RESUMEN – TRABAJO DE GRADO

AUTORES	LINA MARCELA VARGAS TORRES SANDRA SEPULVEDA LÓPEZ MAIRA ALEJANDRA CANDIA JAIME
FACULTAD	DE INGENIERIAS
PLAN DE ESTUDIOS	INGENIERIA DE SISTEMAS
DIRECTOR	ALVEIRO ROSADO GOMEZ
TÍTULO DE LA TESIS	DISEÑO DE UN PLAN DE CONTINUIDAD PARA LA SUBDIRECCIÓN ACADÉMICA DE LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA APLICANDO LA NORMA ISO/IEC 22301

RESUMEN
(70 PALABRAS APROXIMADAMENTE)

EL SISTEMA DE GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO (SGCN) SE HA CONVERTIDO EN UNA EXIGENCIA PARA LAS EMPRESAS QUE COMPITEN EL DÍA DE HOY EN LOS MERCADOS GLOBALIZADOS. LA TENDENCIA MUNDIAL ES QUE YA LAS EMPRESAS NO COMPITAN ENTRE SÍ: LA COMPETENCIA ES ENTRE CADENAS DE SUMINISTROS. UNA CADENA DE SUMINISTROS, PARA MANTENERSE OPERANDO, NO PUEDE TENER NINGÚN ESLABÓN DÉBIL; NINGUNO DE SUS COMPONENTES PUEDE DEJAR DE OPERAR.

CARACTERÍSTICAS

PÁGINAS: 72	PLANOS:0	ILUSTRACIONES:0	CD-ROM:1

DISEÑO DE UN PLAN DE CONTINUIDAD PARA LA SUBDIRECCIÓN ACADÉMICA DE LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA APLICANDO LA NORMA ISO/IEC 22301.

AUTORES:

LINA MARCELA VARGAS TORRES

SANDRA SEPULVEDA LÓPEZ

MAIRA ALEJANDRA CANDIA JAIME

Trabajo de grado para optar el título de Especialistas en Auditoria de Sistemas

Director:

ALVEIRO ROSADO GOMEZ

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

FACULTAD DE INGENIERÍAS

ESPECIALIZACIÓN EN AUDITORIA DE SISTEMAS

Ocaña, Colombia Octubre 2017

Agradecimientos

Los autores expresan los agradecimientos al director del trabajo de grado Ing. ALVEIRO ROSADO GOMEZ, por su guía y orientación en la realización del mismo, de igual forma a todos los docentes de la Universidad Francisco de Paula Santander Ocaña, que de una u otra manera contribuyeron al logro del mismo.

Dedicatoria

A Dios.

Por haberme permitido llegar hasta este punto y haberme dado salud para lograr mis objetivos, además de su infinita bondad y amor.

A mi incondicional esposo Carlos Vega.

Por haberme apoyado en todo momento, por sus consejos, sus valores, por la motivación constante que me ha permitido ser una persona de bien, pero más que nada, por su amor.

A la motivación de mi vida mi hijo Alejo.

Índice

Lista de figuras

Resumen

El Sistema de Gestión de la Continuidad del Negocio (SGCN) se ha convertido en una exigencia para las empresas que compiten el día de hoy en los mercados globalizados. La tendencia mundial es que ya las empresas no compitan entre sí: la competencia es entre cadenas de suministros. Una cadena de suministros, para mantenerse operando, no puede tener ningún eslabón débil; ninguno de sus componentes puede dejar de operar ya que si un elemento del todo dejara de funcionar se paraliza toda la serie, generando el caos.

Este proyecto se fundamenta en aplicar la norma ISO 22301 para el diseño del sistema de gestión de continuidad del negocio en la subdirección académica de la Universidad Francisco de Paula Santander Ocaña, con el fin de lograr y mejorar la disponibilidad de los servicios que esta presenta hacia otras dependencias.

Se realizó el plan de continuidad de negocio para la dependencia al igual que se hizo un análisis de la auditoria pasiva para conocer el estado actual de los procesos que se llevan, se establecieron estrategias que permitan la continuidad de los procesos de la Subdirección Académica, para consignarlas en un plan de gestión de la continuidad y determinaron los posibles riesgos para los activos de información en la subdirección Académica.

Introducción

La Gestión de Continuidad del Negocio, se puede definir como la identificación y protección de los procesos y recursos del negocio considerados críticos para sostener un desempeño aceptable, mediante la identificación de potenciales amenazas, la definición de estrategias para su eliminación, minimización o delegación y la preparación de procedimientos para asegurar la subsistencia de los mismos al momento de concretarse dichas amenazas.

La subdirección académica utiliza la tecnología de información como soporte a sus procesos y en ese sentido, el desarrollo de la Gestión de Continuidad del Negocio permitirá definir como se prepararán para evitar y afrontar situaciones de crisis. Es por ello, que el director como principal responsable de cumplir con los objetivos del negocio, debe asumir la implementación del plan de contingencia como un elemento fundamental para el éxito de su gestión.

El plan de Continuidad del Negocio según la Norma ISO/IEC 22301, en el cual se hará un análisis de los riesgos y vulnerabilidades que permitirán establecerlo y mantenerlo, para así estar preparados contra cualquier amenaza natural, humana o tecnológica.

Capítulo 1. Diseño de un plan de continuidad para la Subdirección Académica de la universidad Francisco de Paula Santander Ocaña aplicando la norma ISO/IEC 22301.

1.1 Planteamiento del problema.

La Subdirección Académica de la Universidad Francisco de Paula Santander Ocaña, es un organismo de gobierno; dependencia adscrita a la Dirección de la Seccional encargada de las funciones de: orientación, planeación, organización y supervisión de las actividades docentes, investigativas y de extensión de la Universidad Francisco de Paula Santander, Seccional Ocaña, en concordancia con las políticas y normas generales de la misma; lo cual la vuelve una dependencia crucial para cumplir con las responsabilidades que tiene el proceso misional de gestión académica (Universidad Francisco de Paula Santander Ocaña, 2017).

Una parte considerable de las actividades del proceso de gestión académica es adelantado por la subdirección académica, recibir, validar y dar trámite a una serie de documentos hace parte del día a día de esta dependencia; esta situación produce una administración de la información considerable y de importancia para las labores misionales de la universidad. Haciendo un balance de las transacciones documentales hasta noviembre de 2016, se encontraron 586 documentos de trámite y expedición, que son correspondientes a los diferentes reportes que representan las variables de la responsabilidades de la subdirección académica; adicionalmente existen documentos más frecuentes como cargas académicas 26, homologaciones de inglés 66, solicitudes y respuestas de reposición 8, renovación de Licencias Internas 5, e informes 12.

Sumando estos diferentes documentos se alcanzan la cifra de 703 documentos en solo un mes (Secretaria Distrital del Ambiente, 2008).

De otra parte se debe decir que el plan de continuidad para la subdirección académica, permite contrarrestar las interrupciones en las actividades académicas y proteger sus procesos críticos contra los efectos de fallas importantes en los Sistemas de Información o contra desastres, y asegurar su recuperación oportuna. En la Subdirección se desarrollaran actividades relacionadas con los procesos académicos en la Universidad, estando los sistemas interconectados a la red de la Institución; y viéndose expuesta a riesgos que vulneran su seguridad física (como robos o sabotajes) y lógica (como fallos del software o virus).

La Universidad Francisco de Paula Santander Ocaña, cuenta con un Plan de Contingencia de TI para el Proceso de Apoyo: Sistema de Información, Telecomunicaciones y Tecnología, siendo éste desconocido por el 80% del personal administrativo, debido a la falta de capacitación y actualización del mismo, esto se evidencia en cuestionario realizado a un total de 40 entrevistados en diferentes dependencias de la UFPSO.

Además, se puede apreciar que actualmente dicha oficina no está preparada para recuperarse y continuar con sus operaciones en un tiempo razonable frente a un desastre de cualquier tipo que pueda ocurrir, ya que no cuentan con un plan de continuidad que le permita minimizar el impacto (económico y duración) de un evento de riesgo que no pueda ser evitado, ocasionando de esta manera que la Universidad paralice sus operaciones academicas.

Por esta razón la información de dicha dependencia puede estar expuesta a riesgos tanto de eventos naturales, fallos tecnológicos o humanos, existen incidentes que ponen en peligro el activo más relevante de La Subdirección Académica los cuales pueden provocar anomalías impidiendo la continuidad de las labores de dicha organización.

1.2 Formulación del problema.

¿Es posible elaborar un plan de gestión de continuidad del negocio que permitirá garantizar el desarrollo de las operaciones cotidianas ante una posible eventualidad adversa en la Subdirección Académica de la UFPS Ocaña?

1.3 Objetivos.

1.3.1 Objetivo General. Diseñar un plan de continuidad para la dependencia de Subdirección Académica de la Universidad Francisco de Paula Santander Ocaña aplicando la norma ISO/IEC 22301.

1.3.2 Objetivos Específicos. Aplicar una auditoria pasiva en la subdirección académica para conocer el estado actual de los procesos que se llevan.

Definir estrategias que permitan la continuidad de los procesos de la Subdirección Académica, para consignarlas en un plan de gestión de la continuidad.

Establecer los posibles riesgos para los activos de información en la subdirección Académica.

1.4 Justificación.

La norma ISO 22301 faculta a las organizaciones para tomar decisiones al momento de ocurrir un imprevisto ante cualquier eventualidad como por ejemplo: malware, desastres naturales, fallos internos, ataques cibernéticos, accidentes entre otros, los cuales pueden poner en peligro la continuidad del negocio. Teniendo en cuenta que se debe cumplir con la misión y los objetivos que están establecidos en Subdirección Académica es importante manejar estrategias planes de respuestas y demás componentes que ayuden a su cumplimiento.

Todas las instituciones se encuentran expuestas a riesgos operativos inherentes a su actividad económica, recursos tecnológicos y características específicas de la región. Prever las situaciones de emergencia y prepararse para enfrentarlas, es la forma más apropiada para disminuir el impacto lesivo que podría afectar a las personas y a la economía de ésta. Para lograr una efectiva disminución del impacto de las emergencias y desastres que afecten la salud de las personas y los bienes de la Institución, se requiere un plan estructurado que cuente con el apoyo de la dirección y con la participación de toda la comunidad universitaria, para adoptarlo, aplicarlo y mantenerlo.

De igual forma se debe decir que la Universidad Francisco de Paula Santander Ocaña, se encuentra en una zona de alto riesgo expuesta a amenazas tales, como tormentas eléctricas,

disturbios civiles, incendios, accidentes, entre otros; lo que hace indispensable establecer planes, programas y proyectos enfocados en la prevención y manejo de cualquier tipo de desastre, ya sea de origen natural o humano. Por lo que la subdirección académica, con el fin de actuar de forma eficiente y minimizar el impacto en caso de emergencia o desastre, con la participación de toda la comunidad: personal administrativo, docente, estudiantes, contratistas, visitantes y demás personas que se encuentren en el campus Universitario, requiere desarrollar el plan de continuidad, que le permita contrarrestar las interrupciones en las actividades propias y proteger sus procesos críticos contra los efectos de fallas importantes en los sistemas de información o contra desastres y asegurar su recuperación oportuna.

1.5 Delimitación y alcances

1.5.1 Operativas. Las posibles dificultades que se puede encontrar en este proyecto son: No encontrar la información completa acerca de la dependencia o que las diferentes oficinas que la conformes no brinden la información completa.

1.5.2 Conceptual. La propuesta estuvo enmarcada dentro de los conceptos y lineamientos establecidos en la norma ISO/IEC 22301 “Gestión de la continuidad del negocio” y articulada con el sistema de gestión de la calidad de la UFPSO.

1.5.3 Geográficas. Este proyecto se desarrolló en la Subdirección Académica de la Universidad Francisco de Paula Santander seccional Ocaña Temporal.

1.5.4 Temporales. El tiempo necesario para el desarrollo de esta investigación, fue de tres (3) meses.

Capítulo 2. Marco de referencial

2.1 Marco Histórico.

En la realización de este documento se tomaron como referencias proyectos de investigación con temas afines y que se relacionan con la continuidad del negocio ISO 22301, realizados a nivel internacional, nacional y regional.

2.1.1 Antecedentes de los planes de continuidad a nivel internacional. El término Plan de Continuidad de Negocio o Business Continuity Plan (BCP por sus siglas en inglés), cada vez expande más su alcance. Esto se compara con términos utilizados anteriormente que sólo estaban enfocados a áreas específicas como Disaster Recovery y Contingency Planning que han pasado a formar parte del BCP(BSI GROUP, 2007).

En el siglo pasado, en los setenta Norman L. Harris, Edward S. Devlin y Judith Robey, al tratar de encontrar un método de planificación y gestión que evitara la continua atención de los problemas de forma aleatoria, dieron inicio a una actividad que llamaron Disaster Recovery Planning. Con esto se aseguraba la planeación de cómo reaccionar en caso de un desastre. Más tarde, esa actividad fue llamada Contingency Planning, término que resultó ser más universal puesto que la Contingencia es algo que puede suceder o no suceder o puede también denominarse “riesgo” (Saez vargas, 2011).

En los inicios de la utilización de este enfoque de analizar las contingencias empresariales, cuando se conocía como Disaster Recovery, la actividad estaba dirigida a áreas de Tecnologías de información. Más adelante, cuando las tecnologías de la información comenzaron a formar parte de las áreas de soporte de las operaciones de toda la empresa, el Disaster Recovery expandió su alcance, llamándose ahora Business Continuity Plan (BCP), traducido como Plan de Continuidad de Negocio y Business Continuity Management (BCM), traducido como Gestión de la Continuidad de Negocio. En la actualidad el concepto de continuidad de negocio es aplicado a toda la organización, es un concepto global, que incorpora a toda la cadena logística, es decir desde el cliente hasta el proveedor de insumos (Saez vargas, 2011).

Beneficios del BCP y como se relaciona con la competitividad en las organizaciones. Los beneficios que se pueden alcanzar al tener implementado de forma correcta un Plan de Continuidad de Negocio son:

Ventaja competitiva frente a otras organizaciones: el hecho de mostrar que se toman medidas para garantizar la continuidad de negocio mejora la imagen pública de la organización y revaloriza la confianza frente a accionistas, inversores, clientes y proveedores.

Previene o minimiza las pérdidas de la organización en caso de desastres: es capaz de identificar de forma proactiva los posibles impactos e inconvenientes que una interrupción de sus actividades de negocio puede provocar.

Asegurar que las actividades del negocio soporten y se recuperen ante interrupciones: aumentando la disponibilidad de los servicios dispuestos para el cliente.

Menor riesgo de sufrir sanciones económicas: al adaptarse a requerimientos regulatorios.

Asignación más eficiente de las inversiones en materia de seguridad: gracias al análisis de riesgos (BIA), el cual permite priorizar las actividades críticas y fijar los esfuerzos y los presupuestos en las áreas más necesitadas (Saez vargas, 2011).

De otra parte en Guatemala, el plan de continuidad, por su naturaleza, involucra aspectos tecnológicos como aspectos humanos, tal es el caso de la formación de equipos de continuidad, los cuales están encargados de poner en actividad el plan, partiendo de este punto, el elemento humano que van a estar interactuando con las políticas de continuidad y los criterios de funcionamiento, debe poseer un nivel de cultura de calidad de servicio.

Por lo cual, un aspecto fundamental es la cultura de calidad de servicio, sin embargo, el clima organizacional, también, juega un rol importante para disminuir la resistencia a utilizar, de forma efectiva, un plan de esta naturaleza. En Guatemala, el plan de continuidad no está implementado en la mayoría de empresas ni instituciones, las organizaciones están adoptando las tecnologías de la información (TI) e implementando las mismas para tener control y manejo de la información, sin embargo, los niveles de seguridad no han sido explotados a tal nivel (Juárez Najarro, 2011).

Es por esto que las empresas privadas, de origen extranjero, tienen una visión diferentes a la visión de las nacionales en relación con los procesos de negocio, tal es el caso de los call center, en donde la continuidad de operaciones es vital, porque una interrupción impacta negativamente a nivel económico como a nivel del prestigio. En las pequeñas y medianas empresas de capital guatemalteco, denominadas pyme, no cuentan con un plan de continuidad

debido a que los directivos y trabajadores no tienen la visión ni la cultura de calidad de servicio, en ese sentido es importante mencionar que en este tipo de organizaciones el departamento de la TI es muy pequeño o no existe, esto es un impedimento potencial para la creación de este tipo de políticas.

En cuanto al aspecto institucional, es la burocracia que existe en las organizaciones tanto gubernamentales como no gubernamentales lo que hace difícil la implementación de un plan de continuidad. A pesar de este aspecto, ya se está logrando crear una cultura de servicio apoyada en las TI, por ello, es indispensable implementar políticas que garanticen la continuidad. Por supuesto no se puede generalizar, en virtud que puede haber casos que sean la excepción, sin embargo, el patrón descrito anteriormente es el que predomina según la categoría de organización (Juárez Najarro, 2011).

2.1.2 Antecedentes de los planes de continuidad a nivel nacional. La continuidad del negocio puede definirse como una estrategia y táctica de una organización para recuperar, restaurar sus funciones, planificar y responder ante incidentes o desastres que puedan afectar la disponibilidad, con el fin de darle continuidad a un nivel aceptable a los servicios. El sistema de gestión de continuidad del negocio (SGCN), consiste en tener una preparación proactiva de recuperación desde los planes de contingencias, como de los servicios críticos de la organización, mediante el desarrollo de mecanismos de análisis y procesos claves para la restauración rápida con el fin de minimizar los impactos y mitigar los riesgos.

Según la norma ISO 22301 define el sistema de gestión de continuidad de negocio como Parte del sistema general de gestión que establece, implementa, opera, monitorea, revisa, mantiene y mejora la Continuidad de Negocio ISO 22301. La ISO 22301 es la nueva norma internacional de gestión de continuidad de negocio. Esta ha sido creada en respuesta a la fuerte demanda internacional que obtuvo la norma británica original, BS 25999-2 y otras normas. ISO 22301 identifica los fundamentos de un sistema de gestión de continuidad de negocio, estableciendo el proceso, los principios y la terminología de gestión de continuidad de negocio. Esta norma proporciona una base de entendimiento, desarrollo e implantación de continuidad de negocio dentro de su organización y le da la confianza de negocio a negocio y de negocio a cliente. Se usa para asegurar a las partes interesadas clave que su empresa está totalmente preparada y que puede cumplir con los requisitos internos, regulatorios y del cliente (Tellez Mondragon, 2015).

Objetivo del SGCN. Permitir la administración, planificación, seguimiento, control y mejoramiento permanente de la estrategia de continuidad del negocio de la compañía para garantizar su operación crítica en caso de una contingencia.

CICLO PHVA (PLANEAR – HACER – VERIFICAR – ACTUAR) La norma ISO 2230115, trabaja sobre el ciclo dinámico PHVA Planifique – Haga – Verifique - Actué, este ciclo nos ayuda a la realización de actividades, de una manera más organizada y eficaz. Por tanto aceptar la metodología de trabajo ofrecido por el ciclo PHVA es una guía básica para la gestión de actividades y procesos, ofreciéndonos una estructura ejemplar de un sistema que es aplicable para cualquier organización. A través del ciclo PHVA la organización planea, establece,

implementa, opera, monitorea, revisa, mantiene y mejora continuamente la eficacia de un sistema de gestión de Continuidad de Negocio característica principal de un sistema de gestión (Tellez Mondragon, 2015).

En la fase de planeación, se definen los objetivos, metas, controles, y procedimientos de continuidad de negocio, con el fin, de verificar que en efecto dichos objetivos se están cumpliendo y estén alineados a la política de la organización. Luego se implementa y se realizan todas las actividades según, los procedimientos y conforme a las normas técnicas establecidas de continuidad del negocio, comprobando monitoreando y controlando la calidad de la política referente a los objetivos de continuidad, y el desempeño de los procesos claves. Finalmente en la fase Actuar, se mantiene y evoluciona la estrategia de acuerdo a los resultados obtenidos y mediante acciones correctivas que se hallaron en la fase anterior de verificación, desarrollándose un plan de mejoramiento que obliga volver a iniciar el ciclo, con una nueva planificación que mejora y adecua las políticas, objetivos y procedimientos, entre otras que permitan mejorar los hallazgos encontrados, generando un bucle infinito de mejora continua.

El ciclo PHVA se puede resumir de la siguiente manera: ¬ Planificar. Establecen objetivos, procesos, procedimientos de continuidad de negocio, para dar alcance los resultados obtenidos, dándole conformidad a los requisitos establecidos por la alta dirección y las políticas de la organización. ¬ Hacer. Se implementa y pone en marcha los procesos y procedimientos de continuidad de negocio para alcanzar los objetivos. ¬ Verificar. se realiza un seguimiento, a los procesos, conforme a lo establecido en la fase de planificación, reportando los resultados alcanzados, se hacen hallazgos que permiten tomar acciones mejoramiento. ¬ Actuar. Se

realizan acciones, para promover la mejora de los procesos, implementando acciones correctivas y volviendo a iniciarse el ciclo con un nuevo plan de mejora (Tellez Mondragon, 2015).

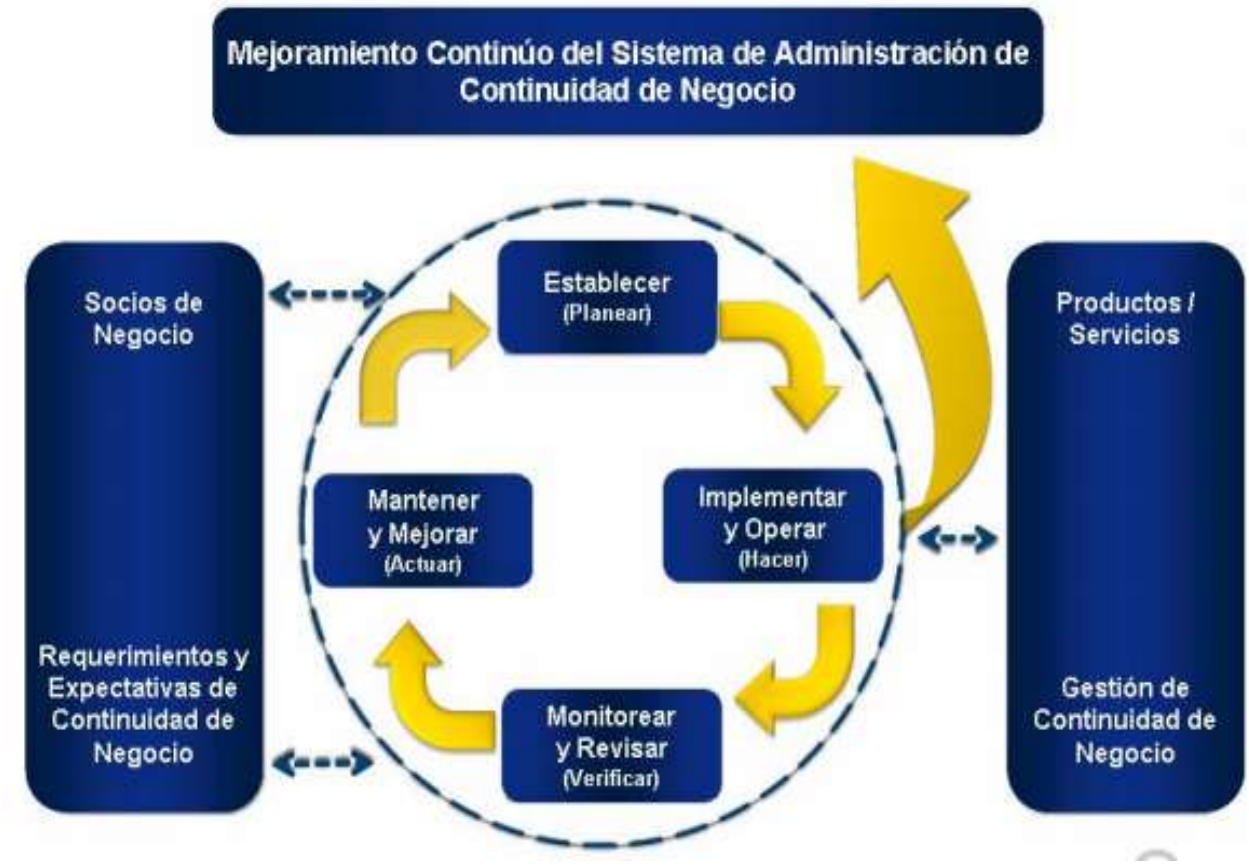

Figura 1. Mejoramiento continuo del sistema de administración

Fuente.

http://implementación%20de%20estrategias%20de%20continuidad%20de%20negocio%20en%20la%20.pdf

De otra parte En los últimos años se ha incrementado la preocupación del mercado y los entes regulatorios por la entrega de productos y servicios que las Compañías prometen a sus clientes en tiempo, condiciones contratadas y compromisos adquiridos; por lo que han establecido leyes, normas y estándares que velan por la promesa hecha a los clientes. Los

clientes a su vez, demandan la entrega de servicio con mayor efectividad y calidad, en el tiempo en que lo necesitan y con la atención oportuna. No quieren escuchar explicaciones técnicas sobre las causas que afectaron los servicios y no quieren esperar que la Compañía esté disponible o recuperada. A pesar de los efectos negativos de no contar con un plan de gestión de la continuidad de negocio, muchas empresas aún no toman medidas para implementar las estrategias que les permitan asegurar los procesos que generan valor y en consecuencia garantizar la sostenibilidad de la empresa a largo plazo (Zapata Atehortua & Echeverry Barrera, 2011).

UNE EPM TELECOMUNICACIONES al ser una empresa en el mercado de las TIC es en gran parte dependiente de la tecnología y compite en escenarios complejos debido a la globalización, se hace más susceptible a que una serie de amenazas puedan penetrar sus vulnerabilidades y causarle daño, al grado de dejarla fuera del mercado. Para la empresa, mantener continuidad de los servicios administrando la continuidad del negocio más que un cumplimiento regulatorio, es un elemento estratégico y táctico que permite afrontar el reto por mantenerse en un mercado cada vez más competido, y el cual debe ser asumido por las Compañías para mantener la fidelidad de sus clientes, y por supuesto, mantener un crecimiento sostenible y rentable.

Este proyecto se enfocará en proponer una metodología de diagnóstico organizacional que permita implementar las estrategias necesarias para mantener la continuidad de negocio en los procesos críticos de la Dirección de Operaciones de UNE EPM TELECOMUNICACIONES. Se indicarán los elementos que hacen parte del proceso de evaluación y finalmente tendremos como

resultado una lista de chequeo que podrá ser interpretada y aplicada por la alta gerencia de la compañía en la toma de las decisiones necesarias para implementar continuidad de negocio. Este proyecto tendrá una duración de un año que es consecuente a la velocidad de cambio en el mercado de las TIC's. No está dentro del alcance de este proyecto sino que es responsabilidad de la empresa, generar un plan de mantenimiento posterior donde se vayan reflejando los cambios de la compañía, el sector y el mercado (Zapata Atehortua & Echeverry Barrera, 2011).

2.1.3 Antecedentes de los planes de continuidad a nivel local. A nivel local se debe decir que el siguiente proyecto tuvo como propósito implementar un plan de continuidad del Negocio a la Unidad de Almacén de la UFPS Ocaña, con el fin de minimizar el impacto (económico y duración) de un evento de riesgo que no pueda ser evitado, ocasionando de esta manera que la Universidad paralice sus operaciones en el manejo de sus inventarios. Ésta investigación busca dar respuesta a: ¿La creación de un Manual de Gestión de Continuidad del Negocio constituirá un instrumento que le facilite a la Unidad de Almacén de la Universidad Francisco de Paula Santander Ocaña, disminuir el impacto lesivo que podría afectar a las personas y a la economía de la misma?, cuyos resultados fue la creación de un manual de procedimientos para la continuidad del negocio de la Unidad de Almacén de la UFPS Ocaña, para afrontar de manera oportuna, adecuada y efectiva, ante la eventualidad de incidentes, accidentes o estados de emergencia que pueden ocurrir en las instalaciones de la misma (Criado Ramirez, Lobo Ruedas, Meneses Arias, Pacheco Solano, & Prado Carrascal, 2014).

De otra parte la siguiente investigación El propósito de éste proyecto es realizar una serie de recomendaciones que orientan la implementación de un Plan de Continuidad del Negocio que

determina las acciones a tomar en caso de una contingencia en el Centro de Desarrollo e Innovación Tecnología de la Ufps Ocaña bajo la Norma ISO 22301.

De tal manera el CEDIT debe implementar una serie de estrategias para elaborar el plan de continuidad, identificando las posibles amenazas al interior y al exterior del centro que le permitan recuperar en un nivel aceptable después de una interrupción no prevista sus sistemas de información buscando minimizar el tiempo de respuesta ante la perturbación.
Los resultados de ésta investigación permitió definir objetivamente tanto las etapas que conllevan a la elaboración del Plan, como también los procesos críticos de la dependencia que sirvió además de apoyo a la toma de decisiones en otros ámbitos (Blanco Lindarte, Martínez Vega, Quintero Prado, & Rincon Angarita, 2015).

2.2 Marco conceptual.

Para las pequeñas y grandes empresas es importante adoptar la Norma ISO 22301, con el fin de conocer las amenazas y proteger a las organizaciones de incidentes que provoquen una interrupción en las actividades del proceso de las empresas, y garantizar la recuperación del servicio prestado. En este caso a continuación se definen de manera clara y sencilla los términos relacionados:

Direccionamiento Estratégico. El “Direccionamiento Estratégico” es una disciplina que integra varias estrategias, que incorporan diversas tácticas. El conocimiento, fundamentado en información de la realidad y en la reflexión sobre las circunstancias presentes y previsibles, coadyuva a la definición de la “Dirección Estratégica” en un proceso conocido como

“Planeamiento Estratégico”, que compila tres estrategias fundamentales e interrelacionadas: a) La Estrategia Corporativa, b) La Estrategia de Mercadeo y c) La Estrategia Operativa o de Competitividad. El Direccionamiento Estratégico podríamos definirlo como el instrumento metodológico por el cual establecemos los logros esperados y los indicadores para controlar, identificamos los procesos críticos dentro de la gestión, los enfoques, y demás áreas importantes que tengan concordancia con la misión, la visión, y los objetivos establecidos (Trujillo, 2006).

En otras palabras, el Direccionamiento Estratégico lo podemos considerar como la materia prima o insumo fundamental para aplicar la Planeación Estratégica, Táctica y Operativa que al final dicha aplicación es la que nos garantiza el poder alcanzar el lugar el cual nos hemos propuesto. La planeación estratégica es el proceso mediante el cual quienes toman decisiones en una organización obtienen, procesan y analizan información pertinente, interna y externa, con el fin de evaluar la situación presente de la empresa, así como su nivel de competitividad con el propósito de anticipar y decidir sobre el direccionamiento de la institución hacia el futuro (Trujillo, 2006).

Estructura organizacional. La estructura organizacional puede ser definida como las distintas maneras en que puede ser dividido el trabajo dentro de una organización para alcanzar luego la coordinación del mismo orientándolo al logro de los objetivos (Garcia & Guerra, 1997).

Plan de Continuidad del Negocio. Un Plan de Continuidad del Negocio es un proceso diseñado para prevenir interrupciones que afecten el desempeño de las actividades normales de un negocio. En caso de que un evento de riesgo no pueda ser evitado, este plan debe minimizar

su impacto (económico y duración). El Plan de Continuidad del Negocio tiene un alcance operativo y tecnológico (Mora Prada, Quintero Mejia, & Camargo Ttigos, 2013).

Antecedentes. En la última década, los riesgos de desastres naturales, fallas técnicas con carácter accidental, y actividades maliciosas han incrementado las posibilidades de interrupciones en las organizaciones. Las empresas que sufren una interrupción por espacio de diez días consecutivos, nunca se recuperan y desaparecen del mercado. Lamentablemente, muy pocas son las empresas que invierten en planificación de actividades para minimizar posibles desastres y asegurarse de continuar operando después de una posible calamidad.

Objetivos de Un Plan de Continuidad del Negocio. Obtener una imagen clara y detallada de los procesos de negocio de la entidad, determinando sus criticidades, interdependencias y riesgos.

Lograr un conocimiento profundo de la plataforma tecnológica.

Determinar las necesidades críticas para permitir un grado de operatividad en línea con la estrategia definida.

Desarrollar una solución cuya relación costo – beneficio cumpla los requisitos y las expectativas de la entidad.

Prever y documentar las acciones necesarias para restaurar la actividad.

Lograr una situación que garantice la continuidad del negocio.

Importancia del Plan de Continuidad del Negocio. Un Plan de Continuidad del Negocio debe ser considerado parte integral de la estrategia del negocio. Un buen plan revisa los procesos

críticos de la operación en las empresas, los clasifica, prioriza y determina cuáles son los más sensibles y cuáles no pueden dejar de operar para que el negocio continúe su funcionamiento. Si las empresas no cuidan ni manejan correctamente su información, en el momento en que padezcan una eventualidad no podrán atender asuntos prioritarios como: a quién le deben pagar, quién les debe, a quién le venden, a quién le deben otorgar un descuento, quién es meritorio de un crédito, entre otras variables vitales del negocio. El hecho de no poder acceder a estos datos puede ocasionar importantes pérdidas al negocio, (como no saber cómo operan, cuántas piezas producen, cuál era el pedido urgente, cuando llega la materia prima para correr la programación de producción, entre otros) (Coronel Ortiz, Guevara Gelvez, Jaime Fernandez, & Salazar Rincon, 2013).

Alcance del Plan de Continuidad del Negocio. Desarrollar un Plan para la Continuidad del Negocio, que tenga como objetivo el mantenimiento de la actividad de la empresa, mediante la recuperación de los procesos de soporte o mediante la aplicación de procesos de emergencia. El proyecto debe involucrar a todos los procesos y áreas críticas del departamento de producción.

Sistema de Gestión de la continuidad del negocio (SGCN). Este sistema es el encargado de la planificación, mantenimiento y mejora continua del negocio.

Interrupción máxima aceptable (MAO). Se trata del tiempo límite máximo que la actividad puede estar suspendida. En el supuesto de sobrepasar este límite, el daño que se produciría sería inaceptable.

MTPD: Periodo Máximo admisible de interrupción.

RPO: Límite mínimo para la continuidad del negocio. Es el nivel más bajo de productos o servicios fundamentales para fabricar una vez que se sigan con las actividades habituales de la organización.

Confidencialidad. Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

Integridad. Propiedad de salvaguardar la exactitud y el estado completo de los activos.

Vulnerabilidad. Debilidad de un activo o grupo de activos, que puede ser aprovechada por una o más amenazas.

Disponibilidad. Es que las personas o procesos autorizados accedan a los activos de información cuando así lo requieran.

Causa. Son los medios, circunstancias y agentes que generan los riesgos.

Control. Es toda acción que tiende a minimizar los riesgos, significa analizar el desempeño de las operaciones, evidenciando posibles desviaciones frente al resultado esperado para la adopción de medidas preventivas. Los controles proporcionan un modelo operacional de seguridad razonable en el logro de los objetivos.

Probabilidad. Una medida (expresada como porcentaje o razón) para estimar la posibilidad de que ocurra un incidente o evento. Contando con registros, puede estimarse a partir de su frecuencia histórica mediante modelos estadísticos de mayor o menor complejidad.

2.3 Marco contextual.

En noviembre de 1973 se suscribió un contrato para la realización de un estudio de factibilidad denominado "Un centro de educación superior para Ocaña", que fue terminado y sugirió la creación pronta de un programa de educación a nivel de tecnología en énfasis en ciencias sociales, matemáticas y física, por el cual en 1975 comenzó la actividad académica en la entonces seccional de la Universidad Francisco de Paula Santander con un total de 105 estudiantes de Tecnología en Matemáticas y Física, y su primera promoción de licenciados en Matemáticas y Física se logró el 15 de diciembre de 1980 (Universidad Francisco de Paula Santander Ocaña, Historia, 2017).

Según Acuerdo No. 003 del 18 de Julio de 1974, por parte del Consejo Superior de la Universidad Francisco de Paula Santander Cúcuta, se crea la Universidad Francisco de Paula Santander Ocaña, como máxima expresión cultural y patrimonio de la región; como una entidad de carácter oficial seccional, con AUTONOMÍA administrativa y patrimonio independiente, adscrito al Ministerio de Educación Nacional.

La Subdirección Académica encargada de las funciones de orientación, planeación, organización y supervisión de las actividades docentes, investigativas y de extensión de la

Universidad Francisco de Paula Santander, Seccional Ocaña, en concordancia con las políticas y normas generales de la misma.

La Universidad Francisco de Paula Santander Ocaña para el 2019, será reconocida por su excelencia académica, cobertura y calidad, a través de la investigación como eje transversal de la formación y el uso permanente de plataformas de aprendizaje; soportada mediante su capacidad de gestión, la sostenibilidad institucional, el bienestar de su comunidad académica y el desarrollo físico. La universidad cuenta con el odelo Estandar de Control Interno MECI, con el fin de desarrollar, implementar y mantener en operación el Sistema de Control Interno regulado en la ley 87 de 1993, actualiza el Modelo Estándar de Control Interno mediante resolución 0158 del 14 de julio de 2014, adoptando la nueva estructura de acuerdo al Manual Técnico, decreto 0943 del 21 de mayo de 2014, como una herramienta básica para evaluar la estrategia, la gestión y los mecanismos propios de evaluación del proceso administrativo, todo ello dirigido al cumplimiento de los objetivos institucionales y de la contribución de los mismos, a los fines esenciales del Estado (Universidad Francisco de Paula Santander Ocaña, https://ufpso.edu.co/sub_academica, 2017).

Figura 2. Información y comunicación

Fuente. Universidad Francisco de Paula Santander Ocaña.

En la Universidad, el Sistema de Control Interno y el MECI, promueven la adopción de un enfoque basado en procesos, donde intervienen todos los servidores de la entidad como responsables del control en el ejercicio de sus actividades; persiguiendo la coordinación de las acciones, la fluidez de la información y comunicación, anticipando de forma preventiva y oportuna las debilidades que se presentan en el quehacer institucional. En esta estructura se admite que el Sistema de Control Interno es complementario con el Sistema Integrado de Gestión, aunque no puede ser visto como tal, por lo tanto se continua sustentándose en los tres aspectos filosóficos esenciales en los que se fundamenta el MECI: AUTOCONTROL, AUTOGESTIÓN, AUTORREGULACIÓN.

Figura 3. MECI

Fuente. Universidad Francisco de Paula Santander Ocaña.

La especialización de Auditoría de Sistemas según la resolución No 244 del 10 de enero del 2012 del Ministerio de Educación Nacional fué otorgada por 7 años, y cuenta con un perfil profesional donde el egresado al culminar el programa, estará en la capacidad de identificar los riesgos, inherentes al manejo de la información empresarial, proponer los controles necesarios para manejar dichos riesgos, construir un modelo de seguridad informática, evaluar la

administración de los recursos informáticos y gerenciar efectivamente el área de Auditoría de Sistemas adaptando modelos de gobernabilidad de TI y su perfil ocupacional

2.4 Marco Teórico.

Contra atacar las interrupciones a las actividades comerciales y proteger los procesos comerciales críticos de los efectos de fallas importantes o desastres en los sistemas de información y asegurar su reanudación oportuna. Se debería implementar el proceso de gestión de la continuidad del negocio para minimizar el impacto sobre la organización y recuperarse de la pérdidas de activos de información (lo cual puede ser resultado de, por ejemplo, desastres naturales, accidentes, fallas del equipo y acciones deliberadas) hasta un nivel aceptable a través de una combinación de controles preventivos y de recuperación. Este proceso debería identificar los procesos comerciales críticos e integrar los requerimientos de gestión de la seguridad de la información de la continuidad del negocio con otros requerimientos de continuidad relacionados con aspectos como operaciones, personal, materiales, transporte y medios (Sistemas de Gestión de seguridad de la información, 2014).

Las consecuencias de los desastres, fallas en la seguridad, pérdida del servicio y la disponibilidad del servicio deberían estar sujetas a un análisis del impacto comercial. Se deberían desarrollar e implementar planes para la continuidad del negocio para asegurar la reinundación oportuna de las operaciones esenciales. La seguridad de la información debería ser una parte integral del proceso general de continuidad del negocio, y otros procesos gerenciales dentro de la organización. La gestión de la continuidad del negocio debería incluir controles para identificar y

reducir los riesgos, además del proceso general de evaluación de riesgos, debería limitar las consecuencias de incidentes dañinos y asegurar que esté disponible la información requerida para los procesos comerciales.

Incluir la seguridad de la información en el proceso de gestión de continuidad del negocio Control. Se debería desarrollar y mantener un proceso gerencial para la continuidad del negocio en toda la organización para tratar los requerimientos de seguridad de la información necesarios para la continuidad comercial de la organización.

Guía de implementación. El proceso debería reunir los siguientes elementos claves de la gestión de continuidad del negocio:

Entender los riesgos que enfrenta la organización en términos de la probabilidad y el impacto en el tiempo, incluyendo la identificación y priorización de los procesos comerciales críticos.

Identificar todos los activos involucrados en los procesos comerciales críticos.

Entender el impacto que probablemente tendrán las interrupciones causadas por incidentes en la seguridad de la información en el negocio (es importante encontrar las soluciones que manejen los incidentes que causan el menor impacto, así como los incidentes serios que pueden amenazar la viabilidad de la organización), y establecer los objetivos comerciales de los medios de procesamiento de la información (Sistemas de Gestión de seguridad de la información, 2014).

Considerar la compra de un seguro adecuado que pueda formar parte de un proceso general de la continuidad del negocio, y que también sea parte de la gestión del riesgo operacional.

Identificar y considerar la implementación de controles preventivos y atenuantes adicionales.

Identificar los recursos financieros, organizacionales, técnicos y ambientales suficientes para tratar los requerimientos de seguridad de la información identificados.
Garantizar la seguridad del personal y la protección de los medios de procesamiento de la información y la propiedad organizacional.

Formular y documentar los planes de continuidad del negocio tratando los requerimientos de seguridad de la información en línea con la estrategia acordada para la continuidad del negocio. Pruebas y actualizaciones regulares de los planes y procesos.
Asegurar que la gestión de la continuidad del negocio se incorpore a los procesos y estructura de la organización. Se debería asignar la responsabilidad del proceso de la gestión de la continuidad del negocio en el nivel apropiado dentro de la organización.

Continuidad del negocio y evaluación del riesgo. Control. Se deberían identificar los eventos que pueden causar interrupciones a los procesos comerciales, junto con la probabilidad y el impacto de dichas interrupciones y sus consecuencias para la seguridad de la información.

Guía de implementación. Los aspectos de la seguridad de la información de la continuidad del negocio se deberían basar en la identificación de los eventos (o secuencia de eventos) que pueden causar las interrupciones en los procesos comerciales de la organización. por ejemplo, fallas en el equipo, errores humanos, robo, fuego, desastres naturales y actos de terrorismo. Esto debería ir seguido por una evaluación del riesgo para determinar la probabilidad e impacto de dichas interrupciones, en términos de tiempo, escala del daño y período de recuperación. La evaluación del riesgo de la continuidad el negocio se debería llevar a cabo con

la participación total de los propietarios de los recursos y procesos comerciales. Esta evaluación debería considerar los procedimientos comerciales y no se deberían limitar a los medios de procesamiento de la información, y deberían incluir los resultados específicos para la seguridad de la información. Es importante vincular los diferentes aspectos del riesgo para obtener una imagen completa de los requerimientos de continuidad comercial de la organización. La evaluación debería identificar, cuantificar y priorizar los riesgos en comparación con los criterios y objetivos relevantes para la organización, incluyendo los recursos críticos, impactos de las interrupciones, tiempos de desabastecimiento permitidos y prioridades de recuperación. Dependiendo de los resultados de la evaluación del riesgo, se debería desarrollar una estrategia de continuidad del negocio para determinar el enfoque general para la continuidad del negocio. Una vez que se ha creado la estrategia, la gerencia debería proporcionarle su respaldo, y crear y respaldar un plan para implementar esta estrategia (Sistemas de Gestión de seguridad de la información, 2014).

Desarrollar e implementar los planes de continuidad incluyendo la seguridad de la información Control. Se deberían desarrollar e implementar planes para mantener restaurar las operaciones y asegurar la disponibilidad de la información en el nivel requerido y en las escalas de tiempo requeridas después de la interrupción, o falla, de los procesos comerciales críticos.

Guía de implementación. El proceso de planeación de la continuidad del negocio debería considerar lo siguiente:

Identificar y acordar todas las responsabilidades y los procedimientos de continuidad del negocio.

Identificar la pérdida aceptable de la información y los servicios.
Implementación de los procedimientos para permitir la recuperación y restauración de las operaciones comerciales y la disponibilidad de la información en las escalas de tiempo requeridas. Se debería prestar particular atención a la evaluación de las dependencias comerciales internas y externas y el establecimiento de los contratos debidos (Blanco Lindarte, Martínez Vega, Quintero Prado, & Rincon Angarita, 2015).

Los procedimientos operacionales a seguir dependiendo de la culminación de la recuperación y restauración.
Documentación de los procesos y procedimientos acordados.
Educación apropiada del personal en los procedimientos y procesos acordados, incluyendo la gestión de crisis.

Prueba y actualización de los planes. El proceso de planeación debería enfocarse en los objetivos comerciales requeridos. Por ejemplo, restaurar los servicios de comunicación específicos a los clientes en una cantidad de tiempo aceptable. Se deberían identificar los servicios y los recursos que facilitan esto. Incluyendo personal, recursos de procesamiento no-información. Así como los arreglos de contingencia para los medios de procesamiento de información. Estos arreglos de contingencia pueden incluir acuerdos con terceros en la forma de acuerdos recíprocos, o servicios de suscripción comercial.

Los planes de continuidad del negocio deberían tratar las vulnerabilidades organizacionales y, por lo tanto, pueden contener información confidencial que necesita protegerse

apropiadamente. Las copias de los planes de continuidad del negocio se deberían almacenar en locales remotos, a una distancia suficiente para escapar de cualquier daño de un desastre en el local principal. La gerencia debería asegurarse que las copias de los planes de continuidad del negocio estén actualizadas y protegidas con el mismo nivel de seguridad aplicado en el local principal. Otro material necesario para ejecutar los planes de continuidad también debería almacenarse en el local remoto.

Si se utilizan ubicaciones temporales alternativas, el nivel de los controles de seguridad implementados en esos locales debería ser equivalente al de los controles del local principal.

Información adicional. Se debería notar que estos planes y actividades de gestión de crisis pueden ser diferentes a los de la gestión de la continuidad del negocio. Es decir, puede ocurrir una crisis que puede ser acomodada por los procedimientos gerenciales normales.

Marco Referencial de la planeación de la continuidad del negocio. Control. Se debería mantener un solo marco referencial de los planes de continuidad del negocio para asegurar que todos los planes sean consistentes, tratar consistentemente los requerimientos de seguridad de la información e identificar las prioridades para la prueba y el mantenimiento (Mora Prada, Quintero Mejia, & Camargo Ttigos, 2013).

Guía de implementación. Cada plan de continuidad comercial describe el enfoque para la continuidad, por ejemplo el enfoque para asegurar la disponibilidad y seguridad de la información o sistema de información. Cada plan también debería especificar el plan de

intensificación y las condiciones para la activación, así como las personas responsables de ejecutar cada componente del plan.

Con los nuevos requerimientos identificados, cualquier procedimiento de emergencia existente. Por ejemplo, los planes de evacuación o arreglos de emergencia. Debería ser enmendado conforme sea apropiado. Los procedimientos deberían incluirse dentro del programa de gestión de cambio de la organización para asegurar que los ítems de continuidad del negocio siempre sean tratados apropiadamente (Mora Prada, Quintero Mejia, & Camargo Ttigos, 2013).

2.5 Marco legal.

Constitución Política de 1991. En los artículos 209 y 269 se fundamenta el sistema de control interno en el Estado Colombiano, el primero establece: "La administración pública, en todos sus órdenes, tendrá un control interno que se ejercerá en los términos que señale la ley" y en el 269, se soporta el diseño del sistema: "En las entidades públicas, las autoridades correspondientes están obligadas a diseñar y aplicar, según la naturaleza de sus funciones, métodos y procedimientos de control interno, de conformidad con lo que disponga la ley, la cual podrá establecer excepciones y autorizar la contratación de dichos servicios con empresas privadas colombianas".

Ley estatutaria 1266 del 31 de diciembre de 2008. Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos

personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

Ley 1273 del 5 de enero de 2009. Delitos informáticos. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Ley 1341 del 30 de julio de 2009. Por la cual se definen los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.

Ley estatutaria 1581 de 2012. Entró en vigencia la Ley 1581 del 17 de octubre 2012 de protección de datos personales, sancionada siguiendo los lineamientos establecidos por el Congreso de la República y la Sentencia C-748 de 2011 de la Corte Constitucional.
Como resultado de la sanción de la anunciada ley toda entidad pública o privada, cuenta con un plazo de seis meses para crear sus propias políticas internas de manejo de datos personales, establecer procedimientos adecuados para la atención de peticiones, quejas y reclamos, así como ajustar todos los procesos, contratos y autorizaciones a las disposiciones de la nueva norma.
Aspectos claves de la normatividad:

Cualquier ciudadano tendrá la posibilidad de acceder a su información personal y solicitar la supresión o corrección de la misma frente a toda base de datos en que se encuentre registrado.

Establece los principios que deben ser obligatoriamente observados por quienes hagan uso, de alguna manera realicen el tratamiento o mantengan una base de datos con información personal, cualquiera que sea su finalidad.

Aclara la diferencia entre clases de datos personales construyendo las bases para la instauración de los diversos grados de protección que deben presentar si son públicos o privados, así como las finalidades permitidas para su utilización.

Crea una especial protección a los datos de menores de edad.

Establece los lineamientos para la cesión de datos entre entidades y los procesos de importación y exportación de información personal que se realicen en adelante.

Define las obligaciones y responsabilidades que empresas de servicios tercerizados tales como Call y Contact Center, entidades de cobranza y, en general, todos aquellos que manejen datos personales por cuenta de un tercero, deben cumplir en adelante.

Asigna la vigilancia y control de las bases de datos personales a la ya creada Superintendencia Delegada para la Protección de Datos Personales, de la Superintendencia de Industria y Comercio.

Crea el Registro Nacional de Bases de Datos.

Establece una serie de sanciones de carácter personal e institucional dirigidas a entidades y funcionarios responsables del cumplimiento de sus lineamientos.

Ley 603 de 2000. Esta ley se refiere a la protección de los derechos de autor en Colombia. Recuerde: el software es un activo, además está protegido por el Derecho de Autor y la Ley 603 de 2000 obliga a las empresas a declarar si los problemas de software son o no legales.

Ley 734 de 2002, Numeral 21 y 22 del Art. 34, son deberes de los servidores Públicos "vigilar y salvaguardar los bienes y valores que le han sido encomendados y cuidar que sean utilizados debida y racionalmente", y "responder por la conservación de los útiles, equipos, muebles y bienes confiados a su guarda o administración y rendir cuenta oportuna de su utilización".

Artículo 175. La Unidad de Almacén e Inventarios es la encargada de la planificación, programación y manejo de los elementos, equipos, bienes y suministros para el desarrollo de las actividades propias de la Universidad.

Artículo 176. Funciones de la Unidad de Almacén e Inventarios.

Las normas que rigen un Plan de Continuidad del Negocio son: BSI 25999 Parts 1 and 2 Business Continuity Management. Se trata de una norma certificable en la que se tiene como objeto la gestión o plan de continuidad del negocio fundamentalmente enfocado a la disponibilidad de la información, uno de los activos más importantes hoy en día para cualquier organización. La norma se creó ante la necesidad de que actualmente tienen las organizaciones de implementar mecanismos y técnicas, que minimicen los riesgos a los que se está expuesta, para conseguir una alta disponibilidad de las actividades de su negocio. La norma consiste en una serie de «recomendaciones o buenas prácticas» para facilitar la recuperación de los recursos que permiten el funcionamiento normal de un negocio, en caso de que ocurra un desastre. En este contexto, se tienen en cuenta tanto los recursos humanos, como las infraestructuras, la

información vital, las tecnologías de la información y los equipos que la soportan (Criado Ramirez, Lobo Ruedas, Meneses Arias, Pacheco Solano, & Prado Carrascal, 2014).

NIST 800-34, Contingency Planning Guide for Information Technology (IT). El Laboratorio de Tecnologías de la Información (DIT) del Instituto Nacional de Estándares y Tecnología (NIST) promueve la economía de EE.UU. y el bienestar público, proporcionando liderazgo técnico para la medición de la nación y la infraestructura de las normas. ITL desarrolla pruebas, métodos de prueba, datos de referencia, la prueba de las implementaciones de concepto, y el análisis técnico para avanzar en el desarrollo y uso productivo de las tecnologías de la información. Responsabilidades de ITL incluyen el desarrollo de técnicas, físicas, normas y directrices para la seguridad económica y la privacidad de la información sensible no clasificada en los sistemas informáticos federales administrativos y de gestión. Esta publicación especial los informes de la serie 800 en la investigación de ITL, orientación y divulgación esfuerzos en seguridad informática y de sus actividades de colaboración con la industria, el gobierno y organizaciones académicas (Criado Ramirez, Lobo Ruedas, Meneses Arias, Pacheco Solano, & Prado Carrascal, 2014).

ITIL Continuity Management, IT Security and Availability Management. La Tecnología de la Información Biblioteca de Infraestructura de TI (ITIL) es un conjunto de prácticas para la gestión de servicios de TI (ITSM) que se centra en la adaptación de los servicios de TI con las necesidades del negocio. En su forma actual (conocido como ITIL edición 2011), ITIL se publica en una serie de cinco publicaciones principales, cada uno de los cuales cubre una etapa del ciclo de vida de ITSM. ITIL sustenta la norma ISO / IEC 20000 (anteriormente

BS15000), la Norma Internacional de Gestión de Servicios para la gestión de servicios de TI, aunque las diferencias entre los dos marcos existen. ITIL describe los procesos, procedimientos, tareas y listas de control que no son específicos de cada organización, utilizados por una organización para establecer la integración con la estrategia de la organización, la entrega de valor y el mantenimiento de un nivel mínimo de competencia. Esto permite a la organización para establecer una línea de base desde la que se puede planificar, implementar y medir. Se utiliza para demostrar el cumplimiento y para medir la mejora (Criado Ramirez, Lobo Ruedas, Meneses Arias, Pacheco Solano, & Prado Carrascal, 2014).

ISO/PAS 22399:2007 Incident preparedness and operational continuity management. Proporciona la dirección general de una organización - las organizaciones privadas, gubernamentales y no gubernamentales - para desarrollar sus propios criterios de rendimiento específicos de preparación para incidentes y continuidad operativa, y el diseño de un sistema de gestión apropiado. Proporciona una base para la comprensión, desarrollo e implementación de la continuidad de las operaciones y servicios dentro de una organización y para proporcionar la confianza en los negocios, la comunidad, los clientes, primero en responder, y de organización interacciones. También permite a la organización para medir su capacidad de recuperación de una manera consistente y reconocida (Criado Ramirez, Lobo Ruedas, Meneses Arias, Pacheco Solano, & Prado Carrascal, 2014).

Capítulo 3. Diseño metodológico

3.1 Tipo de Investigación.

La investigación cualitativa o metodología cualitativa es un método de investigación usado principalmente en las ciencias sociales que se basa en cortes metodológicos basados en principios teóricos tales como la fenomenología, hernenéutica, la interacción social empleando métodos de recolección de datos que son no cuantitativos, con el propósito de explorar las relaciones sociales y describir la realidad tal como la experimentan los correspondientes.

La investigación cualitativa requiere un profundo entendimiento del comportamiento humano y las razones que lo gobiernan. A diferencia de la investigación cuantitativa, la investigación cualitativa busca explicar las razones de los diferentes aspectos de tal comportamiento. En otras palabras, investiga el por qué y el cómo se tomó una decisión, en contraste con la investigación cuantitativa la cual busca responder preguntas tales como cuál, dónde, cuándo. La investigación cualitativa se basa en la toma de muestras pequeñas, esto es la observación de grupos de población reducidos, como salas de clase, etc.

3.2 Población y muestra.

Para este proyecto, la Subdirección Académica estuvo conformada por el subdirector académico, dos profesionales de apoyo y dos secretarias, quienes realizarán su aporte, brindando información útil para los procesos de gestión académica y la comunidad estudiantil.

3.3 Técnicas para la recolección de la información.

Como técnica de indagación directa se utilizó la observación documental siendo el más viable para el desarrollo de los objetivos y el instrumento de recolección de información más importante que consiste en el registro sistemático, válido y confiable de comportamientos o conducta manifiesta.

3.4 Procesamiento de la información recolectada.

Teniendo en cuenta la información recolectada esta fue presentada de forma cualitativa describiendo cada uno de los aspectos relevantes para la investigación y desarrollo de los objetivos.

Capítulo 4. Presentación de resultados

4.1 Aplicar una auditoria pasiva en la subdirección académica para conocer el estado actual de los procesos que se llevan.

La información es un recurso que, como el resto de los activos, tiene valor para el Organismo y por consiguiente debe ser debidamente protegida. Las Políticas de Seguridad de la Información protegen a la misma de una amplia gama de amenazas, a fin de garantizar la continuidad de los sistemas de información, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos del Organismo. Para esto, se debe asegurar un compromiso manifiesto de las máximas Autoridades de la institución, tanto de la dependencia como de las TIC`S en la entidad, consolidación y cumplimiento de la Política diseñada, con el objetivo de proteger los recursos de información de la institución y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

Después de aplicar la auditoria pasiva en la subdirección académica se evidencia que las actividades de los docentes de planta que se encuentren en periodo de prueba son organizadas por los Departamentos al cual pertenece el docente.

Mediante oficio el Consejo de Facultad, presenta a la Dirección de manera justificada la necesidad del docente que no puede ser suplida por los docentes que conforman la base de datos

de docentes Catedráticos y Tutores, o no se cuenta con docentes en áreas específicas del conocimiento.

El Consejo Superior Universitario otorga a través de Acuerdo Comisión de Estudio a los docentes que soliciten estudios de Doctorado y Posdoctorado donde se evidencia los compromisos que los docentes deben cumplir para hacerse acreedor a la comisión.

Para realizar la inscripción de un programa de posgrado se diligencia el formulario en línea a través de la página Web de la UFPS y el aspirante cumplirá con los requisitos que se establezcan según el programa.

Los Departamentos Académicos definen los perfiles; con lo cual se establece a través de la Subdirección Académica la Convocatoria de concurso público de méritos docentes tiempo completo y se organiza el cronograma que se publica en página y es establecido en la presente Resolución.

Publicaciones de convocatoria de concurso docente en el sitio web de la universidad y la inscripción se hace el portal habilitado para tal fin

Programas que oferta posgrado en modalidad presencial y virtual, inscripciones en línea en la página Web de la universidad con el cumplimiento de los requisitos exigidos.
Cumple los lineamientos del Decreto para la presentación de programas nuevos al Ministerio para obtención del Registro calificado.

Con la creación de la Unidad Virtual cuyo propósito principal es el desarrollo de la estrategia virtual al interior de la institución que permite integrar el uso de las TIC en los procesos académicos. Apoyo a la creación de programas virtuales, al desarrollo de recursos educativos virtuales.

El estudiante que se encuentra en esta condición solicita al Comité de Apoyo Académico, a través de un oficio la aplicación del Acuerdo 112/2012, para levantamiento de ceros. El comité de Apoyo Académico, analiza la situación del estudiante y emite respuesta de aprobación, que oficia al mismo, para que cancele el costo respectivo y trámite la matricula en la oficina de Admisiones, Registro y control.

Cada plan de estudios realiza solicitud de asignación de carga académica a los Departamentos. El Departamento revisa la base de datos y asigna a los docentes. Los departamentos en el F-AC-SAC-017 registran la carga la cual se aprueba en acta. Luego se radica la asignación de carga por departamentos en las oficinas de Subdirección, Personal y Control Interno.

Los Departamentos asignación la vinculación de docentes ocasionales y el proceso se realiza con la convocatoria a través de la oficina de personal.

La Subdirección Académica y la Oficina de Personal, definen los Lineamientos establecidos según el Acuerdo 005/2011, para realizar convocatoria abierta para conformar la

base de datos de docentes catedráticos y/o tutores, que servirá de soporte a los Departamentos para escoger por áreas sus respectivos docentes.

Se estructuran los documentos Maestros con los lineamientos que trata el Decreto 1295 para la oferta y desarrollo de programas académicos de educación superior.
Formato de solicitud de traslado F-AC-SAC-003.

A través de Actas de Comité de Apoyo Académico, se evidencia la publicación de los puntajes de los aspirantes al concurso docente, donde aplica lo estipulado en el Acuerdo.
Actas del consejo académico donde se definen los perfiles para abrir convocatoria docentes de planta de la seccional.

Se reúnen los Acuerdos 133 de 22/12/1994; Acuerdo 025/04/1995; Acuerdo 104/12/1993; Acuerdo 071/09/1998; Acuerdo 073/09/1999; que con el fin de brindar seguridad jurídica en torno a las normas que rigen la Universidad, se hace necesario actualizar el texto del Acuerdo 091/12/1993.

Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad, asegurando de esta forma la continuidad del negocio.

Aprobar las principales iniciativas para incrementar la seguridad de la información, de acuerdo a las competencias y responsabilidades asignadas a cada área.

Teniendo en cuenta lo anterior se debe dar una especial importancia a la información y la continuidad del negocio siendo estas dos preocupaciones muy importantes para la dependencia de subdirección académica, sin importar su tamaño. El perder datos o tener que cerrar operaciones por alguna contingencia puede representar altos costos para la organización. Una forma de asegurar la continuidad del negocio es a través de normas y el aseguramiento de la información que permite a la dependencia resistir el problema, levantarse y seguir operando, mientras que el resto de la entidad tienen la necesidad de parar operaciones por no estar preparado, lo que permite un crecimiento de la dependencia mientras se aprovecha la contingencia.

Por lo que es necesario en la dependencia proteger el equipamiento de procesamiento de información crítica del Organismo ubicándolo en áreas protegidas y resguardadas por un perímetro de seguridad definido, con medidas de seguridad y controles de acceso apropiados.

Impedir el acceso no autorizado a los sistemas de información, bases de datos y servicios de información. Implementar seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización. Controlar de mejor forma la seguridad en conexiones entre la División de TIC y los proveedores externos. Mantener un registro de eventos y actividades críticas llevadas a cabo por los usuarios en los sistemas.

Adquisición, desarrollo y mantenimiento de sistemas de Información. En este control se deben revisar las aplicaciones como puntos críticos de vulnerabilidades, es necesaria una adecuada administración de la infraestructura de base, Sistemas Operativos y Software de Base,

en las distintas plataformas, para asegurar una correcta implementación de la seguridad, ya que en general los aplicativos se asientan sobre este tipo de software.

Gestión de Incidentes de Seguridad de la Información. Divulgación de eventos y de debilidades de la seguridad de la información. Es importante que la División de TIC tenga un procedimiento a seguir cuando se presente un incidente de seguridad en la red, pues es necesario que pueda aprender de los errores y evitar que un ataque ocurra.

Implementación del Plan de Tratamiento de Riesgos. El objetivo de esta etapa es tomar la acción más apropiada de tratamiento para cada uno de los riesgos identificados, en base a las secciones. Identificación de amenazas e identificación de vulnerabilidades.

4.2 Estrategias que permitan la continuidad de los procesos de la Subdirección Académica, para consignarlas en un plan de gestión de la continuidad.

En la gestión de la continuidad de los procesos de la subdirección académica se deben controlar riesgos que podrían impactar seriamente los servicios. La Gestión de la Continuidad del Servicio de TI (IT Service Continuity Management, ITSCM) se ocupa de que el proveedor de servicios de TI siempre pueda proveer un mínimo nivel del servicio propuesto reduciendo el riesgo de eventos desastrosos hasta niveles aceptables y planificando la recuperación de servicios de TI. Por lo que a continuación se proponen algunas estrategias que pueden ayudar a asegurar la continuidad del negocio.

No hacer nada: Este tipo de actuación podría utilizarse en aquellas funciones o actividades que se han clasificado como “no urgentes” en el Análisis de Impacto. En este tipo de estrategia se asume el riesgo.

Reutilización de recursos: Reubicación de personal con funciones no urgentes en tareas que requieren una mayor prioridad. En este caso se debe poner cuidado en convertir la función no urgente en urgente por ser desatendida durante demasiado tiempo.

Trabajo Remoto o Teletrabajo: Posibilidad de trabajar desde ubicaciones exteriores a la compañía mediante conexión remota.

Acuerdos Recíprocos: Acuerdos entre dos dependencias con características de equipamiento/espacio similares que permitiría a cada una de las partes recuperar funciones en la otra localización. En este caso es importante definir las condiciones de uso y la realización de pruebas periódicas para asegurar las condiciones pactadas.

Sitio alternativo subcontratado a terceros: Contratación con empresas especializadas de espacios alternativos para la recuperación de la actividad. En este caso hay que asegurar que estas pueden proporcionar unos tiempos de recuperación acordes con las necesidades de la organización. Este tipo de empresas pueden proporcionar diferentes soluciones:

- Espacio dedicado: Se garantiza la disponibilidad inmediata del espacio. En contrapartida este servicio es más caro que otras alternativas.
- Espacio compartido: Se comparte el espacio con otras dependencias. Es más barato que un centro dedicado.
- Espacios móviles: Se pueden utilizar rápidamente, pero tienen un espacio limitado.

Localizaciones diversas: Se traslada la operación pero no el personal.

Centro replicado: Solución que permite trasladar de forma inmediata la operación y continuar la actividad de forma inmediata. También puede denominarse “centro espejo”. Esta solución es normalmente la más cara, pero también la mejor solución en el caso de que se necesite una recuperación muy rápida de la operación.

Plan de gestión de la continuidad propuesto. Para llegar a este punto es necesario haber definido y establecido, el conocimiento de los procesos y servicios de la dependencia, valorando cuales son los críticos para el funcionamiento de esta, valoración de los riesgos que pueden afectar los procesos y que pueden propiciar para el plan de continuidad de negocio y la estrategia de continuidad más adecuada para el negocio. A partir de estos insumos se desarrolla el plan de continuidad que constara de:

Los equipos necesarios para el desarrollo del plan.

Las responsabilidades y funciones de cada uno de los equipos.

El desarrollo de los procedimientos de alerta y actuación ante eventos que puedan activar el plan.

Los procedimientos de actuación ante incidentes.

La estrategia de vuelta a la normalidad.

Organización de los equipos. Los equipos de emergencia están formados por el personal clave necesario en la activación y desarrollo del plan de Continuidad. Cada equipo tiene unas funciones y procedimientos que tendrán que desarrollar en las distintas fases del plan. Aunque la composición y número de equipos puede variar según el tipo de estrategia de recuperación, para

la necesidad se deben conformado los siguientes equipos que pueden formar parte del Plan de continuidad:

Equipo de crisis: Encargado de dirigir las acciones durante la contingencia y recuperación. El objetivo de este comité es reducir al máximo el riesgo y la incertidumbre en la dirección de la situación. Este equipo debe tomar las decisiones "clave" durante los incidentes, además de hacer de enlace con la dirección de la dependencia, manteniéndoles informados de la situación regularmente. Las principales tareas y responsabilidades de este comité son:

- Análisis de la situación.
- Decisión de activar o no el Plan de Continuidad.
- Iniciar el proceso de notificación a los empleados a través de los diferentes responsables.

Cuando se comunica un incidente el equipo de crisis, deberá reunirse y tomar la decisión para afrontar la situación. Deben estar continuamente informados de la situación y determinar si será necesario iniciar con el plan de continuidad y comunicar hacia los responsables de los demás grupos el comienzo de las actividades acuerdo a lo planeado para la restauración.

Equipo de recuperación: Su función es restablecer todos los sistemas necesarios (voz, datos, comunicaciones, etc.). El equipo de recuperación es responsable de establecer la infraestructura necesaria para la recuperación. Esto incluye todos los servidores, PC's, comunicaciones de voz y datos y cualquier otro elemento necesario para la restauración de un servicio. De igual forma está encargado de proceder con las actividades de recuperación con el

fin de poner en marcha los servicios críticos afectados, ya sea activando el plan de contingencias interno, o activando los servicios desde el data center alterno.

Equipo logístico: Responsable de toda la logística necesaria en el esfuerzo de recuperación. Este equipo es responsable de todo lo relacionado con las necesidades logísticas en el marco de la recuperación, tales como:

- Transporte de material y personas (si es necesario) al lugar de recuperación.
- Soporte técnico para las operaciones de recuperación.
- Realizar el trabajo en conjunto con los demás para asegurar que todas las necesidades logísticas sean cubiertas.

El equipo de logística es responsable de todo lo relacionado con las necesidades logísticas, es decir en caso de un incidente este equipo de encargar de:

Atender necesidades logísticas, transporte de personas, transportes de servidores, switches, o cualquier elemento físico necesario para la recuperación.

Contactar con los proveedores para solicitar el material necesario que indiquen los responsables de la recuperación.

Gestionar el suministro de comida al personal involucrado.

El equipo de pruebas básicamente está encargado por velar de que lo implementado esté funcionando de acuerdo al plan establecido, realizando puntos de control y verificando mediante pruebas que los servicio están en un punto normal.

El equipo de Relaciones Públicas es responsable de “ser la voz” de la asesoría en el contexto de la contingencia. Las tareas a realizar serán:

Si el tipo de incidente lo requiere, emitir un comunicado oficial a clientes y proveedores en el que se indique que se restablecerán los servicios lo antes posible.

Atender a los clientes para proporcionarles información sobre el incidente y tranquilizarles lo máximo posible

Etapas de alerta del plan. Las fases de alerta del plan de recuperación se desarrollaran según la organización de los equipos y funciones establecidas por cada uno de los funcionarios, y deberán seguir los procedimientos establecidos por las siguientes fases del plan.

Etapa de alerta. Procedimiento de notificación del desastre. Cualquier funcionario de la dependencia que sea consciente de un incidente grave que pueda afectar a alguno de los servicios de la asesoría de informática y telemática, debe comunicarlo al ingeniero de Seguridad, el asesor de informática y telemática o cualquiera de los funcionarios de este proporcionando el mayor detalle posible en la descripción de los hechos. El ingeniero debe evaluar la situación e informar al equipo de Crisis, que en este caso coincide con la figura del asesor. Procedimiento de ejecución del plan. El equipo de Crisis reunido en el punto de encuentro evaluará la situación.

Con toda la información de detalle sobre el incidente, se decidirá si se activa o no el Plan de Continuidad de Negocio. En caso de ser afirmativo, se iniciará el procedimiento de ejecución del Plan. En el caso de que el equipo decidida no activar el Plan de Continuidad porque la gravedad del incidente no lo requiere, sí será necesario gestionar el incidente para que no

aumente su gravedad. Procedimiento de notificación de ejecución del plan. Activar el árbol de llamadas para avisar a los integrantes de los diferentes equipos que van a participar en el Plan.

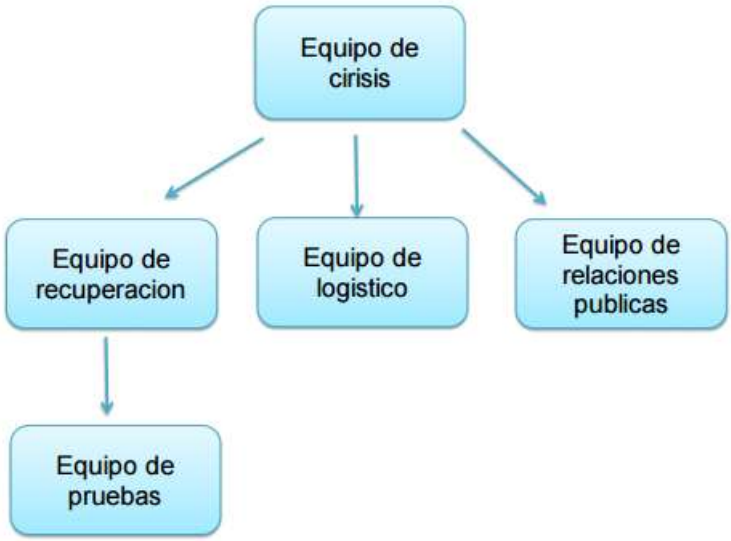

Figura 4. Procedimiento de notificación de ejecución del plan

Fuente. Autores del proyecto

Etapa de transición. Procedimiento de concentración y traslado de material y personas. Una vez avisados los equipos y puesto en marcha el Plan, deberán acudir al punto de reunión indicado en caso de que haya ocurrido un incidente grave que lo deje inoperante. Además del traslado de personas al punto, hay que trasladar todo el material necesario para poner en marcha el centro de recuperación (cintas de backup, material de oficina, manuales de operaciones, documentación). Esta labor queda en manos del equipo logístico. Procedimiento de puesta en marcha del centro de recuperación, estos procedimientos se dividirán en dos en un plan alterno de operación y una interna en caso de que el incidente sea más controlable:

Establecer el Plan alterno de operación (PAO), con el presente plan se permitirá la continuidad de la operación de los servicios críticos, en situaciones de contingencia que no sea posible acceder. Coordinar las actividades operativas requeridas para asegurar el registro de la información generada durante una situación de contingencia, al restaurar la plataforma tecnológica que soporta la asesoría de informática y telemática. Los escenarios posibles para este tipo de plan serian lo siguientes:

- Se pierde todo tipo de comunicación con las dependencias.
- Daño física en las instalaciones del centro de datos de la asesoría de informática, causadas por fenómenos naturales como fuego, terremotos, revueltas, sabotaje.
- Falla eléctrica en las instalaciones.
- Imposibilidad de ingreso a la dependencia.

En base de la necesidad de una contingencia interna se ha diseñado un nuevo plan de contingencia que asegure la disponibilidad de todos los servicios, el esquema es el siguiente:

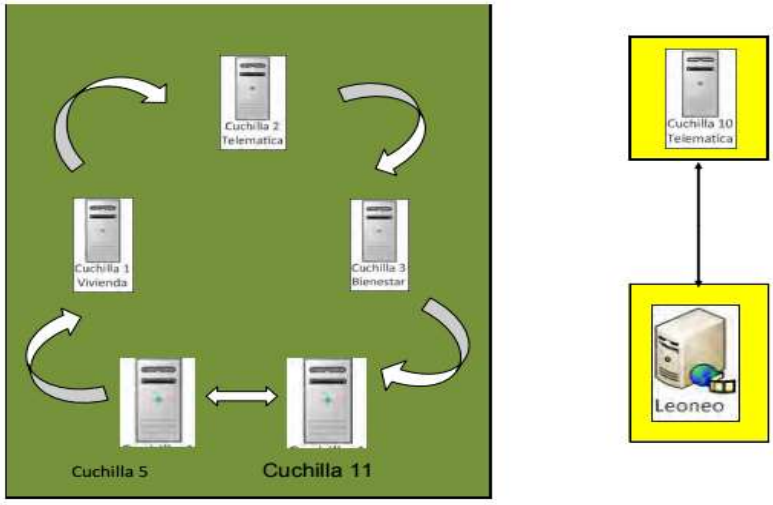

Figura 5. Mapa de contingencia futuro.

Fuente. Autores del proyecto

Como se observa en la figura 2 ahí una eficiencia en la optimización de recursos ya que no se utilizaran tantos servidores, para alojar los servicios, en cambio se contemplan 5 cuchillas tipo blade virtualizadas en donde cada una sirve de contingencia y está respaldada de las otras 4.

Etapa de recuperación. El orden de recuperación de las funciones se realizará según la criticidad los sistemas es: Orfeo, correo institucional, canal de Internet, intranet. El servicio de Orfeo debe recuperarse lo antes posible, en 1 hora a más tardar. Los demás servicios pueden empezar a recuperarse después de Orfeo en el orden secuencial y los tiempos establecidos de RTO. Procedimiento de soporte y gestión. Una vez recuperados los sistemas, se avisará a los equipos que gestionan los sistemas para que realicen las comprobaciones necesarias que certifiquen que funcionen de manera correcta y pueda continuarse dando el servicio.

Además el equipo de Seguridad, deberá comprobar que existen las garantías de seguridad necesarias (confidencialidad, integridad, disponibilidad) antes de dar por terminada la fase de recuperación. Procedimientos Preventivos y Correctivos. Una vez con los procesos críticos en marcha y solventada la contingencia, debemos plantearnos las diferentes estrategias y acciones para recuperar la normalidad total de funcionamiento. Para ello se debe dividir esta fase en diferentes procedimientos:

Realizar una valoración a los equipos e instalaciones dañadas por el incidente para volver a definir una estrategia temporal.

Procedimientos de vuelta a la normalidad, una vez determinado el impacto del incidente deberá establecer los mecanismos que en la medida de lo posible lleven a recuperar la normalidad total del funcionamiento. Estas acciones pueden incluir compra de los equipos, servidores, materiales dañados, entre otros.

4.3 Establecer los posibles riesgos para los activos de información en la subdirección Académica.

La tendencia del mundo actual a emplear nuevos mecanismos para hacer negocios, a contar con información actualizada permanentemente que permita la toma de decisiones, ha facilitado el desarrollo de nuevas tecnologías y sistemas de información, que a su vez son vulnerables a las amenazas informáticas crecientes y por ende a nuevos riesgos. En la dependencia de la subdirección académica y pensando en la seguridad de los estudiantes y funcionarios, se exponen las principales amenazas informáticas y los posibles riesgos que podrían materializarse, para evitar que su información caiga en manos inescrupulosas o sea víctima de fraude electrónico.

SPAM Son mensajes no solicitados, habitualmente de tipo publicitario, enviados en forma masiva. La vía más utilizada es la basada en el correo electrónico (SPAM) pero puede presentarse por programas de mensajería instantánea (SPIM) , por teléfono celular (SPAM SMS), por telefonía IP (SPIT) ; el objetivo de esta amenaza es recolectar direcciones de correo electrónico reales para obtener beneficios económicos, transmitir de virus, capturar de contraseñas mediante engaño (phisihing), entre otros.

Recomendaciones.

• No enviar mensajes en cadena ya que los mismos generalmente son algún tipo de engaño (hoax).

• Cuando necesite enviar un email por internet a varios destinatarios, es recomendable hacerlo con la opción con copia oculta con copia oculta con copia oculta (CCC), ya que esto evita que un destinatario vea, o se apodere, del email de los demás destinatarios.

• No publicar una dirección privada en sitios webs, foros, conversaciones online, etc., ya que sólo facilita la obtención de las mismas a los spammers (personas que envían spam).

• Si desea navegar o registrarse en sitios de baja confianza hágalo con cuentas de e-mails destinadas para tal fin.

• Nunca responder este tipo de mensajes ya que con esto sólo estamos confirmando nuestra dirección de e-mail y sólo lograremos recibir más correo basura.

• Es bueno tener más de una cuenta de correo (al menos 2 o 3): una cuenta laboral que sólo sea utilizada para este fin, una personal y la otra para contacto público o de distribución masiva.

De otra parte se debe tener en cuenta mecanismos de control dentro de la norma agrupa todo el conjunto de acciones, documentos, procedimientos y medidas técnicas adoptadas para garantizar que cada amenaza, identificada y valorada con un cierto riesgo, sea minimizada. Dichos controles se presentan para reducir el riesgo se necesita la mejora de Salvaguardas existentes o la incorporación de otras nuevas. Se define la función o servicio de salvaguarda como la acción que reduce el riesgo; el mecanismo de salvaguarda como dispositivo, físico o lógico, capaz de reducir el riesgo y opera bien de forma preventiva sobre la vulnerabilidad.

Para complementar lo anterior en la subdirección académica, se realizó la evaluación de posibles riesgos que se pueden presentar para lo cual se tuvo en cuenta varias categorías como son:

G: Gestión.

T: Técnico.

P: Personal.

F: Seguridad física.

De igual forma las normas ISO/IEC 27001, ISO/IEC 27002 están enfocadas a todo tipo de organizaciones (por ej. empresas comerciales, agencias, gubernamentales, organizaciones sin ánimo de lucro), tamaños (pequeña, mediana o gran empresa), tipo o naturaleza. Por lo que los controles pueden ser:

Políticas. Basándose en el contexto en el que opera una organización y suelen ser considerados en su redacción los fines y objetivos de la organización, las estrategias adoptadas para alcanzar sus objetivos, la estructura y los procesos adoptados por la organización, los objetivos generales y específicos relacionados con el tema de la política y requisitos de las políticas procedentes de niveles más superiores.

Se debe tener en cuenta la política de alto nivel (más genérica) habitualmente relacionada con el sistema de gestión para la seguridad de la información (SGSI) suele estar apoyada por políticas de bajo nivel, específicas a aspectos concretos en temáticas como el control de accesos, la clasificación de la información, la seguridad física y ambiental, uso aceptable de activos,

escritorio y pantallas libres de información sensible, dispositivos móviles y teletrabajo, backups, protección contra el malware.

En cuanto al recurso humano de la dependencia se le debe explicitar las responsabilidades en materia de seguridad en la etapa de reclutamiento de personal e incluirlas en los acuerdos a firmarse y verificar su cumplimiento durante el desempeño del individuo como empleado, así como, garantizar que los usuarios estén al corriente de las amenazas e incumbencias en materia de seguridad de la información, y se encuentren capacitados para respaldar la Política de Seguridad de la organización en el transcurso de sus tareas normales.

Físico y ambiental. El objetivo es minimizar los riesgos de daños e interferencias a la información y a las operaciones de la organización. El establecimiento de perímetros de seguridad y áreas protegidas facilita la implementación de controles de protección de las instalaciones de procesamiento de información crítica o sensible de la organización, contra accesos físicos no autorizados. El control de los factores ambientales de origen interno y/o externo permite garantizar el correcto funcionamiento de los equipos de procesamiento y minimizar las interrupciones de servicio.

La información almacenada en los sistemas de procesamiento y la documentación contenida en diferentes medios de almacenamiento, son susceptibles de ser recuperadas mientras no están siendo utilizados. Es por ello que el transporte y la disposición final presentan riesgos que deben ser evaluados, especialmente en casos en los que el equipamiento perteneciente a la

organización estén físicamente fuera del mismo (housing) o en equipamiento ajeno que albergue sistemas y/o preste servicios de procesamiento de información (hosting/cloud).

Continuidad negocio. El objetivo es preservar la seguridad de la información durante las fases de activación, de desarrollo de procesos, procedimientos y planes para la continuidad de negocio y de vuelta a la normalidad. Se debería integrar dentro de los procesos críticos de negocio, aquellos requisitos de gestión de la seguridad de la información con atención especial a la legislación, las operaciones, el personal, los materiales, el transporte, los servicios y las instalaciones adicionales, alternativos y/o que estén dispuestos de un modo distinto a la operativa habitual.

Se deberían analizar las consecuencias de los desastres, fallas de seguridad, pérdidas de servicio y la disponibilidad del servicio y desarrollar e implantar planes de contingencia para asegurar que los procesos del negocio se pueden restaurar en los plazos requeridos las operaciones esenciales, manteniendo las consideraciones en seguridad de la información utilizada en los planes de continuidad y función de los resultados del análisis de riesgos.

Del mismos modo se debe llevar a cabo las pruebas pertinentes (tales como pruebas sobre el papel, simulacros, pruebas de failover, etc.) para (a) mantener los planes actualizados, (b) aumentar la confianza de la dirección en los planes y (c) familiarizar a los empleados relevantes con sus funciones y responsabilidades bajo condiciones de desastre. Minimizar los efectos de las posibles interrupciones de las actividades normales de la organización asociadas a desastres naturales, accidentes, fallas en el equipamiento, acciones deliberadas u otros hechos, protegiendo

los procesos críticos mediante una combinación de controles preventivos y acciones de recuperación. Instruir al personal involucrado en los procedimientos de reanudación y recuperación en relación a los objetivos del plan, los mecanismos de coordinación y comunicación entre equipos (personal involucrado), los procedimientos de divulgación en uso, los requisitos de la seguridad, los procesos específicos para el personal involucrado y responsabilidades individuales.

Para concluir y teniendo en cuenta lo anterior se debe mencionar que en la subdirección académica, se debe implementar la ISO 22301 teniendo en cuenta la importancia de la ISO 27001 que nos indica cómo gestionar la seguridad de la información de una empresa y la podemos tener en cuenta para dar buenos resultados en la continuidad del negocio y posteriormente aplicar los controles, para la protección de la información ya que contiene datos confidenciales, Protección de las comunicaciones para garantizar conectividad y también evitar la captura de datos a través de las redes de comunicaciones. La gestión de claves criptográficas para dar mayor seguridad al acceso a los recursos de información ya que se debe tener un mayor control de los funcionarios o personas que ingresan a las aplicaciones o equipos que guardan la información.

Capítulo 5. Conclusiones

La ISO 22301, es una norma que contempla todos los componentes para asegurar una alta disponibilidad de los procesos de cualquier organización sea pública o privada, en la cual se sigue un procedimiento desde el levantamiento de información de la organización hasta las alternativas de respaldo y planes de continuidad.

Con el análisis de riesgo se identificaron los riesgos altamente potenciales, es decir, están calificados como extremos después de la implementación del control, y aunque no se lograron mitigar, se sugiere implementar nuevos controles que ayuden a mitigar el impacto y/o la probabilidad y hacer un seguimiento más a menudo.

La continuidad del negocio no solo va orientado a los sistemas de información que se manejan en la dependencia como bien se sabe el activo principal de cualquier organización son las personas por lo tanto se debe considerar cuidar la integridad de estas que son los que alimentan los sistemas de información.

Capítulo 6. Recomendaciones

Como alternativas de respaldo, se recomienda la búsqueda de una solución e implementación de back up que asegure tener la información sincronizada en tiempo real de los servicios críticos.

Se recomienda realizar seguimiento constantemente ya que este siempre va a estar actualizándose y presentando cambios en nuevos servicios críticos, tiempos de respuesta, nuevos controles y estrategias que representas acciones de mejora.

Se sugiere dar seguimiento a los tiempos de recuperación con indicadores que permitan identificar más fácilmente el cumplimiento de estos.

Referencias

Blanco Lindarte, J. A., Martínez Vega, L. F., Quintero Prado, C. d., & Rincon Angarita, J. F. (2015). Plan de continuidad para el centro de desarrollo e innovación tecnologica de la universidad Francisco de Paula Santander OcañaD . Ocaña.

Camelo, L. (2010). Seguridad de la Información en Colombia. Obtenido de http://seguridadinformacioncolombia.blogspot.com.co/2010/02/marco-legal-de-seguridad-de-la.html

Collazos Balaguer, M. (s.f.). Obtenido de file:///C:/Users/ufpso/Downloads/PRESENTACION_MANUEL_COLLAZOS_-_1.pdf

Coronel Ortiz, Y. A., Guevara Gelvez, R. A., Jaime Fernandez, J. C., & Salazar Rincon, R. D. (2013). Formulación de un documento que de soporte a la gestión de la seguridad física basada en la norma NTC- ISOIEC 27002 en el Centro de Investigación Tecnológico (CDIT) de la van Ocaña. Ocaña, Colombia. Obtenido de http://www.ufpso.edu.co/ftp/doc/otrospro/sitt/L-TT-DSS-002A.pdf.

Criado Ramirez, Y., Lobo Ruedas, M. P., Meneses Arias, J. L., Pacheco Solano, A. A., & Prado Carrascal, M. d. (2014). Gestión de continuidad del negocio para la unidad de almacen de la Universidad Francisco de paula Santander. Ocaña.

Garcia, J. M., & Guerra, J. (1997). Diseño organizativo de la empresa. Madrid: Editorial Civitas.

ISO 27000. (s.f.). Obtenido de http://www.iso27000.es/download/doc_iso27000_all.pdf

Juárez Najarro, A. R. (2011). Plan de continuidad TI en biblioteca central de la universidad de San Carlos de Guatemala. Guatemala: Universidad de San Carlos de Guatemala.

Mora Prada, L. M., Quintero Mejia, J., & Camargo Ttigos, M. F. (2013). http://www.ufpso.edu.co/ftp/doc/otrospro/sitt/L-TT-DSS-002A.pdf. Obtenido de Adaptación Diseño del Manual de Políticas de Seguridad de la Información basadas en la Norma ISO 27002 para el proceso de compras de la Universidad Francisco de Paula Santander.

Parra Casallas, J. (s.f.). Obtenido de http://openaccess.uoc.edu/webapps/o2/bitstream/10609/43114/6/jparracasaTFM0715memoria.pdf

Saez vargas, V. A. (2011). Modelo Integral para la implementación de un Plan de Continuidad de Negocio en Chile. Chile: Universidad Austral de Chile.

Secretaria Distrital del Ambiente. (3 de Diciembre de 2008). Informe de gestión. Obtenido de http://ambientebogota.gov.co/c/document_library/get_file?uuid=03cac9fc-97e9-4b37-acde-00b6eefa1a44&groupId=10157.

Sistemas de Gestión de seguridad de la información. (18 de Noviembre de 2014). ISO 27001: La Seguridad de la Información en la Gestión de la Continuidad de Negocio. Obtenido de http://www.pmg-ssi.com/2014/11/iso-27001-la-seguridad-de-la-informacion-en-la-gestion-de-la-continuidad-de-negocio/.

Tellez Mondragon, C. A. (2015). Diseñar un plan de plan de continuidad del negocio en el proceso de administración de recursos de TI de la oficina de informatica y telematica de la alcaldía de Santiago de Cali . Cali: UNIVERSIDAD AUTÓNOMA DE OCCIDENTE.

Trujillo, F. (2006). Direccionamiento estratégico CMAPS . Obtenido de http://cmc.ihmc.us/cmc2006Papers/cmc2006-p69.pdf.

Universidad Francisco de Paula Santander Ocaña. (2017). Historia. Obtenido de https://ufpso.edu.co.

Universidad Francisco de Paula Santander Ocaña. (2017). https://ufpso.edu.co/sub_academica. Obtenido de Subdirecion académica.

Zapata Atehortua, H. D., & Echeverry Barrera, C. C. (2011). Proceso de diagnóstico para la implementacion de estrategias de continuaidad del negocio en la direccion de oporaciones de UNE EPM Telecomunicaciones. Medellín: Universidad de Medellín.