

La interrupción se puede evitar teniendo un procedimiento que, o bien proporciona alguna forma alternativa de la continuidad del negocio o corrige el problema dentro de un tiempo aceptable. El impacto no siempre se produce inmediatamente después de una interrupción y la mayoría de las empresas pueden sobrevivir durante algún tiempo antes de que las pérdidas comiencen. Este período es vital para el negocio y varía entre empresas y líneas de negocio.Si se realiza un análisis de riesgos basado de tipo cuantitativo de impacto y las probabilidades, las escalas cualitativas del impacto son: catastrófico o extremo, grave, medio, moderado o bajo e insignificante probable. En la Figura 2.3 se muestra la matriz 5x5 conocida para la cuantificación de riesgos.

Cabe mencionar que la matriz mostrada se ajustará según las políticas que emplea la entidad referenciada en la presente tesis. Es decir, va a depender del tipo de organización y de los activos de información que se tengan para clasificar los riesgos y calcular los impactos.

[3] Evento que interrumpe las operaciones o procesos normales del negocio bien sea de manera anticipada (huracanes, inestabilidad política) o imprevista (bloqueos, ataques terroristas, fallas tecnológicas, o terremotos). [BCI 2012]

[4] Posibilidad de que suceda algo, siendo definida, medida o estimada de manera objetiva o subjetiva, o en términos descriptores generales (ejemplo: raro, poco, poco probable, probable casi seguro), frecuencias o probabilidades matemáticas.

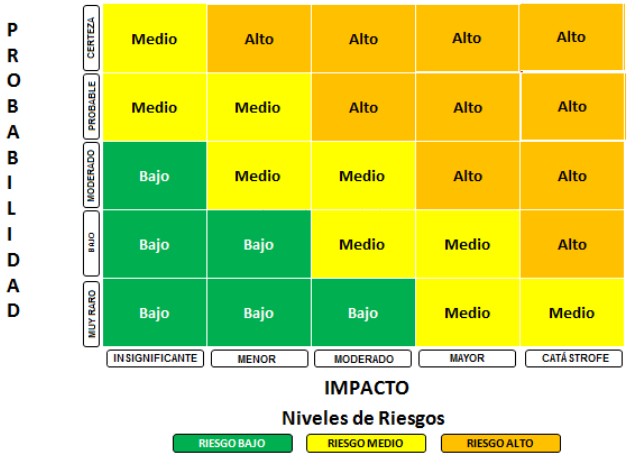


Figura 2.3. Matriz de riesgos basado en un análisis cualitativo de impacto y probabilidad [Sánchez, 2005]

- **Controles**

Son las políticas, medidas de seguridad, procedimientos y prácticas para reducir riesgos y que proveen cierto grado de certeza de que se lograrán los objetivos del negocio [Tupia, 2011]. Estos permiten que se realicen las correcciones necesarias en caso se detecten eventos que escapan de su alcance.

Los objetivos relevantes de los controles son:

- Garantizar que mediante los mecanismos de control establecidos se logren las metas de la organización.
- Salvaguardar los activos de la organización para mantener la integridad de la información.

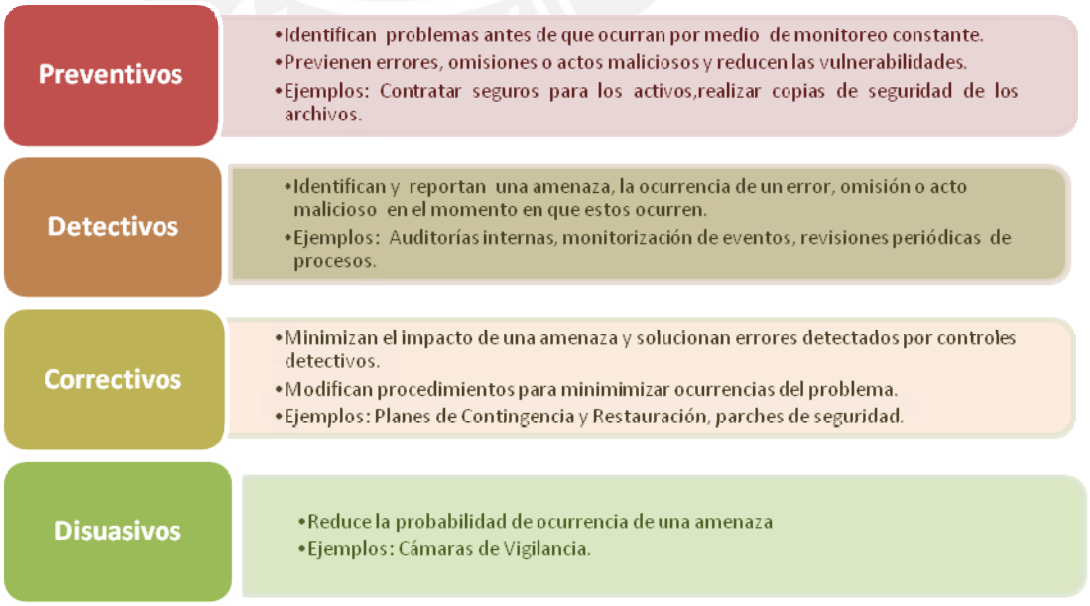


Figura 2.4. Tipos de Controles [Tupia, 2011]

2.1.2 Conceptos relacionados al control de continuidad de negocio

Normas Técnicas

- **BS25999**

Es la norma predecesora –remplazada por la actual ISO 22301– y es la primera norma británica para la gestión de continuidad y fue concebida con el fin de ayudar a minimizar el riesgo a las interrupciones, como un siniestro o una catástrofe.

Consta de dos partes:

Parte 1: Código de Práctica

Establece el proceso por el cual una organización puede desarrollar e implementar la continuidad de negocio, incluyendo una completa lista de controles basada en las mejores prácticas de BCM (Business Continuity Management) [BSI, 2006].

Parte 2: Especificación

Especifica los requisitos para establecer, implementar, operar, supervisar, revisar, probar, mantenery mejorar un sistema de gestión de continuidad de negocio en el contexto de la gestión global de riesgos de una organización [BSI, 2007].

- **ISO/IEC 22301:2012**

La norma ISO/IEC 22301:2012 Seguridad de la sociedad – Sistemas de gestión de la continuidad del negocio – Requisitos, es el nuevo estándar internacional para la gestión de continuidad del negocio. Se ha creado en respuesta al gran interés internacional en el original norma británica BS 25999-2 y otras normas regionales. Proporciona el mejor marco de referencia y es el nuevo estándar global para gestionar la continuidad del negocio en una organización.

Este estándar especifica requisitos para la creación y gestión de un negocio en efectivo de un SGCN. Es sólo para uso interno por y las partes externas, incluyendo organismos de certificación, para evaluar la capacidad de organización para cumplir los requisitos reglamentarios y del cliente así como los propios de la organización. La ISO/IEC 22301 contiene sólo aquellos requisitos que pueden ser auditados objetivamente, por lo tanto puede ser utilizado por una organización para asegurar que las partes interesadas usen un SGCN apropiadas en su lugar; y ha sido diseñada para lograr una mayor seguridad social (proporcionar protección de la

sociedad, y responder a, incidentes, emergencias y desastres provocados por actos humanos intencionales, riesgos naturales y fallas técnicas). [ISO, 2011].

La ISO/IEC 22301 ha remplazado a la norma británica BS 25999-2. Estas dos normas son bastante similares, pero la ISO/IEC 22301 puede ser considerada como una actualización de la BS 25999-2 y a diferencia de la norma británica ha sido aceptada por institutos de normas nacionales en 163 países.

Según John Sharp [2012, pg. 14] *"Las adiciones en la ISO/IEC 22301 han añadido más profundidad y claridad, mientras que las omisiones no son detrimento de las prácticas de BCM, en general son buenas principios".* Lo cierto es, que esta nueva norma pone mucho más énfasis en la comprensión de requisitos, el establecimiento de los objetivos y en la medición del desempeño y se mantienen los aspectos más importantes de la continuidad de negocio como son el análisis del impacto, la estrategia y la planificación.

Al igual que la norma predecesora, ISO/IEC 22301 es una norma adecuada para todo tipo de organización, grande o pequeña y perteneciente a cualquier sector. Es especialmente empleada para organizaciones que operan en sectores críticos de riesgo, como finanzas, transporte, telecomunicaciones y sector público, donde la necesidad de continuar la actividad comercial es primordial para el beneficio de la organización, los clientes y los interesados.

Cabe mencionar que la BCI está en revisión de una nueva norma internacional: **ISO DIS 22313: Seguridad social - Sistemas de Gestión de la Continuidad,** esta nueva norma está orientada a apoyar a las organizaciones con la implantación de un Sistema de Gestión de Continuidad de negocio eficaz (BCMS). [BCI, 2012].

Esta última norma complementará a la actual ISO/IEC 22301, ya que esta se logra destacar el "qué" se debe hacer y con la ISO 22313, el "cómo" implementar, operar y mejorar continuamente un sistema de gestión de continuidad de negocio.

- **ISO/IEC 27031:2011**

La norma ISO/IEC 27031:2011 Tecnología de Informacion - Técnicas de Seguridad - Directrices para la preparación de la información y tecnología de comunicación para la continuidad del negocio, es un estándar que ayuda a las organizaciones a prepararse para los incidentes, responder a riesgos de seguridad y ser menos susceptible a interrupciones [ISO 27031,2011].

Describe los conceptos y principios de la preparación de las tecnologías de la información y las comunicaciones (TIC) para la continuidad del negocio, y proporciona un marco de métodos y procesos para identificar y especificar todos los aspectos (tales como los criterios de desempeño, diseño e implantación) para la mejora de la preparación de las TIC de una organización para garantizar la continuidad del negocio.

Se aplica a cualquier organización (privadas, gubernamentales y no gubernamentales, independientemente de su tamaño) desarrollando su programa de adecuación de las TIC para la continuidad del negocio (ATCN, por sus siglas en inglés), y exigiendo que sus servicios e infraestructura TIC estén listos para apoyar las operaciones de negocios en el caso de nuevos eventos e incidentes, y las interrupciones relacionadas que puedan afectar la continuidad (incluida la seguridad de la información) de las funciones críticas del negocio. También permite a una organización medir los parámetros de desempeño correlacionados con su Continuidad de Negocio de una manera consistente y reconocida.

El ámbito de aplicación de esta norma abarca todos los eventos e incidentes (incluidos los relacionados con la seguridad de la información) que podrían tener un impacto en la infraestructura de las TIC y en los sistemas. Incluye y extiende las prácticas de manejo y gestión de incidentes de seguridad de la información y la planificación de la preparación de las TIC y sus servicios).

La norma incorpora el enfoque cíclico PDCA de la norma ISO 9000, extendiendo la continuidad convencional de procesos de negocio que plantean tener más en cuenta las TIC. Incorpora “fracaso métodos de evaluación correspondientes a los escenarios como FMEA (Análisis de Modo de Falla y Efectos), con énfasis en la identificación de” sucesos desencadenantes “que podrían precipitar incidentes graves”.

- **ISO/IEC 27001 / 27002**

Es la norma internacionalmente reconocida para la Gestión de Seguridad de la Información (ISO 27001) y su Código de Práctica (ISO 27002), ambas contemplan la continuidad de negocio como un elemento clave dentro de la gestión de la seguridad de la información.

Tiene como fin, contrarrestar interrupciones en las actividades empresariales y en los procesos críticos de negocio derivados de fallos importantes en los sistemas de información y garantizar su reanudación.

Esta norma indica que crear un SGSI es vital para preservar la Continuidad del Negocio. En la siguiente tabla se muestra la relación entre La gestión de Riesgos de la ISO27001 y la Gestión de Continuidad de Negocio de la ISO/IEC 22301.

ELEMENTO	ISO 27001: Gestión de Riesgos	ISO 22301: Gestión de Continuidad de Negocio
Herramientao Método	Análisis de Riesgos (AR)	Análisis de Impacto del Negocio (BIA)
Claves	Impacto y Probabilidad	Impacto y Tiempo
Tipos de Incidente	Todo tipo de eventualidades (segmentadas)	Fallos críticos para el negocio (no segmentadas)
Magnitud	Toda, generalmente segmentada	Incidentes estratégicos críticos para el negocio.
Enfoque	PREVENTIVO: Gestión de Riesgos para los objetivos del negocio.	CORRECTIVO: Gestión de Incidentes
Escenarios e Intensidad	Todos (segmentados)/Toda	El peor escenario(s)/Incidentes súbitos

Figura 2.5: Matriz de Relación entre la ISO 27001 y la ISO 22301[BSI, 2012]

Además en el capítulo 14 de la ISO/IEC27002 se tratan los siguientes aspectos de la seguridad de información y de la gestión de la continuidad del negocio:

- Incluir la seguridad de la información y evaluación de riesgos en el proceso de gestión de continuidad del negocio.
- Desarrollar e implementar los planes de continuidad incluyendo la seguridad de la Información.
- Marco referencial de la planeación de la continuidad del negocio.
- Prueba, mantenimiento y re-evaluación de los planes de continuidad del negocio.

- **COBIT**

Objetivo de Control para la Información y la Tecnología relacionada –conocido como COBIT– es una herramienta para la administración de las tecnologías de información. Desarrollada por ISACA como un estándar para la seguridad de la

tecnología de información y buenas prácticas de control. Constituye un marco unificador internacionalmente aceptado como una buena práctica para la gestión, el control de la información, de la tecnología de información y de los riesgos que estas sufren. *"Esta* última versión incorpora la última evolución de pensar en la gobernabilidad empresarial y técnicas de gestión, y establece los principios globalmente aceptados, prácticas, herramientas y modelos analíticos para ayudar a aumentar la confianza en, y el valor de los sistemas de información. Además incorpora la integración de otros marcos importantes, normas y recursos, incluyendo *Val IT*[5]*, Risk IT*[6]*, BMIS(*Business ModelforInformation Security)[7]*, ITAF* (IT Assurance Framework)[8]" [ISACA[9], 2012].

COBIT también está relacionado a la continuidad de negocios, en el proceso para administración de empresas de TI: DSS (Deliver, Service and Support), se concentran los aspectos de administración de la tecnología de la información. Cubre áreas tales como la ejecución de las aplicaciones dentro del sistema de TI y sus resultados, así como, los procesos de apoyo que permitan la ejecución eficaz y eficiente de estos sistemas de TI. Un proceso efectivo de continuidad de servicios, minimiza la probabilidad y el impacto de interrupciones mayores en los servicios de TI, sobre funciones y procesos claves del negocio [COBIT 5- DSS4, 2012].

"Probar el plan de continuidad de TI de forma regular para asegurar que los sistemas de TI pueden ser efectivamente recuperados, las deficiencias se aborden y el plan sigue siendo pertinente. Esto requiere una preparación cuidadosa, documentación, reporte de resultados de la prueba y, de acuerdo a los resultados, la implementación de un plan de acción. Considere el alcance de las pruebas de recuperación de aplicaciones individuales a escenarios de pruebas integrados a las pruebas de extremo a extremo y pruebas vendedor integrada ", [COBIT5- DSS4.5, 2012].

[5]Es un marco de referencia de gobierno que incluye principios rectores generalmente aceptados y procesos de soporte relativos a la evaluación y selección de inversiones de negocios de TI [ISACA, 2012].

[6]Es un marco de referencia normativo basado en un conjunto de principios rectores para una gestión efectiva de riesgos de TI.[ISACA,2012].

[7]Es una aproximación holística y orientada al negocio para la administración de la seguridad informática. [ISACA,2012]

[8]Es un marco para el diseño, la ejecución y reporte de auditorías de TI y de tareas de evaluación de cumplimiento. [ISACA,2012]

[9]Organización líder en Auditoria de Sistemas y Seguridad de los Activos de Información.

Las organizaciones pueden beneficiarse en la utilización de este marco para el manejo de continuidad de negocio, el cual les permitirá tener enfoques coherentes y mensurables ante interrupciones no planificada de servicios de TI.

Principios de COBIT

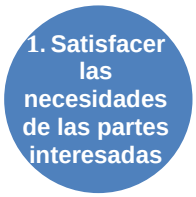


Figura 2.6. Principios de COBIT 5 [ISACA, 2012]

1. **Satisfacer las necesidades de las partes interesadas:** Las organizaciones deben considerar a todas las partes interesadas al tomar decisiones con respecto a la evaluación de riesgos, los beneficios y el manejo de recursos.
   Los objetivos en cascada de COBIT 5 traducen las necesidades de las partes interesadas en metas específicas, accionables y personalizadas dentro del contexto de la organización, de las metas relacionadas con TI y las metas habilitadoras.

   Beneficios de los objetivos en Cascada:

   - Permiten definir las prioridades para asegurar y mejorar el gobierno de TI, en base a los objetivos estratégicos de la organización y los riesgos relacionados.
   - Definen los objetivos y metas tangibles en diferentes niveles de responsabilidad.
   - Identifican y comunican qué importancia tienen los habilitadores para lograr sus metas.

2. **Cubrir la Organización de forma general:** COBIT no sólo se concentra en la "Función de TI", sino que cubre las funciones y procesos de la organización.
3. **Aplicar un solo marco integrado:** Permite a la organización poder usar COBIT como un único integrador en el marco de gobierno y administración.
4. **Habilitar un enfoque holístico:** Los habilitadores de COBIT son factores que –individual o colectivamente–influyen sobre la TI corporativa.

Existen 7 categorías de los habilitadores en COBIT 5:

Figura 2.7. Habilitadores de COBIT 5 [ISACA, 2012]

5. **Separar el Gobierno de la Gestión:** El marco COBIT plasma una distinción entre Gobierno y Gestión. El Gobierno asegura que se evalúen las necesidades de las partes interesadas para determinar los objetivos corporativos acordados a lograr; fijando directivas al definir prioridades y tomar decisiones; así como monitorear el desempeño, cumplimiento y progreso comparándolos contra directivas y objetivos fijados (EDM).La Administración planifica, construye, ejecuta y monitorea las actividades conforme a las directivas por el ente de Gobierno para lograr los objetivos de la Compañía.

- **NFPA 1600:2010**

El NFPA[10] 1600 establece una base de normalización para el planeamiento y operaciones de manejo de desastres/ emergencias al brindar elementos comunes del programa, técnicas, y procedimientos enfocados en su totalidad en el programa.

[10]Organización encargada de crear y mantener las normas y requisitos mínimos para la prevención contra incendio, capacitación, instalación y uso de medios de protección contra incendio.

Esta norma establece los componentes importantes de un plan que permita a las organizaciones desarrollar un programa para satisfacer sus necesidades particulares.

Algunos de los elementos más importantes mencionados son:

- **Identificación de peligros, evaluación de riesgos y su mitigación:** La evaluación de riesgos debe cuantificar la probabilidad de incidentes y la gravedad de sus consecuencias. Se debe cuantificar el impacto que tendría un desastre en sus activos, así como las consecuencias financieras directas o indirectas. El análisis del impacto debe cuantificar las emergencias potenciales de un riesgo, que permita evaluar el costo-beneficio por los esfuerzos de investigación y determinar cuánto invertir en planes de mitigación, respuesta y recuperación.
- **Administración de recursos:**Los recursos necesarios deben ser catalogados para su recuperación, y el acceso a éstos debe disponerse con anterioridad. Cualquier limitación debe ser identificada para que fallas puedan ser corregidas.
- **Planificación:** Todas las organizaciones deben tener un plan que cumpla con el reglamento, este debe contar con estrategias de mitigación a corto y largo plazo, una lista de funciones críticas, en orden de prioridades, un análisis de impacto, un programa de respuesta y recuperación total y un plan de evacuación.
- **Dirección, control y coordinación:** Toda organización debe contar con un sistema de administración de incidentes (IMS) y procedimientos para el control constante de incidentes.

El NFPA 1600 es una norma que establece un conjunto común de criterios para mitigar, preparase, responder y recuperarse ante desastres y emergencias, ha sido aprobada por el Instituto Americano Nacional de Normas y respaldado por la Asociación de Manejo de Emergencias y la Asociación internacional de Gerentes.

Conceptos directamente relacionados

- **BCM (Business Continuity Management)**

La Gestión de la Continuidad del Negocio es un proceso holístico que identifica amenazas potenciales a la organización e impactos a las operaciones del negocio

que tales amenazas puedan causar en caso de materializarse; y proporciona la estructura para construir resilencia[11] con capacidad para dar respuesta efectiva protegiendo los intereses de las partes interesadas, la reputación, el valor de la marca, la reputación y las actividades[12] creadoras de valor [ISO 22301:2012]

- **Asignación de responsabilidades**: Un programa de BCM exitoso depende de la identificación de roles y responsabilidades y autoridad claramente definidos para manejo del BCM y su proceso a través de la organización.

  El propósito de la asignación de roles y responsabilidades es garantizar que el personal comprenda sus funciones y responsabilidades y asegurar que las tareas requeridas para y mantener el BCM están asignadas a individuos competentes cuyo desempeño pueda monitorizarse.

- **Mantenimiento de BCM en la organización:** El mantenimiento del BCM involucra la gestión de un número de proyectos relacionados y la coordinación de las actividades que lo equilibra:
  - ✓ **Sensibilización**: Eventos que mantienen el entusiasmo para llevar a cabo el BCM.
  - ✓ **Planificación**: Desarrollo de planes para responder a los incidentes que pudieran no ocurrir.
  - ✓ **Medidas de Mitigación:** Implementación de medidas para mitigar el impacto de un incidente que pueda ocurrir mientras el programa está siendo desarrollado.
  - ✓ **Ejercicio:** Ejercicios para practicar los planes de contingencia.

  El propósito de este paso es asegurar que se mantiene un BCM sostenible en la organización. Al decir sostenible, es que se ha ganado el compromiso de la organización y cuenta con estructura y procedimientos en sitio para asegurar que está mantenido y mejorado y está disponible para el futuro previsible.

- **Gestión del Proyecto:** Cuando se compromete al mantenimiento del BCM en una organización se deben adoptar las disciplinas de Gestión de Proyectos. Los métodos seleccionados de Gestión de Proyectos deben ser adecuados al tamaño y complejidad de la organización.

[11] Habilidad de una organización para resistir al ser afectada por un incidente.

[12] Proceso o conjunto de procesos realizados por una organización (o en su nombre) que produce o apoya uno o más productos o servicios [BCI 2012].

- **Gestión continua de la Continuidad del Negocio:** El BCM necesita gestionarse en un ciclo continuo de mejora para su eficacia. Esto involucra la participación de varias áreas gerenciales, operativas, administrativas y técnicas que necesitan estar coordinadas.
- **Documentación del BCM:** Una parte importante del BCM es la gestión de su documentación, la cual necesita llevarse a cabo de una manera que sea consistente y fácil de entender. El nivel y tipo de documentación debe ser apropiado al tipo y tamaño de la organización.

Elementos del Ciclo de Vida del BCM

Lo conforman un conjunto de actividades de la Continuidad del Negocio que colectivamente cubren todos los aspectos y fases del BCM, que se repite como objetivo general de mejorar la resilencia organizacional. Se divide en seis prácticas profesionales:

Figura 2.8. Ciclo de Vida del BCM (Business ContinuityInstitute [BCI, 2013]

Prácticas de Gestión

1. **Política y Gestión de Programas**

   Es el inicio del ciclo de vida del BCM y se trata de la práctica profesional que define la política de la organización y la forma en que la política se llevará a cabo, controladas y validadas a través de un programa de BCM.

   La política BC incluye: La definición de BC para la organización y del ámbito de aplicación del BCM, asignar roles y responsabilidades de BC; un framework para la gestión del BCM; un conjunto de principios, directrices y estándares

mínimos; una definición clara de presupuesto, auditoría y responsabilidades de gobernanza.

2. **Incorporación de Continuidad de Negocio**

   Es la práctica profesional que continuamente busca integrar BC en las actividades empresariales del día a día y la cultura organizacional. Esta actividad no es exclusiva de BC; otras disciplinas también deben incorporarse en la organización de una manera similar. Disciplinas como la Calidad, Salud y Seguridad, Servicios Ambientales, Seguridad y Gestión de Riesgos tiene retos similares. Así que la oportunidad de compartir experiencias y oportunidades de aprendizaje a través de diversas disciplinas relacionadas es importante.

Prácticas Técnicas

3. **Análisis**

   Es la práctica profesional dentro del ciclo de vida de BCM que revisa y evalúa una organización en términos de cuáles son sus objetivos, su funcionamiento y las limitaciones del entorno en el que opera.

   La información recogida permite determinar la mejor manera de preparar una organización para ser capaz de manejar las interrupciones que de otro modo podrían seriamente o fatalmente dañarlo.
   La principal técnica utilizada para el análisis de una organización para la continuidad del negocio (BC) fines es el análisis del impacto del negocio (BIA). A nivel estratégico, puede hacer preguntas a la Alta Dirección que se refieren a la misión de la organización, sus objetivos, los objetivos y las prioridades. También se pueden utilizar los niveles táctico y operacional para profundizar e identificar información más detallada.

   Esta práctica profesional cubrirá la estimación de los recursos, instalaciones y servicios externos que requerirá cada actividad, tanto en la reanudación y volver a las operaciones normales. Dentro del programa de BCM, esta etapa debe centrarse en las amenazas inherentes a las actividades de negocios identificados como más urgentes en el BIA, en lugar de todas las amenazas a la organización.

4. **Diseño**

   Es la práctica profesional dentro del ciclo de vida de BCM que identifica y selecciona las estrategias y tácticas para determinar la continuidad y

recuperación de las pérdidas que se lograrán.La información obtenida de la etapa de análisis y decisiones tomadas en la etapa de Políticas y Gestión de Programas se utilizan para diseñar soluciones en las siguientes tres áreas:

- **Continuidad y estrategias de recuperación y tácticas**

El propósito de diseñar estrategias de recuperación y tácticas es fijar plazos para la recuperación e identificar los medios para que estos objetivos sean alcanzados. Esto puede llevarse a cabo en tres niveles de organización:

- ✓ Estratégico - productos y servicios;
- ✓ Táctica - Infraestructura de proceso y;
- ✓ Operacional - actividades que ofrecen los productos y servicios.

A nivel táctico, el proceso consiste en la infraestructura de los servicios e instalaciones necesarias para ofrecer un producto o servicio. Es donde:

- ✓ Las soluciones que harán planes viables en la práctica se han diseñado y
- ✓ Las decisiones probablemente incurrirán en la mayoría de los gastos.

El diseño de soluciones operativas puede requerir conocimientos técnicos más allá de las de un profesional. Asesoramiento técnico que tenga que ser solicitada a expertos en otros campos.

- **Medidas de mitigación de amenazas**

El propósito de diseñarlases identificar y seleccionar las medidas preventivas que se pueden implementar para reducir la probabilidad y/o el impacto de la interrupción de las actividades de la organización, la mayoría de tiempo crítico y urgente.

- **Estructura de respuesta a incidentes**

El propósito de diseñar una estructura de respuesta a incidentes es asegurar que existe un mecanismo documentado y entendido por completo para responder a un incidente que tiene el potencial de causar la interrupción de la organización, independientemente de su causa.

5. Implementación

Es la práctica profesional dentro del ciclo de vida del BCM que ejecuta las estrategias acordadas y tácticas a través del proceso de elaboración del Plan de Continuidad de Negocios (BCP).

El objetivo es identificar y documentar las prioridades, procedimientos, responsabilidades y recursos para ayudar a la organización en la gestión de un

incidente perturbador, mientras que la aplicación de estrategias de continuidad y recuperación a un nivel predeterminado de servicio.

Los requisitos fundamentales para una respuesta eficaz por parte de la organización son los siguientes:

- La capacidad de reconocer y evaluar las amenazas existentes y potenciales cuando se producen y para determinar una respuesta adecuada;
- Un procedimiento claro y entendido por la activación, la escalada y la estructura de respuesta a incidentes;
- Contar con el personal responsable y la capacidad para poner en práctica las estrategias de continuidad acordados (u objetivos) tal como se definen en los planes de la organización
- Seguir y recuperar las actividades interrumpidas;
- La capacidad de comunicarse de manera efectiva con las partes interesadas internas y externas.

Los resultados se pueden lograr por varios métodos y técnicas, y es importante que sea adecuado para las necesidades de la organización.

Las acciones descritas en los planes no están destinadas a cubrir todas las eventualidades que, por su naturaleza, todos los incidentes son diferentes. Los procedimientos pueden ser necesarios adaptar el evento específico que se ha producido y las oportunidades que pueda haber creado.

6. Validación

Es la práctica profesional dentro del ciclo de vida de BCM que confirma que el Programa de BCM responde a los objetivos establecidos en la Política de BC y que el BCP de la organización es apto para el propósito.

El objetivo de la validación es garantizar que la capacidad BC refleja la naturaleza, escala y complejidad de la organización que apoya y que es actual, precisa y completa, y que se adopten medidas para mejorar continuamente la resilencia organizacional.

La validación se logra a través de las siguientes tres actividades:

- **Hacer ejercicio:**

Un programa de ejercicio planificado es necesario para asegurar que todos los aspectos de la respuesta a un incidente que se han ejercido. En particular: toda la información en los planes se verifica; todos los planes se ensayan, y todo el personal pertinente (incluyendo diputados) se ejercen.

La capacidad de una organización no puede ser considerada fiable hasta que se haya ejercido. No importa lo bien diseñado una estrategia BC o Plan de Continuidad de Negocios (BCP), parece ser, los ejercicios fuertes y realistas que identificar problemas y supuestos que requieren atención.

Para tener éxito un programa de ejercicio debe empezar sencillamente y escalar gradualmente en términos de complejidad y desafío.

- **Mantenimiento:**

Mantiene acuerdos de la organización hasta la fecha, permite asegurar que la organización está preparada para responder a gestionar eficazmente los incidentes, a pesar del cambio constante.

Una parte importante del ciclo de vida de BCM es la gestión de la documentación, y el mantenimiento del programa de BCM se asegura de que esta documentación se mantiene actualizada y que la documentación actual y relevante es distribuido a las partes interesadas pertinentes.

- **Revisar:**

El objetivo de revisar es evaluar el programa de BCM e identificar las mejoras que tanto la ejecución de la organización del ciclo de vida del BCM y el nivel de resilencia organizacional.

Hay cinco tipos básicos de opinión:

- **Auditoría (interna y externa)** - un proceso formal de revisión que mide programa BCM frente a un estándar acordado previamente;
- **Auto-evaluación** - una evaluación del programa de BCM a sí misma;
- **Garantía de calidad (QA**) - un procedimiento que garantice que las diferentes salidas del programa de BCM cumplen con los requisitos;
- **Evaluación del Desempeño** - una revisión de la actuación de las personas encargadas de las funciones y responsabilidades; y
- **Rendimiento Proveedor** - un proveedor clave o una revisión del desempeño de un proveedor de servicios de recuperación.

Beneficios de un programa BCM eficiente:

- Ser capaz de entender a la empresa, de los procesos y ayudar a mejorarlos
- Identificar los diversos eventos que podrían impactar a la continuidad de las operaciones y su impacto financiero, humano y de reputación.
- Prevenir o minimizar las pérdidas para el negocio en caso de desastre.

- Clasificar los activos para priorizar su protección en caso de desastre.
- Evitar que los incidentes se conviertan en una verdadera crisis, ya que se asegura una mínima interrupción del flujo de trabajo.
- Implicar a los recursos humanos de la compañía en las actividades de continuidad.
- Mejorar una reputación corporativa y ventajas competitivas debido a la demostrada capacidad de mantener la entrega de servicios.

- **Plan- Do- Check- Act (PDCA)**

Es un modelo para la planificación, establecimiento, implementación, operación, supervisión, revisión y mantenimiento de la mejora continua de la eficacia de un BCMS de la organización.

Las fases del modelo Planificación- Implementación- Verificación- Mantenimiento son:

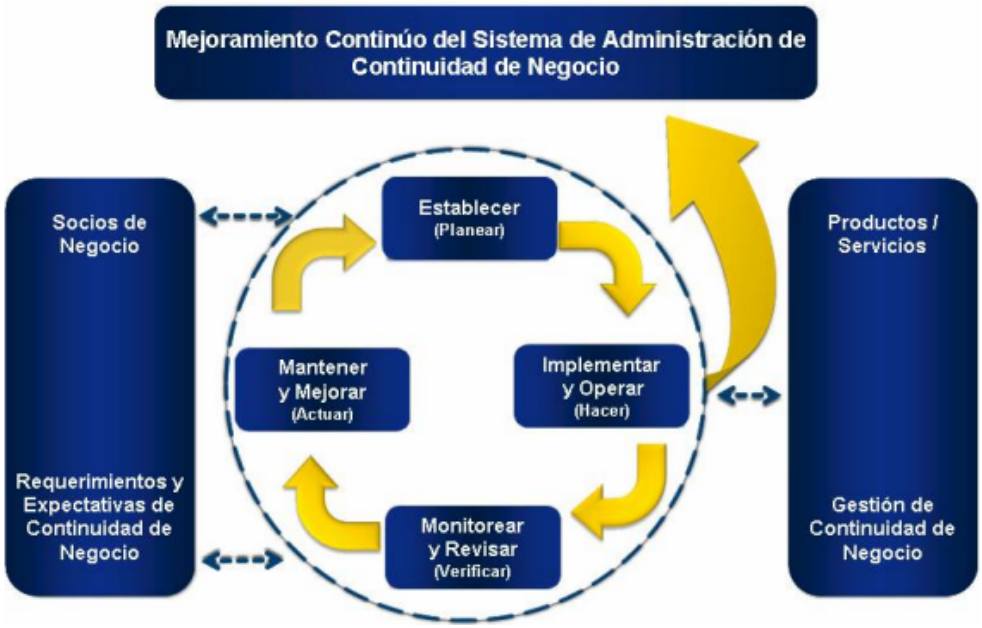


Figura 2.9. Fases del modelo PDCA [BSI, 2012]

Plan (Establecer): Establecer la política, objetivos, controles, procesos y procedimientos de continuidad de negocio con el fin de obtener resultados que se alinean con las políticas generales y los objetivos de la organización.

Do (Implementar y Operar): Implementar y operar la política de la continuidad de negocios, controles proceso y procedimientos.

Check (Monitorear y Revisar): Monitorear y evaluar el desempeño de la política de continuidad de negocio y los objetivos, informando de los resultados a la

gerencia para su revisión, y determinar y autorizar las acciones de remediación y mejoramiento.

Act (Mantener y Mejorar): Mantener y mejorar los BCMS mediante la adopción de medidas correctivas, con base en los resultados de la revisión de la gestión y la revalorización del alcance de las BCMS y la política y objetivo de continuidad de negocio.

- **BIA (Business ImpactAnalysis)**

BIA es el proceso que consiste en analizar las funciones del negocio y el efecto que una interrupción del negocio pudiera causar sobre ellas. De acuerdo al BCIes *"el análisis a nivel de gestión por el cual una organización evalúa los impactos cuantitativos y cualitativos, los efectos y la pérdida que podría resultar si se tuviera que sufrir una emergencia, incidente o crisis. Los hallazgos de un BIA se utiliza para tomar decisiones sobre la estrategia de Continuidad del Negocio y soluciones".*

Un BIA ayuda a identificar lo que se perderá si el negocio se interrumpe, lo que podría costar la pérdida de beneficios e ingresos, el deterioro de las relaciones con los clientes, pérdida de reputación. También es un proceso clave para entender cuánto de una interrupción cada proceso o tarea puede tolerar antes de que el daño sea irremediable y de cuales recursos (personas, máquinas, documentos u otros procesos) depende la empresa.

Los propósitos de un BIA para cada actividad, producto o servicio son:

- Documentar los impactos en tiempo que se derivarán de su pérdida o interrupción.
- Identificar el Máximo Periodo Tolerable de Interrupción (MTPD).
- Identificar las dependencias–tanto internas como externas– que son necesarias para que la actividad funcione de forma eficaz.

BIA es la base para la toma de decisiones y la planificación estratégica de recuperación en la cual la estructura de gestión de la continuidad reside y es sin duda uno de los resultados más importantes y fundamentales del ciclo de vida de la continuidad del negocio. Es a través del BIA que las necesidades de la organización en respuesta a un desastre pueden ser adecuadamente evaluadas y priorizadas.

- **Business Continuity Plan (BCP)**

El plan de continuidad de negocios es un conjunto de procedimientos documentados e información que ha sido desarrollada, recopilada y mantenida a disposición para su uso durante un incidente, para permitir a la organización continua con la entrega de sus actividades más importantes y urgentes a un nivel aceptable predefinido. El plan de continuidad de negocios se actualiza y mantiene a través del proceso de BCM que se definió anteriormente. Este reducirá el número y la magnitud de las decisiones que se toman durante un período en que los errores pueden resultar mayores. El Plan establecerá, organizará y documentará los riesgos, responsabilidades, políticas y procedimientos, acuerdos con entidades internas y externas.

Un claro ejemplo de la ausencia de un plan de continuidad de negocios es cuando se malogra el disco duro de una computadora, en realidad no cuesta nada repararlo, pero el daño y el impacto que puede causar es inmensurable si es que no hay ningún plan de mitigación ante su pérdida (mitigación podría ser alguna forma de copia de seguridad, por ejemplo).

Como menciona Hotchkiss [2010, p. 26.]. *"Eventos*[13]*de pequeño impacto también pueden causar daño en términos de tiempo de reparación"*, como en el ejemplo antes mencionado, una pequeña deficiencia puede causar un impacto bastante limitado en negocio, pero puede llegar a costar un montón de dinero para reparar debido a la falta de planificación. Esto significa que se debe tener en cuenta el impacto y el daño, así como el costo de recuperación llegar a una idea razonable del costo de no tener un plan de continuidad.

Los elementos claves de un BCP son:

- **Respuesta a la emergencia:** Respuesta inmediata a una emergencia. Por ejemplo un Plan de Evacuación.
- **Gestión del Incidente:** La gestión de Respuesta al incidente como por ejemplo un Plan de Continuidad en Crisis.
- **Continuidad:** La repuesta inicial del negocio para asegurar que las actividades esenciales pueden continuar operando a un nivel mínimo aceptable.
- **Recuperación:** Un plan para recuperar actividades a un nivel sostenible.
- **Reanudación:** Un plan para reanudar las operaciones de la organización.

[13] Algo que ocurre - por ejemplo, un incendio en un edificio. Es de interés principalmente por sus consecuencias.

Un Plan de Continuidad de Negocio (BCP) está formado por los siguientes planes: Plan de Emergencia, Plan de Comunicación de Crisis, Plan de Gestión de Crisis y Plan de Recuperación de Desastres

- **DisasterRecovery Plan (DRP)**

Es un proceso documentado o conjunto de procedimientos o acciones para recuperar y proteger la infraestructura de TI de una organización en caso de un desastre . Refiriéndose con desastre a todo evento súbito, imprevisto catastrófico que interrumpe los procesos de negocio lo suficiente como para poner en peligro la viabilidad de la organización .Un desastre podría ser el resultado de un daño importante a una parte de las operaciones, la pérdida total de una instalación, o la incapacidad de los empleados para acceder a esa instalación.EL DRP es "una declaración exhaustiva de acciones coherentes que deben tomarse antes, durante y después de un desastre". [Geoffrey, 2012]

El Plan de Recuperación de Desastres tiene como objetivo proporcionar un marco para la reconstrucción de las operaciones vitales de la organización, para garantizar la seguridad de los empleados y la reanudación de las operaciones sensibles a tiempo y los servicios en caso de una emergencia.

El DRP incluye la planeación de pasos para evitar riesgos y mitigarlos, DRP es aplicable en todos los aspectos de un negocio, sin embargo se utiliza normalmente en el contexto de operaciones para el procesamiento de datos.

Beneficios de un Plan de Recuperación ante un desastre:

- Permite a la organización evitar riesgos de retrasos o mitigar el impacto de estos al: minimizar potenciales perdidas económicas y; decrementar la exposición a escenarios de desastre;
- Reducir la probabilidad de que ocurran al mejorar la capacidad de recuperar las operaciones normales del negocio.
- Reducir las interrupciones de la operación.
- Provee un procedimiento pre- planificado minimizando el tiempo de toma de decisiones en caso de desastre.
- Elimina la confusión y reduce la probabilidad de error humano debido al estrés que produce una crisis.
- Protege los activos de la organización incluyendo al recurso humano.

Instituciones

- **BCI (Business ContinuityInstitute)**

El BCI fue establecido en 1994 para permitir a los miembros obtener orientación y apoyo de los compañeros practicantes de continuidad del negocio.

El rol más amplio de la BCI es promover los más altos estándares de competencia profesional y ética comercial en la provisión y mantenimiento de la planificación de la continuidad del negocio y Servicios.

Los objetivos principales del BCI consiste en:

- Establecer, mantener y promover altos estándares para la práctica ética de BCM, incluyendo entrega de bienes y servicios
- Establecer y fomentar una educación de calidad y el desarrollo personal de los practicantes de todos los niveles
- Para iniciar, desarrollar, evaluar y comunicar el pensamiento BCM, estándares y buenas prácticas
- Para influir en los responsables políticos, líderes de opinión y otros grupos de interés en todo el mundo en el tema de BCM.

- **DRI International (Disaster Recovery Institute)**

DRI International es una organización sin fines de lucro fundada en 1988 como el Instituto de Recuperación de Desastres para lograr que profesionales de diversas industrias y sectores empresariales entiendan los principios de continuidad de negocio y mantengan su nivel de conocimiento a través de una educación continua.

DRI Internacional tiene como objetivo promover base de conocimiento para la continuidad del negocio y la recuperación de desastres. Esto lo logran a través de la educación, la asistencia y la publicación de labase de recursos estándar. Por otro lado, administra los principales programas de certificación para las personas comprometidas en la práctica y gestión de continuidad de negocios.

Sus objetivos son:

- Promover una base común de gestión de la continuidad de la profesión.
- Promover la credibilidad y la profesionalidad de las personas certificadas.
- Lograr que los certificados tengan claro el tema de recuperación de desastres.

- **NIST (National Institute of Standards and Technology)**

El Instituto Nacional de Estándares y Tecnología (NIST) es un organismo federal no regulador que forma parte de la Administración de Tecnología del Departamento de Comercio de los EE.UU. cuyos objetivos son elaborar y promover patrones de medición, normas y tecnología. Tiene una relación con la continuidad de negocios ya que, en su publicación 800-34 (ContingencyPlanning Guide for InformationTechnology Systems) de su serie 800 [NIST, 2010], desarrolla una guía de planes de contingencia de los sistemas de información de cualquier empresa.

- **BSI (British StandardsInstitution)**

Es una institución independiente y global, la cual se basa en la creación de normas para lograr la estandarización de procesos, mejorar las prácticas de gestión y promover la innovación, proporciona soluciones basadas en estándares en más de 150 países. Es un organismo colaborador de ISO y proveedor de dichas normas.

BSI ayuda a las empresas, gobiernos y organizaciones de todo el mundo a aumentar la calidad y el rendimiento de una forma sostenible y socialmente responsable. BSI Group es reconocido a nivel mundial por la publicación de BS 25999 y la certificación como líder y proveedor de formación en este campo.
En la actualidad, BSI apoya el despliegue de las nuevas Normas Internacionales de Continuidad de Negocio - ISO 22301 e ISO 22313.

Entre sus actividades principales se incluyen:

- Certificar sistemas de gestión y productos.
- Desarrollar normas nacionales e internacionales.
- Proporcionar formación e información sobre normas y comercio internacional.
- Realizar auditorías a las organizaciones.

2.1.3 Marco regulatorio / legal

- **NTP 27001:2008**

Norma Técnica Peruana de Seguridad de Información es una norma elaborada por el Comité Técnico de Normalización de codificación e Intercambio Electrónico de Datos (EDI) en el año 2008, utilizando como antecedente las ISO/IEC 27001:2005.

La NTP 27001:2008 [INDECOPI, 2009], tiene como objetivos proporcionar un modelo para establecer, implementar, operar, monitorear, mantener y mejorar un efectivo Sistema de Gestión de Seguridad de Información como una buena práctica de la gestión de la seguridad.

Cabe mencionar que se hará mayor énfasis en lo relacionado de esta norma a la continuidad de negocios.Comprende de 11 ítems de control de seguridad que envuelven un total de 39 categorías principales, los cuales se muestran a continuación, enfatizando en el ítem de continuidad:

1. Política de seguridad
2. Seguridad Organizacional
3. Gestión de Activos
4. Seguridad en Recursos Humanos
5. Seguridad física y del entorno
6. Gestión de comunicaciones y operaciones
7. Control de accesos
8. Adquisición, desarrollo y mantenimiento de sistemas de información
9. Gestión de incidentes en la Seguridad de Información
10. **Gestión de continuidad del negocio**

    Aspectos de la gestión de continuidad del negocio: Reaccionar ante las interrupciones a las actividades del negocio y proteger los procesos críticos del negocio de los efectos de fallas mayores o desastres en los activos y asegurar la reanudación oportuna.

Este ítem en particular menciona que las formas de lograr una buena continuidad de negocio son:

- Incluyendo la seguridad de información en la gestión de la continuidad del negocio, para ello se deben establecer procedimientos y responsabilidades de gestión con el fin de asegurar una respuesta efectiva ante cualquier tipo de incidente.
- Relacionando la continuidad de negocios con la evaluación de riesgos, para ello deben ser identificadas las amenazas que pueden causar interrupciones, así como las probabilidades e impacto de dichas interrupciones.
- Desarrollando e implementando planes de continuidad que incluyan la seguridad de información

- Contando con un marco de planificación de la continuidad del negocio, con el fin de asegurar consistencia e identificar prioridades de prueba y mantenimiento.
- Probando, manteniendo y reevaluando los planes de continuidad del negocio, con el fin de asegurar que estén actualizados y sean efectivos.

11. Cumplimiento

- **Basilea II– Comité de Supervisión Bancaria de Basilea**

Se proponen medidas para proteger a las entidades financieras frente a los riesgos financieros y operacionales. Entre las medidas para alcanzar estos niveles de protección se encuentran el desarrollo de planes de continuidad y recuperación.
La actual regulación de la SBS para la gestión de riesgo operacional, se ajusta a los lineamientos de Basilea II, e incluye exigencias de continuidad de negocios.

- **Sarbanes – OxleyAct (SOX)**

Creada en el 2002 de la voluntad de controlar las empresas que cotizan en la bolsa de Nueva York y sus filiales, para evitar que los procesos con transacciones económicas pudieran ser alterados de forma fraudulenta. Establece requerimientos de seguridad relacionados con la continuidad del negocio (los artículos 302, 404 y 409 afectan a la continuidad de negocio). Hace varios años que la SOX traspasó las fronteras y actualmente existen versiones de la misma en Japón (llamada J-SOX) o en la Unión Europea (llamada EuroSOX).

2.2 Estado del Arte

En la actualidad, son pocas las empresas alrededor del mundo que se han certificado con la ISO 22301 y existen en el mercado algunas herramientas que contribuyen con la realización de algunos de los ítems que son parte de un SGCN, como el Análisis de Impacto de Negocio (BIA), el Plan de Continuidad de Negocios (BCP) y el Plan de Recuperación de Desastres (DRP). A continuación, se presentarán algunos de los ejemplos más relevantes, que de acuerdo al criterio del autor, aportan parte de la solución del problema planteado.

2.2.1 Formas exactas de resolver el problema

- **BANKINTER**

Es una entidad financiera española reconocida por su alto desarrollo tecnológico. Bankinter ha sido pionero en España en la puesta en marcha de sistemas de banca a distancia complementarios a la tradicional red de oficinas, como el teléfono, Internet o, ahora, el móvil, lo que le ha llevado a ofrecer una diversidad de posibilidades de relación y comercialización de productos desde una estrategia multicanal perfectamente integrada. Actualmente reconocida por su concientización sobre la importancia de un SGCN para identificar las amenazas potenciales sobre la organización y el impacto que supondrían tales amenazas en las operaciones de negocio en caso de materializarse.

BankInter ha sido la primera entidad del sector financiero a nivel mundial en obtener la nueva certificación de la norma ISO/IEC 22301 emitida por el BSI Group.Han enfatizado en ampliar el análisis de impacto al negocio, la gestión de los riesgos y el cumplimiento con los requisitos legales, regulatorios y de partes interesadas. La gestión de la crisis y las comunicaciones necesarias, han madurado y los requisitos de la nueva norma lo que hace que las situaciones que supongan una amenaza para la seguridad física de las personas o para la disponibilidad de los procesos críticos sean gestionadas de una forma muy eficaz**.**

BankInter es un ejemplo de un buen manejo de un SGCN y está preparada para cualquier incidente o desastre.Un último estudio desarrollado en Febrero del 2012 por la IDC a organizaciones españolas reveló que el 71,3% de los encuestados usa un SGCN y el 29,2% asegura estar certificados bajo la norma BS- 25999, mientras, en realidad, tan sólo el 0,99% de dichas empresas está certificado[IDC, 2012].

2.2.2 Productos comerciales para continuidad de negocios

- **LDRPS (Living Disaster Recovery Planning System)**

En un software de planificación para la continuidad, creado por la compañía Sistemas StrohlGroup, el cual fue adquirido por el actual proveedor SunGardAvailabilityServices[14], este software proporciona una flexibilidad esencial

[14]Segmento de negocio de SunGard Data Systems Inc. que proporciona recuperación de desastres , servicios en la nube , servicios gestionados , consultoría ITy de continuidad del negocio de gestión de servicios.

del diseño del plan, recolección, importación y exportación de datos, personalización, generación de informes, y plan de mantenimiento. También proporciona la opción de personalizar los programas de continuidad de acuerdo a las necesidades o las preferencias de la organización que la adquiera.

Existen tres versiones de LDRPS, creadas dependiendo del nivel de funcionalidad que se necesita:

- **Essential:** Ofrece la funcionalidad de escalabilidad, para ajustarse a las necesidades de las organizaciones que están en las etapas emergentes de desarrollo del programa.
- **Professional:** Proporciona personalización con muchas más opciones, una interfaz master para administradores y una mayor seguridad de acceso para el usuario.
- **Enterprise:** Incluye capacidades de personalización completas, un mayor acceso de seguridad, notificación por correo electrónico, e importación y aprobación del plan para satisfacer las necesidades de los programas de planificación.

Algunas características de este software son:

- **Nivel de planeamiento Experto:** Sus interfaces están diseñadas para ayudar a los usuarios a alcanzar sus objetivos de planificación con instrucciones paso a paso. Ofrecen metodología incorporada y ayuda a los usuarios a introducir los datos más relevantes para completar su planificación.
- **Sencillez:** Es fácil de entender y usar, específicamente diseñado para seguir los pasos de la planificación, utiliza un árbol de navegación y tiene un aspecto consistente en todas las pantallas.
- **Posibilidades de creación:** Cuenta con más de 200 informes estándar que sintetizan detalles críticos sobre los empleados, clientes y proveedores necesarios en el caso de una interrupción. Y al igual que los navegadores, los usuarios individuales pueden personalizar sus propios CrystalReports.
- **Seguridad:** Permite proteger la información confidencial del plan y filtrarla para su público objetivo. Muchos de los paquetes de seguridad estándar y filtros de acceso se pueden personalizar, permitiendo a los planes adaptarse a los cambios organizativos.
- **Planificación del Alcance:** Permite elaborar planes generales (por ejemplo, de evacuación o planes de gestión de crisis), o planes dirigidos a la recuperación de componentes principales (procesos, aplicaciones y hardware).

- **Mapa de Dependencias:** Proporciona una interfaz gráfica que permite identificar fácilmente las dependencias dentro del plan, y de toda la organización.

Este software puede integrarse con BIA Professional, un software que ayuda a recopilar la información que se necesita para identificar las unidades y procesos críticos del negocio, el impacto de las interrupciones en el tiempo, y el equipo necesario para recuperarse. Este software permite ahorrar tiempo y asegurar consistencia de datos a través de todo el programa.Algunas características de BIA Professional son:

- **Preguntas correctas:** Con más de 55 preguntas diseñadas por expertos, plantillas estandarizadas que se pueden utilizar como están o personalizarlas.
- **Control inteligente de la encuesta:** Cuenta con guías de estudio para responder sólo preguntas que son relevantes, proporciona informacion necesaria para garantizar la integridad de los resultados.
- **Análisis y presentación de datos simplificada:** La funcionalidad de informes de BIA Profesional simplifica el análisis y la presentación de los resultados de la encuesta. Los usuarios tienen más de 150 informes estándares para analizar los datos desde múltiples ángulos, o pueden crear informes personalizados para profundizar en las respuestas específicas.

A continuación se muestra algunas funcionalidades del software LDRPS:

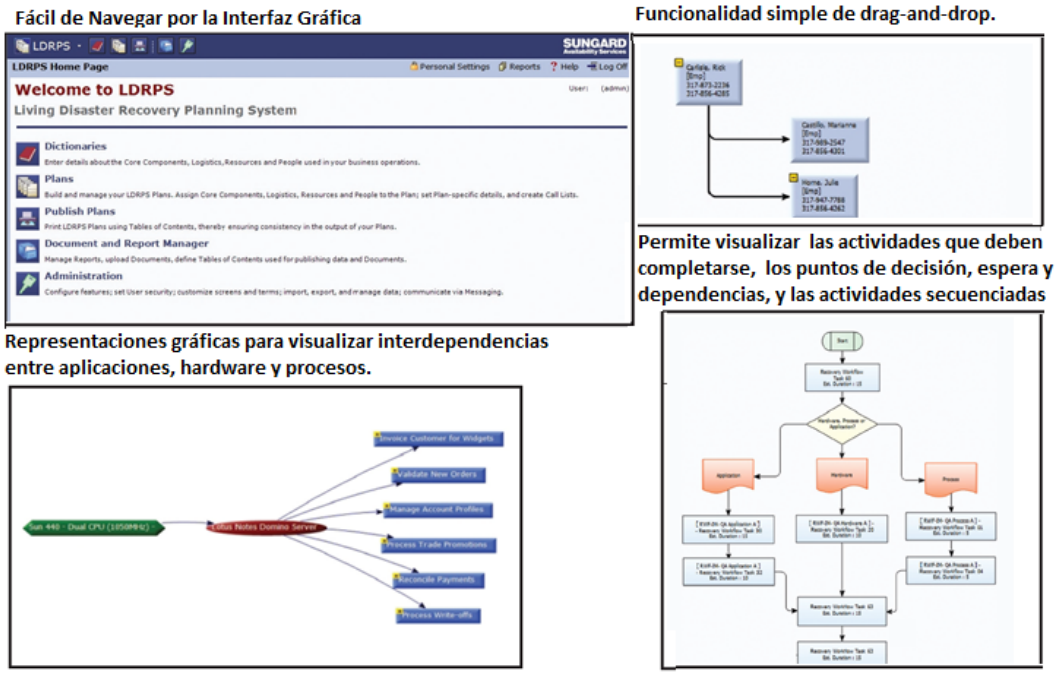


Figura 2.10. LDRPS Software [SunGard Availability Services, 2012]

- **BC- 3 Intelligent Business Continuity**

Es un software web creado por la compañía australiana RISKLOGIC[15], que apoya a las organizaciones a gestionar de forma efectiva sus actividades de continuidad de negocio. Es ideal para organizaciones financieras o de amplio alcance. Permite construir algunos documentos que forman parte de un SGCN como son: el BIA, evaluaciones de amenazas, estrategias y planes de cumplimiento, informes de auditoría y el programa de ejercicios.Algunas características del software son:

- **Accesibilidad:** Asegura que la información crítica esté disponible en Internet.
- **Capacidad de utilización:** Intuitivo, interfaz fácil de usar para los usuarios, los aprobadores y administradores.
- **Flexibilidad:** Adaptable y diseñado para satisfacer necesidades específicas.
- **Integración:** Se integra con las tecnologías existentes y los sistemas internos, incluidas las herramientas de notificación de crisis.
- **Control:** visibilidad y gestión del programa a través de su organización.
- **End-to-end:** Escalable, es decir un mismo diseño para todas las ventanas de los requisitos de su programa de continuidad de negocio.
- **Automatización:**De programas de auditoría, mantenimiento y conformidad.

- **Business Catalyst Software**

Es un software web empresarial creado por AvalutionConsulting[16] para el manejo de continuidad de negocio.Las características que incluye el software son:

- **Política y Procedimiento:** Permite documentar políticas de continuidad del negocio de forma rápida mediante las plantillas proporcionadas.
- **Business ImpactAnalysis**: Permite identificar principales dependencias de las áreas de la organización, incluidas las instalaciones, aplicaciones, proveedores. Además permite la cartografía visual de cada área.
- **Hacer ejercicio, y Gestión de Programas General:** Proporciona un panel para revisar el progreso del programa (comentarios o mejora del plan BIA).

[15] Es una de las principales empresas de consultoría australiana enfocada en la creación de resilencia organizacional para el negocio, gobierno, además provee software para facilitar el proceso de gestión de continuidad de negocios. [RISKLOGIC, 2012].

[16] Es un negocio que se especializa en la continuidad del negocio y recuperación ante desastres de TI consultoría, outsourcing y soluciones de software para organizaciones de los sectores público y privado. [AvalutionConsulting , 2012].

- **Recuperación de definición de estrategias:** Identifica los requisitos mínimos de recursos para elementos como instalaciones, tecnologías y comunicaciones.
- **Plan de Desarrollo (Negocio y TI):**Permite el desarrollo de las comunicaciones, la respuesta y los planes de recuperación basado en uno o más escenarios, como pérdida de la instalación, del personal o de la tecnología

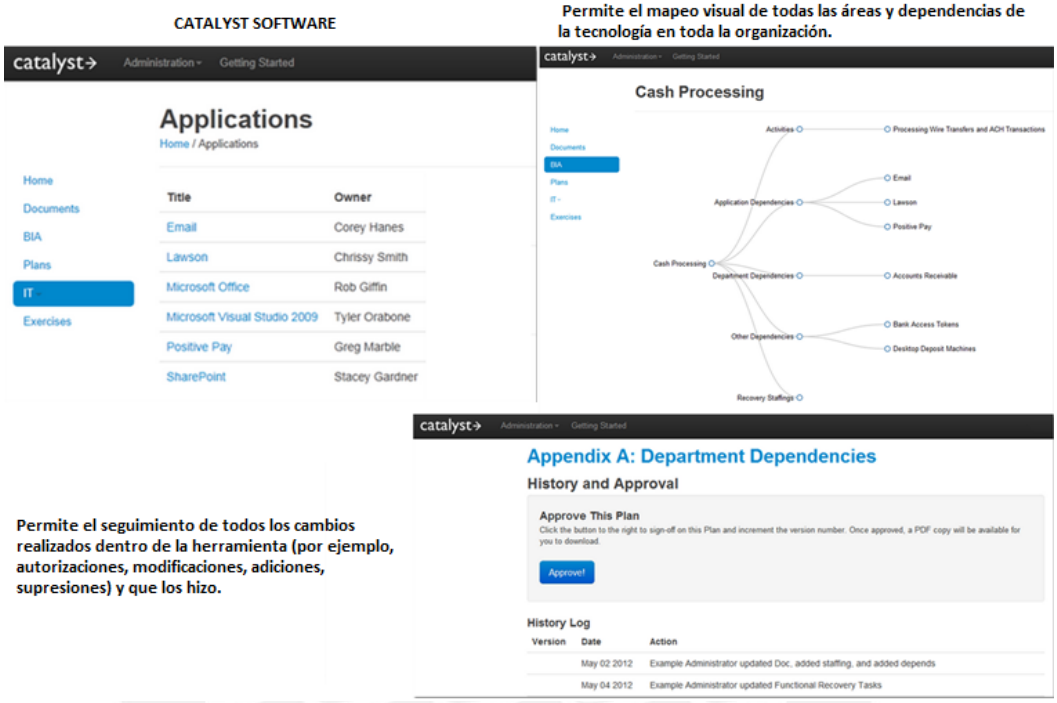


Figura 2.11. Pantallas de Catalyst Software [Avalution, 2012]

2.2.3 Conclusiones sobre el estado del arte

En la actualidad existen empresas reconocidas a nivel mundial por contar con un adecuado SGCN. En el Perú entidades financieras y públicas han desarrollado un correcto SGCN que llevan actualmente a la práctica, algunas empresas medianas privadas en el país no cuentan con un SGCN o un plan de continuidad en caso exista algún incidente o desastre. Erróneamente se ha creído que un SGCN sólo aplica a organizaciones de alcance internacional las cuales manejan grandes cantidades de recursos o procesos de alta criticidad; lo cierto es que, toda empresa debe estar respaldada por una planificación de mitigación para cualquier incidente y proteger sus activos y procesos vitales para así asegurar sus operaciones y continuidad del negocio. Además el tema de continuidad de negocios aún no ha sido explotado en el Perú y menos en el sector público.Es por ello que el diseño de SGCN a realizaren la presente tesis, pretende colaborar con la actividad de gestión de continuidad de negocios para una organización pública en el Perú.

Capítulo 3. Análisis

En el presente capítulo se presenta el ciclo para realizar un SGCN, incluyendo lo mencionado en cada punto por la norma ISO, cómo implementarlo en RENIEC y el entregable correspondiente a cada apartado.

3.1 Inicio de la Gestión de Continuidad de Negocios

En esteapartado del capítulo de Análisis se presentan los principios del inicio de la Gestión de Continuidad de Negociospara lograr comprender detalladamente esta práctica profesional. A continuación, se muestran los aspectos que disponen la norma ISO/IEC 22301 y la Guía de Buenas Prácticas del BCI para iniciar el BCM. Por último, se describen las acciones necesarias para efectuarlo en RENIEC.

3.1.1 Síntesis

En RENIEC se debe instaurar la necesidad de un Sistema de Gestión de Continuidad de Negocios, incorporandoestrategias, planes de recuperación ante desastres, planes de continuidad de negocios y plan de gestión de crisis y emergencia,para lo cual es vitalconseguirel respaldo de la Alta Dirección paralograr organizar y comprender políticas, y procesos críticos para construir el marco del BCM (Gestión de Continuidad de Negocio).

La política del BCM permite establecer el alcance del programa BCM y refleja las razones del porqué está siendo implementado este. La política proporciona el contexto en el cual serán implementadas las capacidades requeridas e identifica los principios a los que la organización aspira.

La NormaTécnica Peruana NTP–ISO 27001: 2008 obliga a entidades públicas como RENIEC, a instaurar, implementar, mantener y documentar un Sistema de Gestión de Seguridad de Información (SGSI), cuyo objetivo es garantizar que los riesgos de la seguridad de la información son conocidos, asumidos, minimizados y gestionados por la organización de una forma documentada, sistemática, estructurada, continua, repetible, eficiente y adaptada a los cambios que se produzcan en la organización, los riesgos, el entorno y las tecnologías. Todo ello en base a los activos de información más importantes, los cuales se obtienen del resultado del análisis de riesgos previamente realizado y los que cumplen con las expectativas de los stakeholders del sistema, ciudadanos y proveedores.

La Norma ISO/IEC 22301 define a la continuidad de negocios como “la capacidad estratégica de la organización para permitir la continuidad de la entrega de productos o servicios a niveles aceptables, previamente definidos”.

Al no manejar medios de control, la organización se encuentra vulnerable ante un desastre o incidente, es por ello que, la gestión de continuidad de negocios están estrechamente ligadas a la gestión de seguridad de información y a RENIEC y comparten un mismo objetivo el cual es asegurar la disponibilidad de los procesos críticos y la informaciónsegún lo requieran.

3.1.2 ISO/IEC 22301:2012 – Guía de Buenas Prácticas del BCI

La ISO/IEC 22301 junto con la Guía de Buenas Prácticas del BCI provee aspectos y requisitos que todo SGCN debe cumplir:

- **Definir Políticas de Continuidad de Negocio**

La Alta Dirección establece, valida, aprueba y se compromete con la política del BCM, logrando hacer referencia a los objetivos y al alcance (incluyendo limitaciones)del SGCN dentro de la organización. Una vez establecida, es necesario que se informe dichas políticas a todo el personal de la organización, para lograr así llevar un control de ellas ante cambios relevantes cada cierto periodo de tiempo.

- **Aprovisionamiento de recursos**

Como primer paso, la Alta Dirección debe establecer y asignar roles y responsabilidades, según el conocimiento, al personal competente para el BCM y así, proporcionar los recursos necesarios para determinar, implementar, operar, monitorear, revisar y mejorar el SGCN a realizar.

Por otro lado, al iniciar este nuevo proyecto es relevante y necesario elaborar un presupuesto base de los principales recursos que requiere el SGCN y que refleje elfinanciamiento del proyecto;conforme se vaya desarrollando el mismo, será necesario adicionar presupuestos relacionados a nuevas estrategias de recuperación para el proyecto a realizar.
La Alta Dirección debe lograr analizar el nivel de riesgo aceptable del alcance del SGCN, comunicar a todo el personal y los stakeholders la relevancia del mismo y lograr establecer sus políticas para realizar una mejora continua. Además, debe elegir un responsable capacitado parael manejo de las políticas y otros para el mantenimiento del SGCN independientemente del rol que desempeñan actualmente, para ello es necesario establecer revisiones periódicas del SGCN.

- **Concientización, Conocimiento y Preparación**

La organización debe asignar responsabilidades a todo el personal competente y capacitado para realizar los roles previamente definidos en el SGCN, una vez establecidos los responsables, se debe analizar si es necesario una previa preparación y entrenamiento al personal seleccionado para las diferentes tareas continuas referentes al SGCN. De ser necesario se proporciona entrenamiento y se documenta cualquier preparación o entrenamiento impartidos, que proveen habilidades, grados de calificación o experiencias ganadas y finalmente se analiza la efectividad del entrenamiento realizado.

3.1.3 Aplicación en RENIEC

Para efectuar e implementar el Inicio de Gestión de Continuidad de Negocios en la RENIEC se sugiere:

a. Analizar el grado de necesidad de Continuidad de Negocios en la organización

- Identificar exigencias del ámbito regulatorio o legal.
- Alinear las políticas necesarias para el SGCN con las recomendaciones del ámbito regulatorio/ legal.
- Identificar recomendaciones relevantes brindadas por las autoridades.

- Identificar desastres o incidentes que puedan impactar negativamente la operación de procesos de negocio críticos.
- Explicar la relevancia de los Planes manejados dentro del SGCN.

b. Involucrar a la Alta Dirección de RENIEC con el BCM

- Comunica el rol y la responsabilidad de Alta Dirección para el BCM.

c. Participar al personal la necesidad del BCM

- Alinear las ventajas del BCM con las estrategias y objetivos de la organización.
- Convencer al personal la relevancia del manejo de un BCM mediante estadísticas o reportes realizados referentes al tema.
- Comprometer a todo el personal con el BCM.

d. Establecer Roles, Responsabilidades y Relaciones referentes al BCM

- Seleccionar el personal adecuado.
- Definir los roles y responsabilidades.
- Desarrollar un conjunto de objetivos apropiado para el programa BCM.

e. Establecer una estimación de costos para el BCM

- Establecer y Validar los recursos necesarios para el BCM.
- Realizar una estimación de costos financieros.
- Validar y garantizar el compromiso de alta gerencia para cubrir los recursos requeridos.

f. Establecer Comités requeridos por el BCM

- Comité de Comunicación de crisis, de Gestión de crisis, de Emergencia, de Planificación de Continuidad y Restauración ante Desastres.

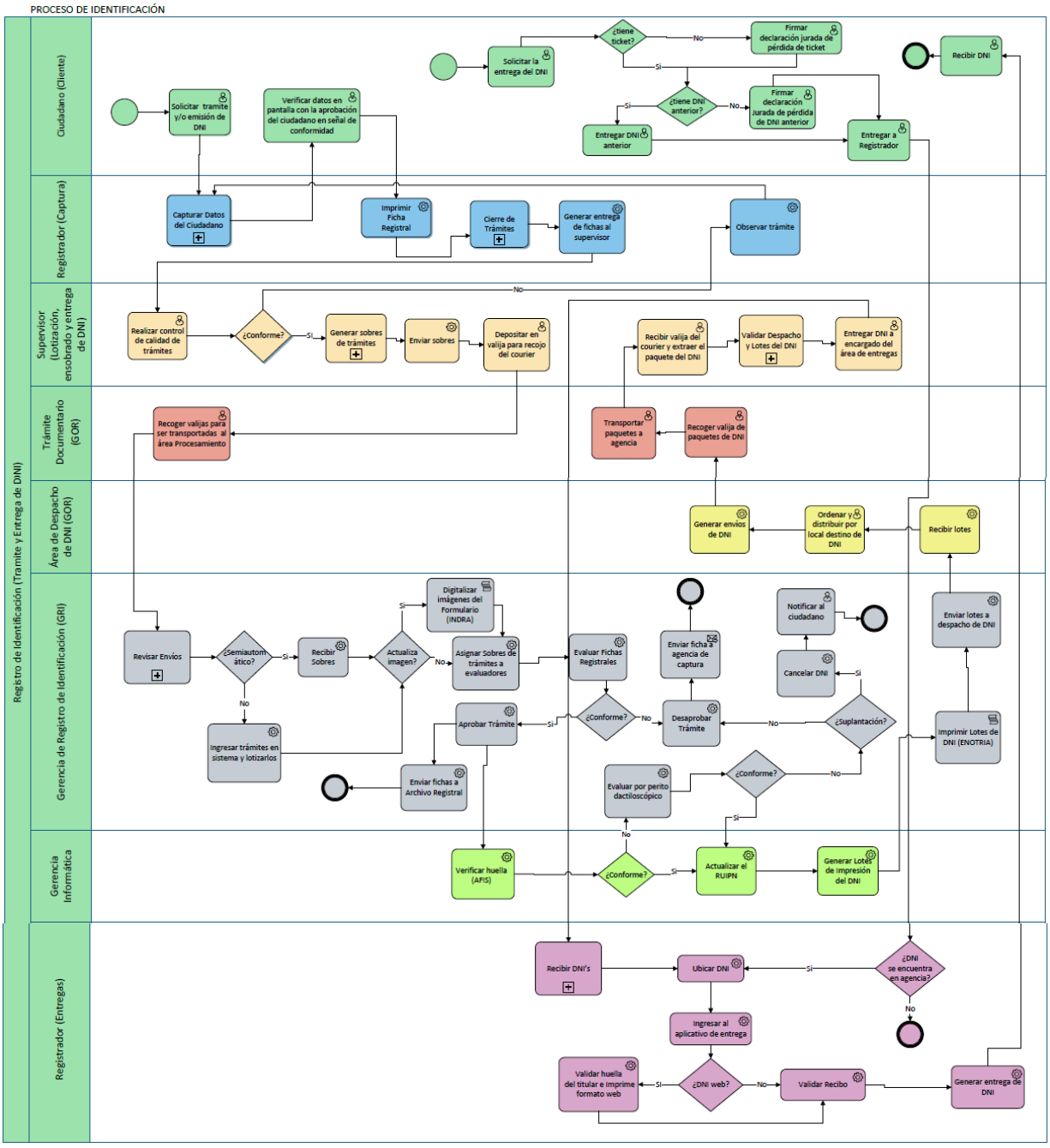
g. Establecer un plan de proyecto del BCM y los requerimientos de gestión y planes necesarios para el SGCN.

h. Obtener Aprobación y Compromiso de la Alta Dirección, estableciendo períodos para reportar el avance para la respectiva validación.

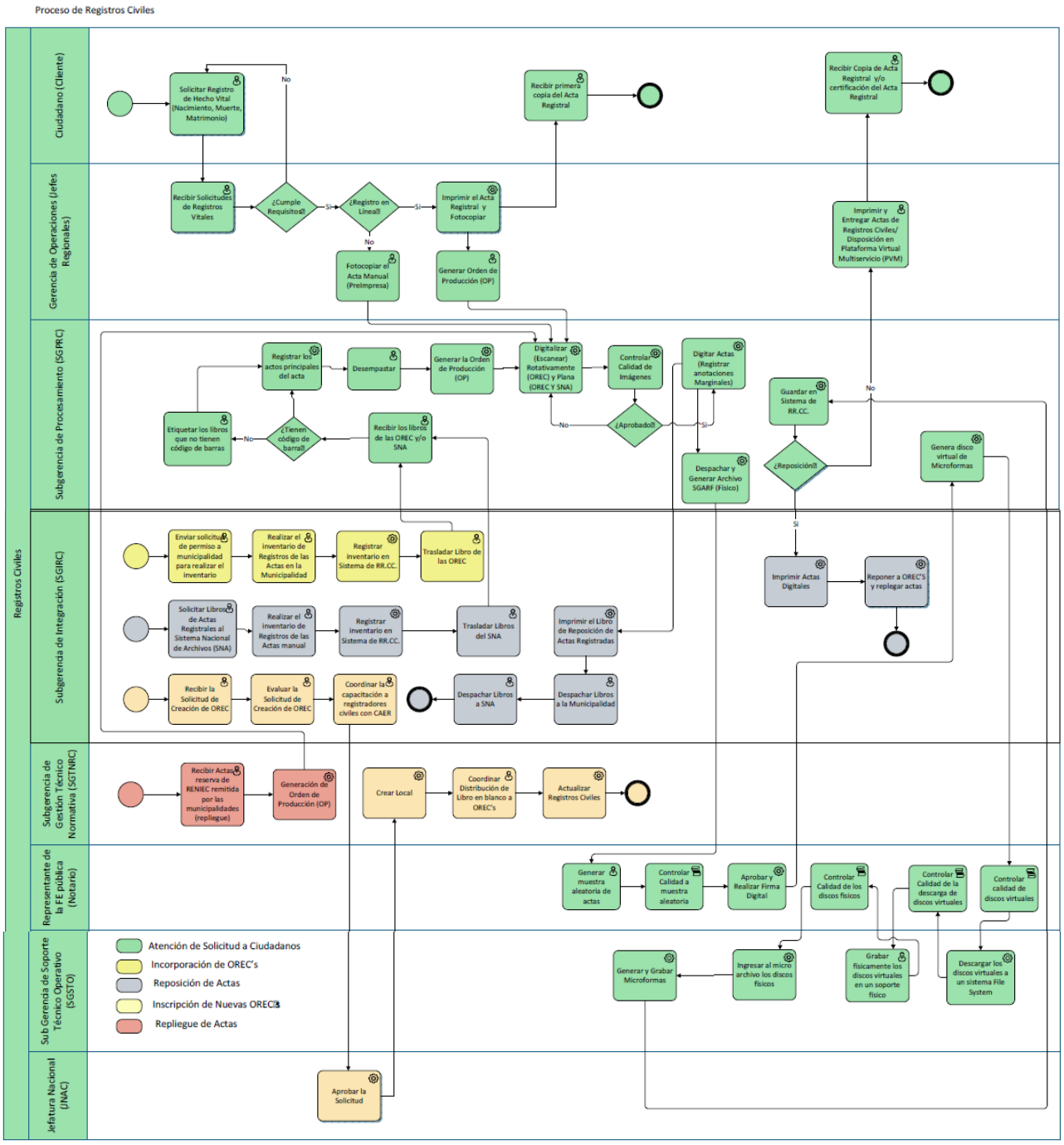
3.1.4 Entregable:Diagrama de Procesos bajo la notación BPMN 2.0

Nota: Los subprocesos se encuentran como **ANEXO B.**

- **Proceso de Identificación**



- **Proceso de Registros Civiles**



3.2 Identificación, Gestión y Control de Riesgos.

En este apartado se presenta la identificación, gestión y control de los principales riesgos que existen en los procesos críticos de RENIEC. A continuación se muestran los aspectos que disponen la norma ISO/IEC 22301 y la Guía de Buenas Prácticas del BCI para la evaluación y gestión de los riesgos. Por último, se describen las acciones necesarias para efectuarlo en RENIEC.

3.2.1 Síntesis

En RENIEC se deberá determinar acontecimientos internos y externos que puedan impactar en forma negativa a la organización y los controles necesarios para prevenir o mitigar los efectos potenciales de riesgos, que de materializarse, pueden causar daños y pérdidas.

Cabe mencionar, que dependiendo de la relevancia del riesgo para el negocio y el tipo, la Alta Dirección puede decidir aceptar que existe un riesgo de interrupción y monitorearlo, eliminar la fuente que origina el riesgo, implementar controles pertinentes, transferir el riesgo a un tercero (Ejemplo: Aseguradora), compartirlo, o suspender y dar por terminado el servicio y/o producto que causa dicho riesgo.

3.2.2 ISO/IEC 22301:2012 – Guía de Buenas Prácticas del BCI

Es necesario que la organización adopte una metodología para la identificación, evaluación, gestión y control de los riesgos existentes en los procesos críticos del negocio, para que a través de la identificación previa de las amenazas y vulnerabilidades de incidentes en los mismos, se logre determinar las causas, las probabilidades y estimar el impacto de un determinado incidente en la organización.

La organización debe:

- Identificar Amenazas
- Identificar Vulnerabilidades
- Estimar el impacto en la organización de cada amenaza identificada.
- Determinar los riesgos a partir de las amenazas y vulnerabilidades identificadas.
- Registrar los riesgos y documentar toda la información identificada.
- Identificar los riesgos de procesos críticos y tratarlos de acuerdo al nivel de aceptación del riesgo que ha sido determinado previamente por la Alta Gerencia.

- Realizar el mantenimiento de los riesgos y controles de cambios relevantes en los procesos críticos de la organización cada cierto tiempo.

3.2.3 Aplicación en RENIEC

De acuerdo a las buenas prácticas del BCI y lo mencionado en la norma ISO 22301, se sugieren las siguientes acciones para realizar en RENIEC:

a. Conocimiento y comprensión de los potenciales de pérdidas:

- Identificar las amenazas internas y externas conocidas que pueden causar interrupción de las actividades más urgentes de la organización. Tales como: Desastres Naturales, ocasionados por el hombre de manera intencional o accidental, amenazas externas, tecnológicas, con identificación previa y sin ella y controlables o que escapan del nivel del control de la organización.
- De acuerdo al enfoque de la Alta Dirección, determinar un sistema de puntuación en la evaluación del riesgo para los impactos y las probabilidades.
- Estimar el impacto en la organización de cada amenaza utilizando el sistema de puntuación de acuerdo.
- Determinar la probabilidad de ocurrencia de cada amenaza y el peso utilizando el sistema de puntuación.
- Calcular el riesgo de cada amenaza mediante la combinación de las puntuaciones de impacto y la probabilidad, de acuerdo con una fórmula acordada.
- Dar prioridad a las amenazas según el nivel de impacto en las actividades más urgentes.
- Determinar temas legales o regulatorios relacionados.
- Establecer un continuo soporte al proceso de evaluación.

b. Determinar controles para prevenir y/o mitigar el efecto de los potenciales de incidentes que causan daños y pérdidas

c. Identificar, evaluar y escoger metodologías adecuadas para facilitar el análisis y gestión de riesgos, para ello es necesario previamente realizar un análisis costo beneficio, ventajas-desventajas de la metodología a usar.

d. Revisar la efectividad de los controles a implementar

- Realizar una planificación previa de los controles a implementar.

- Validar el costo/ beneficio y prioridades de dichos controles.
- Establecer comunicaciones efectivas y acuerdos de nivel de servicios referente a continuidad de negocios con proveedores, entidades estrechamente ligadas y ciudadanos, así como los integrantes propios de la organización.
- Seleccionar las respuestas efectivas y oportunas ante los riesgos: aceptar, evitar, controlar, monitorear, compartir o transmitir.

e. Evaluar y Controlar los Riesgos

- Determinar escenarios de desastres de acuerdo a los riesgos expuestos de la organización
- Clasificarlos riesgos considerando: riesgos bajo el control de la organización, riesgos más allá del control, amenazas con aviso previo (lluvias) y sin aviso previo (terremoto).
- Evaluar el impacto de los riesgos en activos tangibles e intangibles de la organización como: personal, tecnologías de información e infraestructura.
- Evaluar controles alineados a los impactos debido a riesgos de incidentes o desastres, como por ejemplo: controles preventivos (detectores de humo en caso incendio), detectivos (uso de antivirus) y correctivos (Planes de contingencia).

f. Administración de registros vitales

- Identificar documentos, registros vitales y electrónicos en la organización y qué métodos de respaldo se utilizan.
- Efectuar procedimientos efectivos y viablespara larecuperación de registros vitales de la organización.

3.2.4 Entregable: Matriz de Riesgos de RENIEC

Leyenda:

TIPO DE CONTROL	Descripción
PM	Preventivo Manual
PA	Preventivo Automático
DM	Detectivo Manual
DA	DetectivoAutomático
CM	Correctivo Manual
CA	Correctivo Automático

FRECUENCIA	Descripción
PERM	Permanente
PERIO	Periódico
OCA	Ocasional

RIESGOS DEL PROCESO DE IDENTIFICACIÓN

Riesgo del Proceso					Controles efectivos						Evaluación de Riesgos Controlados			
ID	Descripción	Escenario	Evento	Causa	ID	Descripción	Responsable	Tipo de Control	Nivel de Control	Frecuencia	**Impacto**	Probabilidad	Nivel de Riesgo	Criticidad
R01	Daños en el Centro de Cómputo (destrucción y/o deterioro de los equipos como, Centrales de Comunicaciones, Ambiente de Pre-producción, Equipos de monitoreo y Central de Ejecución de Proceso de Identificación)	Incendio	Error de respaldo y backup	Desempeño, respaldo y proceso inadecuado	C01	Tener backup de equipos críticos en el Sitio Alterno	Área de TI	PA	Regular	PERM	5	3	8	Extrema
					C02	Contar con Sistema de detección y extinción de incendios.	Área de TI	PM	Regular	PERM				
					C03	Supervisión Constante para evitar el desorden y acumulación de desperdicios y mal uso de los toma corrientes.	Área de TI	PM	Regular	PERM				
					C04	Equipos de emergencia (Brigadistas).	Área de TI	PM	Regular	PERM				
					C05	Capacitación a los brigadistas sobre la ubicación y uso de los equipos contra incendio (grifos, gabinetes de manga, extinguidores).	Área de TI	PM	Regular	PERM				
					C06	Mantenimiento y conservación de los equipos contra incendios.	Área de TI	PM	Regular	PERIO				
R02	Pérdidas de registros vitales (planos de red, software (Sistemas de Identificación, de RUIPN), u hardware, bases de datos, etc.),	Incendio	Error de respaldo y backup	Falta de disponibilidad de procesos relevantes	C07	Manejo de copias de respaldo en caso de información relevante y backup de quipos críticos, de base de datos en Sitio Alterno.	Área de TI	PA	Regular	PERM	3	3	6	Moderado
					C08	Realizar revisiones de hardware y conexiones de redes para evitar cortos circuitos.	Soporte	PM	Regular	PERIO				

R03	Pérdida parcial o total de Infraestructura de central administrativa de RENIEC.	Sismo/ Incendio	Error	Falta de espacio físico para operar	C09	Señalización de: Rutas de escape, puertas y escaleras de emergencia; así como las tareas de seguridad.	Mantenimiento	PM	Regular	PERM	5	4	9	Alto
					C10	Supervisión constante de que las rutas de escape se encuentren libres (evitando acumulación de paquetes y material en desuso) y bien definidas.	Área de TI	PM	Regular	PERM				
					C11	Formación de brigadas de evacuación.	Área de TI	PM	Regular	PERM				
					C12	Realizar Simulacros de evacuación	Área de TI	PM	Regular	PERIO				
R04	Daño a la infraestructura de telecomunicaciones (interrupción del servicio de voz (telefonía) y/o datos, cualquier problema físico que detenga las operaciones de los equipos de comunicación entre áreas para el buen manejo del proceso o afecte el medio de transmisión).	Sismo	Error de respaldo	Respaldo y Control inadecuado	C13	Contar con Centro de Cómputo de Respaldo (en otra ubicación física con igual número de equipos y de idénticas características a los del en el Centro de Cómputo Principal.	Gerente de Finanzas	PA	Regular	PERM	4	5	4	Moderado
					C14	Poseer doble fuente de alimentación deenergía (diferentes UPS) en todos los Equipos Críticos (de Comunicación, Servidores, etc.)en ambosCentros de Cómputo.	Soporte	PA	Regular	PERM				
					C15	Contar con idénticas características en los Enlaces de Comunicación de los principales proveedores de telecomunicaciones.	Soporte	PA	Regular	PERM				
					C16	Realizar pruebas periódicas de disponibilidad de comunicaciones.	Soporte	PA	Regular	PERIO				

R05	Daño en la Infraestructura Administrativa por los cables de energía del edificio y daño en el centro de cómputo, a causa de una sobrecarga de energía por parte del proveedor externo que abastece energía	Incendio	Error de cableado y conectividad	Proceso y control inadecuado	C17	Contar con interruptores termomagnéticos en la sub-estación eléctrica, que no permite el paso de sobretensión y cortocircuito.	Soporte	PA	Regular	PERO	8	4	10	Extremo
					C18	Contar con servicios de mantenimiento preventivo a la sub-estación eléctrica e interruptores termomagnéticos.	Soporte	PM	Regular	PERM				
R06	No definir personal alterno en caso de no contar con el directo.	Sismo/ Incendio	Error	Falla de personal	C19	Establecer personal alterno para las actividades críticas del proceso de identificación	RRHH	PM	Regular	PERM	3	4	7	Moderado
R07	Personal alterno de GOR Y GRI no capacitado para restauración de operaciones.	Sismo/ Incendio	Incumplimiento de roles y capacitaciones	Desempeño y Control inadecuado	C20	Realizar capacitaciones y entrenamiento de las principales funciones y manejo de sistemas para personal alterno identificado.	RRHH	PM	Regular	PERM	4	3	2	Bajo
R08	Falla en prestación de servicios tercerizados (Digitalización de Imágenes de Formulario por INDRA e Imprimir Lotes de DNI por ENOTRIA)	Sismo	Error de Servicio	Falta de disponibilidad de proveedor	C21	Contar con proveedores de emergencia para casos de interrupciones o falta de disponibilidad de proveedores principales.	Logística	PM	Regular	PERM	6	4	7	Moderado
					C22	Garantizar continuidad de negocios en los SLA establecidos con los proveedores involucrados.	Logística	PM	Regular	PERM				

RIESGOS DEL PROCESO DE REGISTROS CIVILES

Riesgo del Proceso					Controles efectivos						Evaluación de Riesgos Controlados			
ID	Descripción	Escenario	Evento	Causa	ID	Descripción	Responsable	Tipo de Control	Nivel de Control	Frecuencia	**Impacto**	Probabilidad	Nivel de Riesgo	Criticidad
R01	Registro de hechos vitales almacenados en la aplicación de Registros Civiles no accesibles para el personal por falta de backup.	Sismo	Incumplimiento de responsabilidades y respaldo.	Desempeño, respaldo y proceso inadecuado	C01	El sistema genera una copia de respaldo al gestionar hechos vitales en un sistema backup alterno	Área de TI	PA	Regular	PERM	5	3	10	Extrema
R02	Pérdida de libros de hechos vitales físicos al no contar con serie de identificación.	Sismo	Error de respaldo	Falta de disponibilidad de información	C02	Se efectuará una reinscripción, sólo para este tipo de casos, con la mayor responsabilidad y con conocimiento al ente rector (RENIEC).	Reproceso	CA	Regular	PERM	4	6	5	Moderado
R03	Información disponible limitada para la atención de usuarios que requieren de servicios de emisión, certificación y registro de hechos vitales.	Incendio	Software de RRCC	Falta de disponibilidad de información	C03	Se realiza un reproceso para determinar qué información requiere ser detallada en el proceso de respaldo	Reproceso	PA	Regular	PERM	3	1	2	Bajo
R04	Libros de hechos vitales quemados por incendio sin contarcon una justificación del registro probablemente creado.	Incendio	Error de respaldo y backup	Falta de disponibilidad de información	C04	Se efectuará una reinscripción, sólo para este tipo de casos, con la mayorresponsabilidad y con conocimiento al Ente rector (RENIEC).	Reproceso	CA	Regular	PERM	4	5	4	Moderado

R05	No definir activos relevantes del proceso para ser respaldados y/o duplicados en Sitios Alternos de Operación.	Sismo/ Incendio	Error de manejo de datos	Mantenimiento o carga	C05	Al realizar una solicitud de activos de respaldo, considerar en ella una sección de respaldo y recuperación donde se detalla las pautas que se deben tener en cuenta para la definición de activos a respaldar.	Cada Área involucrada en RC (SGIRC, SGRTO,SGPRC,SGSTO,JNAC)	PM	Regular	PERM	5	2	8	Extremo
R06	Soporte físico para discos de Registros civiles sin copia de respaldo	Sismo/ Incendio	Incumplimiento de responsabilidades y respaldo.	Fallas en respaldo de disco	C06	Contar con un procedimiento de respaldo donde la información que se almacena en el disco, primero esté en archivos lógicos para luego pasar a cartuchos físicos de gran almacenamiento.	Almacenamiento	PA	Alto	PERM	2	3	6	Moderado
					C07	Contar con controles y alertas tanto en disco como en los cartuchos físicos que permitan un respaldo fluido sin errores.	Almacenamiento	PA	Alto	PERM				
R07	No definir personal alterno en caso de no contar con el directo.	Sismo/ Incendio	Error	Falla de personal	C08	Establecer personal alterno para las actividades críticas de RRCC.	RRHH	PM	Regular	PERM	3	4	7	Moderado
R08	Personal alterno de GOR Y SGIRC no capacitado para restauración de operaciones.	Sismo/ Incendio	Incumplimiento de roles y capacitaciones	Desempeño y Control inadecuado	C09	Realizar capacitaciones y entrenamiento de las principales funciones y manejo de sistemas para personal alterno identificado.	RRHH	PM	Regular	PERM	4	3	2	Bajo

3.3 Análisis de Impacto del Negocio (BIA)

En este apartado se presenta el propósito y los pasos para realizar un Análisis de Impacto del Negocio (BIA) en RENIEC. A continuación se muestran los aspectos que disponen la norma ISO/IEC 22301 y la Guía de Buenas Prácticas del BCI para la realización de un BIA. Por último, se describen las acciones necesarias para efectuarlo en RENIEC.

3.3.1 Síntesis

Para RENIEC, el BIA será la base sobre la que se construye el SGCN, ya que identifica, cuantifica y califica el impacto en el tiempo de una pérdida, interrupción o alteración de las actividades de los procesos críticos de RENIEC y proporciona los datos para que se puedan determinar estrategias de continuidad adecuadas. El BIA identifica la urgencia de cada actividad llevada a cabo en los procesos críticos de RENIEC mediante la evaluación del impacto en el tiempo de interrupción de la actividad para la entrega del servicio.

3.3.2 ISO/IEC 22301:2012 – Guía de Buenas Prácticas del BCI

Es necesario que en RENIEC exista un proceso claramente definido para determinar el impacto de la interrupción de las actividades que soportan sus procesos críticos.

Es relevante y necesario que la organización logre:

- Identificar las actividades relevantes dentro de sus procesos críticos.
- Comprender el impacto potencial en el tiempo de una falta de operatividad de dichas actividades.
- Estimar un periodo máximo tolerable de interrupción (MTPD) para cada actividad crítica, es decir; el tiempo que le tomaría a los impactos adversos que pudieran surgir como consecuencia de no ofrecer un servicio o la realización de una actividad en RENIEC, a ser inaceptable.
- Identificar todas las dependencias de las actividades, tanto internas como externas, de los propietarios de la gestión de cada proceso y el personal adecuado, como expertos en la materia, para proporcionar información sobre los procesos de negocios, así como proveedores externos.
- Priorizar las actividades de acuerdo a las necesidad de recuperación.
- Estimar los recursos que requiere cada actividad crítica para su reanudación.

- Decidir eltiempo de recuperación objetivo (RTO) para la reanudación de las actividades críticas dentro del periodo de interrupción máxima tolerable (MTPD), el RTO se determina en la etapa de diseño del ciclo de vida de BCM, ya que es una decisión (no es un hallazgo), pero una estimación inicial puede hacerse durante el BIA que se puede confirmar en la etapa posterior, una vez se dispone de toda la información.
- Desarrollar y Actualizar el Análisis de Impacto de Negocio (BIA) en periodos de tiempo previamente definidos, especialmente cuando se producen cambios relevantes en los procesos críticos del negocio.

3.3.3 Aplicación en RENIEC

A continuación se especifican una serie de acciones a realizar para el desarrollo de un BIA en RENIEC:

a. Establecer la fase inicial de un BIA

- Determinar los objetivos y alcance del BIA
- Escoger una metodología o herramientaadecuada para la planificaciónde la realización del BIA.
- Estimar la duración del proyecto BIA.
- Comunicar la necesidad de un BIA a la Alta Dirección y a las personas relacionadas a RENIEC.
- Planificar capacitaciones efectivas dentro de la organización.

b. Determinar los resultados de las interrupciones, la estimación del daño y el impacto directo en la organización.

- Resultados de las interrupciones: Incumplimiento de las regulaciones o leyes, interrupción de los servicios y /o productos críticos brindados, pérdida de activos tangibles e intangibles (incluye personal), pérdida de prestigio e imagen pública.
- Estimar cualitativa y cuantitativamente el grado del daño a la organización.
- Impacto directo en la organización en el ámbito: Legal, operacional, personal, externo (ciudadanos y proveedores), financiero entre otros.

c. Desarrollar el BIA de acuerdo a la metodología escogida.

- Establecer un procedimiento apropiado para la recopilación de la información dentro de RENIEC (entrevistas, juntas de trabajo, cuestionarioso la combinación de ellos).

- ✓ **Recopilación de información por medio de entrevistas**, para ello es necesario: Respetar un formato general para todas las entrevistas realizadas, establecer qué datos son relevantes de obtener en la entrevista, presentar el formato de la entrevista días antes a los implicados, luego de la entrevista, de ser necesario, programar algunas nuevas para aclarar puntos no resueltos o no claros de los proporcionados inicialmente.
- ✓ **Recopilación de información por medio de cuestionarios**, para ello es necesario: realizar formatos comunes para cada tipo de cuestionario, de acuerdo al rol del implicado, programar reuniones para la explicación y repartición de los cuestionarios, asistir a los participantes durante la realización del cuestionario, revisar y levantar información relevante, de ser necesario programar nuevas reuniones para aclarar o solicitar nuevos datos en el cuestionario.
- ✓ **Recopilación de información por medio de juntas de trabajo**, para ello es necesario, evaluar la disponibilidad del personal, seleccionar la locación adecuada, establecer los objetivos de la junta y definir la fecha de la misma, durante la junta es importante, comprometer al cumplimiento de los objetivos acordados y determinar los puntos relevantes durante la junta.

- Establecer una metodología de análisis de la información.
- Desarrollar los resultados del BIA, es necesario: realizar una primera versión de los hallazgos de impacto del BIA para mostrárselos a la Alta Dirección y solicitar sus opiniones o comentarios, luego hacer las correcciones requeridas y preparar los resultados finales del Informe BIA y realizar la exposición final de los principales Hallazgos a la Alta Gerencia de RENIEC.
- Definir el nivel de criticidad de las actividades identificadas y priorizarlas.
- Establecer los registros vitales para la continuidad y reanudación del negocio.

d. Establecer los límitesde tiempo de recuperación para las actividades más relevantes de los proceso críticos

- Alinear el nivel de criticidad con las ventajas de reanudación de las actividades críticas.
- Establecer la prioridad de recuperación de funciones en la actividad crítica.
- Definir los recursos mínimos necesarios (internos, externos, adicionales, existentes) para la reanudación de las actividades.

3.3.4 Entregable: Análisis de Impacto de Negocio (BIA)

ANÁLISIS DE IMPACTO DE NEGOCIO

- **Objetivo**

  El objetivo de un análisis de impacto es determinar de manera cuantitativa y/o cualitativa impactos, efectos, y pérdidas que podrían resultar si la organización sufre un evento serio y establecer las funciones críticas, sus prioridades de recuperación e interdependencias a fin de determinar Tiempos del Negocio.

- **Tiempos del Negocio**

  Son los tiempos asociados a la atención de una interrupción en los cuales se enmarcaron las urgencias de los procesos, donde se puede establecer:

  MTPD (Periodo Máximo Tolerable de Interrupción), es el plazo después del cual la viabilidad de una organización se verá amenazada de forma irrevocable (financiera, pérdida de reputación, etc.) si no puede reiniciar la entrega de un producto, proceso o servicio específico.

  RTO (Tiempo de Recuperación Objetivo), es el tiempo objetivo en el que se debe reiniciar la entrega de un producto, proceso o servicio específico para que la viabilidad de la Organización no se vea amenazada, este tiempo comienza a partir de la invocación del plan. El RTO debe asegurar que no se excede el MTPD.

  RPO (Punto de Recuperación Objetivo), es el punto desde el que la información debe ser restaurada para permitir la operación de una actividad una vez que ésta se haya reiniciado.

- **Procesos Soportados**

  Los procesos soportados son el de Registro de Identificación y el de Registros Civiles por considerarse “core” de RENIEC. Estos incluyen la infraestructura tecnológica que cubre Sistemas relevantes como el de Registros Civiles y el de trámites de DNI.

- **Análisis y Tiempo Objetivo de Recuperación**

  Proceso de Identificación: Horizonte de Tiempo de 3 horas.

  Proceso de Registros Civiles: Horizonte de Tiempo de 2 horas.

- **Recursos Asociados a la recuperación**

  Estaciones de trabajo, teléfonos celulares, LAN, especialistas de Registros Civiles, especialistas en Sistema de trámites de DNI, soporte administrativo (seguridad física).

Capítulo 4. Diseño

En el presente capítulo se presenta el diseñode un SGCN, incluyendo el plan de pruebas de escritorio de cada uno de los entregables realizados.

4.1 Establecer Estrategias de Recuperación de Continuidad de Negocios

En este apartado se presentan las estrategias y tácticas identificadas y seleccionadas en el ejercicio profesional, para determinar cómo se logrará la continuidad y recuperación de incidentes. A continuación se muestran los aspectos que disponen la norma ISO/IEC 22301 y la Guía de Buenas Prácticas del BCI para la identificación de Estrategias de Recuperación. Por último, se describen las acciones necesarias para efectuarlo en RENIEC.

4.1.1 Síntesis

En RENIEC se tendrá como propósito diseñar, determinary seleccionarlas estrategias y tácticas de continuidad y recuperación del negocio fijando plazos para la recuperación, sin sobrepasar el RTO para lograr los objetivos trazados, tanto a nivel estratégico, táctico y operacional.

4.1.2 ISO/IEC 22301:2012 – Guía de Buenas Prácticas del BCI

La organizacióndebe definir a partir de sus actividades críticas los planes de reanudación de las mismas.

Es importante que la organización logre:

- Determinar un plan de reanudación de las actividades críticas dentro del tiempo objetivo de recuperación (RTO), este debe ser menor que el MTPD y se debe estimar los recursos necesarios para la reanudación.
- Establecer la relación entre el personal involucrado en la recuperación y reanudación (interno y externo).
- Documentar la estructura escogida para respuesta a incidentes, teniendo en cuenta el objetivo de punto de recuperación (RPO) o la máxima pérdida de datos soportada por la organización.

4.1.3 Aplicación en RENIEC

a. Determinar requerimientos de estrategias de recuperación para la organización

- Verificar el manejo de Continuidad de Negocios respecto a las comunicaciones y entre el personal.
- Establecer la continuidad de recursos (TI, equipos, materiales), personal e infraestructura.
- Identificar estrategias de continuidad alternativas:
  - ✓ **Diversificación:** Adecuada cuando el RTO se mide en minutos u horas.
  - ✓ **Replicación:** Adecuado cuando el RTO es mayor a unas pocas horas y menor de un día para lograr así, que el personal se pueda mover a la ubicación réplica con rapidez para reanudar actividades dentro del RTO
  - ✓ **Standby:** Cuando el RTO es superior a un día, una estrategia adecuada puede ser la de tener una instalación de reserva disponible que puede ser puesto en funcionamiento dentro del RTO
  - ✓ **Adquisición Post Incidente:** Es adecuado para RTO medido en días o semanas, y depende de tener los proveedores pre-calificados que proporciona recursos a corto plazo.
  - ✓ **Hacer nada:** Esperar hasta después del incidente para decidir qué hacer puede ser una estrategia apropiada cuando el RTO se mide en meses.
  - ✓ **Subcontratación:**Su selección dependerá de la rapidez con la que la organización requiere del subcontrato para continuar sus operaciones.

- ✓ **Seguro:** cuando el seguro es de interrupción de negocio y el RTO se mide en meses y el equipo de especialistas, las instalaciones o las habilidades son fáciles de obtener.

b. Determinar la posibilidad de una estrategia al alinearla con resultados del BIA.

c. Analizar la eficacia y el costo de las estrategias empleando una adecuada metodología; proporcionar a la Alta Dirección un reporte final que contenga las opciones estratégicas y los principales hallazgos del análisis y brindaruna recomendación a la Alta Gerencia alineada a los resultados.

d. Establecer proyectos con financiamiento y determinar los recursos necesarios para la aplicación de las estrategias y tácticas convenidas.

e. Comprender los contratos realizados con externos para brindar los servicios de Continuidad de Negocio de ser el caso

- Preparar los requisitos de recursos de terceros para ser utilizados en su compra, detalle para permitir una estructura de respuesta a incidentes a ser diseñado, este debe incluir requerimientos regulatorios si es el caso.
- Analizar los acuerdos contractuales con los proveedores, para identificar requerimientos incluidos y no incluidos en los estándares sugeridos.

4.1.4 Entregable: Estrategias de Reanudación de Continuidad de Negocio.

ESTRATEGIAS DE CONTINUIDAD DE NEGOCIO

- **Objetivo**

Evaluar y seleccionar estrategias de continuidad que más se adecuen a los procesos críticos del negocio. Las estrategias de continuidad fueron diseñadas considerando los tiempos objetivos de recuperación definidos en el BIA.

- **Componentes**

Los componentes a tomar en cuenta tenemos: Infraestructura, Personal, Recursos, Proveedores Críticos y Registros Vitales.Se debe tomar en cuenta la seguridad del personal, de la información y sitios alternos de operaciones.

- **Tipos de centros de hardware de respaldo en sede alterna**

Hot Side: Recuperación inmediata; el Sitio Alterno requiere de soluciones de replicación tanto a nivel de infraestructura como de datos (0- 4 horas).

WarmSide: Recuperación basada en copias de respaldo; el Sitio Alterno debe existir con conectividad, enlaces de terceros y equipos listos para restaurar las copias de respaldo (24 a 48 horas).

ColdSide: Recuperación basada en copias de respaldo; el Sitio Alterno debe existir con por lo menos la conectividad necesaria (1 semana).

- **Estrategias Propuestas a Nivel de Infraestructura**

Estrategia	Tipo	Responsable
Espacio Físico		
1. Seleccionar los sitios alternos para los procesos críticos de Negocio y TI.	**Táctico**	Gerencia de Finanzas
2. Identificar el local adecuado que tenga los recursos mínimos que se requieren.	**Táctico**	Operaciones
Ordenamiento de aplicaciones/servidores		
3. Para el futuro, considerar las necesidades del negocio para la priorización de las aplicaciones, y con ello definir los servidores críticos que albergarán las aplicaciones críticas; todo esto con el fin de agilizar el proceso de activación de la continuidad.	**Táctico**	Área de TI
4. Revisar los procedimientos de adquisición de nuevas aplicaciones para ver anticipadamente si se deben considerar en Producción y DRP. Contar con una lista de variables que permitan hacer disponible las soluciones en el DRP, considerando RTO, RPO.	**Táctico**	Área de TI
Asegurar enlaces de comunicación		
5. Asegurar en el Sitio Alterno una salida a Internet (mínimo 24 Mb) que cubra los requerimientos de las aplicaciones requeridas dentro de las primeras horas	**Táctico**	Área de TI

- **Estrategias Propuestas a Nivel de Personal**

Estrategia	Tipo	Responsable
Identificación de roles primarios y alternos		
1. Identificar personal primario necesario para la recuperación de los procesos críticos del negocio. Adicionalmente identificar los conocimientos mínimos que debe tener este rol así como también las habilidades y competencias técnicas.	**Estratégico**	Cada Área del Negocio

2. Identificar personal alterno para asegurar la continuidad de las operaciones de RENIEC en caso el personal primario no esté disponible a causa de un desastre. Se debe identificar más de un alterno que cuente con las características necesarias para cumplir las funciones del personal primario. Además se debe considerar el trabajar desde casa en caso no se pueda contar con algún ambiente de trabajo.	**Estratégico**	Cada Área del Negocio
3. Identificar características similares entre el personal de RENIEC para definir posibles roles alternos en los procesos que demanden mayor cantidad de personal, el personal no tiene que ser necesariamente de las misma área o ubicación geográfica.	**Estratégico**	Cada Área del Negocio
4. Designar un responsable del DRP, el cuál tenga una dedicación exclusiva a ello. Dicho responsable se encargará de la gestión de la recuperación de los elementos tecnológicos requeridos por el negocio y deberá contar con conocimientos avanzados para el manejo de la Continuidad de Negocios.	**Estratégico**	Gerencia de Tecnología de Información
Capacitación de personal		
5. Promover a través de un calendario de capacitación que cada gerencia gestione capacitaciones sobre los Planes de Continuidad de Negocios tanto a personal primario como alterno con el fin de reducir brechas de conocimiento entre estos.	**Estratégico**	Cada Área del Negocio
6. Efectuar un programa de capacitación virtual para el personal en general que incluya la prevención de emergencias, protección a la familia, reporte de incidentes en casos de desastre, entre otros.	**Estratégico**	Escuela Registral / OSDN*
7. Realizar talleres para el manejo de situaciones de crisis por parte del personal para asegurar una respuesta adecuada durante un desastre. Invitar autoridades como bomberos, defensa civil o policía nacional para que participen de los talleres	**Estratégico**	Escuela Registral / OSDN
8. Establecer un Plan de Capacitación Anual propio del área de tecnología para los roles primarios y alternos, que considere temas técnicos y de procesos, y la recuperación en sí de los componentes tecnológicos, con el fin de reducir las brechas de conocimiento que se puedan tener entre personal primario y alterno.	**Estratégico**	Área de TI

Comunicación entre el personal		
9. Asegurar que cada área defina un árbol de llamadas integrado a nivel de RENIEC para garantizar la comunicación efectiva entre el personal en caso de desastre.	**Estratégico**	Cada Área del Negocio
10. Incluir dentro de la política de vacaciones una cláusula que prevenga que personal primario y alterno tengan vacaciones o capacitaciones en las mismas fechas, de modo que siempre se contará con un rol disponible.	**Estratégico**	RRHH
11. Identificar posibles canales de comunicación entre RENIEC y el personal. Definir un responsable que administre y difunda cada canal (mensajes telefónicos usando un software o tercerizando, canales virtuales, plataforma virtual).	**Estratégico**	Gerencia de Imagen Institucional / RRHH
12. Identificar posibles canales de comunicación adecuados para la coordinación entre los integrantes del equipo de recuperación de Sistemas involucrados. Se debe definir un responsable que administre y difunde cada canal. a. Utilizar celulares y/o radios. b. Evaluar el uso de mensajes telefónicos masivos. Se debe apoyar en la evaluación y posible de selección alguna que brinde dicho servicio. c. Crear grupos de chat de comunicación y/o grupos de correo en dónde se agreguen los roles de recuperación del área, para utilizarlo como herramienta de comunicación en caso de desastre.	**Estratégico**	Área de TI
Políticas		
13. Incluir dentro de la política de vacaciones una cláusula que prevenga que personal primario y alterno tengan vacaciones o capacitaciones en las mismas fechas, de modo que siempre se contará con un rol disponible.	**Operativo**	RRHH
14. Implementar un mecanismo que permita disponer de dinero (efectivo, cheques, vales de consumo, crédito) para poder apoyar económicamente a los colaboradores afectados por un desastre.	**Operativo**	RRHH
15. Evaluar la asignación de Tablet o Smartphone para los Líderes de recuperación de cada plan y sus	**Operativo**	Cada Área del Negocio

16. Propiciar que todos los personales primarios y alternos tengan acceso al correo electrónico.	**Operativo**	Cada Área del Negocio
17. Establecer indicadores de continuidad del Negocio que midan el desempeño del personal al personal que participa en las actividades de recuperación.	**Operativo**	Riesgo Operacional
Brigadas de emergencia		
18. Mantener un listado de brigadistas actualizado y organizado por funciones y sedes para Evacuación, Seguridad, Incendio y Primeros Auxilios.	**Operativo**	OSDN
19. Replicar el esquema de brigadistas en otras instalaciones de Pacífico donde no esté implementado.	**Operativo**	OSDN
Responsabilidad social		
20. Realizar un plan de responsabilidad social que incluya los siguientes puntos: a. Definir un Kit básico para la asistencia a la comunidad compuesto principalmente por: Alimentos no perecibles, carpas, abrigos, medicinas básicas según primeros auxilios. b. Identificar posibles almacenes para el kit básico de asistencia. c. Identificar alternativas de reutilización del kit básico. d. Presentar un presupuesto total para actividades a implementar.	**Operativo**	OSDN / GTH
21. Definir líderes de responsabilidad social (es independiente a los brigadistas del apoyo interno de RENIEC) cuyo objetivo sea gestionar las actividades orientadas a velar por el bienestar de los familiares de personal y de la comunidad en general.	**Operativo**	OSDN / GTH

- **Estrategias Propuestas a Nivel de Recursos**

Estrategia	Tipo	Responsable
Equipos de cómputo / equipos de comunicaciones		
1. Elaborar un mapa de distribución de los equipos de cómputo y de comunicaciones como impresoras, computadoras o teléfonos que estarán ubicados en el Sitio Alterno de Operación.	**Operativo**	Administración
2. Considerar el stock actual de computadoras y laptop como stock en caso de desastre, las cuales deberán estar configuradas y listas para ser usadas por los	**Operativo**	Sistemas

3. Distribuir el stock actual de computadoras entre las diferentes instalaciones de RENIEC.	**Operativo**	Sistemas (GTI)
4. Revisar el procedimiento de gestión de inventarios para incluir recursos para la Continuidad del Negocio.	**Operativo**	Sistemas (GTI)
5. Asegurar que todo el personal clave de los procesos de Identificación y Registros Civiles cuenten con computadores de escritorio para el desarrollo de las actividades de recuperación a nivel de configuración, monitoreo, entre otros. Además, se debe considerar como recurso adicional una laptop que permita realizar pruebas y/o validaciones de interconectividad, entre otras pruebas.	**Estratégico**	GPRC – GRI – GOR / Área de TI
6. Considerar el uso de switches inalámbricos para lograr acelerar la disponibilidad de la red. Esto sería importante para lograr que las portátiles se conecten de manera rápida, en el caso de que el Sitio Alterno requiera habilitarse para más personal.	**Operativo**	Área de TI
Insumos y suministros (Compras)		
7. Implementar inventario mínimo en el Sitio Alterno de Operación hasta un determinado número de Horas. para insumos y suministros identificados en el BIA.	**Operativo**	Administración
8. Definir listado de proveedores alternos de insumos y suministros.	**Operativo**	Administración
Enseres		
9. Elaborar un mapa de distribución de las posiciones del personal que estará ubicado en el Sitio Alterno de Operación.	**Operativo**	Administración

- **Estrategias Propuestas a Nivel de Proveedores Críticos**

Estrategia	Tipo	Responsable
Relación con autoridades y organismos públicas		
1. Tener un acercamiento con las autoridades	**Operativo**	OSDN / Administración
2. Identificar los protocolos actuales que utiliza el estado para tomar control de los recursos y/o servicios necesarios para atender desastres	**Operativo**	OSDN / Administración
Acuerdos y/o cláusulas en los contratos		

3. Incorporar en los contratos de mantenimiento del edificio, acuerdos de prioridad que permitan formalizar el compromiso de los proveedores para realizar una primera evaluación de los daños y determinar la posibilidad de continuar las operaciones en la instalación afectada.	**Operativo**	Administración
4. Identificar proveedores para la reconstrucción/reparación de las instalaciones y establecer contratos que contengan acuerdos de nivel de servicio requerido.	**Operativo**	Administración
5. Revisar los contratos firmados con los proveedores para asegurar que existan acuerdos de niveles de servicio (SLA) que definan penalizaciones en ellos por incumplimientos, de tal manera que se pueda contar con sus servicios en caso de desastre.	**Operativo**	Administración
Políticas		
6. Revisar la política de proveedores existente para contar con un contrato base que considere la inclusión de la cláusula de Riesgo Operacional, se establezcan los requisitos mínimos con los que debe cumplir un proveedor y contemple la auditoría de los esquemas de continuidad de negocios de los proveedores críticos.	**Operativo**	Aspecto Legal
7. Definir una política que permita realizar gastos adicionales para emergencia en una eventual situación de desastre. Se deben considerar los siguientes aspectos como definir un esquema por área o local y coordinar con otras entidades públicas como SUNARP y ONPE sobre las políticas y/o procedimientos que serán establecidos en RENIEC para que reconozcan las operaciones realizadas por los usuarios autorizados.	**Operativo**	Gerencia de Finanzas
Evaluación de esquemas de continuidad		
8. Indagar cuáles son los esquemas de contingencia manejados por los proveedores más críticos, y evaluar si éstos pueden asegurar el servicio brindado. Adicionalmente, identificar los contactos claves y al menos dos opciones de comunicación con ellos. En caso que el proveedor no cuente con un Plan de Continuidad, se debe solicitar de manera expresa la	**Operativo**	Gerencia de Administración

implementación de planes de contingencia que puedan ser usadas en caso de desastre.		
9. Establecer visitas periódicas a las instalaciones de los proveedores para poder censar/revisar los esquemas de continuidad ofrecidos por ellos.	**Operativo**	Gerencia de Administración
Pruebas de contratos y acuerdos de niveles de servicio		
10. Definir un Plan Anual de Pruebas de los servicios y/o aplicaciones relacionados a los procesos de alcance que involucre a los proveedores más críticos, definiendo pruebas y ejercicios que evalúen diferentes escenarios y niveles de estrés. Se tomará como insumo un formato de Esquema de Pruebas proporcionado por Continuidad de Negocios.	**Operativo**	Áreas Operativas / GTI

- **Estrategias Propuestas a Nivel de Registros Vitales**

Estrategia	Tipo	Responsable
Política para la gestión de registros vitales		
1. Elaborar un reporte consolidado y por área de los registros vitales, tomando como referencia el BIA.	**Estratégico**	Cada Área de Negocio
2. Definir políticas de control de acceso y seguridad para los registros vitales. Considerando a las órdenes de compra uno.	**Estratégico**	Seguridad de la Información
3. Crear un inventario de los registros vitales, que venga acompañado de un procedimiento de manejo de cambios, en el cual se identifique claramente el responsable, las fechas y los motivos de cada actualización realizada. Además, identificar al custodio responsable de los registros vitales requeridos por cada uno de los procesos críticos. Parte de sus actividades serán: a. Definir criterios que permitan catalogar un recurso como registro vital. b. Asegurar el correcto almacenamiento de los registros vitales en un espacio que cuente con las medidas de seguridad necesarias. c. Actualización periódica de registros vitales de ser necesario. d. Determinar los tiempos mínimo y máximo que deben almacenarse los registros vitales.	**Estratégico**	Área de TI

4. Definir procedimientos para obtener los registros vitales desde los sitios alternativos en dónde estén almacenados.	**Estratégico**	Área de TI
5. Digitalizar los contratos y certificados de licencia.	**Estratégico**	Área de TI
Identificación y mantenimiento de registros vitales		
6. Identificar al custodio responsable de los registros vitales tomando como referencia el BIA.	**Operativo**	Cada Área de Negocio
7. Con el reporte de registros vitales por área, evaluar el nivel de seguridad que sea necesario en cada caso.	**Operativo**	OSDN
8. Actualizar la relación de registros vitales.	**Operativo**	Cada Área de Negocio
9. Digitalización de documentos por área o proceso de negocio, asegurando su validez e identificando detalles técnicos con archivos de registros vitales que contienen niveles de prioridad para su recuperación y determinar los tiempos mínimos y máximo de almacén de registros vitales.	**Operativo**	Cada Área de Negocio
Accesos y roles		
10. Identificar al personal afín que puede servir de apoyo en caso de contingencia.	**Operativo**	Cada Área de Negocio
11. Crear roles adicionales para que personal afín pueda tener acceso a la red solo en caso de contingencia.	**Operativo**	Seguridad de la Información
12. Coordinar con el personal de control de accesos y elaborar un procedimiento, para que se puedan habilitar accesos/roles especiales en caso contingencia para el personal de apoyo.	**Operativo**	Seguridad de la Información
Capacitación		
13. Difundir la política de registros vitales	**Estratégico**	Seguridad de la Información

***OSDN=Oficina de Seguridad y Defensa Nacional
* GTN=Gerencia de Talento Humano

Para lograr una recuperación en el área de sistemas se debe garantizar que aplicaciones críticas se encuentren disponibles de uso en el Sitio Alterno de Operaciones.

4.2 Comunicaciones internas y externas para coordinar acciones ante interrupciones

En este apartado se presenta la gestión de comunicaciones necesarias ante un incidente. Asimismo, se detalla cómo se desarrolla esta práctica profesional. A continuación se describen las acciones necesarias para efectuarlo en RENIEC.

4.2.1 Síntesis

En la RENIEC será indispensable elaborar, evaluar y efectuar planes para comunicarse con los implicados internos (personal, alta dirección, gerencias) y externos (proveedores, ciudadanos) y vías de comunicación.

4.2.2 Aplicación en RENIEC

a. Identificar y conformar un Equipo responsable de la comunicación de crisis.

b. Establecer un árbol de comunicaciones entre equipos internos por local, externos, agencias (locales y nacionales), medios de comunicación (internet, radio) entre otros.

c. Incluir en los planes de comunicación de crisis realizados la comunicación con implicados internos y externos, sean personal y familias, ciudadanos clientes, gerentes, proveedores críticos entre otros involucrados.

d. Incluir en los planes de comunicación de crisis realizados la comunicación con agencias externas, mediante procedimientos y herramientas para la adecuada comunicación. Entre las agencias extremas de comunicación tenemos: Defensa Civil Local y Nacional, Cuerpo de Bomberos, Servicios de Emergencia entre otras agencias de gobierno.

e. Incluir en los planes de comunicación de crisis realizados la comunicación con los medios, ya sea por internet, radio, televisión, prensa (periódicos y revistas); y a partir de ello facilitar los programas de ejercicio, posteriormente a realizar, para la adecuada comunicación de crisis.

4.2.3 Entregables: Plan de Comunicación de Crisis

PLAN DE COMUNICACIÓN DE CRISIS

- **Objetivo**

El Plan de Comunicación en Crisis tiene como objetivo establecer una comunicación efectiva con el público objetivo identificado, según la ocurrencia o evento que eventualmente pudiera interrumpir la operatividad normal de la institución y afectar con ello la imagen de la organización.

- **Alcance**

Describe de manera puntual los siguientes aspectos: Esquemas de comunicación, Públicos objetivos (Medios de Comunicación (Voz, Internet, redes sociales,anuncios), entidades reguladoras, proveedores críticos, ciudadanos), Ubicaciones físicas de operación. Actividades antes, durante y después, Personal asociado, Registros vitales y Recursos asociados.

- **Escenarios considerados para comunicación**

Sismos de mayor a 5 grados e Incendios.

- **Equipo de Comunicación**

El equipo de Comunicación de Crisis está conformado por: Coordinador de Comunicación de Crisis, Asesor Legal, Staff de Comunicación, Voceros Externo e Internos. El organigrama con detalle de funciones y responsabilidades se presenta en el **ANEXO C.**

- **Estrategias de Comunicación en Crisis**

Las estrategias a tomar se dividen en:

1. **Antes.-** actividades de preparación
2. **Durante.-** actividades de respuesta y operación alterna
3. **Después.-** actividades de Restauración y Retorno.

Se conoce a mayor detalle las actividades a realizar en cada fase en el **ANEXO C.**

- Al iniciar la red de comunicación efectiva entre el equipo establecido tras un desastre se activa el presente plan.

4.3 Reanudación y Gestión de Crisis y operaciones de Emergencia

En este apartado se presentan los fundamentos de la comunicación y gestión de Crisis, así como las respuestas de emergencia con la finalidad de conocer cómo se desarrolla esta práctica profesional. A continuación se muestran los aspectos que disponen la norma ISO/IEC 22301 y la Guía de Buenas Prácticas del BCI para la Gestión de Crisis y Emergencia. Por último, se describen las acciones necesarias para efectuarlo en RENIEC.

4.3.1 Síntesis

En RENIEC se debe diseñar una estructura de respuesta a incidentes, manejo de crisis, para asegurar que exista un mecanismo documentados completamente entendidos para responder a un incidente que tiene el potencial de causar la interrupción de la organización, sin importar su causa.

4.3.2 ISO/IEC 22301:2012 – Guía de Buenas Prácticas del BCI

La organización deberá ser capaz de determinar equipos responsables de comunicación, gestión de Crisis y respuesta a incidentes en emergencia, cuya función es controlar la situación, activar planes y comunicarlo a Alta Dirección e interesados. Los equipos deben ser capaces de determinar el alcance del incidente y responder efectivamente de acuerdo a las estrategias, planes y procedimientos de Continuidad de Negocio.

4.3.3 Aplicación en RENIEC

a. Determinar el procedimiento de gestión de crisis y respuesta de emergencia

- Procedimientosrealizados: Interno y proveedores.
- Identificar las personas y los equipos responsables, determinando roles y autoridades para utilizar cualquier respuesta de emergencia existente, gestión de crisis y planes de gestión de incidentes
- Preparación de estrategias para la etapaantes del incidente, dependiendo al tipo de desastre: natural, accidental, intencional.
- Preparación de estrategias para la etapa durante el incidente, las acciones de emergencia a realizar como: alejarse de zonas de riesgo o materiales peligrosos; evacuación; atenciónmédicade emergencia al personal; notificar incidente y; activar Planes de Continuidad de Negocios.

- Mitigar el daño, estabilizar la zona y asumir roles de acuerdo a sus funciones.

b. Establecermedios de manejo de crisis y respuesta oportunos

- Protección del personal: Respetar regulaciones, establecer comunicación interna y puntos de reunión en caso incidente.
- Manejo adecuado del incidente: limitar el impacto del mismo, cumplir roles establecidos previamente para controlar la pérdida y daño.
- Estimar las consecuencias: determinar el impacto del incidente, desarrollar una respuesta conjunta de emergencia y gestión de crisis con la adecuada comunicación del personal involucrado.
- Disponer de acciones efectivas: decidir prioridades de continuidad, conservar principio de protección al personal, recursos e infraestructura y comprender las funciones de cada rol asignado.

c. Establecer requisitos de los equipos responsables y control del incidente

- Tomar decisiones durante el incidente de acuerdo al rol; emplear medios de comunicación (teléfono, celular, email); establecer localidad de emergencia; y definir una metodología de registro y documentación.

d. Establecer fases para equipos responsables: Inicio, despliegue, manejo y operación, supervisión y cierre de equipos.

e. Desarrollar procedimientos de emergencia, de comunicaciones, identificando previamente las acciones prioritarias.

f. Definir estrategias de recuperación

- Comunicar a los equipos responsables: Comprender el requerimiento de recursos al momento de un incidente y determinar procedimientos para ofrecer los recursos relevantes como respuesta del incidente ocurrido.
- Determinar estrategias a realizar en el desastre o incidente
  - ✓ Entender la necesidad de identificarrápidamente la mitigación de perdida y los requerimientos de rescate
  - ✓ Entender la veces y si es necesario, preparar un plan de acción de protección, seguridad y estabilización del lugar
  - ✓ Identificar métodos apropiados para la protecciónde activos en el lugar, incluyendo equipo, localidad y documentar.

- ✓ Reconocer la necesidad potencial de establecer enlace con agencias externas (reguladoras,servicios de emergencia como bomberos y policía, aseguradores, ajustadores de perdidas, etc.) y especificar el tipo de información que pueden requerimientos las agencias.
- ✓ Establecer procedimientos con proveedores de servicios tercerizados incluyendo los contratos correspondientes.
- ✓ Entender los requerimientos del negocio e interpretarlos para facilitar la recuperación de activos físicos

4.3.4 Entregables:Plan de Gestión de Crisis yPlan de Respuesta de Emergencia.

PLAN DE GESTIÓN DE CRISIS

- **Objetivo**

Coordinar el manejo de la crisis a fin de actuar en caso de presentarse un posible evento de desastre en RENIEC, en tal sentido permite el restablecimiento oportuno del negocio según las necesidades de supervivencia del mismo, las que consideran la continuidad del servicio de transmisión en todas las localidades a las que sirve.
Además logra guiar las acciones del Comité de Crisis para que en el tiempo se evalúe información, se decida, se notifique o activen los Planes de Continuidad del Negocio y se actúe según sea necesario en el antes, durante y después de una situación de amenaza de desastre o de desastre evidente.

- **Alcance**

Describe las acciones para cada uno de los roles del Comité de Crisis descritos en este plan y principalmente del Gestor de Continuidad en donde se muestra la coordinación a todo nivel de RENIEC.
Es parte de los Planes de Continuidad del Negocio junto con el Plan de Respuesta a la Emergencia, Plan de Comunicación en Crisis y Plan de Recuperación Desastre (DRP).

- **Principales escenarios considerados**

Sismo de gran intensidad (Mayor igual a 5 grados) y Explosión / Fuego /Incendio

- **Principal audiencias objetivo**

Sociedad en general, Medios de comunicación (Escrita, televisiva, radio, internet), Estado/autoridades, Cliente/Ciudadano y Proveedores.

- **Organización de Gestión de Crisis.**

Comité de Crisis que cuenta con: Gestor de Continuidad, Miembros consultores de Asuntos Legales, de Administración, de Negocios, de Comunicación y personal de apoyo. El organigrama con detalle de funciones y responsabilidades se presenta en el **ANEXO D.**

- **Estrategias de gestión de crisis generales**

Las principales estrategias generales definidas para el Manejo de Crisis las cuales serán aplicadas por parte de los integrantes del Comité de Crisis, ya sea en un posible desastre o evento ocurrido, se definen Antes, Durante y Después de un desastre. Se conoce a mayor detalle las actividades a realizar encada fase en el **ANEXO D.**

- **Estados de desastre:**

  - ✓ **Posible Desastre**, ocurre cuando el evento ha tenido una seria afectación en el área evaluada y la reparación de la falla no es inmediata.
  - ✓ **Alerta de Desastre**, ocurre cuando el RTO del área está comprometido. Tiene como objetivo movilizar a todo el personal que da soporte a la activación del sitio/centro alterno, así como habilitar los recursos, registros vitales, documentos y aplicaciones.
  - ✓ **Desastre Declarado**, ocurre antes que se venza el RTO del área, y tiene como objetivo que el área movilice su personal al Sitio Alterno de Operación y deje todo listo para operar en contingencia al momento que el RTO esté próximo a cumplirse.
  - ✓ **Desastre Controlado**, ocurre cuando los procesos y servicios tecnológicos afectados llevan operando un tiempo prudente en el Sitio Alterno de Operación. Una vez que el desastre se ha controlado, se deberá iniciar la restauración del sitio primario afectado y cuando esta haya finalizado se dará inicio a la vuelta a la normalidad.
  - ✓ **Fin del Desastre**, ocurre cuando se ha vuelto a la normalidad y tiene como objetivo efectuar la sesión de lecciones aprendidas del desastre ocurrido.

- **Procedimientos de Gestión de Crisis**

Se comienza con la declaración del incidente o desastre; para luego reunirse el personal vital junto con el de gestión de crisis en el Sitio Alterno de Operación o Centro de Operaciones de Emergencia (EOC), previamente equipado, para casos de recuperación, para seguir con las actividades cotidianas. El objetivo es operar en

el menor tiempo posible el trabajo cotidiano en el Sitio Alterno sin sobrepasar el umbral de criticidad (punto del tiempo en el que un desastre genera impactos negativos mayores al presupuesto para contrarrestarlo).

PLAN DE RESPUESTA A EMERGENCIAS

- **Objetivo**

El Plan de Respuesta a Emergencia de RENIEC tiene como objetivo principal salvaguardar la integridad física del personal y prepararlo para estabilizar la situación de emergencia. Considera tareas preventivas y de respuesta a través de procedimientos internos de escalamiento y notificación, en caso aplique proporciona un lugar seguro de atención al público concurrente.

- **Alcance**

Describe de manera macro los siguientes aspectos: Estrategia de protección humana, Brigadas de Emergencias, Actividades antes, durante y después, Selección de rutas y sitios seguros, Personal asociado, Recursos asociados y Agencias externas.

- **Organización de emergencia**

Existe emergencia parcial y total. El Comité de Emergencia que cuenta con: Coordinación de Seguridad y Salud Ocupacional, Coordinación de evacuación y control de daños, cada uno con brigadas relacionadas, ya sea para incendio, evacuación o primeros auxilios. El organigrama con detalle de funciones y responsabilidades se presenta en el **ANEXO E**.

- **Estrategias de Respuesta a Emergencia**

Las estrategias generales de respuesta adoptadas para los escenarios de emergencia de Sismo e Incendiose encuentras agrupadas en tres (3) fases según el esquema general de continuidad del negocio:

4. **Antes.-** actividades de prevención y preparación
5. **Durante.-** actividades de respuesta y activación, rescate y, atención de daños
6. **Después.-** actividades para la evaluación de daños del sitio(s) afectado(s).

Se conoce a mayor detalle las actividades a realizar encada fase en el **ANEXO E.**

- **Medios de evacuación**

Es vital señalizar las vías de emergencia preestablecidas en RENIEC, de ser necesario emplear luces de salida para el caso de Incendio, pues el humoen

grandes medidas causa desconcierto y desorientación y, es muchos casos, no se ven las salidas señalizadas.

- **Zonas de Seguridad Externa para reunión del personal**

Las personas relevantes del equipo de emergencia deben evacuar al personal; socorrer a las víctimas e informar a agencias externas de personal a rescatar, atrapado o herido.

- **Coordinación con Organismos Nacionales**

Es necesario coordinar y estar en constante contacto con organismos como INDECI,Cuerpo General de Bomberos, ya que ellos son responsables de emitir las acciones de prioridad a realizar. Además se debe manejar una lista de emergencia con los números de dichas organizaciones, hospitales, policía, ambulancia entre otros.

- **Pruebas y Reajustes**

Se debe seguir paso a paso lo mencionado en el presente plan, para ello es necesario hacer simulaciones o ensayos y de haber cambios hacer reajustes y actualización del plan, manejando un control de cambios

- **Aprobación del Plan de Emergencia**

Una vez hechas las pruebas y los reajustes necesarios, la Alta Dirección aprueba este plan.

- **Activación y Desactivación del Plan de Emergencia**

Al sonar la sirena continuamente de RENIEC, sea local administrativo u operativo, se procede a realizar la evacuación y se activa el presente plan, siguiendo las actividades mencionadas en el mismo de acuerdo al rol y responsabilidad establecidos. Cuando el Coordinador general de Emergencia; o en caso de no encontrarse él, cualquiera de los coordinadores de seguridad y control de daños, autorizan volver a las oficinas de manera ordenada y organizada, es ahí donde se desactiva el plan llevado a cabo.

4.4 Desarrollo de Planes de Continuidad de Negocios (BCP's) ante desastres específicos

En este apartado se el desarrollo de los Planes de Continuidad de Negocio. A continuación se muestran los aspectos que disponen la norma ISO/IEC 22301 y la Guía de Buenas Prácticas del BCI para su entendimiento, clasificación y desarrollo. Por último, se describen las acciones necesarias para efectuarlo en RENIEC.

4.4.1 Síntesis

En RENIEC se debe identificar y documentar las prioridades, procedimientos, responsabilidades y recursos para ayudar a la organización en la gestión de un incidente perjudicial, además de aplicar estrategias de continuidad y recuperación a un nivel pre-determinado de servicio cumpliendo el RTO y el RPO, para ello se debe pasar a la fase de diseño,desarrollo e implementación de Planes de Continuidad de Negocio.

4.4.2 ISO/IEC 22301:2012 – Guía de Buenas Prácticas del BCI

Los BCP's de la organización deben estar destinados a ser utilizados en situaciones de alta presión cuando las personas están bajo estrés de la interrupción o incidente.

Los BCP's previamente son validados por Alta Dirección, alineados con cualquier acuerdo externo y entendidos por los equipos claves, para ello deben ser directos, esto significa que deben proporcionar una dirección clara, orientada y basada en el tiempo; adaptables para que así puedan responder a una amplia gama de incidentes; conciso, con orientaciones, información y herramientas que son susceptibles de ser utilizados por el equipo en un incidente perturbador. Finalmente, debe ser relevante, significa que debe estar vigente (actualizado y con control de versiones de cambios relevantes) y aplicable y accesible al equipo de responsables que lo va a utilizar.

4.4.3 Aplicación en RENIEC

a. Determinar los requisitos clave para el desarrollo del plan

- Designar a un propietario / patrocinador del plan y definir los objetivos y el alcance.
- Elaborar y aprobar un proceso de desarrollo del plan y los programas.
- Crear un equipo de planificación.

- Aceptar las responsabilidades del equipo de respuesta y su relación con otros planes y equipos de respuesta (estratégico, táctico y operativo).
- Crear un equipo de respuesta que tienen las habilidades requeridas.
- Desarrollar lista de acciones o checklist.
- Determinar las estrategias en el que se basa el plan.
- Desarrollar medios para recopilar información para rellenar el plan y de ser necesario, desarrollar otra documentación de soporte.

b. Definirla estructura, el formato y los componentes del plan

- Diseño y estructura del plan
  - ✓ Alinear la estructura del plan definida a la organización.
  - ✓ Determinar la técnica de recopilación de información para el contenido del plan.
  - ✓ Realizar la documentación del diseño y la estructura del plan para garantizar herramientas para simplificar el mantenimiento y vigencia del plan.
- Designarroles y responsabilidades
  - ✓ Determinar roles de acuerdo a las tareas previamente identificadas.
  - ✓ Establecer equipos de respuesta (Líder, los miembros principales y suplentes) a ser responsables de las tareas predefinidas.
  - ✓ Identificar los grupos necesarios a llevar a cabo las tareasrequeridas.
  - ✓ Designar lasresponsabilidades a los equipos conformados.
  - ✓ Determinar recursos críticos y proveedores y la forma de contactarlos.

c. Redactar y desarrollar los planes

- Identificar y seleccionar mecanismos adecuados para la realización y actualización del plan.
- Garantizar la participación de los equipos de planificación, respuesta y personal clave para la redacción del plan.
- Realizar revisiones del plan redactado para garantizar que este al ser finalizado, sea relevante, conciso, confiable y directo,

d. Determinar procedimientos para la Continuidad de Negocios

- Asegurar la adecuada realización de documentación clave para la organización.
- Identificar proveedores críticos y procesos críticos a replicar.
- Indicar los métodos de operación y transferencia alternativa de los procesos críticos del negocio ante cualquier incidente o interrupción, cómo

- Desarrollar procedimientos para la continuidad de información de acuerdo a los requerimientos normativos legales, del negocio y de la tecnología.

e. Establecer técnicas de restauración y estimación de perjuicios

- Establecer técnicas de restauración, para ello debe seleccionar un método adecuado para la restauración de activos críticos del negocio (registros vitales, infraestructura física, documentación, tecnologías de información), a partir de ello se debe utilizar un enfoque práctico, entendible y aplicable para lograr los requerimientos de la recuperación de la organización y así tener la capacidad de aminorar el impacto de relevantes pérdidas.
- Realizar un plan de acciones para la estimación de perjuicios según costos de restauración y reemplazo y alinearlo a la continuidad de negocios de la organización para cualquier operación a realizar.

f. Establecer y desarrollar documentación del equipo de operaciones del negocio

- Establecer acciones para activación del plan de acuerdo a las necesidades tecnológicas de las operaciones realizadas en respaldo de cada área.
- Realizar planes de acción, checklists, procedimientos técnicos tanto por área como individuales.
- Establecer al personal, recursos y responsabilidades necesarios para el equipo de restauración.

g. Establecer y desarrollar documentación del equipo de restauración de TI

- Establecer acciones para activación del sitio alterno (equipo nuevo, operaciones, redes, soporte, logística, administración, manejo de información y relación con el usuario final) e identificar requerimientos del usuario final.
- Establecer componentes de registros vitales.
- Realizar planes de acción, checklists, procedimientos técnicos por área.
- Establecer al personal, recursos y responsabilidades necesarios para el equipo de restauración.

h. Establecer y desarrollar documentación de uso exclusivo de los equipos responsables

- Identificar relaciones del plan con entes reguladores, proveedores y ciudadanos.

- Determinar las competencias y recursos requeridos para la continuidad de acuerdo a la experiencia, capacidad y responsabilidad en el ámbito regulatorio legal, recursos humanos, seguridad, adquisición de nuevos equipos y suministros, comunicaciones (medios de comunicación, personal, contratistas y ciudadanos) y manejo de riesgos.

i. Establecer y desarrollar planes de recuperación de sistemas de comunicación de datos, de voz (telefonía, correo de voz) y garantiza una adecuada documentación de dichos planes.

j. Implementar planes de continuidad de negocio y proceder a su control

- Garantizarla finalización de las tareas delegadas (contratos, respaldos, nuevos equipos) y documentar adecuadamente los planes.
- Efectuar procedimientos de actualización y mantenimiento del plan; así como de prueba de los procedimientos.
- Efectuar procedimientos de control para sus resultados y mantener vigente el plan.

4.4.4 Entregable: Plan de Recuperación de Desastres

PLAN DE RECUPERACIÓN DE DESASTRES

- **Objetivo**

El Plan de Recuperación de Desastres tiene como objetivo principal ser una guía para la coordinación efectiva y el restablecimiento de los **servicios críticos** y así como también permitir restablecer los procesos críticos al interior de la organización. Además, proporciona pasos para que en caso de que ocurra un Sismo o un Incendio, RENIEC pueda poner en operatividad nuevamente todos sus sistemas informáticos, redes, computadoras, etc. lo más rápido posible para no afectar sus operaciones.

- **Alcance**

Describe de manera macro los siguientes aspectos: estrategias de recuperación según la criticidad de los servicios de TI; grupos y roles de recuperación; actividades de Preparación, Respuesta, Operación Alterna, Restauración y, Retorno; identificación de Personal Alterno/Primario por cada Rol de Recuperación; recursos e insumos mínimos para la recuperación; registros vitales y documentación de soporte indispensables para la recuperación y; dependencia de servicios y los recursos asociados.

- **Organización de Recuperación de Desastre**

El Grupo de Recuperación primario de Sistemas cuenta con: Coordinador de Recuperación de TI,Coordinador de Operaciones, Coordinador de Base de Datos, de Networking, de Seguridad de Aplicaciones y de Soporte. El organigrama con detalle de funciones y responsabilidades se presenta en el **ANEXO F**.

- **Fases y Gestión durante el desastre:**
  - ✓ Identificación y respuesta de emergencia
  - ✓ Evaluación del incidente
  - ✓ Evaluación de los daños
  - ✓ Declaración del desastre
  - ✓ Notificación y escalamiento
  - ✓ Notificación de equipos de recuperación
  - ✓ Respuesta y movilización de equipos de recuperación
  - ✓ Ampliación de operaciones de recuperación al conjunto de aplicaciones
  - ✓ Respuesta de operaciones en el sitio primario
  - ✓ Decisión de finalizar las operaciones de recuperación
  - ✓ Revisión, balance y auditoria del incidente

4.5 Programa de Entrenamiento, Concientización y Capacitación

En este apartado se presentan el manejo de programa de entrenamiento, concientización y capacitación y cómo se desarrolla esta práctica profesional. A continuación se muestran los aspectos que disponen la norma ISO/IEC 22301 y la Guía de Buenas Prácticas del BCI. Por último, se describen las acciones necesarias para efectuarlo en RENIEC.

4.5.1 Síntesis

En RENIEC se requiere un programa de entrenamiento planificado para asegurarse de que se han ejercido todos los aspectos de la respuesta a un incidente. En particular: se verifica toda la información de los planes; se ensayan y se capacita y concientiza. Por ello, el objetivo es mejorar las habilidades al efectuar un plan de continuidad de negocios según los procesos críticos de su alcance.

4.5.2 ISO/IEC 22301:2012 – Guía de Buenas Prácticas del BCI

Es necesario que la organización adopte la continuidad de negocio como parte de sus políticas con una adecuada gestión, garantizando:

- Conocimiento (Cultura Organizacional) de la relevancia y trascendencia de las estrategias y planes de continuidad de negocio para lograr una respuesta efectiva ante incidentes y desastres; y cumpliendo los objetivos inicialmente trazados.
- Concientización en la organización mediante las actualizaciones y gestión de la información brindada al personal para tener resultados durante un incidente.
- Realizar capacitaciones y entrenamientos al personal, para desarrollar capacidades, competencias y habilidades de respuesta ante incidentes o interrupciones.
- Definir técnicas o métodos para evaluar la efectividad y eficacia de las capacitaciones y programas de entrenamiento impartidos al personal.

4.5.3 Aplicación en RENIEC

a. Acordar alcance, objetivos y resultados del entrenamientoy capacitación.

b. Determinar el presupuesto para elentrenamiento, concientización y capacitación.

c. Verificar la disponibilidad del personal y las instalaciones necesarias.

d. Proponer varios tipos de programa de capacitación de acuerdo a la situación: Basados en discusión, de puestos de mando (simulando un incidente real), en aulas de clase, en computadora, con guías instructivas, con pruebas y ejercicios.

e. Elaborar programa de entrenamiento y concientización donde participen la Alta dirección, los equipos conformados, para contar con la vigencia del plan.

f. Realizar conferencias, publicaciones y conformar asociaciones y equipos para la planificación de la continuidad de negocios.

g. Realizar un seguimiento del programa y abordar las cuestiones planteadas por el entrenamiento y capacitaciones.

4.6 Pruebas de Planes de Continuidad de Negocio

En este apartado se presenta el manejo de pruebas y mantenimiento de planes de continuidad para corroborar su eficiencia y efectividad. Asimismo, se detalla cómo se desarrolla esta práctica profesional. A continuación se muestran los aspectos que disponen la norma ISO/IEC 22301 y la Guía de Buenas Prácticas del BCI relacionado a las pruebas. Por último, se describen las acciones necesarias para efectuarlo en RENIEC.

4.6.1 Síntesis

En RENIEC se debe establecer y coordinarprogramas de ejerciciosde los planes realizados, documentar dichos ejercicios y evaluar la efectividad de los mismos.

Es de vital importancia reportar los resultados y hallazgos de forma concisa y directa a la Alta dirección respecto a los ejercicios realizados de acuerdo a estándares o metodologías seguidas.

4.6.2 ISO/IEC 22301:2012 – Guía de Buenas Prácticas del BCI

La organización debe determinar el alcance y objetivos de los ejercicios a realiza y en base a ello:

- Determinar escenarios específicos de acuerdo al alcance de los incidentes que cubre el presente SGCN.
- Establecer periodos de tiempo para la actualización de los programas de ejercicios de acuerdo a un control de cambios.
- Determinar activos para los ejercicios definidos que sirvan de respaldo.

- Determinar el presupuesto para el programa de ejercicios.
- Decidir sobre tipos adecuados de ejercicio de las áreas a ser ejercidas durante el período de planificación.
- Verifique la disponibilidad de personal y las instalaciones necesarias.
- Elaborar un programa de ejercicios escrito, con hallazgos, resultados y retroalimentación. Además se debe considerar recomendaciones de cambios o actualizaciones con fechas establecidas.
- Presentar a la Alta Dirección para su aprobación, si procede, e
- Identificar cualquier requisito de capacitación para los participantes de ejercicios o planificadores e integrarse en el programa de ejercicios.

La organización debe garantizar la adecuada alineación del programa de ejercicios con sus objetivos estratégicos para lograr sus metas.

4.6.3 Aplicación en RENIEC

a. Disponer un programa de ejercicios

- Desarrollar guías de ejercicio estructuradas con el fin de entrenar, evaluar, practicar y mejorar el rendimiento de la organización.
- Establecermétodos o técnicas para realizar los programas deejercicios adecuados para la recuperación efectiva con inversiones pertinentes.

b. Desarrollar detalles del programa de ejercicio

- Determinar el objetivo del ejercicio y revisar el alcance (los planes de recuperación, recursos y actividades) para identificar las áreas críticas y así establecer calidad de resultado mínima.
- Determinar el alcance del programa, incluyendo integrantes, duración, tipo de programa.
- Analizar las ventajas y desventajas de los diferentes tipos de ejercicio (prueba de escritorio, simulación de incidente real, evacuaciones, planificados o no anunciados, realizados por aplicación o componente, por área o funcionamiento específico).
- Establecer escenarios de incidentes o desastres posibles en RENIEC, de acuerdo al alcance e identificar que interrupciones o impactos pueden producirse.

c. Identificar criterios de evaluación del ejercicio en base a sus objetivos y alcance,y documentar los hallazgos o resultados en base a los criterios establecidos.

d. Establecer el programa de ejercicio que sea mediable y cuantificable, incremental o cualitativo, en base a ello se debe determinar niveles por períodos, alineando los resultados planificados con los esperados.

e. Proveer controles del programa de ejercicios

- Seleccionar un escenario específico y determinar objetivos, alcance y limitaciones.
- Determinar el presupuesto requerido de acuerdo a los recursos y suministros, los integrantes relacionados según sus roles y responsabilidades.
- Detallar especificaciones del ambiente a acondicionar para el ejercicio.

f. Efectuar los ejercicios planificados y analizar la efectividad de sus acciones.

g. Evaluar e informar los resultados, incluyendo un resumen escrito de los participantes inmediatamente después del ejercicio con recomendaciones de acuerdo a la experiencia.

h. Realizar seguimientos para retroalimentar las acciones definidas durante el ejercicio:

- Establecer reuniones para revisar los hallazgos del ejercicio y buscar la mejora del plan puesto a prueba.
- Involucrar a los equipos relacionados y comprometerlos en el cambio en un determinado tiempo preestablecido.

i. Realizar una agenda de revisión y mantenimiento de los procedimientos en los planes involucrados para así; supervisar las actividades realizadas; documentar, controlar y asegurar efectivas recomendaciones.

j. Establecer guías de retroalimentación y procedimientos de control de cambios para mantener los planes actualizados y vigentes.

k. Realizar reportes del programa de acuerdo al alcance, argumento, periodos de ocurrencia e integrantes.

l. Determinar y efectuar procedimientos de control para la documentación del BCP.

4.6.4 Entregable: Plan de Pruebas

PLAN DE PRUEBAS

- **Objetivo**

Planear, realizar y documentar los procedimientos que son necesarios ejecutarse para realizar las pruebas que permita validar el diseño del presente SGCN para RENIEC. Permite identificar si las estrategias definidas son capaces de proveer la respuesta y recuperación deseada dentro de los tiempos definidos para cada proceso. Además permite validar la capacidad de recuperación de RENIEC.

Para la elaboración del Plan de Pruebas y Ejercicios se consideraron como insumos los siguientes documentos:

- Información del Análisis de Impacto (BIA)
- Información de Estrategias de Recuperación
- Plan de Comunicación en Crisis
- Plan de Gestión de Crisis
- Plan de Recuperación ante Desastres (DRP)
- Planes para la Respuesta a la Emergencia

- **Política de pruebas**

Establece la guía para diseñar y mantener un programa de pruebas que valide la capacidad de recuperación de RENIEC.

- **Fundamento de las Pruebas**

Las pruebas se realizan cuando existen actualizaciones, adquisiciones o modificaciones en el hardware, software, en cualquier tipo de aplicativos, infraestructura y también si existen cambios en los procesos del negocio (Identificación y Registros Civiles) que cubren los planes realizados.

Los equipos de recuperación, de crisis y de emergencia deben definir pruebas periódicas para asegurar la calidad respecto al SGCN y a su recuperación. El equipo de crisis será el encargado de definir y asegurarse el cumplimiento de las políticas en los planes realizados.

- **Tipo de Pruebas**

El tipo de prueba a realizarse es la prueba de escritorio, que consiste en realizar un ejercicio en un ambiente “sin estrés” y para ello cada representante de rol se sienta alrededor de una mesa de trabajo. Usualmente dispuesta en forma de “U”, y sigue exclusivamente las actividades tal y como están descritas en el rol que representa

según el plan (BCP), no se improvisa. Además cualquier necesidad no documentada debe anotarse como una mejora al plan. Este tipo de ejercicio es útil para validar el uso del documento o plan por parte del personal, para validar incoherencias entre actividades de los diferentes roles y para que el personal se familiarice con la estructura del mismo, sobre todo los alternos a quienes se recomienda hacer participar de este tipo de ejercicios.

- **Fases de las Pruebas**
  - Planificación y preparación (pre-prueba)
  - Ejecución (prueba)
  - Revisión (post-prueba)

- **Riesgos de las Pruebas**

  Es relevante que durante la etapa de planificación y preparación de las pruebas se documenten los riesgos detectados durante su ejecución.

- **Estructura de las Pruebas**
  - Objetivos de la Prueba y Resultados Esperados
  - Alcance: Infraestructura, participantes, aplicaciones relacionadas, software, hardware y comunicaciones.
  - Escenarios y Premisa del ejercicio
  - Preparación del “Guión” de la Prueba
  - Preparación de formatos de seguimiento al ejercicio.
  - Ejecución del Ejercicio
  - Evaluación de la Prueba: Problemas y desviaciones de la prueba, fortalezas y lecciones aprendidas.
  - Documentación de resultados con oportunidades de mejora
  - Actualizaciones y ajustes en los planes de continuidad.

- **Identificación de riesgos de las pruebas**

  Durante la fase de planeacióny preparación de las pruebas se logra identificar, analizar y evaluar los riesgos que podrían surgir durante la prueba.

- El detalle de las pruebas se encuentra en el **ANEXO G.**

Capítulo 5. Conclusiones, ObservacionesyRecomendaciones

5.1 Conclusiones

- Respecto al modelamiento de los procesos se identificó que es relevante el mantenerlo actualizado, pues el no tener documentados ni actualizados los procesos de negocio en RENIEC,implicó realizar el modelamiento, produciéndose una demora en la realización del SGCN.

- En el Análisis de Riesgos, se identificó que RENIEC no cuenta conuna matriz actualizada de los mismos, lo que implica no identificar riesgos que a futuro pueden ser perjudiciales para la organización e incluso para la continuidad del negocio.
- El Análisis de Impacto de Negocios abarcó ambos procesos core de RENIEC (Proceso de Identificación y de Registros Civiles) y los tiempos objetivos de recuperación hallados están estrechamente ligados a cambios en los procesos o manejo de los mismos.

- Las Estrategias de Continuidad de Negocios han sido propuestas y divididas a nivel estratégico, táctico y operacional que implica cubrir toda la organización y que se deben adoptar en RENIEC para lograr una recuperación de las áreas implicadas garantizando que aplicaciones críticas se encuentren disponibles para uso en el Sitio Alterno de Operaciones luego de ocurrido el desastre.

- El Plan de Comunicación de Crisis logró identificar roles adecuados que logren informar y ser los voceros ante un desastre y probar los diferentes canales de comunicación en RENIEC.
- El Plan de Gestión de Crisis y El Plan de Respuesta de Emergencia cubren el objetivo de los mismos y cuentan con roles adecuados para comunicaciones y gestión interna, así como la relación con organismos externos como Bomberos e INDECI en caso se necesite de su apoyo.Cabe mencionar el desconocimiento del personal de RENIEC frente a este tipo de planes (Comunicaciones, Crisis y Emergencia), lo cual implicó realizar una capacitación previa de dichos planes con el personal clave, con el fin de lograr la comprensión de sus objetivos y funciones.

- El Plan de Recuperación de Desastres logró identificar las aplicaciones críticas y los roles necesarios para conseguir operar en el Sitio Alterno de Operaciones una vez declarado el desastre.
- El Plan de Pruebas ha sido realizado a nivel de escritorio como se menciona en las limitaciones de la presente tesis, si bien implicó inconvenientes el contar con todos los comités implicados, se realizó y se pudieron hacer las pruebas adecuadamente.

- Finalmente, es relevante mencionar que el presente diseño del SGCN va a generar un valor agregado y una estrategia desarrollada para RENIEC, ya que se busca lograr con él la continuidad del negocio en caso ocurra un desastre. Por ello, es relevante que la entidad implemente el presente SGCN, pues si bien se presenta el diseño del mismo, es de vital importancia lograr que sea operado y gestionado permanentemente.

5.2 Observaciones

- La presente tesis se encuentra basada en los lineamientos de la norma ISO/IEC 22301; sin embargo para la realización de la misma también se empleó las buenas prácticas del BCI, las cuales se encuentran estrechamente ligadas a la norma base de continuidad de negocios mencionada.
- Al haber establecido miembros de equipos disponibles de recuperación, de comunicación, de crisis, de emergencia; con diferentes funciones y responsabilidades para realizar las tareas planeadas, se logró crear un ambiente de cultura organizacional, concientización y compromiso en RENIEC, para la prevención ante un incidente y mejora de las operaciones según sea el caso.

5.3Recomendaciones

- Se recomienda documentar y definir adecuadamente todos los procesos y funciones críticas del negocio ante cualquier cambio; para lograr así el conocimiento a fondo de las actividades claves, productos brindados y servicios prestados al ciudadano.

- Se recomienda mantener siempre actualizado el Mapa de Riesgos del Negocio en todas sus áreas, con el objetivo de mantenerse siempre alerta ante cualquier circunstancia, tomando en cuenta su grado de criticidad, probabilidad de ocurrencia e impacto, con la mitigación y medios de control respectivos; y actualizar los planes de continuidad de negocio presentados en la presente tesis como medida para estos casos.

- Clarificar los lineamientos sobre los cuales se debe actuar en caso de un incidente, pues las políticas de la organización ya están definidas aún en situaciones de crisis (Confidencialidad, declaraciones a los medios, y salud, relaciones con proveedores, beneficios y relaciones con los ciudadanos).

- Es relevante constituir el equipo de continuidad del negocio, donde estén involucradas la Alta Gerencia y todas las áreas de la organización, ya que la continuidad se encuentra estrechamente ligada a una naturaleza estratégica, táctica y operacional en donde la Alta Gerencia debe participar como patrocinador del proyecto, definiendo las estrategias, aceptando las políticas de continuidad y tomando decisiones de forma proactiva. Por ello se recomienda el siguiente esquema:Jefe general y Gerentes deÁrea.

- Se recomienda, identificar todos los recursos asociados a cada actividad críticas de los procesos de negocio y presupuestarlos de acuerdo a su disponibilidad.
- Se sugiere, identificar las relaciones entre funciones y procesos del negocio, para conocer a fondo las interacciones y dependencias y determinar el impacto a los procesos ante posibles incidentes.

- Se sugiere tomar en cuenta los registros vitales, los cuales son documentos físicos o electrónicos relevantes para la organización, como hojas membretadas, procedimientos, formatos necesarios para llevar a cabo alguna tarea, documentos legales como contratos con proveedores, otros documentos importantes para el trabajo diario; sin los cuales no es posible la recuperación de un proceso o función del negocio. Por ello será necesario resguardarlos por

- Se recomienda, establecer una estrecha comunicación con los proveedores ante cualquier interrupción o incidente, ya que es de vital importancia al constituir fichas vitales para la restauración de operaciones específicas.
- Se recomienda, identificar y determinar ambientes o áreas alternas adecuadas para las operaciones en caso de incidentes; estosdeben de contar con los recursos tangibles e intangibles necesarios para la activación del sitio. Asimismo, es necesario estimar el personal indispensable para la operación alterna.

- Se recomienda, establecer los tiempos críticos de operación y tiempos máximos de impacto tolerable en un determinado proceso, para posteriormente lograr la recuperación de todas las actividades críticas relacionadas al proceso.

- Estimar impactos legales, en el País, respecto a la reputación e imagen, respecto a entes de regulación o control, al ambiente interno y la opinión pública en caso de no manjar una adecuada continuidad del negocio.

- Se recomienda que anualmente se identifiquen períodos críticos en cada uno de los proceso del negocio; para identificar con mayor facilidad y detallelos diferentes incidentes que pueden ocurrir en la organización y el impacto en la recuperación de los proceso críticos, de acuerdo a una fecha y hora específica.

- Se recomienda establecer períodos de actualización de información, archivos, documentos críticos del negocio, para que con base de esta información se planteen nuevas estrategias de recuperación por áreas o procesos.

- Se recomienda evaluar la adquisición de herramientas automatizadas para optimizar la gestión del SGCN (Ejemplo: La mencionadas en el Estado del Arte).
- Se recomienda realizar las pruebas dos veces año para su respectivo ajuste y actualización según sea el caso.
- Se sugiere revisar el Sistema de Gestión de Continuidad de Negocios mínimo una vez al año para controles de cambio y actualizaciones según adquisiciones o alguna modificación en la organización.

- Se sugiere la operación simultánea del SGCN con un SGSI. Ambos sistemas se complementan y son de vital importancia para una organización.

ReferenciasBibliográficas

FLYNN, Stephen
2007 The Edge of Disaster: Rebuilding a Resilient Nation. USA: Random House.ISBN: 978-1-4000-6551-6.

HILES, Andrew
2007 The Definitive Handbook of Business Continuity Management. Segunda Edición. Reino Unido: Wiley&Sons.ISBN: 978-0-470-51638-6.

HOTCHKISS, Stuart
2010 Business Continuity Management: A Practical Guide.ReinoUnido: BCS, the Chartered Institute for IT. ISBN: 978-1-906124-72-4.

SHARP, John
2012 The Route Map to Business Continuity Management: Meeting the Requirements of ISO 22301. Reino Unido: The British StandardsInstitution. ISBN: 978-0-580-74341-2.

TUPIA, Manuel
2011 Principios de auditoría y control desistemas de información. Segunda Edición.
Lima: Tupia Consultores y Auditores S.A.C.ISBN: 978-612-45494-4-1.

SANCHEZ, José
2005 Ingeniería de Proyectos informáticos: Actividades y Procedimientos. Madrid: Universitat Jaume. ISBN: 978-84-8021-408-7.

PMI – PROYECT MANAGEMENT INSTITUTE
2008 Guía de los Fundamentos para la Dirección de Proyectos (Guía del PMBOK). CuartaEdición. USA: PMI. ISBN: 978-1-933890-72-2.

CMI – CHARTERED MANAGEMENT INSTITUTE
2012 “Planning for the worst: The 2012 Business Continuity Management Survey. Que están asociados a cada una de las funciones de negocio Reino Unido: BCI Y BSI.ISBN: 0859464032.

IBM – INTERNATIONAL BUSINESS MACHINES
2012 How security and business continuity can shape the reputation and value of your company.USA: IBM.

AT&T – AMERICAN TELEPHONE AND TELEGRAPH
2012 Business Continuity Study: Disaster Recovery. USA: AT&T.

APECOSE – Asociación Peruana de Empresas de Corredores de Seguros
2012 Conferencia sobre Gestión de Continuidad de Negocio. Perú: APECOSE.

BCI –BUSINESS CONTINUITY INSTITUTE
2013 Good Practice Guidelines 2013. Edición Global.ReinoUnido: BCI.

BCI – BUSINESS CONTINUITY INSTITUTE
2010 Good Practice Guidelines 2010. ReinoUnido: BCI.

SANSI – SYSADMIN AUDIT NETWORKING AND SECURITY INSTITUTE
2005 The Disaster Recovery Plan. USA: SANSI.

DELOITTE GLOBAL SERVICES LIMITED
2010 Guía práctica de cómo implantar un Plan de Continuidad de Negocio. Perú: CELARAYN.

SUNGARD AVAILABILITY SERVICES
2011 LDRPS: Living Disaster Recovery Planning System. USA: SunGard.

SUNGARD AVAILABILITY SERVICES
2012 Business Continuity Mangement Software. USA: SunGard.

SUNGARD AVAILABILITY SERVICES
2012 ISO 22301: A framework for Business Process Definition. USA: SunGard.

RISK LOGIC
2012 About BC-3 Marketing Brochure. Australia: RISK LOGIC.

AVALUTION CONSULTING
2012 About Business Catalyst Software.USA: Avalution.

IDC – INTERNATIONAL DATA CORPORATION
2012 Análisis de la Seguridad de Información en España 2012.España: IDC.

INFORMATION SECURITY & BUSINESS CONTINUITY ACADEMY
2011 "Continuidad de Negocios ¿Es necesaria o no?".BlogISO27001. USA, 2011.

OMG –OBJECT MANAGEMENT GROUP
2011 Business Processes Model and Notation (BPMN). Versión 2.0. USA: 2011.

AUDISEC
2012 Global Suite. Análisis y Gestión de Riesgos basados en ISO 31000 y su integración en Planes de Continuidad de Negocio vasados en ISO/IEC 22301. Madrid: AUDISEC.

DIRECTORS&BOARDS
2006 "Survey about Business Continuity and Disaster Recovery".Boardroom Briefing. Philadelphia: 2012, Vol. 3, No. 1, pp. 19-22.

DRI – DISASTER RECOVERY INSTITUTE
2012 "A culture of Business Continuity".Disaster Recovery Journal. Nueva York, 2012, pp. 17-19.

BCI – BUSINESS CONTINUITY INSTITUTE
2012a "How are companies planning for risk in 2012?".Continuity.ReinoUnido, 2012, Q2, pp.10.

BCI – BUSINESS CONTINUITY INSTITUTE
2012b "Should we test BCM plans against the 'worst case' Continuity.ReinoUnido, 2012, Q2, pp. 13-14.

BCI – BUSINESS CONTINUITY INSTITUTE

2012 "Speaking to the community: BCM standards and the new ISO 22301".Continuity.Reino Unido, 2012, Q3,pp. 27-28.

BCI – BUSINESS CONTINUITY INSTITUTE
2012 "Dispelling the Standard Myths Comparison ISO 22301 to BS25999".Continuity.Reino Unido, 2012, Q3, pp. 29-30.

BUSTAMANTE, Sheilla
2010 Diseño de un sistema de gestión de continuidad de negocios para una entidad bancaria peruana. Tesis (Lic.). Lima: Pontificia Universidad Católica del Perú. Facultad de Ciencias e Ingeniería. Mención: Ingeniería Informática, 2010.

DEL PINO, Laura
2007 Guía de Desarrollo de un Plan de Continuidad de Negocio. Tesis (Lic.). Madrid: Universidad Politécnica de Madrid. Facultad de Informática. Mención: Ingeniería Informática, 2007.

SALAZAR, Jorge
2008 Guía para crear un Plan de Recuperación en caso de desastre en el Sistema Informático del centro de datos de un grupo financiero. Tesis (Master).San José: Universidad para la Cooperación Internacional. Mención: Administración de Proyectos, 2008.

ISACA – INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION
2011 Manual de preparación para el examen de certificación CISA (CertificationInformationSystem Auditor) USA: ISACA Publishing.

2012 COBIT 5 EnablingProcesses. USA: ISACA

2012 COBIT 5 Implementation. USA: ISACA

2012 CiGRAS. ISO 31000:2009. Herramientas para evaluar la gestión de Riesgos.USA: ISACA Publishing.

ISO – INTERNATION ORGANIZATION FOR STANDARIZATION
2005 ISO/IEC 27001:2005 Information technology - Security techniques – Information security management systems. USA: ISO.

2005 ISO/IEC 27002:2005 Information technology - Security techniques – Code of practice for information security management. USA: ISO.

2008 ISO24762:2008 Guidelines for Information and Communications technology disaster recovery services. Suiza: ISO.

2009 ISO 31000:2009 Risk Management – Principles and Guidelines. USA: ISO.

2011 ISO 27031:2011 Information technology — Security techniques — Guidelines for information and communications technology readiness for business continuity. USA: ISO.

2012 ISO 22301:2012 Societal security – Business Continuity Management System – Requirements. Suiza: ISO. 16 de Mayo del 2012

BSI– BRITISH STANDARDS INSTITUTION

2006 BS 25999-1Code of Practice for Business Continuity Management. ReinoUnido: BSI.

2007 BS 25999-2 Business Continuity Management- Part 2: Specification. ReinoUnido: BSI.

NIST – NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

2010 Contingency Planning Guide for Federal Information Systems, Publication 800-34. USA: NIST

NFPA – NATIONAL FIRE PROTECTION ASSOCIATION

2007 Standard on Disaster/Emergency Management and Business Continuity Programs.USA:NFPA.

INDECOPI Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual

2008 NTP-ISO/IEC 27001. EDI. . Tecnología de la Informacion.Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información.12 de Diciembre del 2008.

SBS – Superintendencia de Banca, Seguros y AFP

2009 Circular Nº G- 139 -2009 Referente a Gestión de la continuidad del Negocio: 02 de Abril del 2009.

BCI – BUSINESS CONTINUITY INSTITUTE

2012 Frequently Asked Questions about the BCI.Consulta: 15 Setiembre del 2012 <http://www.bcifiles.com/FAQsabouttheBCI2011.pdf>

DRI – DISASTER RECOVERY INSTITUTE

2012 About the DRI International. Consulta: 13 Setiembredel 2012. <https://www.drii.org/docs/DRII%20Factsheet.pdf>

BSI – BRITISH STANDARDS INSTITUTION

2012 About THE BSI Group. Consulta: 13 de Setiembre del 2012. <http://www.bsigroup.com/en/About-BSI/>

NIST– NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

2012 General Informationabout NIST. Consulta: 13 de Setiembre del 2012. <http://www.nist.gov/public_affairs/general_information.cfm>

INDECI – INSTITUTO NACIONAL DE DEFENSA CIVIL EN EL PERÚ

2012 Emergencias y daños personales a nivel nacional según fenómeno del año 2011. Consulta: 07 de Abril del 2013. <http://www.indeci.gob.pe/objetos/secciones/MTM=/NTM=/lista/NjUx/201203051717581.pdf>

INEI – INSTITUTO NACIONAL DE ESTADÍSTICAS E INFORMÁTICA

2012 Anuario de Estadísticas Ambientales 2012. Consulta: 07 de Abril del 2013. <http://www.inei.gob.pe/biblioineipub/bancopub/Est/Lib1037/Libro.pdf>