Documento de Tesis para la Elaboración de la Guía Metodológica para Elaborar un BCP en Entidades del Estado

Luz Andrea Peña Castro

Escuela Colombiana de Ingeniería Julio Garavito

Nota del autor

Luz Andrea Peña Castro, Facultad de Ingeniería de Sistemas, Escuela Colombiana de Ingeniería Julio Garavito

La información concerniente a este documento deberá ser enviada a Facultad de Ingeniería de Sistemas, Escuela Colombiana de Ingeniería Julio Garavito, Avenida carrera 45 205-59 Autopista Norte. E-mail: luz_andyp@yahoo.com

Nota de Aceptación

_____

_____

_____

_____

_____

_____

Firma del Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

Dedicatoria

Este trabajo está dedicado a Dios por darme la fuerza y el valor para cumplir mis sueños y a mi jefe Álvaro Márquez, por ver en mí competencias y aptitudes que con su apoyo he venido desarrollando y mejorando cada vez más, lo que me ha permitido mejorar como profesional y de esta forma aportar a la sociedad.

Agradecimientos

Al fondo de Talento Digital del Mintic por el apoyo financiero para realizar mi Maestría en Gestión de Información.

Al Ingeniero Jorge Bejarano, Director de Estándares y Arquitectura del Mintic por su apoyo en la asignación del proyecto y a todo su equipo de la Subdirección de Seguridad y Privacidad de TI, por sus aportes, lineamientos, comentarios y tiempo dedicado a la lectura de las diferentes versiones del proyecto.

A la ingeniera Victoria Eugenia Ospina, Directora de la Maestría en Gestión de Información, por su apoyo y colaboración en el desarrollo de este proyecto.

A mi esposo Félix Uriza y a mis dos hijas Sarah e Isabella, por su apoyo incondicional y su comprensión.

Luz Andrea Peña Castro

Abstract

The purpose of this document is to describe a methodology to create the business continuity plan for the information technologies in the state entities; updating and complementing the "Guía para la preparación de las TIC para la continuidad de Negocio", which is part of Security Model and the Information Privacy emitted by the Information Technology and Communications Ministry (MINTIC), in the version 3.0 of march 2015; taking as base of reference the framework for Security of MINTIC, Cobit 5.0 and it process DSS04 Continuity Management, and ISO 22301 and ISO 27001: 2013.

TABLA DE CONTENIDO

Pág

LISTA DE FIGURAS

LISTA DE TABLAS

INTRODUCCION

Todos los días escuchamos noticias de diferentes catástrofes, desastres naturales, atentados terroristas, y asonadas, que afectan diferentes países a nivel mundial, sin importar su economía y si están preparados o no. Colombia no es la excepción y es deber de las empresas públicas garantizar que ante cualquier evento van a continuar prestando los servicios a los ciudadanos de una manera adecuada y manteniendo la seguridad de la información. El Ministerio de las Tecnologías de la Información y las Telecomunicaciones MINTIC, a través de su Modelo de Seguridad para las entidades del estado, entregó una guía para que las entidades puedan construir su Sistema de Gestión de Seguridad de la Información (SGSI). Dentro de estas guías se encuentra la "*Guía para la preparación de las TIC para la continuidad de negocio*" creada el 15 de diciembre de 2010 en su versión 1. La cual es el primer avance para promover la creación de los Sistemas de Gestión de la Continuidad de Negocio en el sector público. Esta guía es el punto de partida de este proyecto de grado.

El objetivo del proyecto es el de crear la versión 2 de la "*Guía para la preparación de las TIC para la continuidad de negocio*". Para esto seguimos las mejores prácticas definidas en la norma ISO 22301 y COBIT 5.0; así como los lineamientos del Decreto 2573 de 2014, donde se reglamenta el Marco de Referencia de la Arquitectura Empresarial. El valor agregado de este proyecto es el de generar una guía fácil de implementar, con ejemplos para el desarrollo de los componentes del modelo de operación de la continuidad de negocio, plantillas, formatos y guías

creadas con base a la experiencia de 8 años diseñando e implementando planes de continuidad para empresas del sector servicios y financiero.

La "*Guía para la preparación de las TIC para la continuidad de negocio*" en su versión 1.0, plantea un modelo de operación de la continuidad de negocio, la cual consta de cinco componentes: diagnóstico, planificación, implementación, gestión y mejora continua. Mediante este trabajo de investigación vamos a revisar cada uno de los componentes y vamos a aplicar las mejoras y actualizaciones que haya lugar.

En el componente de diagnóstico, diseñaremos un GAP de cumplimiento con el proceso DS04 de COBIT 5.0, con un modelo de capacidad de la entidad para dar respuesta a un evento de contingencia y por último definiremos el modelo de madurez de implementación del plan de continuidad; para el modelo de capacidad y de madurez, nos basaremos en el estándar ISO IEC 15504. Actualmente no hay metodología definida para este componente.

Una vez tengamos el diagnóstico inicial, podremos iniciar el componente de planificación. Las entradas de este proceso inicialmente es la conformación de un equipo interdisciplinario o dueños de proceso; este equipo será llamado "equipo de continuidad". Quienes serán los encargados de planificar el plan de continuidad, gestionarlos, probarlo y mejorarlo. En el modelo propuesto, se sugiere una estructura, los roles y responsabilidades de sus integrantes. Para iniciar el proceso de planificación, se debe contar con entradas tales como, la estrategia de la compañía, la arquitectura tecnológica, de aplicaciones y datos, políticas y procedimientos, los

lineamientos de la arquitectura empresarial, flujos de datos, presupuestos, listado de empleados críticos, entre otros. En este componente se definirán guías para crear los objetivos y alcance del plan, gestión de riesgos, análisis de impacto de negocio (BIA) y definición de estrategias de continuidad, de acuerdo a las necesidades de la institución.

Para el análisis de impacto de negocio, definiremos una metodología que le permita al equipo de continuidad, identificar claramente los procesos críticos, los factores críticos de éxito de estos procesos, definir el peso de los procesos en cuanto a su importancia para la empresa, identificar los riesgos y cuantificarlos, identificar los riesgos de los procesos TIC y la dependencia de los procesos, identificación de registros vitales, proceso de backup de información crítica. Al final el producto será definir claramente los tiempos de recuperación.

Con esta información llegamos al componente de implementación, donde identificaremos los posibles escenarios y definiremos planes de recuperación, responsables de su ejecución y presupuesto necesario. En este componente definiremos un indicador para la medición del nivel de implementación de la continuidad de negocio.

Una vez planificado e implementado el plan de continuidad, continuamos con el componente de gestión, donde se definirán planes de capacitación, se diseñará un proceso de generación y recuperación de backups, de acuerdo a la estrategia definida en la fase de planeación.

Es importante, realizar pruebas de continuidad para identificar posibles mejoras al plan y es aquí donde entra en funcionamiento el componente de mejora continua, la guía permitirá al equipo de continuidad definir un plan de pruebas, plantillas de informes y seguimiento a las remediaciones.

Este es un proceso cíclico de mejora continua, donde interviene todo el equipo de continuidad, pero especialmente requiere el compromiso de la dirección, apoyando el plan definido, mediante la asignación de recursos financieros, humanos, entre otros. Al final realizaremos sugerencias para continuar con una versión 3.0 de la "*Guía para la preparación de las TIC para la continuidad de negocio*".

1. PLANTEAMIENTO DEL PROBLEMA

1.1. ANTECEDENTES

En el año 2010, el Gobierno Nacional en el marco del Congreso Internacional TIC, presentó su política de Tecnologías de la Información y las Comunicaciones, denominada Vive Digital, cuyo objetivos son "*ser el país líder en el desarrollo de APPS sociales dirigidas a los más pobres*" y , "*ser el gobierno más eficiente y transparente gracias al uso de la tecnología*"; Lograr que el país pueda ingresar a la sociedad de la información y el conocimiento, para ser más competitivos, disminuir la pobreza y el desempleo. Dentro de las aplicaciones del plan Vive Digital se encuentra la estrategia de Gobierno en Línea, que busca aprovechar los avances tecnológicos para garantizar una mejor comunicación e interacción con la ciudadanía, prestando más y mejores servicios por parte del Estado.

La política de Gobierno en Línea en Colombia inicio en el año 2000, con la directiva presidencial 2; pero su implementación realmente inicio en el año 2008 mediante el Decreto 1151, donde se definieron lineamientos generales de la estrategia. Desde entonces las entidades públicas han generado grandes logros en cuanto a provisión de trámites y servicios electrónicos, mejora en la calidad de la información en sus sitios web, entre otros. De acuerdo con el más reciente reporte Global de las Naciones Unidas (2012), Colombia es el mejor país en servicios en línea y en participación electrónica de América Latina y el Caribe.

La estrategia de Gobierno en Línea se plantea grandes retos, lo cual va a permitir la evolución en términos de tecnología y desarrollo a nuestro país. Temas tales como gobierno abierto, multicanalidad, la conciencia del medio ambiente, la seguridad y el ciudadano como centro de la gestión pública. Esta estrategia es liderada por el Ministerio de las Tecnologías de la Información y las Comunicaciones y busca cada vez generar sinergia entre las entidades del estado y la ciudadanía. Es un gran esfuerzo, ya que deberán aumentar cada vez más servicios en línea, mejorar la calidad de acceso a estos servicios y a la información y los datos.

La estrategia de Gobierno en Línea está compuesta por seis elementos, que son: elementos transversales, información en línea, interacción en línea, transacción en línea, transformación y democracia en línea (MINTIC, Manual para la Implementación de la Estrategia de Gobierno en Línea en las Entidades de Orden Nacional de la República, 2011).

a) Elementos Transversales: en este elemento las entidades se enfocan en el conocimiento de los usuarios y sus necesidades en torno a los servicios que se le prestan a los ciudadanos. Entre las actividades que designan para este componente está el de implementar un Sistema de Gestión de Tecnologías de la Información. Este sistema además de la estrategia, de los planes de actualización tecnológica, se debe plantear un Sistema de Gestión de la Continuidad que garantice que todos los servicios que se van a prestar en línea tengan respaldo y estén siempre al aire.

b) Información en Línea: este componente comprende actividades que permita a los usuarios tener acceso electrónico a toda información relativa a la misión, planeación estratégica de la entidad, trámites y servicios, espacios de interacción, ejecución presupuestal, entre otros. Se deben cumplir todos los requisitos de calidad, disponibilidad, accesibilidad, estándares de seguridad, entre otros.

c) Interacción en Línea: consiste en habilitar herramientas de comunicación de doble vía entre servidores públicos, organizaciones, ciudadanos y empresas. Este componente promueve la habilitación de servicios en línea y otros mecanismos que acerquen a los ciudadanos a la administración pública.

d) Transacción en Línea: este componente se enfoca en la implementación de trámites y servicios a través de diferentes canales electrónicos, con el fin que el ciudadano pueda realizar trámites y servicios en línea, como ventanillas únicas virtuales, pagos en línea, uso de firmas electrónicas y digitales, entre otros.

e) Transformación: Este componente se trata precisamente de la transformación de los procesos internos de la entidad, aplicando la política de cero papel, mejorando y modernizando la comunicación e interacción entre entidades, de manera tal que se genere una sinergia en pro del ciudadano.

f) Democracia en Línea: este componente se busca propiciar que el ciudadano participe activa y colectivamente en la toma de decisiones de un Estado totalmente integrado en línea. (MINTIC, Manual para la Implementación de la Estrategia de Gobierno en Línea en las Entidades de Orden Nacional de la República, 2011) (MINTIC, Manual para la Implementación de la Estrategia de Gobierno en Línea en las Entidades de Orden Nacional de la República, 2011) (MINTIC, Manual para la Implementación de la Estrategia de Gobierno en Línea en las Entidades de Orden Nacional de la República, 2011) (MINTIC, Manual para la Implementación de la Estrategia de Gobierno en Línea en las Entidades de Orden Nacional de la República, 2011)

Los seis componentes de la Estrategia de Gobierno en Línea, implica el desarrollo e implementación de herramientas tecnológicas, que van a tener como propósito publicar y gestionar información para los ciudadanos. Estas herramientas deberán garantizar la continuidad de estos servicios, con calidad y ante todo Seguridad de la Información.

2. OBJETIVO GENERAL

Diseñar y desarrollar una metodología general para que las entidades estatales de orden nacional y territorial, elaboren sus planes de continuidad de negocio de la gestión en tecnologías de información y telecomunicaciones, procesos y personas, basándose en buenas prácticas internacionales, pero ajustada a la infraestructura local de las entidades del estado en Colombia.

2.1. OBJETIVOS ESPECÍFICOS

- Diseño y desarrollo de la metodología para generar el análisis de impacto de negocio.
- Diseño y desarrollo de la metodología para definir estrategias de recuperación.
- Diseño y desarrollo de la metodología para definir el procedimiento de implementación del plan de continuidad.
- Diseño y desarrollo de la metodología para definir el programa de capacitación y concientización del plan de continuidad.
- Diseño y desarrollo de las etapas mínimas de un procedimiento de pruebas y mantenimiento del plan de continuidad.

3. **JUSTIFICACION**

Las entidades del estado al hacer uso creciente de herramientas tecnológicas e internet para la transmisión, procesamiento y almacenamiento de información, hace que se expongan a un tipo de delincuencia más sofisticada, como son los hackers o delincuentes cibernéticos, que pueden robar información para fraudes o utilización inadecuada de la misma, lo que puede conllevar a la entidad a pérdidas millonarias, desprestigio de la marca e incluso el cierre de la misma. El Ministerio de las Tecnologías de la Información y las Comunicaciones (MINTIC) reporta que en el año 2011, se presentaron más de 550 ataques exitosos a entidades del estado. Por esta razón se diseña y crea un modelo de Seguridad de la Información para las entidades del Estado, donde entregó una serie de guías para que las entidades puedan construir su Sistema de Gestión de Seguridad de la Información (SGSI). Sin embargo en sus primeras versiones, no se creó la guía para la implementar el Plan de Continuidad de Negocio, el cual es de vital importancia para la supervivencia de las empresas y la continuidad de funciones críticas o servicios que se le prestan a los ciudadanos, en caso de un incidente o desastre natural. Este modelo fue creado con el fin de dar cumplimiento al Decreto 2693 de 2012, que se derivan de la evolución de las " Fases de Gobierno en Línea", donde se derivan actividades transversales. El objetivo de esta tesis es diseñar una guía para el Modelo de Seguridad creado por el Mintic, que le permita a las entidades del estado crear su propio Plan de Continuidad del Negocio, con el fin de garantizar la continuidad de sus operaciones, funciones, procesos críticos y servicios en línea que se prestan a los ciudadanos u otras entidades en caso de un incidente de seguridad grave o un desastre natural.

El Sistema de Gestión de la Continuidad de Negocio, le permitirá a las entidades actuar de manera preventiva ante posibles materializaciones de riesgos inminentes que puedan afectar su normal funcionamiento. Además, esta práctica les permitirá mantener actualizada su plataforma tecnológica acorde a las necesidades del negocio, se realizará gestión del conocimiento de todas y cada una de las actividades críticas del negocio y dará confianza a los ciudadanos, Gobierno Nacional, clientes e inversionistas nacionales e internacionales, ya que el negocio o servicio de la entidad tendrá continuidad en el tiempo.

Según el informe emitido por el MINTIC en julio de 2014 respecto al avance de Colombia en la Sociedad de la Información y la Dirección de Gobierno en Línea (GEL), la cual es la unidad encargada de coordinar en la administración pública la implementación de la estrategia de Gobierno en Línea en el país, mediante la implementación de mejores servicios y el aprovechamiento de tecnologías de la información, informa que el 100% de las organizaciones gubernamentales tienen presencia en internet con su propio sitio web o en el sitio web de otra entidad; el 89,9% de las empresas de orden nacional y el 86,2% de las entidades de orden territorial, ofrecen plataformas de servicios para interactuar con sus usuarios; en cuanto a servicios en línea suministrados por las entidades del estado:

Tabla 1 Servicios en línea según tipo de actividad

ACTIVIDAD	%
Recibir respuestas a sus consultas vía correo electrónico o telefónicamente	87%
Hacer consultas vía correo electrónico	85,1%
Hacer denuncias, quejas y reclamos	84,4%
Descargar formularios	60,4%
Registrar formularios en línea	53,9%
Realizar pagos en línea (facturas, impuestos, salud, licencias, certificados)	24,0%
Participación ciudadana (sistema de votación/elecciones/ consultas públicas)	25,3%

El porcentaje de servicios en línea, sitios web o utilizando herramientas tecnológicas es alto, es por esto, que se convierte en gran importancia implementar un Plan de Continuidad para garantizar estos servicios a los ciudadanos.

El plan de continuidad y la planificación de recuperación de desastres (BCP/DRP), se ha convertido en un dominio crítico en la gestión de conocimiento de una entidad u organización; en los últimos 10 años el mundo ha experimentado muchos acontecimientos que han quedado marcados en la memoria del mundo, como son: el terrorismo, los terremotos, los huracanes, los tsunamis e inundaciones. Continuidad del negocio y la planificación de recuperación de desastres, es la última línea de defensa de una entidad, cuando los controles han fallado, el plan

de continuidad es el control final, que puede prevenir eventos drásticos, como lesiones, pérdidas de vida o el fracaso de una organización. Además le permite a la empresa crear una cultura de autoconocimiento constante y gestión de los riesgos; sin mencionar la optimización de los recursos de Tecnologías de la Información y los procesos.

La criticidad de la información dentro de la organización y la complejidad de los sistemas de información hacen que las entidades sean más sensibles ante las amenazas de la integridad de la información. Los incidentes de pérdida de información que con cierta frecuencia se presentan o son dados a conocer por los medios de comunicación, provocan alarma en las organizaciones, ya que afectan a la totalidad de las actividades de las mismas, y más aún cuando una entidad presta servicios vitales a millones de ciudadanos.

Es amplio el espectro de amenazas a las cuales se encuentra expuesta una entidad, la primera y la más impredecible y con grandes impactos, son "los desastres naturales". En Colombia desde el año 1970 y el 2011 se han registrado más de 28 mil eventos que han generado pérdidas, de los cuales cerca del 60%, se reportan a partir de las década de 1990. Fenómenos como sismos fuertes y las erupciones volcánicas severas, por lo general ocasionan grandes pérdidas concentradas en un territorio y en un lapso de tiempo relativamente corto, por eso han sido denominados riesgos intensivos. Actualmente el 86% de la población Colombiana se localiza en zonas de amenaza sísmica alta y media. El 44% del territorio colombiano se encuentra expuesto a amenaza sísmica alta e intermedia, principalmente en las regiones Pacífica y Andina, lo cual significa que 960 municipios, entre ellos los de mayor población, están expuestos. Los

municipios con más concentración de riesgo relativo, desde el punto de vista económico, con respecto al PIB y por exposición a la amenaza sísmica, corresponden a Cali, Bogotá, Villavicencio, Pasto y Manizales. Dentro de los eventos que pueden ser más críticos para el país está la posibilidad de un terremoto. Las pérdidas estimadas por sismo con un periodo de retorno de 500 años serían: Bogotá de US$12.700 millones, para Medellín de US$7.500 millones, para Cali de US$6.400 millones, para la región del eje cafetero US$2.000 millones y para la nación en general de US$44.900 millones (COLOMBIA B. M., 2012).

Una segunda amenaza son los Humanos, las cuales se pueden clasificar como intencional y no intencional; las amenazas humanas intencionales son los ataques deliberados, por ejemplo una infección de malware dentro de la organización, denegación del servicio, phishing[1], ingeniería social, entre otros. El ISTR[2] en el Informe Anual sobre Amenazas a la Seguridad en internet de Symantec del año 2012, revela que los ataques maliciosos aumentaron en un 81%, además, que Argentina, Brasil, Chile, Colombia y México se encuentran entre los países con mayor actividad maliciosa en América Latina. Symantec bloqueó más de 5.500 millones de ataques maliciosos en 2012, lo cual representó un aumento del 82% con respecto al año anterior. Los ataques dirigidos utilizan ingeniería social y malware personalizado para obtener acceso no autorizado a la información confidencial (SYMANTEC, 2012). Estos avanzados ataques han hecho foco tradicionalmente en el sector público y el gobierno. Un ataque de este tipo puede impactar la operación y el normal funcionamiento, hasta el punto de requerir activar el plan de continuidad

[1] Definición Phishing, según APWG (Anti-Phishing Working Group), procede de una analogía entre este delito y la pesca. Es una forma de ingeniería social en la cual el atacante intenta de forma fraudulenta adquirir información confidencial de una víctima, haciéndose pasar por un tercero de confianza.
[2] ISTR (Internet Security Threat Report

del negocio, bien sea porque se afecta la arquitectura, los servicios, pérdida de información, la no disponibilidad de los datos para operar o un problema de prestigio que ocasionen cuantiosas demandas.

Una tercera amenaza es la "ambiental", esta amenaza se centra en el medio ambiente en lo que respecta a los sistemas de información o de centro de datos, la amenaza de una interrupción en el ambiente computación es significativa. Esta clase de amenaza incluye elementos tales como problemas de energía (apagón, una baja de voltaje, sobretensiones, picos), componentes del sistema u otras fallas en los equipos, aplicación o defectos de software.

El proceso de planeación de la continuidad de operaciones carecía de un sentido de urgencia previo a los ataques terroristas del 11 de septiembre de 2001. Las consecuencias vividas resultado de estos ataques, nos demostraron escenarios complejos, altos niveles de vulnerabilidad e interdependencia entre procesos y funciones críticas, que hoy nos enseñan la importancia de prever y gestionar los riesgos y sus efectos. "*Ante un escenario de emergencia o desastre en países de América Latina y el Caribe, las empresas públicas y privadas que ofrecen servicios esenciales a la población pueden verse afectadas. Es expectativa de la población y responsabilidad del gobierno estar preparados para enfrentar escenarios adversos e independientemente de la afectación, garantizar estabilidad y permanencia de las entidades del estado"* esta es la frase que enmarcó el II Seminario Regional de Alianzas entre el Sector Público y Privado para la gestión de riesgo de Desastres (CELAC, 2013).

El diseño de una guía para la implementación de un Sistema de Gestión de Continuidad a nivel del Ministerio, permitirá a las empresas que no han iniciado el proceso, guiarse y entrar en el mundo de la prevención y a las que ya tienen un modelo, les servirá para actualizar su plan y generar propuestas de mejora. También permitirá a las empresas del estado generar Sinergia y apoyo mutuo, por ejemplo crear centros alternos entre empresas, de esta forma podrían haber ahorros en la implementación del plan.

El sistema de Gestión de la Continuidad, le permitirá a las empresas revisar y analizar los riesgos asociados a sus procesos donde están involucradas las Tecnologías de la Información y de forma preventiva diseñar planes que implican custodia externa de la información crítica de la empresa, optimizar la infraestructura de Tecnología, ajustarla a al estrategia de la compañía y respaldando los procesos críticos para garantizar el servicio en el máximo porcentaje posible.

La información es el activo más importante de las empresas después del recurso humano, por esta razón es importante identificarla, clasificarla y establecer medidas de protección de la misma. Muchas veces la información crítica no se encuentra identificada e incluso no se sabe que existe y cuál es su impacto para la empresa. En algunas ocasiones esta información se encuentra en el conocimiento de los empleados y no está documentada. El sistema de Gestión de la Continuidad tiene entre sus actividades identificar esta información de gran importancia para la continuidad del negocio, documentarla y generar planes para respaldarla garantizando la seguridad de la información. Esto genera confianza para la Dirección, sus empleados e incluso los ciudadanos y clientes.

Actualmente no existe regulación que exija al 100% de las empresas implementar un Sistema de Gestión de la Continuidad, a excepción del sector financiero. Se hace énfasis en la integridad y confidencialidad de la información, pero no a la disponibilidad de los sistemas, procesos y personas. No obstante, la estrategia de Gobierno en Línea busca ofertar e incrementar los servicios prestados por entidades de los estados a través de internet, automatizar y sistematizar procesos, realizar transacciones en línea, digitalizar los documentos para dar cumplimiento a la política de cero papel. Esto hace imprescindible implementar un Sistema de Gestión de Continuidad de Negocio. Estudios realizados sobre el tema de continuidad de negocio, revelan como cualquier negocio termina rápidamente siendo incapaz de realizar o ejecutar las actividades del día a día, cuando los sistemas, la información, las aplicaciones y componentes de tecnología de información no están disponibles a causa de un siniestro, eventualidad o contingencia. Adicionalmente a esto contratiempos se puede deteriorar la imagen de la entidad, así como múltiples demandas.

El producto de esta tesis es una herramienta que publicará el Ministerio de las Tecnologías de la Información para que las empresas utilicen como guía para documentar y crear el Plan de Continuidad de Negocio. La guía está enfocada a los procesos de tecnología, información, sistemas de información y procesos críticos del negocio. La guía deberá seguir lineamientos de estándares internacionales enfocados en continuidad de negocio, como ISO 27001, COBIT, ISO 22301, entre otros. También tendrá aportes de conocimientos y experiencias adquiridos por la estudiante mediante la ejecución de su trabajo.

4. MARCO TEORICO

4.1. PLAN DE CONTINUIDAD DE NEGOCIO (BCP)

Business Continuity Planning (BCP), Plan de Continuidad del Negocio, tiene como objetivo principal asegurar que la organización seguirá funcionando antes, a lo largo y después de experimentar un desastre o evento de seguridad. El enfoque del BCP está en el negocio como un todo y asegurar que esos servicios fundamentales que la empresa presta o de funciones esenciales que la entidad realiza con regularidad aún se puedan llevar a cabo, tanto durante de la interrupción como después. Con el fin que la organización siga siendo operable la organización tendrá que tomar en cuenta las amenazas comunes para sus funciones esenciales, así como las vulnerabilidades asociadas que podrían afectar el normal funcionamiento en determinado momento. El plan de continuidad proporciona una estrategia a largo plazo para asegurar que la operación continua con éxito, a pesar de los acontecimientos y desastres inevitables (Eric Conrad, 2010).

Según el Instituto Nacional de Estándares y Tecnología de Estados Unidos (National Institute of Standards and Technology, en la NIST Special Publication 800-34 Rev.) El BCP se centra en el mantenimiento de los procesos de misión /crítica durante y después de una interrupción, como un proceso de nómina o de servicio al cliente de la organización.

Según la norma ISO 22301, el BCP debería contener mínimo seis entregables:

a) Política de continuidad de negocios, que consiste en una declaración de interés de la Alta gerencia de la entidad, denota su apoyo en cuanto a la destinación de recursos exclusivos para su implementación.

b) Análisis de impacto de negocio (BIA). Corresponde a un estudio interdisciplinario e inter-áreas, donde se analiza el impacto sobre la normal actividad de la empresa si dejan de operar durante un tiempo determinado.

c) Análisis de riesgos (RA). Se trata de un análisis proactivo a lo que puede suceder y planificar la manera de posibles soluciones.

d) Estrategias de continuidad de negocio. Son las acciones, recursos y necesidades específicas que se deben tener en provisión en caso de necesitarse, en caso de un evento o calamidad.

e) Estructura de respuesta y finalización de incidentes. Corresponde al paso a paso, los responsables, los contactos y las actividades a realizar en caso de la activación del plan de continuidad.

f) Plan de mantenimiento y pruebas. Corresponde a poner en práctica lo planificado para poder ajustar lo que no funciona correctamente.

De acuerdo con lo anterior, Continuidad de Negocio es la Capacidad estratégica y táctica que tiene una organización para planificar y responder a incidentes e interrupciones del negocio, con el fin de continuar con las operaciones críticas del negocio dentro de un nivel de servicio aceptable y asumible por la Organización.

Entonces la Gestión de la Continuidad de Negocio, es el proceso de gestión integral que identifica amenazas potenciales a las que se puede enfrentar una Organización y los impactos a las operaciones que dichas amenazas, en caso de materializarse puedan causar, y que proporciona un marco para construir su recuperación organizativa con capacidad para dar una respuesta eficaz que salvaguarde los intereses de los stakeholders involucrados.

Es decir, el Plan de Continuidad de Negocio (BCP) es un conjunto de procedimientos e información documentada que se desarrolla, almacena y se mantiene preparado para su uso en caso de producirse un evento de seguridad, con el fin que la Organización sigua desempeñando sus actividades críticas a un nivel aceptable previamente definido.

4.1.1. Beneficios y Cómo Se Relaciona Con La Competitividad En Las Organizaciones

El Sistema de Gestión de la Continuidad tiene por objetivo realizar acciones para proteger los procesos críticos y operativos del negocio contra desastres naturales, terrorismo o fallas mayores de la infraestructura tecnológica y sistemas de información. Se busca disminuir el impacto en las pérdidas de tipo financiero, de información crítica de negocio, credibilidad y productividad, en el momento que los recursos de la entidad no estén disponibles.

El Plan de Continuidad le permitirá identificar de manera preventiva los riesgos asociados a la entidad en términos de Tecnologías de la Información y su probabilidad de ocurrencia. Se evaluarán problemas potenciales que puede afectar la infraestructura tecnológica y de operaciones, incluyendo el centro de datos y las estaciones de trabajo.

Una vez identificados los riesgos, se determinan los impactos monetarios, legales, contractuales y de marca, que pudieran afectar los procesos críticos o vitales de la entidad, sus aplicaciones, su tecnología y sus recursos. Esta actividad permitirá dar prioridad a los de más alto impacto, con el fin de generar planes y asignar recursos para su implementación.

4.1.2. Reglamentación Orientada a La Implementación de BCP En El Mundo

- **Costa Rica**

El Ministerio de Ciencia, Tecnología y Telecomunicaciones MICITT, en el Plan Nacional de Desarrollo de las Telecomunicaciones, estableció una línea estratégica de seguridad, en donde el segundo objetivo es "*Garantizar Continuidad del Servicio en Caso de Emergencia*" (Ministerio de Ciencia, 2014). Actualmente se encuentra en el desarrollo de estos planes.

Entre las metas definidas en este plan, se encuentra una especialmente orientada a la ejecución del plan de continuidad y contingencia que es l ade *Crear un plan de continuidad de las operaciones que dicte medidas de seguridad física y lógica de las redes y servicios*.

- **Ecuador**

En el artículo 312 de la Constitución Política de Ecuador, establece que *el estado garantizará que los servicios públicos y su provisión respondan a los principios de obligatoriedad, generalidad, uniformidad, eficiencia, responsabilidad, universalidad, accesibilidad, regularidad, continuidad y calidad.*

En Ecuador se creó la Secretaría Nacional de Gestión de Riesgos, en coordinación con el Ministerio de Seguridad Interna y Externa, este Ente creó el "Plan de Emergencias Institucional", donde se enfoca en el proceso de gestión de riesgos, el cual está enfocado en la reducción de los riesgos, al manejo de las emergencias y desastres, y a la recuperación ante eventos adversos que afecten las vidas humanas o los recursos. También se establece en este plan que es responsabilidad de todas las instituciones públicas y privadas. En el numeral 1.9 de este documento se aborda un capítulo exclusivo para implementar el plan de continuidad.

Ecuador define el plan de continuidad como la herramienta con la cual las instituciones públicas y privadas se preparan para garantizar la continuidad de sus actividades productivas y de servicios cuando se enfrentan a una situación de emergencia (Riesgos, 2012). Entre otras actividades, define las siguientes como lineamientos generales para su construcción:

- Identificar las áreas fundamentales y las actividades críticas de la institución o empresa, según criterios de impacto económico, impacto social por ausencia de los servicios que brinda, o del impacto de seguridad o salud de los usuarios o beneficiarios.
- Una vez identificadas las áreas fundamentales y sus actividades críticas, planificar y organizar el personal y recursos necesarios para la continuidad de las actividades, durante un día, una semana y quince días laborales. Esta planificación debe considerar si habrá cambios entre el horario normal de trabajo, y el horario en situación de emergencia.
- Definir instituciones necesarias y complementarias para el desarrollo de sus actividades críticas (socios, proveedores, clientes…).

- En caso que la institución no pueda continuar sus actividades críticas dentro de sus instalaciones, considerar la adecuación de un lugar temporal con servicios básicos, con equipamiento y suministros indispensables (mesas, sillas, teléfonos, fotocopiadoras, entre otros)
- Considerar las facilidades de transporte adecuado para los trabajadores.
- Contar con un sistema de comunicación operativo
- Contar con responsables claramente identificados.

- **El Salvador**

La constitución del Salvador en su título V sobre orden económico, específicamente en el artículo 112, dispone que el Estado podrá administrar las empresas que presten servicios esenciales a la comunidad, con el objeto de mantener la continuidad de los servicios, cuando los propietarios o empresarios se resistan a acatar las disposiciones sobre la organización económica y social.

En el año 2006 se formuló la primera versión del Plan Nacional de Protección Civil, Prevención y Mitigación de desastres. En noviembre de 2011 se realizó una actualización que abarca todos los capítulos del plan, especialmente los relacionados con prevención, la mitigación y preparación para la respuesta que conforma una estrategia, llevada al nivel de acciones y

metas. En el año 2012, se incluyó en la metodología la articulación de procesos para intervenir en las áreas y se incluyeron componentes de gestión de riesgos.

El objetivo estratégico de este plan busca *reducir los factores de riesgo de la población Salvadoreña, las causas de las pérdidas de vidas humanas, y las consecuencias sociales, económicas y ambientales inducidas por las amenazas de origen natural y antrópico que afecten el territorio nacional* (Sistema Nacional de Protección Civil, 2012).

En el Salvador fue aprobado el Decreto Legislativo No. 777 del 31 de agosto de 2005. De acuerdo con su artículo 1, esta Ley tiene por objeto prevenir, mitigar y atender de forma efectiva los desastres naturales y antrópicos en el país y además desplegar en su eventualidad el servicio, continuidad y regulararidad, para garantizar la vida integral de las personas, así como los bienes privados y públicos.

- **Guatemala**

En Guatemala existe la Ley de la Coordinadora Nacional para la reducción de desastres naturales o provocados en el año 1996, no se refiere directamente a conceptos de continuidad, pero sí al restablecimiento de los servicios públicos y líneas vitales.

- **México**

En México la Ley General de Protección Civil, en la fracción VII del artículo 7, establece la continuidad de las operaciones como una tarea transversal con especial énfasis en áreas con relación directa a los temas de salud, educación, ordenamiento territorial, planeación urbana – regional, conservación y empleo de los recursos naturales.

En el año 2009, la Secretaría de Gobernación Sistema Nacional de Protección Civil, creó la *Guía para la Elaboración e Implementación del Programa Interno de Protección Civil* en donde en su capítulo 4, se encuentra la continuidad de las operaciones. En esta guía se definen lineamientos para el Plan de Contingencias COG, el cual se compone principalmente por cuatro capítulos: 1) Evaluación de riesgo por cada puesto de trabajo; 2) medidas y acciones de autoprotección; y 3) Difusión y Socialización. También define lineamientos para el Plan para la Continuidad de las Operaciones COOP, en el cual define las siguientes actividades: 1) Operaciones y funciones críticas; 2) requerimientos mínimos; 3) dependencias e interdependencias; 4) metas de recuperación y tiempos; 5) pasos para la recuperación; 6) supuestos; 7) métodos de comunicación; 8) elementos financieros claves; 9) información tecnológica clave; 10) implementación del plan; y 11) Mantenimiento, revisión y ejecución (México, 2009).

Entre los componentes definidos para el plan de continuidad son:

- Identificar operaciones y funciones críticas
- Identificar los requerimientos mínimos para realizar las funciones críticas
- Identificar las dependencias e interdependencias internas y externas.
- Establecer las metas de recuperación y sus tiempos.
- Determinar los métodos alternativos de operación y los lugares en donde poder realizarlos.
- Identificar los pasos para la recuperación.
- Examinar supuestos
- Examinar métodos de comunicación.
- Examinar elementos financieros claves
- Examinar información tecnológica clave
- Implementar el plan
- Mantener, revisar y ejecutar el plan

México vive su propio contexto político, social y de infraestructura, además de sus condiciones climáticas específicas. De ahí que deban considerarse, no solo inundaciones, terremotos o incendios, sino también escenarios de amenazas biológicas o pandemias, ataques

terroristas, cortes en servicios básicos como la energía eléctrica o fallas en los sistemas de comunicación, entre otros.

- **India**

Los acontecimientos del 11 de septiembre donde se realizaron ataques terroristas a sitios claves de EE.UU, generaron un gran impacto en el mundo corporativo. Los directores de TI, incluso los CEOs se toman muy en serio los planes para proteger sus bienes más preciados y la infraestructura de activos. Un año después de estos eventos el 79% de las empresas no contaban con un BCM documentado y probado (Gestión de la Continuidad de Negocio). De estas empresas el 64% tienen alta dependencia de TI (Magazine, 2002).

- **África**

En África la mayoría de las empresas dependen de sistemas de información complejos que pueden fallar, algunas de las empresas críticas son las de salud, seguridad y las de gestión de riesgos del entorno. África tiene grandes desafíos, para minimizar la pobreza y la corrupción. El continente sufrió en el año 2014, inundaciones en África Occidental y del Sur, ciclones en Madagascar y un terremoto en Malawi, los ataques cibernéticos son una amenaza a nivel mundial. Los impactos económicos que estos eventos conllevan, ponen a la orden del día la planificación en continuidad a los Gobiernos y el sector privado. El Foro Económico Mundial

sobre África 2013, discutió sobre las acciones que el sector público, privado y social puede tomar para construir sociedades que sean más resistentes a los riesgos.

En este contexto la gestión de la continuidad tiene un papel importante, en pro de aumentar la resiliencia organizacional, la protección de valor para el accionista mediante la prevención de pérdidas financieras y daños a la reputación.

KPMG[3] realizó una encuesta a altos ejecutivos de negocio en 18 países africanos acerca de su percepción del riesgo y su continuidad de negocio, donde se evidenció que estos ejecutivos centran su preocupación de continuidad en factores tales como interrupciones, corrupción y ataques cibernéticos que puedan afectar de manera grave los sistemas de información y las infraestructuras críticas. También les preocupa los incidentes de salud, seguridad, economía, interrupciones en la cadena de suministro, problemas sociales, desastres naturales, humanos, guerra y terrorismo.

Otro riesgo general es el Gobierno Corporativo y la Estrategia de Negocios, el rápido crecimiento económico de África, ha puesto en manifiesto la creciente necesidad de prestar más atención a la gestión de riesgos y en la última instancia de los negocios, la gestión de la continuidad, como disciplina corporativa.

[3] KPMG: es una red global de firmas de servicios profesionales que ofrece servicios de auditoria, fiscales, y de asesoramiento financiero y de negocio en 156 países. Fuente: http://www.kpmg.com/co/es/paginas/default.aspx

En África el 28% de las empresas de diversos sectores no cuentan con un Sistema de Gestión de la Continuidad; el 27% de la empresas cuentan con un sistema de gestión de la continuidad maduro con más de 5 años; el 22% de 1 año a 3 años; el 16% de 3 años a 5 y el 7% menos de 1 año. (Portugal, 2012).

- **Estados Unidos**

Estados Unidos cada vez más ha incrementado su temor a posibles violaciones de seguridad y a eventos de desastres naturales, tales como la súper tormenta de arena y el reciente tornado de Oklahoma que pesa en gran medida en los ejecutivos de TI, las empresas en todo el país han avanzado en la gestión de la continuidad de negocio, donde planean e implementan planes de recuperación basándose en la capacidad de red inalámbrica, servicios en la nube y aplicaciones móviles.

Los resultados del último estudio de Continuidad de Negocio anual de AT&T, sacó a la luz varias tendencias, respecto a cómo las empresas se preparan para posibles desastres y amenazas. Esta encuesta se ha venido realizando desde hace 12 años a ejecutivos de empresas con más de $25 millones de dólares anuales de ingresos, con el fin de medir el pulso nacional sobre la planificación de la continuidad del negocio. La encuesta que relacionamos en este documento

fue realizada en el año 2013 a 500 empresas, donde las principales conclusiones fueron (AT&T, 2013):

- Con el aumento de presupuesto a las áreas de TI, las empresas están utilizando cada vez más los servicios en la nube. El 76% de los encuestados están utilizando la nube o planean utilizarla en el corto tiempo.
- El 78% de las empresas indicaron que su plan de continuidad prevé evento de seguridad en redes.
- El 73% incluye en sus planes acciones preventivas y correctivas para la denegación del servicio (DDoS)
- EL 63% citan la inminente amenaza de violaciones de seguridad, como el más importante problema de seguridad en el año 2013.
- El 38% de las empresas han experimentado ataques de denegación de servicio en los últimos 24 meses y el 12% en los últimos 6 meses.
- El 13% de las empresas no cuentan con Sistema de Gestión de la Continuidad.

- **Uruguay**

Uruguay cuenta con el Centro Nacional de Respuesta a Incidentes de Seguridad Informática, llamado CERTuy. AGESIC lidera la estrategia e implementación de Gobierno en Línea en el país, como base de un estado eficiente y centrado en el ciudadano. Impulsa la Sociedad de la

Información y del Conocimiento promoviendo la inclusión, la apropiación y el buen uso de las tecnologías de la información.

El CERTuy está conformado por un grupo de expertos responsables del desarrollo de medidas preventivas y reactivas ante incidentes de seguridad y confianza en el uso de las TIC. Sus principales objetivos son: centralizar, coordinar y optimizar los procesos de respuesta a incidentes en seguridad de la información; difundir mejores prácticas en seguridad de la información.

4.2. PLANES DE LA GESTION DE LA CONTINUIDAD

4.2.1. Continuidad de Negocio

Capacidad de la Organización para continuar con la entrega de productos o servicios a los niveles predefinidos aceptables después de un evento perjudicial (INCONTEC ISO 22301:2012, 2012).

4.2.2. Gestión de la Continuidad de Negocio

Proceso de gestión integral que identifica las amenazas potenciales para la organización y los impactos que dichas amenazas podrían causar a las operaciones del negocio en caso de

materializarse, las cuales proporcionan un marco para la construcción de la resiliencia de la organización con la capacidad de una nueva respuesta efectiva que salvaguarde los intereses de sus partes interesadas clave, su reputación, marca y las actividades que crean valor (INCONTEC ISO 22301:2012, 2012).

4.2.3. Sistema de Gestión de Continuidad de Negocio (BCMS)

Parte del sistema general de gestión que establece, implementa, opera, monitorea, revisa, mantiene y mejora la Continuidad de Negocio (INCONTEC ISO 22301:2012, 2012).

4.2.4. Plan de Continuidad de Negocio

Procedimientos documentados que guían a las organizaciones para responder, recuperar, reanudar y restaurar a un nivel pre-definido de operación debido a la interrupción (INCONTEC ISO 22301:2012, 2012).

Según la norma ISO 22301:2012, propone que los planes de continuidad de negocio deben contener colectivamente:

a) Los roles y las responsabilidades definidos para las personas y los equipos que tienen autoridad durante y después de un incidente.

b) Un proceso para la activación de la respuesta.

c) Los detalles para gestionar las consecuencias inmediatas de un incidente perjudicial, teniendo en cuenta:

- El bienestar de los individuos
- Las opciones estratégicas, tácticas y operativas para la respuesta a la interrupción, y
- La prevención de la pérdida o no disponibilidad de las actividades prioritarias.

d) La información detallada sobre cómo y bajo qué circunstancias las organización se comunicará con los empleados y sus familiares, las partes interesadas claves y los contactos de emergencia.

e) Cómo la organización va a continuar o recuperar sus actividades prioritarias dentro de los plazos determinados.

4.2.5. Programa de Continuidad de Negocio

Proceso continuo de gestión y la gobernabilidad con el apoyo de la alta dirección y los recursos adecuados para implementar y mantener la gestión de la Continuidad de Negocio (INCONTEC ISO 22301:2012, 2012).

4.2.6. Plan de Recuperación de Desastres – DRP (Disaster Recovery Planning)

Mientras la planificación de continuidad de negocio, proporciona el plan estratégico orientado a los negocios a largo plazo para la operación continua después de un suceso. El plan de recuperación de desastres es más táctico en su enfoque. El DRP proporciona un plan a corto plazo para hacer frente a las interrupciones del área de Tecnología. La mitigación de una infección de malware[4] que muestra riesgo de propagación a otros sistemas, podría ser un ejemplo de interrupciones en Tecnología. El DRP se centra en la manera eficiente de intentar mitigar el impacto de un desastre y la respuesta inmediata a la recuperación de los sistemas críticos de Tecnología (Eric Conrad, 2010).

Un DRP implica la recuperación oportuna de recursos y servicios de tecnología de la información, una vez ocurre un incidente que obliga a suspender las actividades normales de la

[4] Malware, malicious o código malicioso. Se trata de cualquier software, mensaje o documento con capacidad de producir daños en los sistemas informáticos y en las redes. En este grupo de programas peligrosos, se encuentran las bombas lógicas, los gusanos, los virus y los troyanos, entre otros. Álvaro Gómez – Vieites (2006). *Enciclopedia de la Seguridad Informática*, 144. Madrid.

empresa. El DRP incluye planes para instalaciones de trabajo, la comunicación de información crítica a empleados, contingencias para el servicio de internet y así garantizar la operatividad de los servicios que se encuentran en línea, contingencia de estaciones de trabajo, servidores y respaldo de información y recuperación.

La diferencia principal entre el DRP y el BCP, consiste en que el DRP es asociado a la recuperación de los Sistemas de Tecnologías de la Información, mientras que el BCP tiene un contexto de negocio más amplio. En un DRP se define el sistema de Back-up o respaldo de información, mientras que en el BCP se define cuál es la información vital para la empresa, como datos, información financiera y operativa, aplicaciones, sistemas operativos y documentación entre otros.

4.2.7. COOP Plan de Continuidad de Operaciones.

Continuity of Operation Plan (COOP). Este plan describe los procedimientos requeridos para mantener las operaciones durante un desastre o incidente. El plan debe incluir traslado de personal a un sitio alterno y control y gestión de la operación en este sitio.

4.2.8. BRP Plan de Recuperación de Negocio

Business Resumption/Recovery Plan (BRP). Este plan describe las actividades para reestablecer las operaciones normales del negocio.

4.2.9. Plan de Soporte de Continuidad

Este plan se enfoca en las actividades de soporte específico de los Sistemas de Información y Tecnología y aplicaciones. Este es el plan de contingencia de IT.

4.3. GESTION PÚBLICA COLOMBIANA

4.3.1. Estructura y Organización de la Administración Pública

La ley 489 de 1998 en su capítulo X – artículo 38 define que la Rama Ejecutiva del Poder Público en el orden nacional, está integrada por los siguientes organismos y entidades:

- Del sector central: La presidencia de la república, la Vicepresidencia de la República, los consejos superiores de la administración, ministerios y departamentos administrativos, las superintendencias y unidades administrativas especiales sin personería jurídica.

- Del sector descentralizado: los establecimientos públicos, las empresas industriales y comerciales del estado, las superintendencias y las unidades administrativas especiales con personería jurídica, las empresas sociales del estado, las empresas oficiales de servicios públicos domiciliarios, los institutos científicos y tecnológicos, sociedades públicas y sociedades de economía mixta, las demás entidades administrativas nacionales con personería jurídica que cree, organice o autorice la ley para que formen parte de la Rama Ejecutiva del Poder Público.

En el orden nacional, los ministros y directores del departamento administrativo orientan y coordinan el cumplimiento de las funciones a cargo de las superintendencias, las entidades descentralizadas y las sociedades de economía mixta que les estén adscritas o vinculadas o integren el sector administrativo correspondiente.

4.3.2. Políticas de Desarrollo Administrativo

El Decreto 2482 de 2012 en su artículo 3, define las Políticas de Desarrollo Administrativo, los cuales son:

a) Gestión Misional y de Gobierno: orientada al logro de metas establecidas, para el cumplimiento de su misión y de las prioridades que el gobierno defina. Incluye entre otros, para las entidades de la Rama Ejecutiva del orden nacional, los indicadores y metas del gobierno que se registran en el sistema de seguimiento de metas de gobierno, administrado por el departamento nacional de planeación.

b) Transparencia, participación y servicio al ciudadano. Orientada a acercar al estado al ciudadano y hacer visible la gestión pública. Permite la participación activa de la ciudadanía en la toma de decisiones y su acceso a la información, a los trámites y servicios, para una atención oportuna y efectiva. Incluye otros, el plan anticorrupción y atención al ciudadano y los requerimientos asociados a la participación ciudadana, rendición de cuentas y servicio al ciudadano.

c) Gestión del Talento Humano. Orientada al desarrollo y cualificación de los servidores públicos buscando la observancia del principio de mérito para la provisión de los empleos, el desarrollo de competencias, vocación del servicio, la aplicación de estímulos y una gerencia pública enfocada a la consecución de resultados.

d) Eficiencia administrativa. Orientada a identificar, racionalizar, simplificar y automatizar trámites, procesos, procedimientos y servicios, así como optimizar el uso de recursos, con el propósito de contar con organizaciones modernas, innovadoras, flexibles y abiertas al entorno, con capacidad de transformarse, adaptarse y responder en forma ágil y oportuna a las demandas y necesidades de la comunidad para el logro de los objetivos del estado. Incluye entre otros, los temas relacionados con gestión de calidad, eficiencia administrativa y cero papeles, racionalización de trámites, modernización institucional, gestión de tecnologías de información y gestión documental.

e) Gestión financiera. Orientada a programar, controlar y registrar las operaciones financieras, de acuerdo con los recursos disponibles de la entidad. Integra actividades relacionadas con la adquisición de bienes y servicios, la gestión de proyectos de inversión y la programación y ejecución del presupuesto.

4.3.3. Organización de la Administración Municipal

La estructura organizacional del estado se divide en las entidades de carácter central y las descentralizadas. En las entidades de naturaleza central están integradas por la al alcaldía, que a su vez está compuesta por el despacho del alcalde, las secretarias de despacho y las unidades administrativa.

En cuanto a las entidades de carácter descentralizado, pueden ser establecimientos públicos, empresas industriales y comerciales del estado, sociedades de economía mixta, empresas sociales del estado, sociedades de economía mixta, empresas de servicios públicos de naturaleza oficial y algunas entidades indirectas como sociedades y asociaciones entre entidades públicas y de carácter mixta.

4.3.4. Nomenclatura, Clasificación y Requisitos para el Ejercicio de Empleos Municipales

El Decreto de Ley 1569 de 1998 "*por el cual se establece el sistema de nomenclatura y clasificación de los empleos de las entidades territoriales que deben regularse por las disposiciones de la Ley 443 de 1998 y se dictan otras disposiciones",* en el cual se establecieron los siguientes niveles y se fijaron los requisitos mínimos requeridos (Robles, 2004):

a) Nivel directivo: comprende los empleos a los cuales corresponden funciones de dirección general, de formulación de políticas constitucionales y de adopción de planes, programas y proyectos.

b) Nivel asesor: agrupa los empleos cuyas funciones consisten en asistir, aconsejar y asesorar directamente a los empleados públicos del nivel directivo.

c) Nivel ejecutivo: comprende los empleados cuyas funciones consisten en la dirección, coordinación, supervisión y control de las unidades o áreas internas encargadas de ejecutar y desarrollar las políticas, planes, programas y proyectos de las entidades.

d) Nivel profesional: agrupa aquellos empleos a los cuales corresponde funciones cuya naturaleza demanda la aplicación de conocimientos propios de cualquier carrera profesional reconocida por la Ley.

e) Nivel técnico: en este nivel están comprendidos los empleos cuyas funciones exigen el desarrollo de procesos y la aplicación de tecnologías.

f) Nivel administrativo: comprende los empleados cuyas funciones implican el ejercicio de actividades de orden administrativo, complementarias de las tareas propias de los niveles superiores.

g) Nivel operativo: comprende los empleos cuyas funciones implican el ejercicio de labores que se caracterizan por el predominio de actividades manuales o tareas de simple ejecución.

4.4. MARCO LEGAL

4.4.1. LEY 872 DE 2003 (Sistema de Gestión de Calidad)

La Ley 872 de 2003, es reglamentada por el Decreto Nacional 4110 de 2004, por la cual se crea el sistema de gestión de la calidad en la Rama Ejecutiva del Poder Público y en otras entidades prestadoras de servicios (Colombia, 2003).

Mediante esta Ley, se decreta la creación del sistema de gestión de la calidad de las entidades del estado, como herramienta de gestión sistemática y transparente que permita dirigir y evaluar el desempeño institucional, en términos de calidad y satisfacción social en la prestación de los servicios a cargo de las entidades y agentes obligados, la cual estará enmarcada en los planes estratégicos y de desarrollo de tales entidades. El sistema de gestión de la calidad adoptará en

cada entidad un enfoque basado en los procesos que surten al interior de ella y en las expectativas de los usuarios, destinatarios y beneficiarios de sus funciones asignadas por el ordenamiento jurídico vigente.

Esta norma es de vital importancia para el desarrollo del plan de continuidad, ya que en su artículo 4 *Requisitos para su Implementación* en el literal c) *la entidad debe identificar y priorizar aquellos procesos estratégicos y críticos de la entidad que resulten determinantes de la calidad en la función que les ha sido asignada, su secuencia e interacción, con base en criterios técnicos previamente definidos por el sistema explícitamente en cada entidad*.

También en el literal e) *obliga a identificar y diseñar, con la participación de los servidores públicos que intervienen en cada uno de los procesos y actividades, los puntos de control sobre los riesgos de mayor probabilidad de ocurrencia o que generen un impacto considerable en la satisfacción de las necesidades y expectativas de calidad de los usuarios o destinatarios, en las materias y funciones que le competen a cada entidad.*

4.4.2. LEY 87 DE 1993 (Control Interno en las Entidades)

La Ley 87 de 1993, establece normas para el ejercicio de control interno en las entidades y organismos del estado. Se entiende por control interno el sistema integrado por el esquema de

organización y el conjunto de los planes, métodos, principios, normas, procedimientos y mecanismos de verificación y evaluación adoptados por una entidad, con el fin de procurar que todas las actividades, operaciones y actuaciones, así como la administración de la información y los recursos, se realicen de acuerdo con las normas constitucionales y legales vigentes dentro de las políticas trazadas por la dirección y en atención a las metas u objetivos previstos (COLOMBIA C. D., 1993).

La Gestión de la Continuidad del Negocio da cumplimiento al Artículo 2 *Objetivos del Sistema de Control Interno*, específicamente en sus literales, a) proteger los recursos de la organización buscando su adecuada administración ante posibles riesgos que los afecten; e) asegurar la oportunidad y confiabilidad de la información de sus registros; f) definir y aplicar medidas para prevenir los riesgos, detectar y corregir las desviaciones que se presenten en la organización y que pueden afectar el logro de sus objetivos.

Esta Ley, soporta el proceso de Gobierno de la Continuidad de Negocio, ya que el auditor interno y el comité de coordinación del Sistema de Control Interno, deben participar activamente en la planeación, toma de decisiones, desarrollo e implementación del sistema.

4.4.3. Ley 594 de 2000 (gestión documental)

La Ley 594 de 2000, por medio de la cual se dicta la Ley General de Archivos, cuyo objeto es el de establecer las reglas y principios generales que regulan la función archivística del estado (COLOMBIA C. D., LEY 594 DE 2000, 2000).

El plan de continuidad debe dar cumplimiento a la Ley 594 de 2000, en su artículo 4, literales a) fines de los archivos. El objetivo esencial de los archivos es el de disponer de la documentación organizada, en tl forma que la información institucional sea recuperable para uso de la administración en el servicio al ciudadano y como fuente de la historia; por lo mismo, los archivos harán suyos los fines esenciales del estado, en particular los de servir a la comunidad y garantizar la efectividad de los principios, derechos y deberes consagrados e la constitución y los de facilitar la participación en comunidad y el control ciudadano en las decisiones que los afecten, en los términos previstos por la Ley. También el literal b) Responsabilidad. Los servidores públicos son responsables de la organización, conservación, uso y manejo de los documentos.

4.4.4. LEY 489 DE 1998 (Responsabilidad y Autoridad)

Por la cual se dictan normas sobre la organización y funcionamiento de las entidades del orden nacional, se expiden las disposiciones, principios y reglas generales. El objeto de esta Ley es la de regular el ejercicio de la función administrativa, determina la estructura y define los principios y reglas básicas de la organización y funcionamiento de la Administración Pública (COLOMBIA C. D., LEY 489 DE 1998, 1998).

La Gestión de la Continuidad del Negocio, basa sus lineamientos en la Ley 489 de 1998 en su capítulo IX *Sistema General de Información Administrativa del Sector Público. Artículos 36. Sistema General de Información Administrativa*. Créase el Sistema General de Información Administrativa del Sector Público, integrado, entre otros, por los subsistemas de organización institucional, de edición de recursos humanos, materiales y físicos, y el desarrollo administrativo. Artículo 37. Los sistemas de información de los organismos y entidades de administración pública servirán de soporte al cumplimiento de su misión, objetivos y funciones, darán cuenta del desempeño institucional y facilitarán la evaluación de la gestión pública a su interior como, a la ciudadanía en general.

En esta Ley también se establece la estructura y organización de la administración pública, en su capítulo X. Se define la clasificación de los organismos y entidades por:

- **Sector Central**: (La Presidencia de la República, la Vicepresidencia de la República, los consejos superiores de la administración, los ministerios y departamentos administrativos; las superintendencias y unidades administrativas especiales sin personería jurídica).

- **Sector Descentralizado por servicios**: (los establecimientos públicos, las empresas industriales y comerciales del estado, las superintendencias y las unidades administrativas especiales con personería jurídica, las empresas sociales del estado y las empresas oficiales de servicios públicos domiciliarios, los institutos científicos y tecnológicos, las sociedades públicas y las sociedades de economía mista, la demás entidades administrativas nacionales con personería jurídica que cree, organice o autorice la ley para que formen parte de la Rama Ejecutiva del Poder Público).

4.4.5. DECRETO 2170 DE 2002 (Adquisición de Bienes)

Decreto por el cual se reglamenta la Ley 80 de 1993, para la adquisición de bienes y contratación de terceros por parte de las entidades del estado. Aunque en esta reglamentación no se obliga a los proveedores contar con un plan de continuidad de negocio, si se reglamenta en el pliego de condiciones o términos de referencia evaluación de riesgos. Artículo 8. *De los estudios previos*. Numeral 5. El análisis de los riesgos de la contratación y en consecuencia el nivel y extensión de los riesgos que deben ser amparados por el contratista (OFICIAL, 2002).

Al establecer en la evaluación de riesgos la necesidad de la continuidad de los procesos contratados, se establecen acuerdos de servicio que lo garanticen y el proveedor está obligado a cumplirlos.

Según el capítulo III *De la selección objetiva en la contratación directa*. Artículo 10. *Contenido mínimo de los pliego de condiciones o términos de referencia.* Los pliegos de condiciones o términos de referencia que sirven de base para el desarrollo de los procesos de selección de contratación directa, deberán incluir como mínimo la siguiente información:

- (1) Objeto del contrato
- (2) características técnicas de los bienes, obras o servicios requeridos por la entidad.
- (3) presupuesto oficial
- (4) factores de escogencia de la oferta y la ponderación matemática precisa, concreta y detallada de los mismos.
- (5) criterios de desempate
- (6) requisitos o documentos necesarios para la comparación de las ofertas, referidos a la futura contratación.
- (7) fecha y hora límite de presentación de las ofertas
- (8) término para la evaluación de las ofertas y adjudicación del contrato.
- (9) plazo y forma de pago del contrato.

4.4.6. Circular 041 de 2007 SARO (Administración del Riesgo Operativo)

Es un sistema de gestión que la Superintendencia Financiera de Colombia reglamenta para las entidades sometidas a su inspección y vigilancia, donde mediante la circular 041, obliga a las entidades a establecer, implementar y mantener un Sistema de Administración de Riesgo Operativo (SARO), acorde con su estructura, tamaña, objeto social y actividades de apoyo, estas últimas realizadas directamente o a través de terceros, que les permita identificar, medir, controlar y monitorear eficazmente este riesgo.

La norma define Riesgo Operativo (RO), como la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o, por la ocurrencia de acontecimientos externos, incluyendo aquellas situaciones relacionadas con asuntos legales y reputaciones.

El sistema debe comprende un conjunto de elementos tales como políticas, procedimientos, documentación, estructura organizacional, registro de eventos de riesgo operativo, órganos de control, plataforma tecnológica, divulgación de información y capacitación, mediante los cuales las entidades vigiladas identifican, miden, controlan y monitorean el riesgo operativo.

La circular en su numeral 3.1.3.1 *Administración de la continuidad del negocio.* De acuerdo con su estructura, tamaño, objeto social y actividades de apoyo, las entidades deben definir,

implementar, probar y mantener un proceso para administrar la continuidad del negocio que incluya elementos como: prevención y atención de emergencias, administración de la crisis, planes de contingencia y capacidad de retorno a la operación normal.

Los planes de continuidad del negocio deben cumplir, como mínimo, con los siguientes requisitos:

a) Haber superado las pruebas necesarias para confirmar su eficacia y eficiencia.

b) Ser conocidos por todos los interesados

c) Cubrir por lo menos los siguientes aspectos: identificación de riesgos que puedan afectar la operación, actividades a realizar cuando se presentan fallas, alternativas de operación y regreso a la actividad normal.

4.4.7. Circular 042 de 2012 (Requerimientos de Seguridad y Calidad)

Las instrucciones de que trata el capítulo décimo de la circular 042, deben ser adoptadas por las entidades sometidas a la inspección y vigilancia de la Superintendencia Financiera de Colombia. En el numeral 3.2.3. se debe exigir que los terceros contratados dispongan de planes de contingencia y continuidad debidamente documentados. Las entidades deberán verificar que los planes, en lo que corresponde a los servicios convenidos, funcionen en las condiciones pactadas.

4.4.8. Decreto 1151 de 2008 (Estrategia de Gobierno en Línea)

En este decreto se definen los principios de la estrategia de Gobierno en Línea, los cuales son: gobierno centrado en el ciudadano, visión unificada del estado, acceso equitativo y multicanal, protección de la información del individuo y credibilidad y confianza en el Gobierno en Línea. En este decreto se definen las fases o componentes del Gobierno en Línea, fase de información en línea, fase de interacción en línea, fase de transacción en línea, fase de transformación en línea y la fase de democracia en línea.

4.4.9. Decreto 2482 de 2012 (Integración de la Planeación y la Gestión)

En este Decreto, entre otros objetivos está el de implementar la herramienta en línea de reporte de avances de la gestión, como insumo de monitoreo, evaluación y control de los resultados institucionales y sectoriales, el "Formulario Único Reporte de Avances de la Gestión. El Ministerio de las Tecnologías de la Información y las Comunicaciones, es el encargado de desarrollar esta herramienta en línea.

4.4.10. Ley 1523 (Gestión del Riesgo de Desastres)

El objetivo general del Sistema Nacional es llevar a cabo el proceso social de la gestión del riesgos con el propósito de ofrecer protección a la población en el territorio colombiano, mejorar la seguridad, el bienestar y la calidad de vida y contribuir al desarrollo sostenible (COLOMBIA C. D., Ley 1523, 2012).

En esta Ley se persiguen entre otros los siguientes objetivos específicos:

- Desarrollar, mantener y garantizar el proceso de conocimiento del riesgo mediante acciones como:

a) Identificación de escenarios de riesgo y su priorización para estudio con mayor detalle y generación de los recursos necesarios para su intervención.

b) Identificación de los factores de riesgo, entiéndase: amenaza, exposición, con fines de información pública, percepción y toma de conciencia.

c) Análisis y evaluación de riesgo incluyendo la estimación y dimensionamiento de sus posibles consecuencias.

d) Monitoreo y seguimiento del riesgo y sus componentes.

e) Comunicación del riesgo a las entidades públicas y privadas y a la población, con fines de información pública, percepción y toma de conciencia.

- Desarrollar y mantener el proceso de reducción de riesgo, mediante acciones como:

  a) Intervención prospectiva mediante acciones de prevención que eviten la generación de nuevas condiciones de riesgo.

  b) Intervención correctiva mediante acciones de mitigación de las condiciones de riesgo existente.

  c) Protección financiera mediante instrumentos de retención y transferencia del riesgo.

- Desarrollar, mantener y garantizar el proceso de manejo de desastres mediante acciones como:

  a) Preparación a la respuesta frente a desastres mediante organización, sistemas de alerta, capacitación, equipamiento, entrenamiento, entre otros.

  b) Preparación para la recuperación, llámese: rehabilitación y reconstrucción.

  c) Respuesta frente a desastres con acciones dirigidas a atender la población afectada y restituir los servicios esenciales afectados.

  d) Recuperación, llámese: rehabilitación y reconstrucción de las condiciones socioeconómicas, ambientales y físicas, bajo criterios de seguridad y desarrollo sostenible, evitando reproducir situaciones de riesgo y generando mejores condiciones de vida.

Esta Ley establece un principio sistémico que garantizará la continuidad de los procesos, *la interacción y el enlazamiento de las actividades mediante bases de acción común y coordinación de competencias*. Además de asignar la obligación a Gobernadores, como *jefes de la administración seccional respectiva, tienen el deber de poner en marcha y mantener la continuidad de los procesos de gestión de riesgo de desastres en su territorio*. Además, asigna obligatoriedad a todos *los proveedores de redes y servicios de comunicaciones a permitir el acceso y uso de sus redes e infraestructuras al operador que lo solicite de manera inmediata, con el fin de atender las necesidades relacionadas con los motivos de declaratoria de situación de desastre, para garantizar la continuidad en la provisión de los servicios y redes de telecomunicaciones*.

4.5. METODOLOGIAS Y ESTÁNDARES PARA ELABORAR UN BCP

4.5.1. BS 25999

El BS-25999 es un estándar británico que establece las mejores prácticas, recomendaciones y actividades específicas para lograr la continuidad de negocio teniendo en cuenta a los riesgos que enfrenta una organización. Esta metodología fue creada por la organización DRI (Disaster Recovery Institute Internacional) (Yolima, 2012).

Este estándar se basa en el Plan de Continuidad de Negocio o BCM por sus siglas en inglés (Business Continuity Planning) el cual, al ser implementado en una organización, se le debe

hacer un seguimiento con el fin de conocer su evolución permanente en los procesos de la empresa. El BS-25999 posee dos partes esenciales: Desarrollo del BCM e implementación del mismo. El Desarrollo del BCM básicamente se centra en recopilar información necesaria para entender el negocio.

Para la implementación del BCM en una organización se deben tener en cuenta varios estados o fases necesarias para el funcionamiento eficaz y ágil de las actividades en una empresa. Estas fases son:

a) Inicio y gestión del proyecto

b) Evaluación y control del riesgo

c) Análisis de impacto de negocio (BIA)

d) Desarrollo de las estrategias para la continuidad del negocio

e) Respuesta ante emergencias

f) Desarrollo e implementación del BCM

g) Programa de concientización y capacitación

h) Mantenimiento y ejercicio del BCM

i) Comunicación de crisis

j) Coordinación con autoridades públicas

La realización del BCM en la organización traerá grandes ventajas como por ejemplo:

- Administrar la continuidad del negocio
- Resistencia del negocio ante las interrupciones
- Protege y asegura la imagen de la empresa
- Abre nuevas oportunidades de mercado y ayuda a ganar nuevos negocios
- Aumenta la disponibilidad del negocio.

A continuación hacemos una breve descripción de las diez fases propuestas por la norma para el desarrollo e implementación de un Plan de Continuidad de Negocio (BCM):

a) Inicio y Gestión del Proyecto

El objetivo de esta primera fase, es establecer la necesidad de desarrollar el BCM en la empresa, de tal manera que se comunique la importancia de realizar este plan, involucrando a los directivos y el personal de la empresa. Para esto, es importante:

- Definir un comité responsable del plan
- Asignar responsabilidades por cada equipo de trabajo
- Indicar las actividades de cada una de las fases del proyecto

- Documentar los procesos
- Presentar los avances
- Obtener la aprobación por parte de los directivos.

b) Evaluación y Control de Riesgos

En este numeral la norma propone realizar la evaluación de riesgos, con el fin de identificar las amenazas internas y externas, incluyendo concentraciones de riesgos, que pueden causar la interrupción o pérdida de las actividades críticas de la organización, así como la probabilidad o frecuencia de que ocurra una amenaza. En esta fase se identifican los riesgos, se realiza un proceso de análisis y evaluación y se gestionan o se definen controles para mitigarlos.

c) Análisis del Impacto de Negocio (BIA)

El Análisis de Impacto del Negocio (BIA – Business Impact Analysis) consiste en técnicas y metodologías que permiten identificar, cuantificar y cualificar los impactos de negocio y sus efectos en la organización en cao de pérdida o interrupción de la actividades de misión crítica. Sin embargo, la clave para realizar un Análisis de Impacto del Negocio es analizar el negocio como un todo más no como componentes, procesos o funciones individuales.

El análisis BIA tiene en cuenta el RTO (Recovery Time Objetive) y RPO (Recovery Point Objetive) que deben ser establecidos por la organización. Están definidos como:

- **RTO (Recovery Time Objetive)**: El tiempo entre el punto de interrupción, y el punto en el cual los sistemas sensibles en el tiempo deben estar funcionando nuevamente, con los datos actualizados.
- **RPO (Recovery Point Objetive)**: el punto en el cual fueron interrumpidas las actividades del sistema debió a la ocurrencia de un determinado evento.

En el Análisis de Impacto del Negocio, se identifican las actividades de misión crítica de la empresa, sus dependencias y sus puntos de falla, así como el análisis del impacto y el efecto que generaría en caso de una interrupción.

Los componentes clave de un BIA son:

- Cuestionarios de autovaloración
- Listas de comprobación
- Matriz de Análisis de Impacto del Negocio.

Las salidas del BIA son:

- Objetivos y salidas (servicios y productos)
- Actividades de misión crítica, dependencias y puntos de falla
- Impactos y efectos (consecuencias) financieros y no financieros como resultado de una interrupción o pérdida de una o más actividades de misión crítica, durante varios periodos de tiempo.
- Priorización mínima y aceptable de la recuperación de recursos.

d) Desarrollo de Estrategias para la Continuidad de Negocio

El propósito del desarrollo de las estrategias consiste en identificar las alternativas de recuperación de las operaciones en los marcos de tiempo definidos.

- Identificar los requerimientos de la continuidad de la organización
- Evaluar la compatibilidad de las estrategias contra los resultados del BIA
- Presentar el análisis costo /beneficio de las estrategias de continuidad.
- Seleccionar el sitio alterno y de almacenamiento externo.
- Entender los términos contractuales de los servicios de continuidad del negocio.

e) Desarrollo e Implementación del BCM

Esta fase involucra el diseño, desarrollo e implementación de planes de continuidad del negocio para evitar interrupciones de acuerdo a los marcos establecidos por los RTO, RPO. Las actividades que define la norma son:

- Identificar requerimientos para el desarrollo de los planes
- Definir requerimientos de control y administración de la continuidad
- Identificar y definir un formato y la estructura principal de los componentes de los planes
- Desarrollar la documentación de los equipos de recuperación de tecnología de la información
- Desarrollar el sistema de comunicaciones
- Desarrollar los planes de los usuarios finales de aplicaciones
- Implementar los planes
- Establecer procedimientos de control y distribución de planes.

f) Programa de Concientización y Entrenamiento del BCM

Es necesario que la organización prepare a sus empleados ante la presencia de un cambio, logrando minimizar esa resistencia y obteniendo mejor disposición ante situaciones de este tipo creando una cultura de aceptación ante un evento que perturbe su labor.

g) Mantenimiento y Ejercicio del BCM

Es necesario realizar pruebas para determinar la eficacia de los planes de continuidad definidos, así mismo evaluar el equipo y personal a cargo de cada actividad crítica.

h) Comunicación de Crisis

En esta etapa se desarrollan, coordinan, evaluar y ejercitan planes para comunicarlos a directivos, personal, usuarios, proveedores y medios de comunicación, de tal forma que el entorno de la organización se entere de su estado y en caso de crisis poder reaccionar de forma adecuada para minimizar los costos de interrupción de los procesos internos.

i) Coordinación con Autoridades Públicas

En esta etapa se requiere que la organización tenga una clara definición y documentación de las políticas a implementar como un documento obligatorio en la organización.

4.5.2. Modelo de Seguridad de la Información GEL 2.0

El Modelo de Seguridad de la Información GEL 2.0, presenta una estrategia de preparación por parte del gobierno para soportar el Sistema de Administración de Seguridad de la Información de Gobierno en Línea (SASIGEL), como modelo sostenible, y cubre desde la preparación de la entidad para comenzar la implementación del modelo, la definición de brechas, la alineación y la implementación del SGSI como modelo sostenible.

El modelo está compuesto por lineamientos, políticas, normas, procesos en 16 anexos de apoyo. Basado en el ciclo PHVA, etapas alineadas con el estándar NTC: ISO/IEC 27001:2005 y complementado armónicamente con otras iniciativas y estándares nacionales e internacionales, tales como MECI-Modelo Estándar de Control Interno; COBIT, ITIL, entre otros.

El modelo está dirigido a entidades públicas de orden nacional, entidades públicas de orden territorial, proveedores de servicios de Gobierno en línea y terceros que deseen adoptar el modelo. Está dividido en etapas de implementación en la preparación, análisis de la situación actual, alineación del SGSI, control y seguimiento (MINTIC, Modelo de Seguridad de la Información, 2012).

El modelo de operación del Modelo de Seguridad y Privacidad de la Información, contempla en su implementación un ciclo de cinco (05) fases, las cuales permiten que las entidades puedan gestionar la seguridad y privacidad de la información, con el fin de fortalecer la protección de los

datos y dar cumplimiento a lo establecido en la Estrategia de Gobierno en Línea, cubriendo de una manera integral cada uno de sus componentes.

En el modelo de Seguridad y Privacidad la guía No. 8 corresponde a la gestión de Continuidad de Negocio. En este documento se encuentran conceptos y principios para la preparación de las tecnologías de la información y comunicaciones (TIC), para la continuidad de negocio.

4.5.3. Continuidad de las Operaciones, Gobierno y Desarrollo

El Sistema Económico Latinoamericano y del Caribe (SELA) en el marco del II Seminario Regional Alianzas entre el Sector Público y Privado para la Gestión de Riesgo de Desastres, define tres niveles conceptuales de la continuidad: de Operaciones, de Gobierno y del Desarrollo:

- Continuidad de Operaciones (COOP): Se entiende como el proceso de planeación que nos permite garantizar que el trabajo de las instituciones públicas y de la sociedad no sea interrumpido ante la ocurrencia de una crisis. Es el esfuerzo que cada institución efectúa para garantizar la operación de sus funciones básicas ante la irrupción de una crisis.

- Continuidad del Gobierno (COGO): Se refiere al proceso de planeación que le permite garantizar continuar con su responsabilidad y función de estado de acuerdo a lo establecido en la constitución.
- Continuidad del Desarrollo (CODE): Se refiere al proceso de generación de un ordenamiento jurídico que establezca los principios básicos para garantizar la concurrencia de los sectores.

4.5.4. NISP SP-800-34

El Instituto Nacional de Estándares y Tecnología (NIST), generó una publicación especial 800-34 "Guía de Planificación de Contingencia para Sistemas de Tecnología de Información". Esta guía proporciona instrucciones, recomendaciones y consideraciones para la contingencia del sistema de información federal. Permite realizar la planificación, donde se definen medidas para recuperar los servicios del sistema de información después de una interrupción. Las medidas provisionales pueden incluir reubicación de los sistemas de información y las operaciones a un sitio alterno, la recuperación de las funciones de los sistemas de información que utilizan equipos suplentes o rendimiento de las funciones que utilizan métodos manuales. Esta guía está dirigida a los planes de contingencia específicamente para tres tipos de plataformas y proporciona estrategias y técnicas comunes para todos los sistemas:

- Cliente / Servidor
- De Telecomunicaciones

- Sistemas integrados

La guía presenta siete capítulos de implementación (US, 2010):

a) Desarrollar la declaración de la política de la planificación de la contingencia.

b) Lleva a cabo el análisis de impacto del negocio (BIA). El BIA ayuda a identificar y dar prioridad a la información, sistemas y componentes críticos, los cuales apoyan los procesos de misión crítica.

c) Identificar los controles preventivos.

d) Crear estrategias de contingencia

e) Desarrollar un plan de contingencia del sistema de información

f) Realizar pruebas a plan

g) Garantizar el mantenimiento del plan.

4.5.5. ISO / IEC 27031:2011

Este estándar describe los conceptos y principios de la Tecnología de Información y Comunicación (TIC), la preparación para la continuidad de negocio y proporciona un marco de métodos y procesos para identificar y especificar todos los aspectos, tales como criterios de

rendimiento, el diseño y puesta en marcha, para mejorar la preparación de las TIC de una organización para garantizar la continuidad del negocio. Se aplica a cualquier tipo de organización (privado, gubernamental, no gubernamental e independientemente de su tamaño (ORG, 2011).

4.5.6. COBIT 5.0

La Asociación para la Auditoria y Control de Sistemas de Información, ISACA (Information System Audit and Control Association) y su IT Governance Intitute, ITGI, desarrollaron los Objetivos de Control para la Información y Tecnologías relacionadas, COBIT (Control Objetives for Information and related Technology). COBIT es el único marco de negocio para el gobierno y la gestión de Tecnología de la empresa, proporciona principios globalmente aceptados, prácticas, herramientas analíticas y modelos para ayudar a aumentar la confianza en el valor de los sistemas de información. COBIT 5 se construye y se expande en COBIT 4.1 mediante la integración de otros grandes marcos, normas y recursos, incluyendo riesgos de TI, tecnología de la información Biblioteca de Infraestructura de TI de ITIL y las normas relacionadas de la Organización Internacional de Normalización (ISO) (Association, 2014).

4.5.7. ISO 22301

La primera entidad de estandarización en el Reino Unido y en el Mundo, British Standards Institution (BSI), cuenta con una reconocida reputación de independencia en la realización de

estándares e información de productos que promueven las mejores prácticas. Entre estos productos se encuentra la BS ISO 22301:2012, es la norma internacional para la gestión de la continuidad del negocio, y se basa en éxito de la norma Británica BS 25999 y otras normas regionales. Está diseñada para proteger la entidad de una interrupción potencial, incluyendo las condiciones meteorológicas extremas, incendios, inundaciones, desastres naturales, robos, corte de Información y Tecnología, enfermedad general del personal o ataque terrorista. El sistema de gestión ISO 22301 permite identificar amenazas relevantes de la entidad y las funciones críticas del negocio que podría tener un impacto.

La continuidad del negocio contribuye al desarrollo de una sociedad más resiliente. Organizaciones sin un BCMS eficaz en la gestión y prevención de vulnerabilidades a las que son expuestas, podría llegar a generar impactos negativos en sus empleados, usuarios, clientes y proveedores. El estándar se puede utilizar para evaluar la capacidad de una organización para satisfacer sus propias necesidades y obligaciones de continuidad. Proporciona un marco para la implementación de mecanismos efectivos de continuidad de negocio (INTITUTION, 2014).

Esta norma aplica el modelo "Planear-Hacer-Verificar-Actuar" (PHVA) para planear, establecer, implementar, operar, monitorear, mantener y mejorar continuamente la eficacia de un sistema de gestión de Continuidad de Negocio en la organización.

La norma específica requisitos para planificar, establecer, implementar, operar, supervisar, revisar, mantener y mejorar continuamente un sistema de gestión documentado para protegerse,

reducir la probabilidad de ocurrencia, prepararse, responder y recuperarse de los incidentes perjudiciales que puedan surgir.

La norma está compuesta por los siguientes numerales a nivel general:

1. Alcance
2. Referencia normativas
3. Términos y definiciones
4. Contexto de la organización
5. Liderazgo
6. Planificación
7. Recursos
8. Operación
9. Evaluación de desempeño
10. Mejora

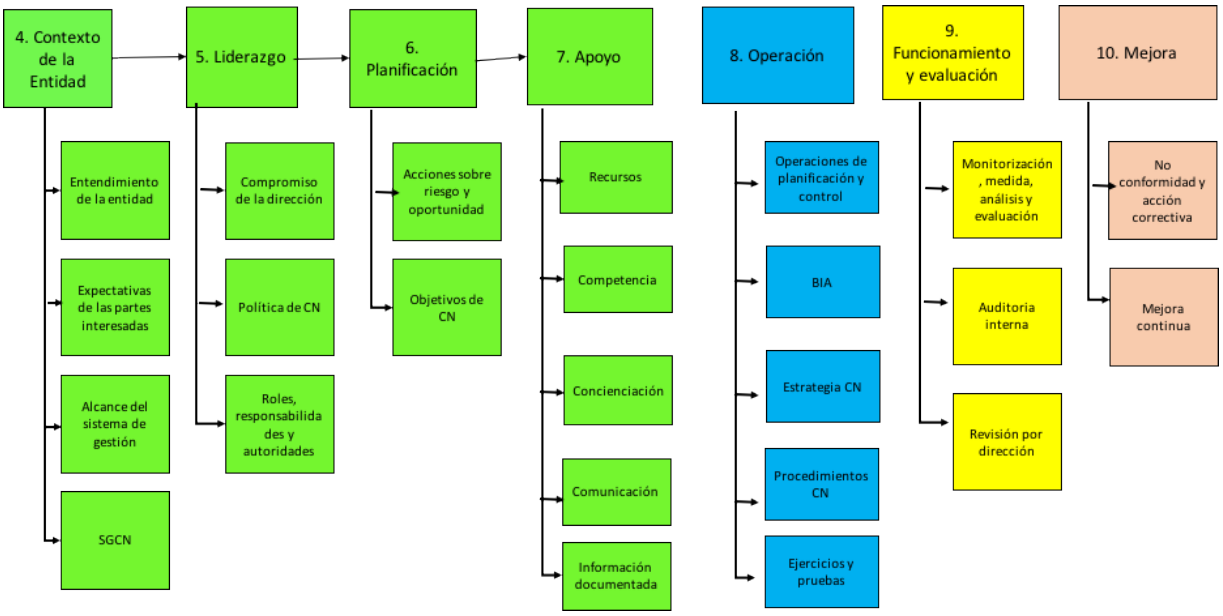

Ilustración 1.Estructura de Alto Nivel ISO 22301

4.5.8. ISO 10000:2009

La ISO 10000:2009, es la Norma Técnica de Calidad en la Gestión Pública (NTCGP 10000:2009). En cumplimiento de lo establecido en el artículo 6 de la Ley 872 de 2013, esta norma establece los requisitos para la implementación de un sistema de gestión de calidad aplicable a la rama ejecutiva del poder público y otras entidades prestadoras de servicios (ISO, 2009).

Esta norma está dirigida a todas las entidades, y tiene como propósito mejorar su desempeño y su capacidad de proporcionar productos y/o servicios que respondan a las necesidades y expectativas de sus clientes.

La orientación de esta norma promueve la adopción de un enfoque basado en procesos, el cual consiste en identificar y gestionar, de manera eficaz, numerosas actividades relacionadas entre sí. Una ventaja de este enfoque es el control continuo que proporciona sobre los vínculos entre los procesos individuales que hacen parte de un sistema conformado por procesos, así como sobre su combinación e interacción.

La norma define proceso como el conjunto de actividades mutuamente relacionadas o que interactúan para generar valor y las cuales transforman elementos de entrada en resultados.

Cada entidad define los tipos de procesos con los que cuenta, típicamente pueden existir, según sea aplicable, los siguientes:

Tabla 2 Clasificación de los procesos

CLASIFICACION DEL PROCESO	**DEFINICION**	**PROCESOS**
Procesos Estratégicos	Incluyen procesos relativos al establecimiento de	Comunicación pública Planeación

CLASIFICACION DEL PROCESO	DEFINICION	PROCESOS
	políticas y estrategias, fijación de objetivos, provisión de comunicación, aseguramiento de la disponibilidad de recursos necesarios y revisiones por la dirección.	Direccionamiento
Procesos Misionales o de realización del producto o la prestación del servicio	incluyen todos los procesos que proporcionan el resultado previsto por la entidad en el cumplimiento de su objeto social o razón de ser	Gestión en educación. Gestión de la seguridad social en salud Gestión pública territorial Gestión ambiental Gestión de minas y energía Gestión de la infraestructura pública Gestión turística Gestión empresarial

CLASIFICACION DEL PROCESO	DEFINICION	PROCESOS
		Gestión de participación y democracia. Gestión cultural y desarrollo humano. Gestión del desarrollo agropecuario.
Procesos de Apoyo	Incluyen todos aquellos procesos para la provisión de los recursos que son necesarios en los procesos estratégicos, misionales y de medición, análisis y mejora.	Gestión del talento humano. Gestión financiera y fiscal. Administración documental Gestión de TIC´s Servicios administrativos logísticos Gestión contractual Soporte jurídico
Procesos de Evaluación	Incluyen aquellos procesos necesarios para medir y recopilar datos destinados a realizar el análisis del	Medición y seguimiento Auditoria interna

CLASIFICACION DEL PROCESO	DEFINICION	PROCESOS
	desempeño y la mejora de la eficacia y la eficiencia.	Gestión de acciones correctivas y preventivas.

4.5.9. Estándar ISO/IEC 15504

En 1993 la ISO aprobó un programa de desarrollo de un modelo que fuera la base de un futuro estándar internacional para la evaluación de los procesos del ciclo de vida de software. Este trabajo inicialmente recibió el nombre de SPICE (Software Process Improvement and Capability Determination). La aparición oficial de la norma se hizo en el año 2003.

La ISO/IEC 15504 define los requisitos mínimos para realizar mejora a los procesos y para medir el nivel de madurez de la organización

La norma ISO /IEC 15504 describe las bases para llevar a cabo evaluaciones por niveles de madurez, para lo cual muestra un conjunto de niveles y procesos asociados, tomando como base la norma ISO 12207:1995 /Adm. 1:2002 y Adm. 2:2004, si bien actualmente está disponible la versión ISO 12207:2008 (REDALYC, 2009).

El modelo define las reglas de derivación para los niveles de madurez:

Tabla 3 Niveles de madurez

NIVEL DE MADUREZ	DESCRIPCION
Nivel de madurez 0	La organización no tiene una implementación efectiva de los procesos.
Nivel de madurez 1	Los procesos objeto de evaluación alcanzan el nivel de capacidad 1, es decir, existen productos resultantes para los mismos y el proceso se puede identificar.
Nivel de madurez 2	Los procesos de nivel de madurez 2, tienen nivel de capacidad 2 o superior.
Nivel de madurez 3	Los procesos de nivel de madurez 2 y 3 tienen nivel de capacidad 3 o superior
Nivel de madurez 4	Uno o más de los procesos tienen nivel de capacidad 4 o superior
Nivel de madurez 5	Uno o más procesos tienen nivel de capacidad 5.

Para que una entidad pueda alcanzar el nivel de madurez, se debe determinar el nivel de capacidad de los procesos correspondientes al nivel de madurez, y con el nivel de capacidad, se derivará un nivel de madurez, de acuerdo a unas reglas de derivación.

Para medir el nivel de capacidad de un proceso, se utiliza un conjunto de atributos de proceso (PAs), donde cada tributo define un aspecto particular de capacidad de proceso, tal y como se muestra en la siguiente tabla. En este sentido los atributos son comunes para todos los procesos y describen las características que deben estar presentes para institucionalizar un proceso:

Tabla 4 Niveles de capacidad y atributos del proceso

NIVEL DE CAPACIDAD	**ATRIBUTO DEL PROCESO (PA)**
Nivel 1: Proceso Realizado	PA 1.1 Realización del proceso
Nivel 2: Proceso Gestionado	PA 2.1 Gestión de la Realización PA 2.2 Gestión del producto de trabajo
Nivel 3: Proceso Establecido	PA 3.1 Definición del proceso PA 3.2 Despliegue del proceso
Nivel 4: Proceso Predecible	PA 4.1 Medición del proceso PA 4.2 Control del proceso
Nivel 5: Proceso en Optimización	PA 5.1 Innovación del proceso PA 5.2 Optimización continua

Asimismo, el cumplimiento de los atributos de proceso predeterminará el nivel de capacidad del proceso, y de ahí el nivel de madurez vendrá determinado por los niveles de capacidad de todos los procesos asociados al nivel de madurez.

También se definen unos criterios de calificación, de cada uno de los componentes de la evaluación. A continuación se definen los rangos establecidos:

- *No logrado* (N): El grado de alcance de los componentes asociados al atributo de proceso es del 0% al 15%.
- Parcialmente logrado (P): El grado de alcance de los componentes asociados al atributo de proceso es del 16% al 50%.
- Gran parte alcanzado (G): El grado de alcance de los componentes asociados al atributo de proceso es del 51% al 85%.
- Completamente alcanzado (C): El grado de alcance de los componentes asociados al atributo de proceso es del 86% al 100%.

La norma también describe los niveles de madurez de la organización, donde propone seis niveles de madurez a los cuales puede aspirar la organización según la calidad y el manejo de los procesos:

- ***Nivel de madurez 0: Organización inmadura***. En este nivel no se han implementado los procesos, por consiguiente no se alcanza el propósito de la organización, ni se identifican productos o salidas de proceso. Por consiguiente no hay atributos que evaluar en este nivel.

- ***Nivel de madurez 1****: Organización básica*. En este nivel la organización simplemente implementa y alcanza de manera básica los resultados del proceso y al alcanzar los resultados propuestos es posible identificar satisfactoriamente las salidas (resultados) del proceso evaluado.

- ***Nivel de madurez 2****:* Organización gestionada. La organización además de implementar los objetivos del proceso, demuestra una planificación, seguimiento y control tanto de los procesos, como de sus productos de trabajo asociados.

- ***Nivel de madurez 3****:* Organización establecida. En este nivel de madurez los procesos se estandarizan para toda la organización.

- ***Nivel de madurez 4****:* Organización predecible. La organización gestiona cuantitativamente los procesos, es decir, se miden y se analiza el tiempo de su realización.

- ***Nivel de madurez 5***. Organización optimizada. Se lleva a cabo una monitorización continua de los procesos y se analizan los datos obtenidos.

4.5.10. ISO/IEC 27035:2012 Gestión de Incidentes de Seguridad de la Información

La ISO/IEC 27035 es la Guía Técnica Colombiana, de Tecnologías de la Información. Técnicas de Seguridad. Gestión de Incidentes de Seguridad de la Información (INCONTEC, 2012).

Esta guía brinda un enfoque planificado y estructurado para:

a) Detectar, reportar y evaluar incidentes de seguridad de la información.

b) Responder a incidentes de seguridad de la información y hacer su gestión.

c) Detectar, evaluar y gestionar las vulnerabilidades de seguridad de la información, y

d) Mejorar continuamente la seguridad de la información y la gestión de incidentes como resultado de la gestión de incidentes y vulnerabilidades de seguridad de la información.

5. DISEÑO METODOLOGICO

5.1. TIPO DE INVESTIGACION

Según el Uso de Resultados. El método utilizado para esta investigación fue de tipo APLICADA, donde el objetivo era obtener un conocimiento técnico para la aplicación utilitaria. Se planteó para satisfacer necesidades de información que conducen a la aplicación inmediata en la solución de problemáticas apremiantes. Este tipo de investigación exige un "saber hacer" al que se llega mediante una última fase de la investigación que se conoce como "desarrollo tecnológico" (Medina Suárez).

5.2. METODOS Y TECNICAS DE INVESTIGACION

5.2.1. Fase Lógica

La primera fase del proceso de investigación, es donde el resultado de su ejecución se asocia con la identificación y planteamiento de la investigación. En esta fase determinamos la necesidad de conocimiento y el "para qué se quiere", para ser usado en la solución de una problemática concreta (investigación aplicada). Este conocimiento faltante constituye el "qué se quiere conocer", el cual corresponde al problema de investigación. Una vez definimos el problema, definimos las condiciones con las que llevamos a cabo la investigación y definimos un plan de acción, los medios y resultados esperados, integrándolos en los objetivos de investigación. Para este proyecto se ha realizado una investigación de corte documental, ya que

existe la solución al problema de investigación, porque con la información secundaria llegamos al conocimiento que buscábamos.

5.2.2. Fase Metodológica

En esta fase determinamos el "cómo se hará". El resultado de la fase es el diseño metodológico del proceso de investigación, definiendo la propuesta de investigación y el plan de investigación.

5.2.3. Fase Técnica

En esta fase se generaron los datos secundarios, se realizó el proceso de análisis para definir las normas que más aplican a la creación de la Guía de Continuidad de las Tecnologías de la Información para entidades públicas.

5.2.4. Fase de Contrastación

En esta fase se definieron las conclusiones de la investigación y oportunidades de mejora a futuro. La información aportada por la investigación es resumida en las conclusiones, se analiza

e interpreta en el contexto de la situación motivo de análisis, convirtiéndose en nuevo conocimiento, que suplirá la deficiencia del mismo identificada en el problema de investigación.

5.3. METODOLOGIA PARA LA ELABORACIÓN DE UN BCP

El Ministerio de la Información y las Comunicaciones MINTIC, cuenta desde el año 2010 con la Guía para la Preparación de las TIC para la Continuidad de Negocio (MINTIC, Guía para la Preparación de las TIC para la Continuidad del Negocio, 2010). Este documento fue la base para el desarrollo de este trabajo de investigación, donde se realizaron los cambios a las políticas generales de acuerdo a las necesidades corporativas y tecnológicas actuales de las entidades Colombianas.

La guía fue diseñada con base al Marco de Seguridad y Privacidad de la Información, el cual define un ciclo de funcionamiento del modelo de operación de continuidad del negocio, su funcionamiento dentro del modelo de operación seguridad y privacidad de la información y la descripción detallada de cada una de las fases. Las cinco (5) fases que comprenden el modelo de operación contienen objetivos, metas y herramientas que permiten que la continuidad del negocio sea un sistema de sostenible dentro de las entidades.

Ilustración 2 Modelo de Operación de Continuidad

Cada fase fue desarrollada con base a los lineamientos de COBIT 5.0 en su dominio DSS04 Entrega, Servicio y Soporte, proceso DS04 Gestión de la continuidad. Para esto se definió un marco de continuidad para la recuperación de procesos de tecnología en las entidades del estado, donde a cada fase se incluyeron actividades del proceso de Gestión de la continuidad de Cobit.

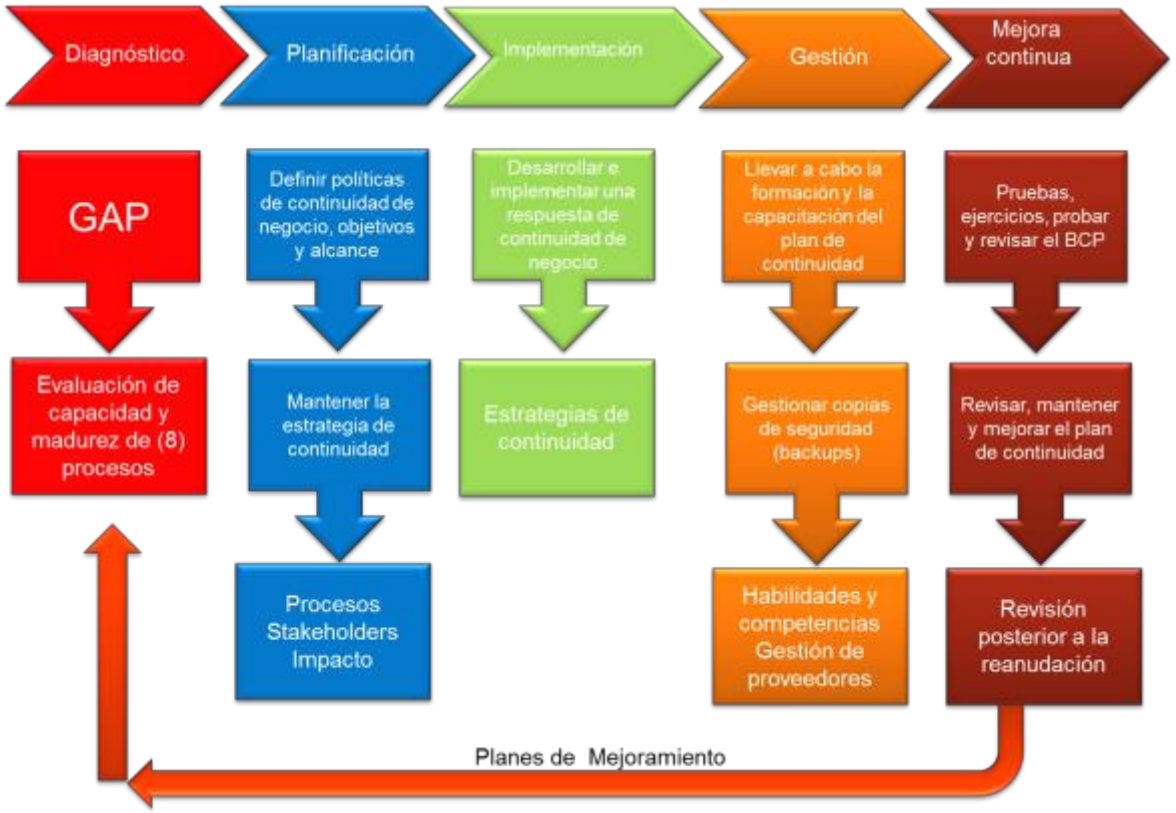

Ilustración 3 Marco de Seguridad y Privacidad de la Información

5.3.1. Diagnóstico GAP

Para desarrollar el GAP, se listaron los ocho subprocesos de COBIT 5.0 procesos DSS04 Gestión de la Continuidad de Negocio, cada uno con el listado de actividades mínimas para su cumplimiento y la opción para registrar si hay cumplimiento o no. Cada actividad tiene un peso dentro del subproceso total, lo cual al final de la resolución de la encuesta genera un valor numérico porcentual de cumplimiento del subproceso.

La medición de la capacidad de la entidad, respecto a la gestión de la continuidad, fue desarrollada apoyándonos en el enfoque de evaluación de capacidad de procesos basado en en el estándar ISO/IEC 15504. A cada subproceso se le genera una evaluación por rango y por niveles de capacidad.

- La evaluación por rango se define de la siguiente forma:

Tabla 5 Rangos de evaluación de capacidad.

ID	NOMBRE	RANGO
N	No alcanzado	0% al 15%
P	Parcialmente alcanzado	15% al 50%
L	Ampliamente alcanzado	50% - 85%
F	Completamente alcanzado	85% - 100%

- La evaluación por nivel de capacidad, está dada por el nivel de implementación del subproceso, en cuanto a cumplimiento del objetivo, alcance y resultados esperados.

Tabla 6 Niveles de capacidad

NIVEL	DESCRIPCION DEL NIVEL
0	Incompleto - El proceso no se ejecuta y no logra su propósito
1	Realizado - El proceso se lleva a cabo y alcanza su propósito
2	Gestionado - El proceso se gestiona y se establecen productos de trabajo controlados que se mantienen.
3	Establecido - Se utiliza un proceso definido basado en un estándar
4	Predecible - El proceso se realiza consistentemente dentro de límites definidos
5	Optimizado - El proceso está siendo mejorado para cumplir con los objetivos relevantes actuales del negocio, y los proyectos

Una vez definido el nivel de capacidad, el modelo define las reglas de derivación para los niveles de madurez, basados en el sistema de evaluación de la norma ISO/IEC 15504[5]:

[5] ISO/ IEC 15504: La ISO/IEC 15504 define los requisitos mínimos para realizar mejora a los procesos y para medir el nivel de madurez de la organización

Tabla 7 Niveles de Madurez

NIVEL DE MADUREZ	DESCRIPCION
Nivel de madurez 0	La organización no tiene una implementación efectiva de los procesos.
Nivel de madurez 1	Los procesos objeto de evaluación alcanzan el nivel de capacidad 1, es decir, existen productos resultantes para los mismos y el proceso se puede identificar.
Nivel de madurez 2	Los procesos de nivel de madurez 2, tienen nivel de capacidad 2 o superior.
Nivel de madurez 3	Los procesos de nivel de madurez 2 y 3 tienen nivel de capacidad 3 o superior
Nivel de madurez 4	Uno o más de los procesos tienen nivel de capacidad 4 o superior

Nivel de madurez 5	Uno o más procesos tienen nivel de capacidad 5.

Así mismo, el cumplimiento de los atributos del proceso predeterminará el nivel de capacidad, y de ahí el nivel de madurez vendrá determinado por los niveles de capacidad de todos los procesos asociados.

También se definen unos criterios de calificación, de cada uno de los componentes de la evaluación. A continuación se definen los rangos establecidos:

- ***No logrado* (N)**: El grado de alcance de los componentes asociados al atributo de proceso es del 0% al 15%.
- **Parcialmente logrado (P)**: El grado de alcance de los componentes asociados al atributo de proceso es del 16% al 50%.
- **Gran parte alcanzado (G)**: El grado de alcance de los componentes asociados al atributo de proceso es del 51% al 85%.
- **Completamente alcanzado (C)**: El grado de alcance de los componentes asociados al atributo de proceso es del 86% al 100%.

La norma también describe los niveles de madurez de la organización, donde propone seis niveles de madurez a los cuales puede aspirar la organización según la calidad y el manejo de los procesos:

- ***Nivel de madurez 0:*** *Organización inmadura*. En este nivel no se han implementado los procesos, por consiguiente no se alcanza el propósito de la organización, ni se identifican productos o salidas de proceso. Por consiguiente no hay atributos que evaluar en este nivel.

- ***Nivel de madurez 1:*** *Organización básica*. En este nivel la organización simplemente implementa y alcanza de manera básica los resultados del proceso y al alcanzar los resultados propuestos es posible identificar satisfactoriamente las salidas (resultados) del proceso evaluado.

- ***Nivel de madurez 2****:* Organización gestionada. La organización además de implementar los objetivos del proceso, demuestra una planificación, seguimiento y control tanto de los procesos, como de sus productos de trabajo asociados.

- ***Nivel de madurez 3****:* Organización establecida. En este nivel de madurez los procesos se estandarizan para toda la organización.

- ***Nivel de madurez 4****:* Organización predecible. La organización gestiona cuantitativamente los procesos, es decir, se miden y se analiza el tiempo de su realización.

- ***Nivel de madurez 5***. Organización optimizada. Se lleva a cabo una monitorización continua de los procesos y se analizan los datos obtenidos.

5.3.2. Planificación del Plan de Continuidad de Negocio

En este proceso, se definen la estrategia metodológica para establecer el políticas, objetivos, procesos y procedimientos, pertinentes que le permitan a la Entidad, la preparación de las TIC para la continuidad del negocio. Se basó en el subproceso de Cobit 5.0 DSS04.01 *Definir las políticas de continuidad de negocio, objetivos y alcance.*

Las principales actividades son:

- Identificar los procesos de negocio internos y subcontratados y actividades de servicios que son críticos para las operaciones de la entidad o necesario para cumplir con las obligaciones legales y / o contractuales.

- Identificar las partes interesadas y los roles y responsabilidades clave para definir y acordar la política de continuidad y alcance.

- Definir y documentar los objetivos para la continuidad del negocio y la necesidad de integrar la planificación de la continuidad a la cultura empresarial.

- Identificar áreas y procesos apoyo a los procesos misionales de negocio y servicios de TI relacionados.

- Identificar posibles escenarios que puedan dar lugar a sucesos que podrían causar incidentes que afecten el normal funcionamiento de la entidad y por tanto la prestación de servicios al ciudadano.

- Realizar un análisis de impacto de negocio para evaluar el impacto en el tiempo de una interrupción de las funciones críticas o misionales de la entidad y el efecto que una interrupción podría tener en ellos.

- Establecer el tiempo mínimo necesario para recuperar un proceso de negocio y de soporte de TI basada en una longitud aceptable de interrupción de negocio y máximo de interrupción tolerable. Esto en términos económicos, legales y contractuales.

- Evaluar la probabilidad de amenazas que podrían causar la pérdida de la continuidad del negocio y determinar las medidas que reduzcan la probabilidad y el impacto a través de una mejor prevención y una mayor capacidad de recuperación.

- Identificar los requisitos de continuidad, Analizar para identificar las posibles opciones estratégicas empresariales y técnicas.

- Volver a Identificar posibles escenarios que puedan dar lugar a sucesos que podrían causar incidentes perturbadores significativos.

- Determinar las condiciones y los propietarios de las decisiones clave que hará que los planes de continuidad para ser invocados.

- Identificar las necesidades de recursos y los costos de cada opción técnica estratégica y hacer recomendaciones estratégicas.

- Obtener la aprobación del ejecutivo de negocios para las opciones estratégicas seleccionadas.

5.3.3. Implementación del Plan de Continuidad de Negocio

Este proceso se define las actividades para la implementación del componente de planificación, teniendo en cuenta los aspectos más relevantes en los procesos de implementación de la estrategia del Plan de Continuidad, las cuales deberán ser implementadas después de la aprobación de la alta dirección.

La alta dirección gestiona y proporciona los recursos necesarios, procedimientos y operación del Plan de Continuidad, así como los programas de entrenamiento y concientización. La implementación se gestiona como un proyecto a través del proceso de control de cambios formales de la Entidad y de los controles de gestión del proyecto de la Gestión de Continuidad del Negocio con el fin de asegurar visibilidad completa de la gestión y del reporte.

Se deben de tener en cuenta estándares internacionales pertinentes durante la implementación de la detección y respuesta de incidentes y de los componentes de recuperación de desastres, incluyendo los siguientes:

a) ISO/IEC 18043 Para la selección y operación de sistemas de detección de intrusos.

b) ISO/IEC 27035 Para el proceso de Gestión de Incidentes.

c) ISO/IEC 24762 Para los servicios de recuperación de desastres

Las actividades generales a desarrollar en este proceso son:

- Definir las acciones de respuesta a incidentes y las comunicaciones que deben adoptarse en caso de perturbación. Definir las funciones y responsabilidades relacionadas, incluyendo la rendición de cuentas de las políticas y su implementación.

- Desarrollar y mantener operativos los procedimientos que deben seguirse para permitir la operación continua de los procesos críticos de negocio y / o régimen de temporales, incluyendo enlaces a los planes de los proveedores de servicios externalizados.

- Asegurar que los proveedores clave tienen planes de continuidad de efectivos. Obtener evidencia auditada según sea necesario.

- Definir las condiciones y procedimientos de recuperación que permitan la reanudación del proceso de negocio, incluida la actualización y la recuperación de las bases de datos de información para preservar la integridad de la información.

- Definir y documentar los recursos necesarios para apoyar los procedimientos de continuidad y recuperación, teniendo en cuenta las personas, las instalaciones y la infraestructura de TI.

- Definir y documentar los requisitos para las copias de seguridad de información necesarias para apoyar los planes, incluyendo los planes y documentos en papel, así como archivos de datos, y considerar la necesidad de seguridad y almacenamiento externo.

- Determinar las habilidades necesarias para las personas involucradas en la ejecución del plan y los procedimientos.

- Distribuir los planes y la documentación de apoyo debidamente autorizada a las partes interesadas y asegurarse de que son accesibles en todos los escenarios de desastre.

5.3.4. Gestión de las TIC para la Continuidad de Negocio

Para el desarrollo de este proceso nos basamos en Cobit 5.0 en su subproceso DS04.06 *Llevar a cabo la formación y capacitación del plan de continuidad.*

En este proceso se determinan temas relacionados con la capacitación y sensibilización de todos los funcionarios de la entidad respecto a la continuidad del negocio, cuales son su roles y responsabilidades en caso de una emergencia.

En gestión también se definen cuáles son las habilidades y perfiles necesarios para restaurar las aplicaciones, sistemas y datos críticos de la organización en términos de conocimientos tecnológicos. Esto es en caso que sea necesario reemplazar en un momento dado a todos los miembros del equipo de TI, por ausencia o incapacidad.

Las principales actividades son:

- Definir y mantener los requisitos de formación y planes para los que realizan la planificación de continuidad, las evaluaciones de impacto, evaluaciones de riesgo, medios de comunicación y respuesta a incidentes. Asegúrese de que los planes de formación consideran la frecuencia y los mecanismos de entrega de capacitación y formación.

- Desarrollar Competencias basados en la Formación Práctica, Incluyendo la Participación en Ejercicios y Pruebas.
- habilidades y competencias del líder en función de los ejercicios y resultados de pruebas.

En este proceso también se ejecuta la actividad que tal vez es la más importante en la Gestión de la Continuidad de Negocio, que es la gestión de backups. Para esto nos basamos en el subproceso de Cobit DSS04.06 Gestionar Copias de Seguridad.

Las actividades generales son:

- Documentación procedimiento de backup. Tener en cuenta:

    - Frecuencia (diario, semanal, mensual)

- Modo de backup (ejemplo: duplicación de copias de seguridad en tiempo real)
- Tipo de Backup (incremental, total)
- Tipo de medios (cintas, DVD, Nube)
- Tipos de datos
- Creación de registros
- Datos informáticos críticos de los usuarios (ejemplo: hojas de cálculo).
- Ubicación física y lógica de la fuente de datos.
- Seguridad y derechos de acceso
- Cifrado

- Asegúrese de que los sistemas, las aplicaciones, los datos y la documentación que mantienen o son procesados por terceros están suficientemente apoyadas o aseguradas de otra manera. Considere la posibilidad de requerir devolución de las copias de seguridad de terceros. Considere la posibilidad de acuerdos de depósito en garantía o depósito.

- Definir los requisitos para el almacenamiento en sitio y en custodia externa, de los datos de copia de seguridad que cumplen con los requerimientos del negocio. Tenga en cuenta la accesibilidad necesaria para realizar copias de seguridad de datos.

- Formación y sensibilización. Establecer un control para asegurarse que el proceso se está llevando correctamente.
- Realizar pruebas periódicas de recuperación de backup.

5.3.5. Mejora Continua

Para definir el proceso de mejora continua, nos basamos en el numeral 10 de la norma ISO 22301:2012 y DSS04.4 *probar y revisar el BCP;* el DSS04.5 *Revisar, mantener y mejorar el plan de continuidad* y el DSS04.8 *Revisión posterior a la reanudación*.

La guía fundamenta la mejora continua en:

- Administración del cambio de la organización. Cambios importantes de los procesos, estrategia, cambio del sector, cambio de políticas externas e internas, nueva regulación, cambios importantes a la infraestructura de tecnología, entre otros.

- Capacitación del personal. Identificar oportunidades de mejora del plan mediante la participación activa los los funcionarios de la entidad.

- Resultados de las pruebas del plan de continuidad. Una vez ejecutadas las pruebas se definen los ítems o actividades que no se ejecutaron de acuerdo a lo planeado y los factores que contribuyeron al no cumplimiento, para definir oportunidades de mejora.

6. DESARROLLO DE LA GUIA DE PLANEACION E IMPLEMENTACIÓN

6.1. ANALISIS DE IMPACTO DE NEGOCIO BIA

La tarea fundamental del Análisis de Impacto de Negocio es la de comprender los proceso vitales del negocio y el impacto que genera la interrupción de los mismos por determinado tiempo. Según el Instituto Nacional de Estándares y Tecnología NIST de Estados Unidos, "el propósito del BIA es correlacionar componentes específicos del sistema con los servicios críticos que proporcionan, y en base a qué información procesan".

De esta forma el BIA se compone de dos partes fundamentales, la primera entender los procesos de negocio y la segunda correlacionarlas con los sistemas de TI.

La metodología que proponemos en esta guía, sigue los siguientes pasos generales:

Ilustración 4 Proceso de Análisis de Impacto BIA

El resultado de la realización de estos siete pasos es un análisis de impacto de negocio formal, el cual es utilizado en conjunto con el análisis y evaluación de riesgo para desarrollar estrategias de mitigación.

- Identificar procesos y funciones claves del negocio

Clasificación

Los procesos se clasifican en:

a) De Misión Crítica

b) Vitales

c) Importantes

d) Menores

a) De Misión Crítica

Corresponde al proceso que tiene mayor impacto en la operación de la entidad. Casi todos los que trabajan en la empresa tienen la comprensión innata de las operaciones de misión crítica dentro de su área o departamento, la clave es reunir toda esta información y desarrollar una visión integral de su misión crítica. La manera de recolectar esta información es por medio de (entrevistas, cuestionarios, talleres, lluvia de ideas, entre otros). Se debe preguntar a los funcionarios cuales serían las cinco primeras cosas que harían en caso de una interrupción, para recuperar la función.

b) Vitales

En las funciones vitales se pueden incluir la nómina, que en sí podría no ser crítica en términos de reestablecer el negocio de inmediato, pero puede ser de vital importancia a la capacidad de la empresa para funcionar más allá del desastre.

c) Importantes

Corresponde a las funciones que no detendrán el normal funcionamiento de la empresa en el corto plazo, pero por lo general tienen un impacto a largo plazo si se pierden. Desde el punto de vista de TI, estos sistemas pueden incluir, el correo electrónico, acceso a internet, bases de datos y otras herramientas del negocio que se utilizan en una función de apoyo, ya sea para apoyar funciones del negocio o de TI.

d) Menores

Los procesos de negocio menores son a menudo los desarrollados con el tiempo para resolver problemas recurrentes pequeños. Una vez se esté regresando a la normalidad, se debe decidir si se recuperan o simplemente se descartan.

- **Identificación de las Operaciones y Funciones Críticas**

Durante la fase inicial del Plan de Continuidad, la entidad debe hacer un listado de todas las operaciones y funciones y el área responsable de cada una.

Puede ser de utilidad pedirle a los empleados que hagan una lista de lo que hacen durante el día para poder identificar las tareas que realizan. Una descripción de cómo realizan estas tareas de manera completa, incluyendo apuntes de lo más básico y necesario.

- **Establecer Metas de Recuperación y Sus Tiempos**

¿Por cuánto tiempo puede mantenerse la interrupción? Y ¿cuánto tiempo tarda en recuperarse la operación normal o alterna de las funciones?. Se debe realizar un análisis de las actividades que se necesitan realizar para estimar el tiempo que se requerirá para restablecer las funciones básicas.

Las metas de recuperación deben identificar que tan rápido se puede restaurar una función u operación. Las consideraciones de las metas para la recuperación incluyen:

- El tiempo que se necesita para cambiar o restaurar las funciones.
- Método alternativo, si el restablecimiento requerido tardase más de lo esperado.
- Aspectos de la operación – función que pueden ser restablecidos en partes.

A continuación definimos los términos necesarios para definir los requerimientos de recuperación en términos de tiempo

- **MTD** (**Maximun Tolerable Downtime**) o Tiempo Máximo de Inactividad Tolerable. Espacio de tiempo durante el cual un proceso puede estar inoperante hasta que la empresa empiece a tener pérdidas y colapse.

- **RTO (Recovery Time Objective)** o Tiempo de Recuperación Objetivo. Es el tiempo transcurrido entre una interrupción y la recuperación del servicio. Indica el tiempo disponible para recuperar sistemas y recursos interrumpidos.

- **RPO (Recovery Point Objective)** o Punto de Recuperación Objetivo. Es el rango de tolerancia que la entidad puede tener sobre la pérdida de datos y el evento de desastre.

- **WRT (Work Recovery Time)**: Es el tiempo invertido en buscar datos perdidos y la realización de reparaciones. Se calcula como el tiempo entre la recuperación del sistema y la normalización de los procesos.

A continuación presentamos gráficamente la interacción entre el MTD, RTO, RPO y el WRT:

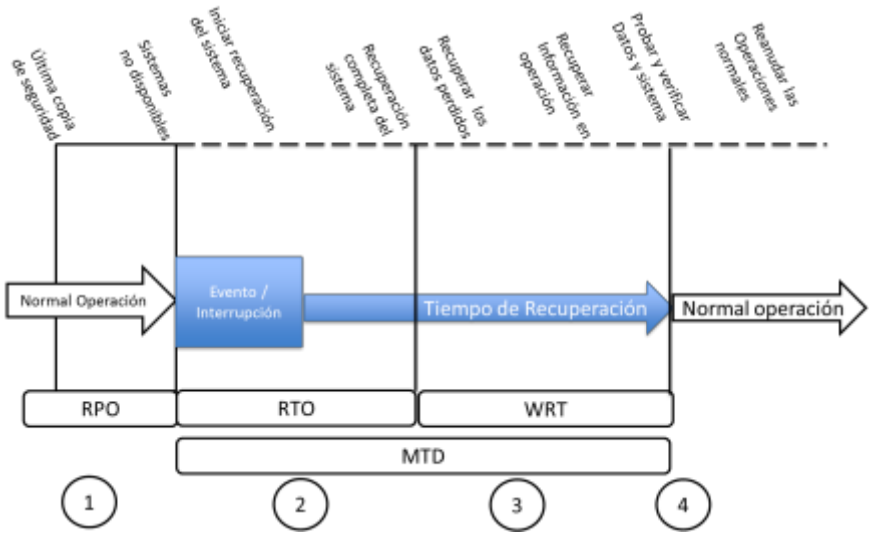

Ilustración 5 Tiempos de Continuidad

- Punto 1. Punto de Recuperación Objetivo (RPO). Corresponde a la pérdida de datos máximo sostenible, basado en los horarios de generación de backups y de acuerdo a las necesidades de información.
- Punto 2. Tiempo de Recuperación Objetivo (RTO). Tiempo máximo requerido para restaurar un sistema crítico.
- Punto 3. Tiempo de Trabajo de Restauración (WRT). Tiempo requerido para recuperar datos.
- Puntos 2 y 3. Tiempo Máximo Tolerable de Caída (MTD). Corresponde a la duración del RTO más el WRT.
- Punto 4. Pruebas y verificación de los datos y sistemas, generación del informe ejecutivo de vuelta a la normalidad.

A continuación se asigna una categoría y tiempos de acuerdo al tipo de procesos:

- Categoría 1. Misión Crítica 0 – 12 horas
- Categoría 2. Vitales 13 - 24 horas
- Categoría 3. Importante 1 – 3 días
- Categoría 4. Menores más de 3 días.

El equipo de continuidad puede determinar el tiempo de inactividad tolerable (MTD) máximos apropiados. Para algunas empresas una función de negocio podría tener un MTD de una semana, para otra puede ser de 0-2 horas. Existe una correlación inversa entre la cantidad de tiempo que puede tolerar un corte y el costo en inversión de sistemas que permitan recuperar en ese tiempo. Si la empresa no se puede permitir mucho tiempo de inactividad, tendrá que invertir en prevención y en sistemas que permitan recuperar la operación en corto tiempo.

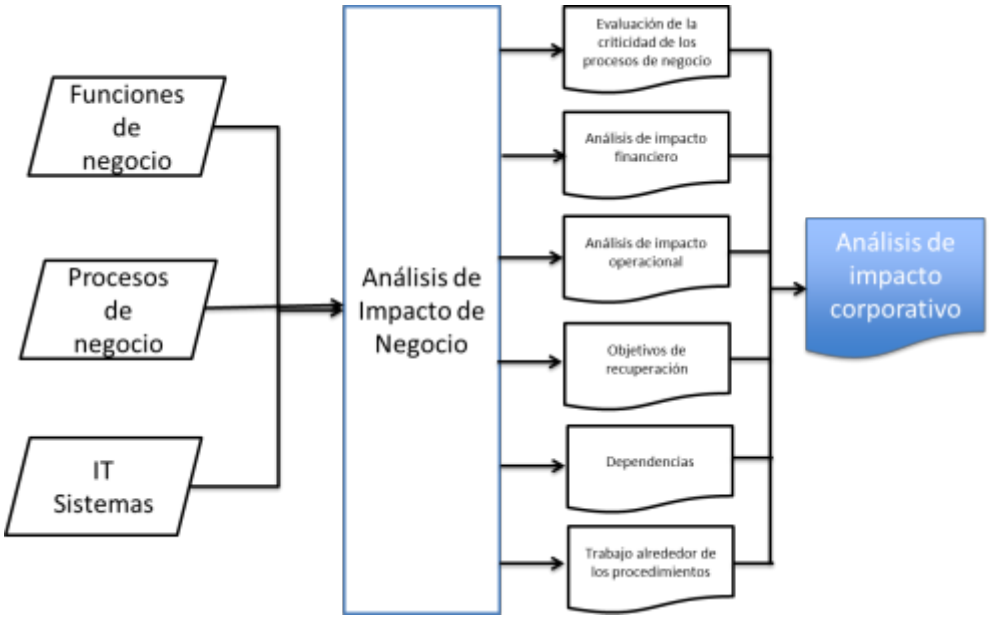

Ilustración 6 Entradas y salidas del Análisis de Impacto de Negocio BIA

Una vez listados y clasificados los procesos del negocio y analizados los tiempos de recuperación, es importante hacer grupos de trabajo y hacerse las siguientes preguntas entre otras:

- ¿Cómo se puede desarrollar la función de su área o departamento si el puesto de trabajo-escritorio, portátiles, equipos de cómputo, servidores, correo electrónico y acceso a internet no está disponible?
- ¿Existen puntos únicos de fallo?
- ¿Cuáles son los procesos críticos tercerizados?
- Si se produce una interrupción ¿cuáles serían los pasos a seguir para recuperar?
- ¿Cuál es el número mínimo de personal que se necesita y cuáles serían sus funciones principales?
- ¿Cuáles son las habilidades clave, conocimiento o experiencia necesarios para recuperarse?
- ¿Qué seguridad crítica y controles operativos son necesarios si los sistemas están abajo?
- ¿Cómo sería esta función en un sitio de recuperación de copia de seguridad?

Determinación del Impacto

El impacto por la interrupción de funciones críticas puede incluir:

- Impacto Financiero: corresponde a la pérdida de ingresos, costos más altos de operación, posibles responsabilidades financieras, sanciones, entre otros.
- Impacto respecto a clientes y proveedores: si una función crítica no funciona la empresa puede perder clientes o proveedores.

- Impacto por pérdida de empleados: La empresa puede perder empleados por muerte, lesiones, estrés o por decisión de cancelar el contrato a raíz de la interrupción o desastre.
- Impacto en la relaciones o credibilidad pública: las empresas que experimentan interrupciones del negocio, debido a los fallos en los sistemas de TI (datos perdidos o robados o modificados, la incapacidad de operar debido a datos faltantes o alterados), tienen un desafío en la no pérdida de la credibilidad y la no afectación de la marca.
- Legal: Corresponde a las reglamentaciones en materia de salud y seguridad en el trabajo, privacidad de los datos y seguridad de la información.
- Regulación y reglamentación: Se debe entender las normas y reglamentaciones vigentes aplicables a su negocio, incluso en tiempos de interrupción.
- Impacto Ambiental. Cuáles son las consecuencias directas sobre el medio ambiente en caso que una función deje de funcionar.
- Operacional: se deben clasificar las funciones y determinar su criticidad.
- Exposición a pérdidas: corresponde a la pérdida de ingresos, multas, flujo de caja, cuentas por cobrar y cuentas por pagar.

6.2. DESARROLLO DE ESTRATEGIAS DE CONTINUIDAD DE NEGOCIO

Proceso de Desarrollo de Estrategias de continuidad de Negocio

Ilustración 7 Proceso para la definición de estrategias

Esta fase se ocupa de identificar y evaluar las opciones para hacer frente a los riesgos identificados en la fase anterior. Estos enfoques se pueden dividir en dos clases: los riesgos que se tratan de forma proactiva, mediante la transferencia o minimizando y aquellos que reaccionan al presentarse un acontecimiento, a través de planes de recuperación de desastres. Para cada riesgo puede haber una o más soluciones para la mitigación.

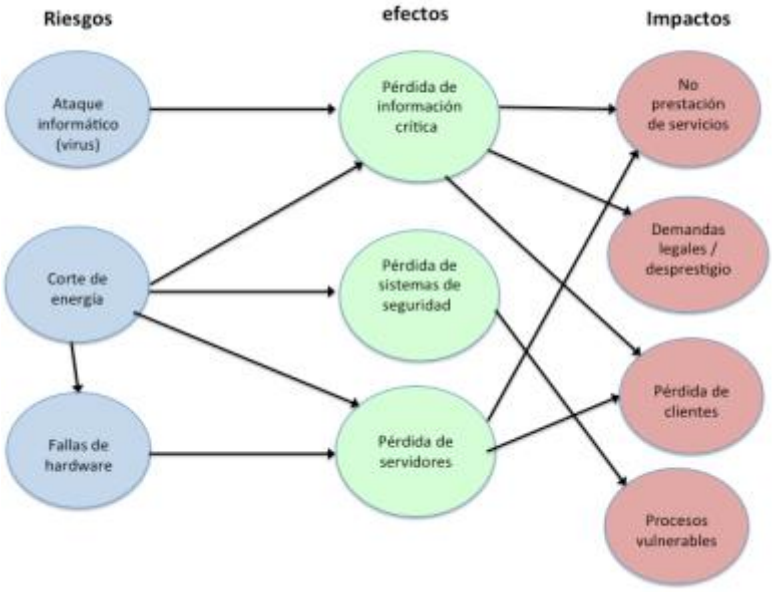

Ilustración 8 Relación Riesgos, Impacto y Efectos

- Estrategias de mitigación del riesgo

Ilustración 9 Estrategias de mitigación de riesgos

Estrategias de mitigación de riesgos. Fuente: Forbes Gibb, A Framework for Business Continuity Management, International Journal of Information Management 26 (2006) 128-141

- **Transferencia del Riesgo**

La transferencia del riesgo se logra generalmente a través de pólizas de seguros, que van desde el cubrimiento de extorsión, virus y hacking; también es importante asegurar a la empresa contra la pérdida de personal clave y la subcontratación, el outsourcing o tercero es la transferencia de responsabilidad a un tercero, para la prestación de servicios. Sin embargo; la externalización

introduce nuevos tipos de riesgo y estos deben ser evaluados como parte del costo total contratado.

- **Mitigación del Riesgo**

La mitigación del riesgo se puede lograr mediante la reducción, eliminación o evitándolo por completo. La redundancia de datos, normalmente se utiliza para eliminar los puntos únicos de fallo, mediante la configuración de componentes en alta disponibilidad o de contingencia, generalmente los componentes que utilizan esta estrategia son los de datos, aplicaciones, almacenamiento, servidores, comunicaciones y servicios públicos.

La redundancia de datos se realiza mediante copias de seguridad que se pueden almacenar de manera local o externa. Las aplicaciones pueden estar disponibles a partir de sistemas alternativos. Los medios de almacenamiento pueden ser replicados en forma de duplicación de discos o matrices redundantes, discos RAID en servidores para proporcionar tolerancia a fallos o la generación de copias de seguridad en cintas. La criticidad de los datos y las aplicaciones definen la complejidad de la estrategia y por tanto el presupuesto asignado. A nivel de hardware se incorporan componentes duplicados, tales como ventiladores, unidades de potencia, discos, memoria intercambiable de manera automática, entre otros. Otra estrategia puede ser la de configurar un servidor fuera del sitio para proporcionar contingencia en caso de evento catastrófico de poder en la ciudad, que involucre la destrucción del edificio. Para las comunicaciones también es importante definir estrategias de contingencia, tales como vías de transmisión alternativas en caso de congestión o falla del enlace, contratar el servicio con diferentes proveedores de telecomunicaciones.

La pérdida de datos también es causada por fallas en la energía eléctrica, tales como apagones, caídas de voltaje y sobretensiones, por esto se deben prever sistemas de protección para componentes clave, fuentes de alimentación UPS y si es posible generadores de respaldo para hacer frente a los cortes de energía prolongados.

- **Aceptación del Riesgo**

Puede ocurrir que es poco rentable o imposible de transferir, eliminar, reducir o evitar un riesgo. En estas circunstancias la empresa deberá aceptar el riesgo y asignar un rubro financiero para soportar la contingencia en caso de que el evento se materialice. Alternativamente puede ser posible combinar el riesgo con otras empresas, por ejemplo al realizar mutuos acuerdos para los servicios de centro alterno fuera de las instalaciones.

- **Diseño de Estrategias**

El objetivo del diseño de estrategias de continuidad de negocio, es evaluar y seleccionar estrategias de continuidad que más se adecuen a los procesos críticos del negocio. Las estrategias de continuidad se deben diseñar considerando los tiempos objetivos de recuperación definidos en el BIA.

  - Estrategias por Ausencia de Personal

Una vez se han identificado y analizado todos los procesos y funciones críticas de la entidad, se puede establecer y diferenciar el personal que es indispensable para realizar estas funciones y aquel que realiza labores de apoyo, también es necesario analizar el escenario de que se presente una disminución del personal que pasa con la ejecución de estas tareas críticas, con el fin de determinar el mínimo personal requerido, cuál debería ser su capacitación, quien la ejecutaría y por último en tiempos de contingencia, cuáles deberían ser los horarios, turnos y el plan de compensación.

Esta estrategia se activa cuando uno o varios colaboradores que ejecutan procesos críticos, no puede asistir a trabajar para desarrollar las actividades propias de su cargo. Se debe establecer un procedimiento que active la contingencia por "Ausencia de Personal", con el fin de distribuir las funciones a los colaboradores backup.

El objetivo de esta estrategia es el de mantener y respaldar el conocimiento y las capacidades del personal crítico.

A continuación realizamos algunas estrategias propuestas a nivel de personal:

Tabla 8 Estrategias de continuidad

ESTRATEGIA	TIPO	RESPONSABLE
Identificación de roles primarios y alternos		
Identificar personal primario necesario para la recuperación de los procesos críticos de la entidad. Adicional a esto, identificar los conocimientos	Estratégico	

mínimos que debe tener este rol, así como las habilidades y competencias técnicas.		Cada área de negocio
Identificar personal alterno para asegurar la continuidad de las operaciones de la entidad en caso de que el personal primario no esté disponible a causa del evento. Se sugiere identificar más de un alterno que cuente con las características necesarias para cumplir las funciones del personal primario. Se puede considerar realizar actividades desde la casa de los funcionarios, en caso de no contar con algún ambiente de trabajo.	Estratégico	Cada área de negocio
Identificar características similares entre el personal de la entidad, para definir posibles roles alternos en los procesos que demanden menor cantidad de personal.	Estratégico	Cada área de negocio
Designar un responsable del Plan de Recuperación de Desastres, quien en lo posible tenga dedicación exclusiva a esta labor. Este responsable se encargará de la gestión de la recuperación de los elementos tecnológicos requeridos por el negocio. Debe contar con conocimientos avanzados para el manejo de la continuidad del negocio.	Estratégico	Gerencia de Tecnología de Información

Capacitación del Personal		
Promover a través de un calendario de capacitación que cada gerencia gestione las capacitaciones sobre los Planes de Continuidad de Negocio, tanto a personal primario como alterno.	Estratégico	Cada área de negocio
Efectuar un programa de capacitación virtual para el personal en general que incluya la prevención de emergencias, reporte de incidentes, entre otros.	Estratégico	Recursos Humanos
Realizar talleres para el manejo de situaciones de crisis por parte del personal para asegurar una respuesta adecuada durante un desastre. Si es posible invitar a autoridades tales como bomberos, defensa civil o policía nacional	Estratégico	Recursos Humanos
Comunicación entre el Personal		
Asegurar que cada área defina un árbol de llamadas integrado a nivel de la entidad, para garantizar la comunicación efectiva entre el personal en caso de desastre.	Estratégico	Cada área de negocio

Incluir dentro de la política de vacaciones una cláusula que prevenga que personal primerio y alterno tenga vacaciones o capacitaciones en las mismas fechas.	Estratégico	Cada área de negocio
Identificar posibles canales de comunicación adecuados para la coordinación entre los integrantes del equipo de recuperación de sistemas involucrados, por ejemplo: • Utilizar celulares y/o radios • Evaluar el uso de mensajes de texto masivo. • Crear grupos de chat de comunicación o grupos de correo.		
Políticas		
Implementar mecanismo que permita disponer de dinero (efectivo, cheques, vales de consumo, crédito) para apoyar económicamente a los colaboradores afectados por un desastre.	Operativo	Recursos Humanos

Establecer indicadores de continuidad de negocio que midan el desempeño del personal al personal que participa en las actividades de recuperación.	Operativo	Riesgo Operacional
Brigadas de emergencia		
Mantener un listado de brigadista actualizado y organizado por funciones y sedes para evacuación, seguridad, incendio y primeros auxilios.	Operativo	Recursos Humanos

Tabla 8. Estrategias de continuidad

- Estrategia de Sitio Alterno por Desastre Total

La alternativa de traslado del personal se presenta cuando los funcionarios no puedan acceder a las instalaciones y de esta manera se afronta un evento de contingencia, que permita la continuidad de las operaciones de la entidad, desde un sitio alterno de operación.

El centro alterno permitirá que la entidad pueda operar en los tiempos estimados. Estos centros pueden ser:

a) Centro Frío: es una sala vacía preparada con las condiciones ambientales necesarias para albergar equipos informáticos. Este centro debe contar con instalaciones de potencia, climatización, falso piso y estructura de comunicaciones.

b) Centro Caliente: es una instalación con centro de base de datos, totalmente configurado a las especificaciones del cliente y disponible en pocas horas, se recomienda para las organizaciones, cuyo umbral de recuperación no de bebe superar las 24 o 48 horas.

c) Centro Espejo: Es utilizado en el caso de las necesidades de respuesta inmediata, consiste en dos instalaciones idénticas y actualizadas permanentemente con el objetivo de que una de ellas respalde la otra de manera automática. Esta opción aunque es la mejor, maneja altos niveles de costo y su implementación es compleja, se utiliza para procesos vitales y de alta disponibilidad.

d) Centro Móvil: es una sala acondicionada, equipada en un contenedor y configurable en pocas horas.

- 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 – 48 horas)
- ColdSide: Recuperación basada en copias de respaldo; el sitio alterno debe existir con por lo menos la conectividad necesaria (1 semana).

- Estrategia Por Ausencia de Tecnología

La contingencia se presenta cuando el hardware y/o software presenta fallas, o por interrupción prolongada de telecomunicaciones.

Para respaldar el recurso tecnológico se debe:

- Identificar de los componentes críticos
- Identificar de aplicaciones críticas
- Identificar las fuentes de información que deben respaldarse y definir un plan de respaldo.
- Realizar procedimientos periódicos de recuperación de información.
- Desarrollar procesos de respaldo de información crítica en custodia externa
- Evaluar y diseñar medidas de seguridad de la información en ejecución de respaldos y activación de contingencias.
- Realizar mejora continua a la infraestructura tecnológica para obtener respuesta rápida y eficiente a los planes de contingencia.
- Planificar la recuperación y reanudación de las operaciones afectadas en el menor tiempo posible.
- Suscribir contratos comerciales necesarios para la ejecución de los procedimientos de reanudación y recuperación.

- Adquirir pólizas de seguros

- Estrategia por Ausencia de Aplicaciones Críticas

Alterno al plan de tecnología, se puede evaluar la posibilidad de activar una contingencia manual, mediante formatos impresos que reemplacen las funciones de un aplicativo crítico. Para esta contingencia se debe definir la seguridad de la información capturada de manera física y el procedimiento de alimentación del aplicativo cuando se haya vuelto a la normalidad.

- Estrategia por Ausencia de Energía Eléctrica

Esta estrategia es activada cuando se detecta que no se va a tener suministro de energía eléctrica por un tiempo determinado, lo cual afectaría la utilización de los sistemas informáticos de la entidad.

En este escenarios generalmente se respaldan los componentes de tecnología y comunicaciones críticos con una planta eléctrica y una UPS de respaldo. La estrategia se define dependiendo del presupuesto asignado para este fin y por su puesto los procesos que se vayan a respaldar y su criticidad. También se tiene en cuenta las instalaciones físicas de la sede, si hay espacio para la ubicación y adecuación de una planta o simplemente se acuerda un contrato de contingencia con un proveedor, que desplazará en determinado tiempo una planta eléctrica. Si se decide alquilar la planta eléctrica, se deben acordar claramente acuerdos de servicio con el proveedor, definir cuál sería la ubicación de la planta en tiempos de contingencia, quien sería el encargado de

suministrar el combustible, como se conectaría a las centrales eléctricas principales del edificio, entre otros.

- Estrategia por Ausencia de Proveedores

Esta estrategia se activa cuando el proveedor de una función o componente de tecnología crítico, no pueda prestar el servicio, afectando las funciones críticas de la entidad. Las estrategias para abordar este escenario, es la de realizar contratos con proveedores con acuerdos de servicio en caso de contingencia, lo cual indica que estos proveedores críticos, deben contar con su propio plan de contingencia y de continuidad. Es el proveedor el que debe generar sus propias estrategias para garantizar el servicio a pesar de las circunstancias. Para verificar periódicamente este cumplimiento, la entidad debe realizar auditorías de seguimiento al proveedor.

Algunas estrategias propuestas a nivel de proveedores críticos (Perú, 2013):

ESTRATEGIA	TIPO	RESPONSABLE
Relación con autoridades y organismos públicos		
Tener un acercamiento con las autoridades	Operativo	
Identificar protocolos actuales que utiliza el estado para tomar control de los recursos y/o servicios necesarios para atender desastres	Operativo	
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.	Operativo	Administración
Identificar proveedores para la reconstrucción /reparación de las instalaciones y establecer contratos que contengan acuerdo de nivel de servicio requerido.	Operativo	Administración
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	Tecnología / Administración
Políticas		
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 auditoria de los esquemas de continuidad de negocios de los proveedores críticos.	Operativo	Aspecto Legal
Definir una política que permita realizar gastos adicionales para emergencia en una eventual situación de desastre.		
Evaluación de esquemas de continuidad		
Indagar cuales son los esquemas de contingencia manejados por los proveedores más críticos, y evaluar si estos pueden asegurar el servicio brindado. Adicionalmente, identificar los contactos claves y al menos dos opciones de comunicación con ellos. En caso que el	Operativo	Aspecto Legal

proveedor no cuenta con un Plan de Continuidad, se debe solicitar de manera expresa la implementación de planes de contingencia que puedan ser usadas en caso de desastre		
Establecer visitas periódicas a las instalaciones de los proveedores para poder censar /revisar los esquemas de continuidad ofrecidos por ellos.	Operativo	Aspecto Legal / Tecnología
Pruebas de Contratos y Acuerdos de Niveles de Servicio		
Definir un plan anual de pruebas de los servicios y/o aplicaciones relacionadas con los proveedores más críticos, definiendo pruebas y ejercicios que evalúen los diferentes escenarios.	Operativo	Áreas operativas / Tecnología

Tabla 9 Estrategias de Continuidad con Proveedores

- Estrategia por Ausencia de Canales de Comunicación

Esta estrategia se activa cuando se presenta falla o caída de un canal de internet donde operen funciones críticas del negocio. Generalmente las estrategias que se definen para este escenario, primero es la de acordar contractualmente con la empresa de Telecomunicaciones acuerdos de servicio y de disponibilidad del canal. Se sugiere contar con un canal alterno adquirido con otro proveedor de Telecomunicaciones.

Otras estrategias que se pueden definir, dependiendo de la criticidad de las funciones, es la de almacenar localmente la información y cuando se reactive el servicio enviar por lotes actualización de la misma, esto en caso de sistemas transaccionales.

j) Respuesta Ante Emergencias

El propósito de esta fase es desarrollar e implementar procedimientos para responder y estabilizar la situación después de un incidente y administrar el centro de operaciones de emergencia a ser utilizado como "centro de mando". Para esto, la norma propone las siguientes actividades:

- Identificar componentes de los procedimientos de respuesta a emergencia.
- Identificar los requerimientos de control y autoridad
- Procedimientos de control y autoridad
- Respuesta a emergencia y recuperación de heridos.
- Seguridad y recuperación.

7. CONCLUSIONES Y RECOMENDACIONES

7.1. CONCLUSIONES

- El proyecto permitió ajustar metodologías y estándares a la empresa Colombiana, para la implementación de un Plan de continuidad de las Operaciones y de los Sistemas de Información críticos; definiendo guías y paso a paso para definir estrategias, tiempos de respuesta y posibles planes de contingencia.

- La continuidad de una empresa pública o privada, depende de la planeación previa a través de metodologías probadas y estandarizadas, pero ajustadas a las necesidades puntuales y críticas de una empresa, las cuales varían de acuerdo al tipo de negocio, su visión, su tecnología y su talento humano.

- La implementación de cualquier estándar de seguridad o de continuidad de negocio, depende directamente de la cultura organizacional y del nivel de compromiso de la dirección; es necesario que sea visualizado como estrategia de la compañía, de tal forma que se unan esfuerzos de talento humano, tecnología y financiero en pro de la consecución del plan de continuidad.

- La gestión de la continuidad del negocio en una empresa fomenta la cultura del autoconocimiento constante, la gestión de detección, prevención y tratamiento de riesgos, el mejoramiento de procesos operativos; así como la optimización de las tecnologías y sistemas de información de la compañía. Todo orientado en el servicio al cliente y en el cumplimiento de acuerdos de servicio.

- La gestión de la continuidad de negocio le permite a la empresa estar preparada para continuar sus operaciones críticas en caso de desastres naturales, errores humanos a nivel interno que generen multas o sanciones de grandes cuantías, amenazas ambientales, tales como problemas de energía, apagones prolongados, fallas de componentes de red y otros, delincuentes informáticos y otros riesgos que detectados y gestionados a tiempo, pueden minimizar el su impacto en caso de materializarse.

- A la hora de gestionar un Plan de continuidad, se presentan varios obstáculos, tales como el día día de la operación, el compromiso de los responsables de actividades, la falta de capacitación y concientización de los miembros de la empresa acerca de la importancia de esta gestión y la asignación de presupuesto necesario para una implementación óptima y adecuada.

- La gestión de la continuidad de negocio, involucra un proceso sistemático que requiere la ejecución constante del diagnóstico, planificación, implementación, gestión y mejora continua, ya que las empresas son dinámicas y todo el tiempo se encuentran en cambios, bien sea por nuevos clientes, proyectos, productos o simplemente mejora en los procesos. Por esta razón el Sistema de Gestión de la Continuidad es un ente vivo dentro de la organización que cambia y mejora al igual que la empresa.

- Cada vez más las empresas cuentan con sistemas de información robustos y los servicios en línea a través de internet, que son el centro de operación de sus procesos Core de negocio, es por esto, que se convierte en vital y fundamental la Gestión de la Continuidad de Negocio de éstos, es la única vía para garantizar la continuidad del servicio y de la operación de los procesos en caso de la materialización de un riesgo, que pueda afectar e impactar de manera importante a la empresa.

- En los procesos de continuidad de negocio, la gestión que realiza las áreas de tecnologías de la información y las comunicaciones, en la implementación de estrategias de contingencia, son fundamentales para el éxito de la continuidad de negocio. Estas actividades deben ser realizadas de acuerdo a estándares y periódicamente probadas para establecer áreas de mejora y estar cien por ciento preparados cuando la empresa lo necesite.

7.2. RECOMENDACIONES

- Crear sinergia entre las empresas del estado para el soporte de contingencias, centro de datos alternos, de esta forma se optimizarían los recursos del estado y se minimizarían los costos de implementación del Sistema de Gestión de la Continuidad del Negocio.

- Realizar auditorías periódicas una vez culminadas las pruebas y ejercicios al plan de continuidad, con el fin de establecer mejoras y ajuste de acuerdo a los estándares y así establecer si los planes son efectivos y aseguran la continuidad de los procesos críticos de la entidad.

- Se recomienda incluir en la reglamentación de contratación de bienes y servicios (Decreto 2170 de 2002), ampliar los requerimientos respecto a planes de continuidad de negocio, para garantizar la prestación de servicios por parte de los proveedores.

- Para la administración del sistema y su mantenimiento, se recomienda sistematizar y automatizar el proceso, de tal forma que sea posible el seguimiento y control de las actividades; así como la identificación y análisis de indicadores. Este proceso va madurando a través del proceso de mejora.

8. LISTA DE REFERENCIAS

Association, I. -I. (2014). *www.isaca.org*. Obtenido de https://www.isaca.org/

AT&T. (Octubre de 2013). *Business Continuity Preparedness Handbook*. Obtenido de AT&T Website: http://www.att.com/Common/about_us/pdf/business_continuity_handbook.pdf

CELAC, F. d. (2013). Continuidad de Gobierno, de Negocios y de Operaciones. *Alianza del Sector Público y Privado para la Reducción del Riesgo de Desastres en América Latina y el Caribe*. Cartagena - Colombia.

COLOMBIA, B. M. (2012). *Análisis de la Gestión de Riesgo de Desastres en Colombia - Un aporte para la construcción de políticas públicas.* Obtenido de file:///C:/Users/felixuriza/Documents/PROYECTO%20DE%20GRADO/INVESTIGACION%20BCP/GESTIONDELRIESGOWEB.pdf

COLOMBIA, C. D. (24 de Abril de 2012). *LEY 1523 del 24 de abril de 2012*. Obtenido de http://www.ifrc.org/docs/idrl/1057ES.pdf

COLOMBIA, C. D. (29 de diciembre de 1998). *LEY 489 DE 1998*. Obtenido de Alcaldía Mayor de Bogotá: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=186

COLOMBIA, C. D. (14 de Julio de 2000). *LEY 594 DE 2000*. Obtenido de ARCHIVO GENERAL DE COLOMBIA: http://www.archivogeneral.gov.co/sites/all/themes/nevia/PDF/Transparencia/LEY_594_DE_2000.pdf

COLOMBIA, C. D. (1993). *LEY 87 DE 1993*. Obtenido de FENALPER - Federación Nacional de Personeros de Colombia: file:///Users/felixuriza/Downloads/ley_87_1993_normas_control_interno_entidades_del_estado%20(1).pdf

Colombia, C. d. (30 de Diciembre de 2003). *LEY 872 DE 2003*. Obtenido de ALCALDIA BOGOTA: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=11232

COMUNICACIONES, M. D. (2012). *MINTIC*. (Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea 2.0) Obtenido de http://programa.gobiernoenlinea.gov.co/lineamientos.shtml

Eric Conrad, S. M. (2010). *Business Continuity and Disaster Recovery Planning*. Obtenido de http://bibliotecavirtual.escuelaing.edu.co:2132/science/article/pii/B978159749563900007X

INCONTEC ISO 22301:2012, I. d. (2012). *ISO 22301:2012. CONTINUIDAD DE NEGOCIO. SISTEMAS DE GESTION DE CONTINUIDAD DE NEGOCIO*. NORMAS TECNICAS Y CERTIFICACION INCONTEC.

INCONTEC. (12 de 12 de 2012). *ISO/IEC 27035 Gestión de Incdientes de Seguridad*. Obtenido de tienda.incontec.org: http://tienda.icontec.org/brief/GTC-ISO-IEC27035.pdf

INTITUTION, B. T. (2014). *ISO 22301 Business Continuity Management*. (BSI) Obtenido de http://www.bsigroup.com/en-GB/iso-22301-business-continuity/

ISO. (2009). *NORMA TECNICA DE CALIDAD EN LA GESTION PUBLICA NTCGP 10000:2009*. Obtenido de http://201.234.74.120:8092/unisucre/hermesoft/portal/home_1/rec/arc_2134.pdf

Magazine, N. (2002). *Cover Story: Business Continuity Implementing a Business Continuity Plan*. Obtenido de http://www.networkmagazineindia.com/200208/cover1.shtml

Medina Suárez, M. N. *LA INVESTIGACION APLICADA A PROYECTOS* (Vol. 1). (E. A. Impresores, Ed.) Bogotá, Colombia.

México, S. d. (Junio de 2009). *Guía para la Elaboración e Implementación del Programa Interno de Protección Civil.* Obtenido de http://www.proteccioncivilbc.gob.mx/folletos/guiaPIPC.pdf

Ministerio de Ciencia, T. y. (2014). *Estado Actual de la Política Pública y Legislación sobre Ciberdelito en Costa Rica.* Obtenido de http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Cybercrime@Octopus/1April/Retos-respuestas-y-reformas-legislativas-Costa-Rica.pdf

MINTIC. (15 de 12 de 2010). *Guía para la Preparación de las TIC para la Continuidad del Negocio*. Obtenido de www.mintic.gov.co: http://www.mintic.gov.co/gestionti/615/articles-5482_Continuidad.pdf

MINTIC. (2011). *Manual para la Implementación de la Estrategia de Gobierno en Línea en las Entidades de Orden Nacional de la República.* Obtenido de Programa de Gobierno en Línea: http://programa.gobiernoenlinea.gov.co/apc-aa-files/eb0df10529195223c011ca6762bfe39e/manual-3.1.pdf

MINTIC. (2012). *Modelo de Seguridad de la Información.* Obtenido de http://www.ideca.gov.co/sites/default/files/files/Presentaciones/Presentaciones_2013/Modelo%20de%20Seguridad_MINTIC_Oct%206_2013.pdf

OFICIAL, D. (2002). DECRETO NUMERO 2170 DE 2002. *DIARIO OFICIAL AÑO CXXXVIII , 44952* (3), 7.

ORG, I. (2011). *Information Technology. Security Techniques - Guidelines for Information and Communication Technology Readiness For Business Continuity*. Obtenido de http://www.iso.org/iso/catalogue_detail?csnumber=44374

Perú, P. U. (Septiembre de 2013). *Diseño de un sistema de gestión de continuidad de negocios para la RENIEC bajo la óptica de la norma ISO/IEC 22301*. Recuperado el 02 de 2015, de http://tesis.pucp.edu.pe/repositorio/bitstream/handle/123456789/5110/CASTRO_LAURA_DISE%C3%91O_SISTEMA_GESTION_CONTINUIDAD_NEGOCIOS_RENIEC_NORMA_ISO_IEC_22301.pdf?sequence=1

Portugal, B. C. (2012). *KPMG* . Obtenido de Business Continuity Management in Africa: https://www.kpmg.com/PT/pt/IssuesAndInsights/Documents/bcm2013-en.pdf

REDALYC, S. d. (2 de Septiembre de 2009). Una Aplicación de la Norma ISO /IEC 15504 Para la Evaluación por Niveles de Madurez. *Innovación , Calidad e Ingeniería de Software , 5* . Madrid.

Revista de Derecho, U. d. (2004). Función Pública colombiana. Bogotá: Revista de derecho 21:67-95.

Riesgos, S. N. (2012). *Gestión de Riesgos, Plan de Emergencia Institucional Ecuador*. (P. C. LTDA., Ed.) Obtenido de http://www.gestionderiesgos.gob.ec/wp-content/uploads/downloads/2012/07/Plan_de_Emergencia_Institucional.pdf

Robles, A. H. (12 de marzo de 2004). *Función Pública de los Servidores Municipales en Colombia*. Recuperado el 2004, de http://search.proquest.com/docview/1435620542?accountid=41816

Sistema Nacional de Protección Civil, P. y. (Marzo de 2012). *Plan Nacional de Protección Civil, Prevención y Mitigación de Desastres*. Obtenido de http://www.proteccioncivil.gob.sv/zonadescargas/Plan%20Nacional%202012/Plan_Nacional_210312.pdf

SOCIAL, C. C. (2007). Manual para Elaborar un Plan de Continuidad de la Gestión en Tecnologías de Información y Comunicaciones. Costa Rica.

SYMANTEC. (2012). *Informe Sobre Amenazas a la Seguridad en Internet - Hallazgos principales América*. (Symantec) Obtenido de http://www.symantec.com/content/es/mx/enterprise/threatreport/ISTR17-americas-spanish.pdf

US, N. I. (Mayo de 2010). *NIST Special PUBLICATION 800-34 Rev-1 CONTINGENCY PLANNING GUIDE FOR FEDERAL INFORMATION SYSTEMS*. Obtenido de http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

Yolima, R. L. (2012). *Plan de Continuidad BS-25999*. Universidad de Boyacá, Facultad de Ingeniería de Sistemas, Tunja.

9. **ANEXOS**

- Guía para la Preparación de las TIC para la Continuidad de Negocio
- GAP para la Continuidad de las Tecnologías de la Información
- Análisis de Impacto de Negocio BIA