RESUMEN - TESIS DE GRADO

AUTORES	**YONIT CRIADO RAMÍREZ** **MAGALY PATRICIA LOBO RUEDAS** **JESÚS LEONARDO MENESES ARIAS** **ANDRÉS ALFONSO PACHECO SOLANO** **MIRIAM DEL SOCORRO PRADO CARRASCAL**
FACULTAD	**DE INGENIERIAS**
PLAN DE ESTUDIOS	**ESPECIALIZACIÓN EN AUDITORÍA DE SISTEMAS**
DIRECTOR	**TORCOROMA VELÁZQUEZ PÉREZ**
TÍTULO DE LA TESIS	**GESTIÓN DE CONTINUIDAD DEL NEGOCIO PARA LA UNIDAD DE ALMACÉN DE LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA**

RESUMEN
(70 palabras aproximadamente)

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 Unidad de Almacén utiliza la tecnología de información como soporte a sus transacciones en el manejo de los inventarios, 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.

CARACTERÍSTICAS			
PÁGINAS: 143	PLANOS:	ILUSTRACIONES: 20	CD-ROM: 1

GESTIÓN DE CONTINUIDAD DEL NEGOCIO PARA LA UNIDAD DE ALMACÉN DE LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

YONIT CRIADO RAMÍREZ
MAGALY PATRICIA LOBO RUEDAS
JESÚS LEONARDO MENESES ARIAS
ANDRÉS ALFONSO PACHECO SOLANO
MIRIAM DEL SOCORRO PRADO CARRASCAL

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
FACULTAD DE INGENIERIAS
ESPECIALIZACIÓN EN AUDITORÍA DE SISTEMAS
OCAÑA
2014

GESTIÓN DE CONTINUIDAD DEL NEGOCIO PARA LA UNIDAD DE ALMACÉN DE LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

YONIT CRIADO RAMÍREZ
MAGALY PATRICIA LOBO RUEDAS
JESÚS LEONARDO MENESES ARIAS
ANDRÉS ALFONSO PACHECO SOLANO
MIRIAM DEL SOCORRO PRADO CARRASCAL

Proyecto de Grado Ppresentado como Requisito para optar al Título de Especialista en Auditoria de Sistemas

Director
TORCOROMA VELÁZQUEZ PÉREZ
Magister en Ciencias Computacionales

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
FACULTAD DE INGENIERIAS
ESPECIALIZACIÓN EN AUDITORÍA DE SISTEMAS
OCAÑA
2014

CONTENIDO

Pág.

LISTA DE FIGURAS

pág.

LISTA DE TABLAS

Pág.

LISTA DE ANEXOS

Pág.

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 Unidad de Almacén utiliza la tecnología de información como soporte a sus transacciones en el manejo de los inventarios, 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 Jefe de la Unidad de Almacén 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.

En la primera etapa se realizara el reconocimiento de la Unidad de Almacén dentro del contexto de la Universidad, identificando la cadena de valor de la dependencia, modelando sus procesos a través del BMM (Business Motivation Model), creando su estructura orgánica e identificando la Tecnología de Información (TI) presente en la Unidad de Almacén.

En la segunda etapa se creara un Manual de Gestión de Continuidad del Negocio según la Norma ISO/IEC 27002, 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.

En la tercera etapa se realizaran los procedimientos de emergencia que describen las acciones a realizarse antes, durante y después del incidente que pone en riesgo los procesos de la Unidad de Almacén de la UFPSO.

1. GESTIÓN DE CONTINUIDAD DEL NEGOCIO PARA LA UNIDAD DE ALMACÉN DE LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

1.1 PLANTEAMIENTO DEL PROBLEMA

La Gestión de la Continuidad del Negocio permite contrarrestar las interrupciones en las actividades del negocio y proteger sus procesos críticos contra los efectos de fallas importantes en los Sistemas de Información o contra desastres, y asegurar su recuperación oportuna.

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. Debido a que la Unidad de Almacén maneja la información de los elementos de consumo y del control de los inventarios, y se halla interconectada a la red de la Institución; esta se vería 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 (ver anexos).

Además, se pudo apreciar que actualmente dicha Unidad 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 una Gestión de Continuidad del Negocio 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 en el manejo de sus inventarios.

1.2 FORMULACIÓN DEL PROBLEMA

¿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?

1.3 OBJETIVOS DEL ESTUDIO

1.3.1 Objetivo General. Plantear la Gestión de Continuidad del Negocio para la Unidad de Almacén de la Universidad Francisco de Paula Santander Ocaña.

1.3.2 Objetivos Específicos. Realizar un reconocimiento de la estructura organizacional, el direccionamiento estratégico y componente tecnológico de la Unidad de Almacén.

Documentar procedimientos de Plan de Continuidad del Negocio, que permitan la prevención y protección de la integridad de las personas, instalaciones, equipos y documentos de la Universidad, en caso de emergencias o amenazas que las pongan en peligro.

Crear un manual de Gestión o Plan de Continuidad del Negocio para la Unidad de Almacén con base en la norma ISO/IEC 27002.

1.4 JUSTIFICACIÓN

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.

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 todo lo anterior, la Unidad de Almacén de la Universidad, 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 del desarrollo de la Gestión de Continuidad del Negocio, 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. Tomar acciones para responder de forma adecuada y a corto plazo definiendo estrategias y acciones de respuesta que conlleve a la continuidad del negocio, para minimizar el impacto.

1.5 HIPÓTESIS

Con la creación de un Manual de Gestión de Continuidad del Negocio, se logrará actuar de forma eficiente y minimizar el impacto provocado por los factores de riesgo, de origen natural o antrópico, para la Unidad de Almacén de la Universidad Francisco de Paula Santander Ocaña.

1.6 DELIMITACIÓN DEL PROBLEMA

1.6.1 Geográficas. Este proyecto se desarrollará en la Unidad de Almacén de la Universidad Francisco de Paula Santander Ocaña.

1.6.2 Temporal. El proyecto de investigación se llevara a cabo en un lapso 5 meses en donde se desarrollaran paso a paso los objetivos propuestos.

1.6.3 Conceptual. Los conceptos que se van a manejar en esta investigación se van a relacionar con la Gestión de Continuidad del Negocio según la norma ISO/IEC 27002, que fue seleccionada teniendo en cuenta que el manejo de las buenas prácticas de la Seguridad de la Información.

1.6.4 Operativa. Este documento sobre la Gestión de Continuidad del Negocio es de voluntaria aplicación para todos los funcionarios, proveedores y personal externo que desempeñen labores o le proporcionen algún tipo de servicio o producto a la Unidad de Almacén de la Universidad.

2. MARCO REFERENCIAL

2.1 ANTECEDENTES HISTÓRICOS

2.1.1 Diseñar un Modelo de Contingencia de Sistemas y Telecomunicaciones para las Entidades Bancarias del Ecuador. Alberto Guevara y Diana López. Guayaquil, Ecuador 2012. El presente tema ha sido elaborado de acuerdo a las necesidades más relevantes en las entidades bancarias actuales, el mismo ayudara al personal del área de TI a responder ante contingentes o desastres que se presenten y atenten contra la correcta operatividad del banco. Nuestro proyecto abarca las buenas prácticas de la dirección de proyecto indicadas en el PMBOK. Se desarrollan las fases de inicio y planificación. Para asegurar la calidad de nuestro proyecto se utilizaran estándares internacionales con respecto a la seguridad de la información y continuidad del negocio[1].

2.1.2 Plan de Continuidad del Negocio de una TIC. Javier García Fort. Madrid, España 2010. Este proyecto consiste en la elaboración de un Plan de Continuidad del Negocio para una empresa del sector de las Tecnologías de la Información. El Plan de Continuidad del Negocio o BCP (Business Continuity Planning) es un documento que analiza la preparación que tiene una empresa para afrontar las situaciones de desastre y realiza un estudio minucioso de las acciones que se han de ejecutar en cada momento para poder resolver dichas situaciones de desastre. El objetivo del BCP es el de conseguir que los procesos de negocio de la empresa puedan estar operativos en el menor tiempo posible en caso de contingencias en los sistemas de información[2].

2.1.3 Plan de Continuidad de Negocios. Instituto Ecuatoriano de Crédito Educativo y Becas. Quito, Ecuador 2012. Entre el negocio y los sistemas de información existe una íntima dependencia, razón por la cual deben estar preparados para afrontar las múltiples amenazas que ponen en riesgo su operatividad y en consecuencia la continuidad del negocio. Las empresas del sistema financiero, para el desarrollo de sus actividades dependen en gran medida de recursos críticos como: tecnología de la información, recurso humano, recurso económico, etc. La pérdida prolongada de tiempo en la disponibilidad de dichos recursos afectaría en alto grado la rentabilidad y viabilidad del negocio. Tomando en cuenta la importancia de estos antecedentes el Instituto Ecuatoriano de Crédito Educativo y Becas cuenta con el presente documento de respaldo a la Continuidad de Negocio como

[1] GUEVARA, Alberto y LÓPEZ, Diana. Diseñar un modelo de contingencia de sistemas y Telecomunicaciones para las entidades bancarias del Ecuador. Guayaquil, Ecuador. 2012. 198h. Trabajo de Grado (Ingeniero en Sistemas Computacionales). Universidad de Santiago de Guayaquil. Facultad de Ingeniería. [en línea]. http://repositorio.ucsg.edu.ec/bitstream/123456789/181/1/T-UCSG-PRE-ING-CIS-7.pdf

[2] GARCÍA FORT, Javier. Plan de Continuidad del Negocio de una TIC. Madrid, España. 2010. 173h. Trabajo de Grado (Ingeniero Técnico en Informática de Gestión). Universidad Pontificia Comillas. Escuela Técnica superior de Ingeniería. [en línea]. http://www.iit.upcomillas.es/pfc/resumenes/4c2474cf9a017.pdf

resultado de la aplicación de una metodología de construcción aplicada y documentada con todos los responsables de los procesos críticos de la Institución[3].

2.1.4 Plan de Contingencia Informático 2012-2015. Instituto del Mar del Perú (IMARPE). Callao, Perú 2012. La Implementación del Plan de Contingencia informático, incluye los elementos referidos a los sistemas de información, equipos, infraestructura, personal, servicios y otros, direccionado a minimizar eventuales riesgos ante situaciones adversas que atentan contra el normal funcionamiento de los servicios de la institución[4].

2.1.5 Plan de Contingencia y Continuidad Dirigido a la Universidad Técnica de Babahoyo. Babahoyo, Ecuador 2013. La Universidad enfrenta un reto significativo como lo es la acreditación, la cual servirá para estar al mismo nivel que otras universidades del país. Existen diversos factores internos y externos que alteran el normal funcionamiento de las actividades dentro de la institución. El factor más importante que afecta directamente el desarrollo y permanencia de la misma, son las inundaciones. Por lo cual lleva a la elaboración de este proyecto. Entre los problemas que se dan en la Universidad Técnica de Babahoyo debido a las inundaciones están las suspensiones de actividades dentro de la institución, donde muchos sectores económicos son afectados, como también la perdida de información, equipos informáticos y otros activos, donde en la mayoría de los casos su pérdida es total[5].

2.1.6 Propuesta de Mejoramiento y Contingencia de Sistemas Informáticos en la Empresa "T". Bogotá, Colombia 2012. Con el análisis de la información recolectada, el equipo consultor y el grupo de trabajo de Sistemas de la compañía detectan las problemáticas de TI y generan las estrategias orientadas a promover la mejora del área y de los servicios informáticos para beneficio de la organización. El equipo consultor sugiere también una propuesta de mejoramiento, basada en guías de buenas prácticas de TI y en su propia experiencia. Este documento presenta el desarrollo del mencionado proceso de consultoría y los resultados obtenidos representados en una propuesta de mejoramiento y un plan de contingencia de TI[6].

---

[3] INSTITUTO ECUATORIANO DE CRÉDITO EDUCATIVO Y BECAS. Plan de Continuidad de Negocios. Quito, Ecuador. 2012. 39h. Fecha de Última Revisión: 11/09/2012. [en línea]. http://www.iece.fin.ec/docs/lotaip/planes_programas_en_ejecucion/2012/plan_de_continuidad_de_negocios.pdf

[4] INSTITUTO DEL MAR DEL PERÚ (IMARPE). Plan de Contingencia Informático 2012-2015. Callao, Perú. 2012. 78h. [en línea].
http://www.imarpe.pe/imarpe/archivos/informes/imarpe_resol_de_158_2012_conting.pdf

[5] TAPIA PIEDRA, Jonathan Oswaldo y ZAPATA CHORRA, Jorge Eduardo. Plan de Contingencia y Continuidad Dirigido a la Universidad Técnica de Babahoyo. Babahoyo, Ecuador. 2013. 173h. Trabajo de Grado. Universidad Técnica de Babahoyo. Escuela de Sistemas y Tecnología. [en línea]. http://190.63.130.199:8080/handle/123456789/2087

[6] RAMÍREZ ROBAYO, Maritza Yohana, LONDOÑO RÚA, Edwin Alberto y GÓMEZ GÓMEZ, Jairo Andrés. Propuesta de Mejoramiento y Contingencia de Sistemas Informáticos en la Empresa "T". Bogotá, Colombia. 2012. 165h. Trabajo de Grado. Universidad EAN. Especialización en Gerencia Informática. [en línea]. http://repository.ean.edu.co/bitstream/10882/2603/1/RamirezMaritza2012.pdf

2.1.7 Plan de Contingencia Basado en Alta Disponibilidad y Virtualización. Pereira, Colombia 2012. Este trabajo de grado se da a conocer un concepto que para muchos puede resultar nuevo, pero que en realidad existe desde hace mucho tiempo, teniendo como empresa pionera a IBM hace más de 30 años. Además del concepto de virtualización y alta disponibilidad, se comparte aquí información acerca los productos de virtualización de las empresas más influyentes en este sector de TI. Cabe anotar que aunque existen más productos de virtualización en el sector, en este trabajo se describen los más destacados y representativos de la industria de la virtualización. Se destaca la importancia de la virtualización dentro de una organización por medio de la inclusión de la misma como elemento principal en un plan de contingencia para mantener la continuidad del negocio[7].

2.1.8 Plan Local de Emergencia y Contingencias (PLEC´s) Municipio de Manaure Departamento de La Guajira. Humberto Martínez Fajardo. Manaure, Colombia 2011. Se hace necesario de forma seria y responsable elaborar un Plan Local de Emergencias y Contingencias para el Municipio de Manaure (PLEC's) con el objetivo de organizar las personas, los recursos y los esfuerzos públicos, privados y comunitarios ante posibles emergencias y para superar de forma rápida y eficiente cualquier situación de emergencia o desastre con el mínimo impacto posible para la población e infraestructura afectada[8].

2.1.9 Plan de Emergencias Corporación Educativa Minuto De Dios. Freddy H. Vargas Daza. Bogotá, Colombia 2009. La edificación ocupada por la CORPORACION EDUCATIVA MINUTO DE DIOS, por estar ubicado en Bogotá se encuentra en una Zona de Riesgo Sísmico Intermedio, con el precedente de la ocurrencia de varios sismos de gran magnitud. Motivo por lo cual al tener un plan de Emergencia bien conformado y estructurado, es un factor importante que permite una rápida y oportuna atención de una emergencia con los recursos internos disponibles, disminuyendo los efectos negativos de la misma[9].

2.1.10 Plan de Contingencia para el Archivo de la Universidad de la Salle como parte de la Implantación del Sistema Integrado de Conservación. **Diana Roció León López. Bogotá, Colombia 2007.** Ante la evidente importancia de la información resulta prioritario el establecimiento de planes de contingencia que le permita a las organizaciones manejar de la mejor forma posible situaciones que atenten contra la continuidad del negocio. Para lograrlo es necesario que las organizaciones identifiquen los documentos esenciales para el

[7] COLLAZOS BRAHAM, José David. Plan de Contingencia Basado en Alta Disponibilidad y Virtualización. Pereira, Colombia. 2012. 59h. Trabajo de Grado. Universidad Tecnológica de Pereira. Programa de Ingeniería de Sistemas y Computación. [en línea]. http://recursosbiblioteca.utp.edu.co/tesisd/textoyanexos/00416C697.pdf

[8] MARTINEZ FAJARDO, Humberto. Plan Local de Emergencia y Contingencias (PLEC´s) Municipio de Manaure Departamento de La Guajira. Manaure, Colombia. 2011. 95h. [en línea]. http://www.sigpad.gov.co/sigpad/archivos/03_PLEC_MANAURE2011.pdf

[9] VARGAS DAZA, Freddy H. Plan de Emergencias Corporación Educativa Minuto De Dios. Bogotá, Colombia. 2009. 82h. [en línea]. http://colegios.minutodedios.org/saludocupacionalcemid/imagenes/plan.pdf

desarrollo de sus funciones y actividades e incluyan políticas y controles específicos para el manejo de este tipo de documentos[10].

2.1.11 Plan de Contingencia de TI para la División de Sistemas. Universidad Francisco de Paula Santander Ocaña. Ocaña, Colombia 2010. Este plan incluye en su primera versión la definición de los objetivos, alcance, responsable, factores críticos de éxito, definiciones, aspectos generales de seguridad, las fases del plan de contingencia teniendo en cuenta análisis de riesgos, acciones ante la probabilidad de que ocurra un riesgo, definición del equipo de trabajo, identificación de eventos entre otros. El plan de contingencia permitirá mantener la continuidad de los sistemas de información frente a eventos críticos, de la Institución y minimizará el impacto negativo sobre la misma, sus recursos y usuarios. Este plan es parte integral de las políticas informáticas de la entidad que servirá para evitar interrupciones, para estar preparado contra fallas potenciales y para guiar hacia una solución oportuna en la restauración del servicio[11].

2.1.12 Creación de un Manual de Seguridad física y Lógica de la Tecnologías de Información utilizadas en la Oficina del Sistema Integrado de Gestión de la Universidad Francisco de Paula Santander Ocaña. Ocaña, Colombia 2013. La oficina del Sistema Integrado de Gestión de la Universidad no cuenta con una guía que provea o sugiera buenas prácticas de seguridad física y lógica para el acceso a la información contenida en las tecnologías de la información y las comunicaciones que se manejan en dicha dependencia. Después de esta investigación, se presenta un manual de políticas para garantizar la seguridad de la información, basado en la norma técnica Colombia a NTC-ISO/IEC 27002[12].

2.1.13 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 Ocaña. Ocaña, Colombia 2013. El objetivo principal de la seguridad es proteger, ya sea medios físicos o tangibles, y en las organizaciones uno de los sectores que se debe implementar es la seguridad de la información. Los sistemas de información tienen procesos de manejo, acceso y divulgación, pero a través del tiempo han surgido cantidades de estratégicas de manipulación maligna de la información, generando

[10] LEON LÓPEZ, Diana Rocío. Plan de Contingencia para el archivo de la Universidad de la Salle como parte de la implantación del sistema integrado de Conservación. Bogotá, Colombia. 2007. 186h. Trabajo de grado (Profesional en Sistemas de Información, bibliotecología y archivística). Universidad La Salle. Facultad de sistemas de Información y Documentación. [en línea]. http://repository.lasalle.edu.co/bitstream/10185/12680/2/33021222.pdf

[11] UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA. Plan de Contingencia de TI para la División de Sistemas. Ocaña, Colombia. 2010. 28h. [en línea]. http://www.ufpso.edu.co/ftp/doc/otrospro/sitt/L-TT-DSS-002A.pdf

[12] BARBOSA DUEÑAS, Luis José, BAYONA URIBE, Carlos Asdrúbal, GALVIZ GUERRERO, Natividad y JÁCOME PRADA, Cecilia. Creación De Un Manual de Seguridad Física y Lógica de la Tecnologías de Información utilizadas en la Oficina del Sistema Integrado de Gestión de la Universidad Francisco de Paula Santander Ocaña. Ocaña, Colombia. 2013. 53h.[en línea]. http://www.ufpso.edu.co/ftp/doc/otrospro/sitt/L-TT-DSS-002A.pdf

pérdidas de gran magnitud y ocasionan en muchos casos el fracaso económico de las empresas[13].

2.1.14 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 2013. La información es uno de los activos más significativos de una organización, la cual representa una ventaja estratégica y para la cual se invierte grandes cantidades de tiempo y dinero con el fin de mantener la mayor productividad posible. La gestión de la seguridad física es una herramienta enfocada en la protección de la información. Debe estar basada en normas o estándares evitando que usuarios no autorizados accedan a ella alterando la infraestructura tecnológica[14].

2.2 MARCO CONTEXTUAL

El desarrollo de la investigación se llevara a cabo en la Unidad de Almacén de la Universidad Francisco de Paula Santander Ocaña, en la ciudad de Ocaña, Norte de Santander, Colombia, donde se estudiará el modelo del negocio de los procesos del área, su estructura orgánica, sus recursos informáticos y de software, y se realizará la elaboración de la Gestión de Continuidad del Negocio según la Norma ISO 27002.

La línea de investigación de Gobernabilidad de TI, tiene establecido un macro proyecto titulado: "Establecimiento de criterios de Gobernabilidad de TI en las empresas Colombianas", el cual se está trabajando para el contexto de Norte de Santander, en su parte inicial la Provincia de Ocaña, por sectores de empresas.

Actualmente existe la necesidad de crear un ámbito de evaluación y seguimientos de los procesos y la seguridad de la información; con miras al mejoramiento de la calidad y las buenas prácticas en la realización de los procesos de las empresas, se busca determinar el grado de madurez en que se encuentra las diferentes dependencias para así medir y realizar un autoanálisis de cómo se están realizando los procesos, un estudio del nivel de madurez a las tecnologías de información permitirá definir donde debe estar, estableciendo oportunidades de mejora y optimización de los procesos alineándolos con las estrategias y objetivos de la empresa y con los requerimientos, permitiendo establecer pautas para tomar decisiones en cuanto a la inversión necesaria para avanzar y lograr el grado de madurez deseado. La finalidad del proyecto consiste en incorporar prácticas de buen gobierno de TI,

[13] MORA PRADA, Luz Milena, QUINTERO MEJÍA, Jennifer y CAMARGO TRIGOS, María Fernanda. 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 Ocaña. Ocaña, Colombia. 2013. 163h.[en línea]. http://www.ufpso.edu.co/ftp/doc/otrospro/sitt/L-TT-DSS-002A.pdf

[14] CORONEL ORTIZ, Yeny Andrea, GUEVARA GELVES, Rocío Alexandra, JAIMES FERNÁNDEZ, Juan Camilo y SALAZAR RINCÓN, Ramón David. 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. 2013. 103h.[en línea]. http://www.ufpso.edu.co/ftp/doc/otrospro/sitt/L-TT-DSS-002A.pdf

en el sector educativo y en el caso específico la dependencia de Almacén de la UFPSO y de este modo contribuir con la línea de investigación Gobernabilidad de TI que se viene desarrollando en la Especialización de Auditoria de Sistemas.

2.3 MARCO CONCEPTUAL

Para propósitos de este proyecto, se aplican los siguientes términos y definiciones.

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.[15]

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.
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.[16]

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.[17]

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.

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

---

[15] TRUJILLLO, Freddy. C.E Soft Colombia. [En línea] [Citado el: 28 de enero de 2013.] http://cesoftco.net/2cmc/PAPER.htm.
[16] BELTRAN, Gustavo. Consultoría Estratégica y coachig de negocios. [En línea] [Citado el: 28 de 01 de 2013.] http://gustavobeltran.com/%C2%BFque-se-entiende-por-direccionamiento-estrategico/.
[17] GÓMEZ, Humberto. Gerencia Estratégica Planeación y Gestión - Teoría y metodología. Santa Fé de Bogotá : 3R Editores, 1994.

debe minimizar su impacto (económico y duración). El Plan de Continuidad del Negocio tiene un alcance operativo y tecnológico.

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).

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[18].

[18] TUMBACO MIELES, Ingrid Tatiana y YÉPEZ MANOSALVAS, Daniela Margarita. Desarrollo de un Plan de Continuidad del Negocio para el Área de Producción de una Empresa dedicada a la Producción y Comercialización de Helados para el año 2009. Guayaquil, Ecuador. 2009. 132 h. Trabajo de grado (Ingeniería en auditoría y control de gestión, especialización calidad de procesos). Escuela Superior Politécnica del Litoral. Instituto de Ciencias Matemáticas. [en línea]. http://www.dspace.espol.edu.ec/bitstream/123456789/16711/2/Tesina%20BCP%20FINAL.pdf

2.4. MARCO TEÓRICO

2.4.1 Gestión de continuidad del negocio[19]

Aspectos de la seguridad de la información de la gestión de la continuidad del negocio

Objetivo. Contraatacar 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.

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:

[19] ISO/IEC 27002:2005 Tecnología de la información - Técnicas de seguridad - Código de buenas prácticas para la gestión de seguridad de la información. [en línea]. http://www.iso.org/iso/home/search.htm?qt=iso+27002&sort=rel&type=simple&published=on

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.

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.

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.

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.

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.

Cada plan debería tener un propietario específico. Los procedimientos de emergencia, planes de contingencia manuales y planes de reanudación deberían estar dentro de la responsabilidad del propietario de los recursos o procesos comerciales apropiados involucrados. Los arreglos de contingencia para los servicios técnicos alternativos, como los medios de procesamiento de la información y comunicaciones, usualmente deberían ser responsabilidad de los proveedores del servicio.

Un marco de planeación de continuidad del negocio debería tratar los requerimientos de seguridad de la información y considerar lo siguiente:

Las condiciones para activar los planes que describen el proceso a seguirse (por ejemplo, cómo evaluar la situación, quién va a participar) antes de activar cada plan.

Los procedimientos de emergencia que describen las acciones a realizarse después del incidente que pone en riesgo las operaciones comerciales.

Procedimientos de contingencia que describen las acciones tomadas para trasladar las actividades comerciales esenciales de los servicios de soporte a locales temporales alternativos, y regresar los procesos comerciales a la operación en las escalas de tiempo requeridas.

Procedimientos operacionales temporales a seguirse hasta la culminación de la recuperación y restauración.

Procedimientos de reanudación que describen las acciones a tomarse para regresar a las operaciones comerciales normales.

Un programa de mantenimiento que especifica cómo y cuándo se va a probar el plan, y el proceso para mantener el plan.

Las actividades de conciencia, educación y capacitación diseñadas para crear el entendimiento de los procesos de continuidad del negocio y asegurar que los procesos continúen siendo efectivos.

Las responsabilidades de las personas, describiendo quién es el responsable de ejecutar cuál componente del plan. Se deberían nombrar alternativas conforme sea necesario.

Los activos y recursos críticos necesitan ser capaces de realizar los procedimientos de emergencia, de respaldo y reanudación.

Prueba, mantenimiento y re-evaluación de los planes de continuidad del negocio

Control. Los planes de continuidad del negocio deberían ser probados y actualizados regularmente para asegurar que sean actuales y efectivos.

Guía de implementación. Las pruebas del plan de continuidad del negocio deberían asegurar que todos los miembros del equipo de recuperación y otro personal relevante estén al tanto de los planes y su responsabilidad con la continuidad del negocio y la seguridad de la información, y que conozcan su papel cuando se invoque el plan.

El programa de pruebas para el(los) plan(es) de continuidad deberían indicar cómo y cuándo se debería probar cada elemento del plan. Cada elemento del(los) plan(es) debería(n) ser probado(s) frecuentemente:

Prueba flexible de simulación (table-top testing) de varios escenarios (discutiendo los acuerdos de recuperación comercial utilizando ejemplos de interrupciones).

Simulaciones (particularmente para capacitar a las personas en sus papeles en la gestión post-incidente/crisis).

Prueba de recuperación técnica (asegurando que los sistemas de información puedan restaurarse de manera efectiva.

Prueba de recuperación en el local alternativo (corriendo los procesos comerciales en paralelo con las operaciones de recuperación lejos del local principal).

Pruebas de los medios y servicios del proveedor (asegurando que los servicios y productos provistos externamente cumplan con el compromiso contraído).

Ensayos completos (probando que la organización, personal, equipo, medios y procesos puedan lidiar con las interrupciones).

Estas técnicas se pueden utilizar en cualquier organización. Esto se debería aplicar de una manera que sea relevante para el plan de recuperación específico. Los resultados de las pruebas deberían ser registradas y, cuando sea necesario, se deberían tomar acciones para mejorar los planes.

Se debería asignar la responsabilidad de las revisiones regulares de cada plan de continuidad del negocio. La identificación de los cambios en los acuerdos comerciales que aún no se reflejan en los planes de continuidad del negocio debería realizarse mediante una actualización apropiada del plan. Este proceso formal de control de cambios debería asegurar que los planes de actualización sean distribuidos y reforzados mediante revisiones regulares del plan completo.

Los ejemplos de los cambios que se deberían considerar cuando se actualizan los planes de continuidad del negocio son la adquisición de equipo nuevo, actualización de los sistemas y cambios en:

Personal.
Direcciones o números de teléfonos.

Estrategia comercial.
Local, medios y recursos.
Legislación.
Contratistas, proveedores y clientes claves.
Procesos, los nuevos o los eliminados.
Riesgo (operacional y funcional).

2.5 MARCO LEGAL

2.5.1 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".

2.5.2 Leyes informáticas 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[20].

El derecho de autor.

Constitución Política de 1991. En su artículo 61, que expresa: "El Estado protegerá la propiedad intelectual por el tiempo y mediante las formalidades que establezca la ley".

[20] UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA. Gerencia de Innovación y Desarrollo Tecnológico. Última actualización el Lunes, 22 de Abril de 2013 09:05. [en línea]. http://www.unad.edu.co/gidt/index.php/leyesinformaticas

Decisión 351 de 1993, o Régimen Común Andino sobre Derecho de Autor y Derechos Conexos, es de aplicación directa y preferente a las leyes internas de cada país miembro del Grupo Andino.

Ley 23 de 1982, contiene las disposiciones generales y especiales que regulan la protección del derecho de autor en Colombia.

Ley 44 de 1993 (febrero 15), modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944.

DECRETO 1360 DE 1989 (junio 23). "Por el cual se reglamenta la inscripción de soporte lógico (software) en el Registro Nacional del Derecho de Autor".

Decreto 460 de 1995, por la cual se reglamenta el Registro Nacional de Derecho de Autor.

DECRETO 1474 DE 2002 (Julio 15). "Por el cual se promulga el "Tratado de la OMPI, Organización Mundial de la Propiedad Intelectual, sobre Derechos de Autor (WCT)", adoptado en Ginebra, el veinte (20) de diciembre de mil novecientos noventa y seis (1996)".

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"[21].

Artículos de la Unidad de Almacén e inventarios de la Universidad Francisco de Paula Santander.

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[22].

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

[21] SUPERINTENDENCIAS DE SOCIEDADES. Manual Manejo y Control Administrativo de los Bienes de Propiedad. Bogotá D.C., Colombia, 2009. 29h. [en línea]. http://www.supersociedades.gov.co/web/Ntrabajo/SISTEMA_INTEGRADO/Documentos%20Infraestructura/DOCUMENTOS/GINF-M-001%20MANUAL%20ADMINISTRATIVO.pdf

[22] UNIVERSIDAD FRANCISCO DE PAULA SANTANDER. Consejo Superior Universitario. Acuerdo No. 126. Diciembre 9 de 1994. [en línea]. http://www.ufpso.edu.co/ftp/pdf/acuerdos/acuerdo_126.pdf

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.

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.

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.

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[23].

[23] TUMBACO MIELES, Ingrid Tatiana y YÉPEZ MANOSALVAS, Daniela Margarita. Desarrollo de un Plan de Continuidad del Negocio para el Área de Producción de una Empresa dedicada a la Producción y Comercialización de Helados para el año 2009. Guayaquil, Ecuador. 2009. 132 h. Trabajo de grado (Ingeniería en auditoría y control de gestión, especialización calidad de procesos). Escuela Superior Politécnica del Litoral. Instituto de Ciencias Matemáticas. [en línea]. http://www.dspace.espol.edu.ec/bitstream/123456789/16711/2/Tesina%20BCP%20FINAL.pdf

3. DISEÑO METODOLÓGICO

3.1 TIPO DE INVESTIGACIÓN

Para llevar a cabo el presente proyecto se utilizará el tipo de estudio descriptivo y exploratorio, pues describe lo que es la Gestión o Plan de continuidad de Negocio y los principales riesgos operativos inherentes a su actividad económica, recursos tecnológicos y características específicas de la región, mediante un diagnóstico se ubica al objeto de estudio en toda la problemática manifestada, también es documental por la investigación realizada en libros, diccionarios, documentos, proyectos de grado y artículos de Internet, necesaria para los temas que involucra el proyecto.

3.2 POBLACIÓN Y MUESTRA

La población está conformada por el Jefe de Almacén, la Coordinadora de Inventarios, la Secretaria de Almacén y el Jefe del Proceso de Apoyo Sistema de Información, Telecomunicaciones y Tecnología para determinar el direccionamiento estratégico de la Unidad de Almacén de la Universidad Francisco de Paula Santander Ocaña. Además se realizó cuestionario a cuarenta empleados de la Institución para verificar que conocimiento tienen del Plan de Contingencia de TI para la División de Sistemas, que se encuentra montado en la página web. Se toma como muestra toda la población involucrada en el proceso.

3.3 TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE INFORMACIÓN

3.3.1 Técnicas de Recolección. Para recolectar la información se aplicó como técnica la observación directa ya que el investigador obtuvo información clara y precisa, percibiendo los hechos tal como éstos se dan naturalmente, siendo apoyado a través de la revisión documental en la cual se consultarán textos e información en línea (consultas de sitios y páginas Web) con la finalidad de ampliar los conocimientos necesarios para alcanzar los objetivos propuestos. La observación directa es aquella a través de la cual se puedan conocer los hechos y situaciones de la realidad social.

Con el propósito de conocer las necesidades de la Unidad de Almacén en la parte concerniente al manejo de la Gestión de Continuidad del Negocio, se realizaron entrevistas con el Jefe de Almacén, la Coordinadora de Inventarios, la Secretaria de Almacén y el Jefe del Proceso de Apoyo Sistema de Información, Telecomunicaciones y Tecnología, para establecer el problema y las posibles soluciones (ver anexos).

3.4 ANALISIS DE LA INFORMACION RECOLECTADA

La información recolectada por medio de las consultas y entrevistas se analizará, clasificará y presentará con el propósito de organizarla y estructurarla en forma ordenada y con objetivos precisos, tomando solo la información relevante que contribuya al buen desarrollo y ejecución del proyecto, de tal manera que tenga la finalidad de ser base a la construcción

de conocimiento a personas que en un futuro utilicen este proyecto como guía para el establecimiento de la Gestión de Continuidad del Negocio.

Análisis Estadístico a la Encuesta al Personal Administrativo y Contratado. El personal administrativo y contratado de la Universidad Francisco de Paula Santander Ocaña, está conformado por cuarenta (40) personas que corresponden al 100% de los encuestados, se les realizó la encuesta arrojando los siguientes resultados.

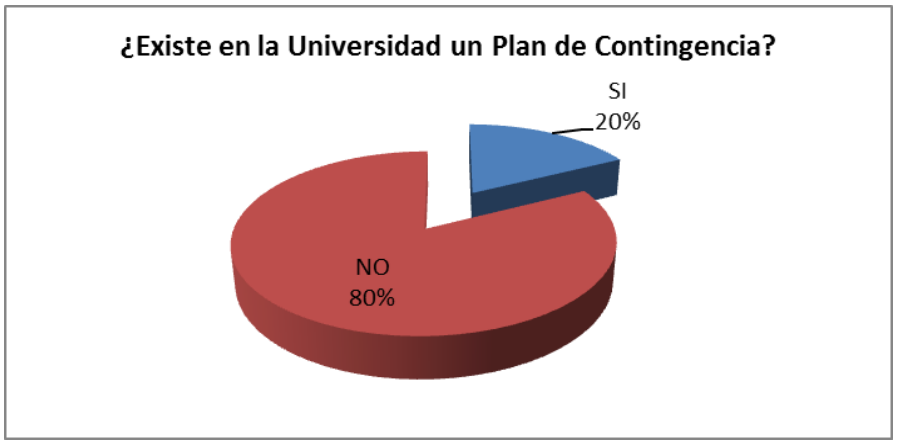
¿Existe en la Universidad un Plan de Contingencia?

Tabla 1. Estadística de la Existencia de un Plan de Contingencia

OPCIONES	RESPUESTA OBTENIDA	TOTAL %
SI	8	20
NO	32	80
TOTAL	**40**	**100**

Fuente. Autores del Proyecto.

Figura 1. Representación Porcentual de la Existencia de un Plan de Contingencia



SI

O SI

Fuente. Autores del Proyecto.

Análisis. Ocho de los empleados contestaron que sí, pero solo tres de los encuestados supieron que el Proceso de Apoyo de Sistema de Información, Telecomunicaciones y Tecnología de la universidad es el único que tiene un Plan de Contingencia de TI.

La dependencia de la Universidad al uso de computadoras, las redes para manejar sus actividades y la disponibilidad de los sistemas de información se ha vuelto crucial. Actualmente, la Institución necesita un nivel alto de disponibilidad, ya que le resultaría extremadamente difícil funcionar sin los recursos informáticos. El desconocimiento del Plan de Contingencia de TI por parte del personal de la Universidad, en caso de un desastre,

no le permite conocer los objetivos, alcance, responsable, factores críticos de éxito, definiciones, aspectos generales de seguridad, las fases del plan y las acciones oportunas ante la probabilidad de que ocurra un riesgo, entre otros. Además el personal no estará preparado para evitar interrupciones, fallas potenciales y para guiar hacia una solución oportuna en la restauración del servicio.

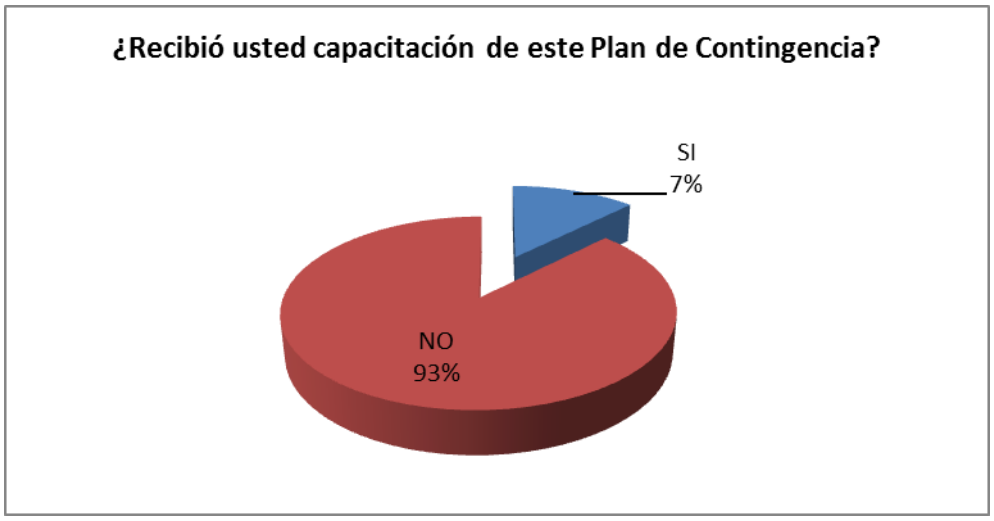
¿Recibió usted capacitación de este Plan de Contingencia?

Tabla 2. Estadística de la Capacitación del Plan de Contingencia

OPCIONES	RESPUESTA OBTENIDA	TOTAL %
SI	3	7
NO	37	93
TOTAL	**40**	**100**

Fuente. Autores del Proyecto.

Figura 2. Representación Porcentual de la Capacitación del Plan de Contingencia



Fuente. Autores del Proyecto.

Análisis. De los ocho empleados que contestaron afirmativo, solo tres de ellos recibieron capacitación del Plan de Contingencia.

La constante capacitación del personal es importante para garantizar en todo momento la continuidad de los Sistemas de Información y de este modo aumentar la confianza de los usuarios en las transacciones y procesos que se realizan a través de ellos. Este instrumento se ha diseñado en este sentido, para dar respuesta oportuna, adecuada y coordinada a situaciones de emergencia causadas por fenómenos destructivos de origen natural o humano. Sin embargo, si el personal no es capacitado no se cuenta con la suma del esfuerzo

de todos, cuya composición permita fortalecer y cumplir en tiempo las acciones tendientes a prevenir y mitigar desastres en modo y tiempo de las circunstancias señaladas, y dar respuesta oportuna a la Institución dentro de un marco de seguridad.

¿Actualmente este Plan de Contingencia se está aplicando en la Universidad?

Tabla 3. Estadística Aplicación Actual del Plan de Contingencia

OPCIONES	RESPUESTA OBTENIDA	TOTAL %
SI	5	12
NO	35	88
TOTAL	**40**	**100**

Fuente. Autores del Proyecto.

Figura 3. Representación Porcentual de la Aplicación Actual del Plan de Contingencia

Fuente. Autores del Proyecto.

Análisis: En esta pregunta 35 de los empleados contestaron que no, porque la realidad es que hay un desconocimiento casi total en la existencia y aplicación del Plan de Contingencia, el cual fue creado en el año 2010 y no ha sido actualizado hasta la fecha[24].

La no aplicación del Plan de TI en la Universidad y su desactualización, puede llevar a pérdidas financieras significativas y perdidas en la información. Se puede perder la

[24] UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA. Plan de Contingencia de TI para la División de Sistemas. Ocaña, Colombia. 2010. 28h. [en línea]. http://www.ufpso.edu.co/ftp/doc/otrospro/sitt/L-TT-DSS-002A.pdf

credibilidad de la comunidad universitaria, ya que los procedimientos manuales, si es que existen, sólo serían prácticos por un corto periodo. Además que los procedimientos e instructivos necesarios para poder continuar con las operaciones, procesos y servicios informáticos críticos, en caso de que se llegara a presentar algún siniestro o contingencia, no serían conocidos por el personal.

4. PRESENTACIÓN DE RESULTADOS

4.1 RECONOCIMIENTO DE LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

4.1.1 Direccionamiento estratégico

Misión. La Universidad Francisco de Paula Santander Ocaña, institución pública de educación superior, es una comunidad de aprendizaje y autoevaluación en mejoramiento continuo, comprometida con la formación de profesionales idóneos en las áreas del conocimiento, a través de estrategias pedagógicas innovadoras y el uso de las tecnologías; contribuyendo al desarrollo nacional e internacional con pertinencia y responsabilidad social.

Visión. 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, el desarrollo físico y tecnológico, la innovación y la generación de conocimiento, bajo un marco de responsabilidad social y ambiental hacía la proyección nacional e internacional.

Reseña Histórica. 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. En diciembre de ese mismo año, el rector de la Universidad Francisco de Paula Santander, José Luís Acero Jordán, le envió copia de dicho estudio al ICFES, Instituto que conceptúo que el proyecto para abrir el centro de estudios en Ocaña, era recomendable.

Según Acuerdo No. 031 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 AUTONOMIA administrativa y patrimonio independiente, adscrito al Ministerio de Educación Nacional.

Su primer coordinador el doctor Aurelio Carvajalino Cabrales, buscó un lugar adecuado para funcionar la sede, en los claustros Franciscanos al costado del templo de la Gran Convención y con las directivas del colegio José Eusebio Caro, se acordó el uso compartido del laboratorio de física.

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.

La consecución de 27 hectáreas de la Hacienda El Rhin, en las riberas del Río Algodonal, en comodato a la Universidad por 50 años, que la antigua Escuela de Agricultura de Ocaña cedió a la Universidad, permitió la creación del programa de Tecnología en Producción Agropecuaria, aprobado por el Consejo Superior mediante el Acuerdo No. 024 del 21 de agosto de 1980, y luego el ICFES otorgó la licencia de funcionamiento el 17 de febrero del año siguiente. Luego se crean las Facultades.

La Facultad de Ciencias Agrarias y del Ambiente, fue creada según Acuerdo 084 del 11 de septiembre de 1995 conformada por los departamentos de Ciencias Agrícolas y del Ambiente y el departamento Ciencias Pecuarias junto a los programas académicos de Tecnología Agropecuaria (Acuerdo Nº 024 del 21 de agosto de 1980), Zootecnia (Acuerdo Nº057 y 058 del 27 de junio de 2007), e Ingeniería Ambiental (Acuerdo 089 del 9 de octubre 1995).

La Facultad de Ciencias Administrativas y Económicas, fue creada según Acuerdo No. 008 del 05 de marzo de 2003; está conformada por el departamento de Ciencias Administrativas y Departamento de ciencias Contables y Financieras. Están adscritos los programas académicos de Tecnología en Administración Comercial y Financiera (Acuerdo No, 024 del 29 de Junio de 1988 y con la Resolución 5243 del 05 de Septiembre del 2006 del MEN), Administración de Empresas (Acuerdo No, 024 del 29 de Junio de 1988) y la profesionalización (Acuerdo No. 118 del 16 de Noviembre de 1994); Contaduría Pública (Acuerdo No. 007 del 05 de Marzo de 2003 y según resolución 3388 del 23 de Diciembre del 2003 del MEN). Así mismo, según Acuerdo No. 0087 del 15 de Diciembre del 2005 se aprueba por Ciclos Propedéuticos el Plan de Estudio de la Técnica Profesional en Administración Comercial Y Financiera, según Resolución 101 del 18 de Enero de 2007 del MEN.

La Facultad de Ingenierías fue creada según acuerdo 007 del 20 de febrero de 2006, conformada con los departamentos de Ingeniería Civil, Ingeniería Mecánica y el departamento de Sistemas e Informática. Con los registros calificados de los programas completos de acuerdo a la Resolución 2909 de julio 21 de 2005 para el programa de Ingeniería Civil e Ingeniería Mecánica (Resolución 2908 de julio 21 de 2005), Ingeniería de Sistemas (Resolución 7062 de noviembre 10 de 2006). La creación de los Técnicos Profesionales en Telecomunicaciones con registro calificado (Resolución 5366 de agosto 25 de 2008) y el Técnico profesional en Informática con registro calificado (Resolución 4613 de julio 18 de 2008).

La Facultad de Educación, Artes y Humanidades de la Universidad Francisco de Paula Santander Ocaña fue creada según acuerdo 063 del 20 de noviembre de 2006, está conformada con los departamentos: de Matemáticas, física y computación y el departamento de Humanidades. Según el Acuerdo No. 010, marzo 29 de 2004 se crea el plan de estudios del programa de Comunicación Social, Derecho con registro calificado (Resolución 10185 de noviembre 22 de 2010). En el mes de noviembre de 2005, se suscribió el convenio de asociación No. 1744/05 con el Ministerio de Cultura, con el objeto de apoyar el proceso de estructuración académica de la Escuela de Bellas Artes.

Objetivos

Desarrollo de Talento Humano. La Universidad mantendrá su preocupación por el desarrollo del talento humano (Estudiantes, Docentes y Administrativos) para que se integren con entusiasmo a los desafíos de la organización y el entorno en general.

Modernización Tecnológica. En los próximos 3 años, deberá concluir la modernización de todos los medios de operación para garantizar la productividad y el permanente control del proceso, con máxima flexibilidad y calidad académica y administrativa.

Fortalecimiento Investigación y Extensión. La universidad considera de vital importancia el liderazgo en el desarrollo tecnológico, para ello propone 2 objetivos fundamentales; la Revitalización de la Investigación y la búsqueda de nuevas tecnologías para el desarrollo de los sectores social y productivo.

Crecimiento de Nuevas Líneas de Productos. Especialmente en el desarrollo de postgrados y Planes de Estudio, Educación Continuada y Universidad a Distancia.

Principios. La Unidad de Almacén de la Universidad Francisco de Paula Santander Seccional Ocaña se fundamenta en los siguientes principios:

Responsabilidad Social. La institución y quienes la integran tienen como responsabilidad contribuir, al desarrollo de la zona de influencia apoyando a la comunidad en la solución de problemas, mediante proyectos de investigación y la entrega de profesionales con alta formación integral en lo humanístico y académico.

Productividad. La Universidad afronta como uno de sus grandes retos, el logro de niveles óptimos de productividad que hagan de su actividad una labor eficiente y eficaz que le permita el cumplimiento de sus objetivos y responsabilidades para con su personal y la comunidad en general.

Respeto por la persona. Las actividades se fundamentan en el respeto por las personas, sus valores, sus creencias, respeto por los derechos y excelencias de las responsabilidades mutuas.

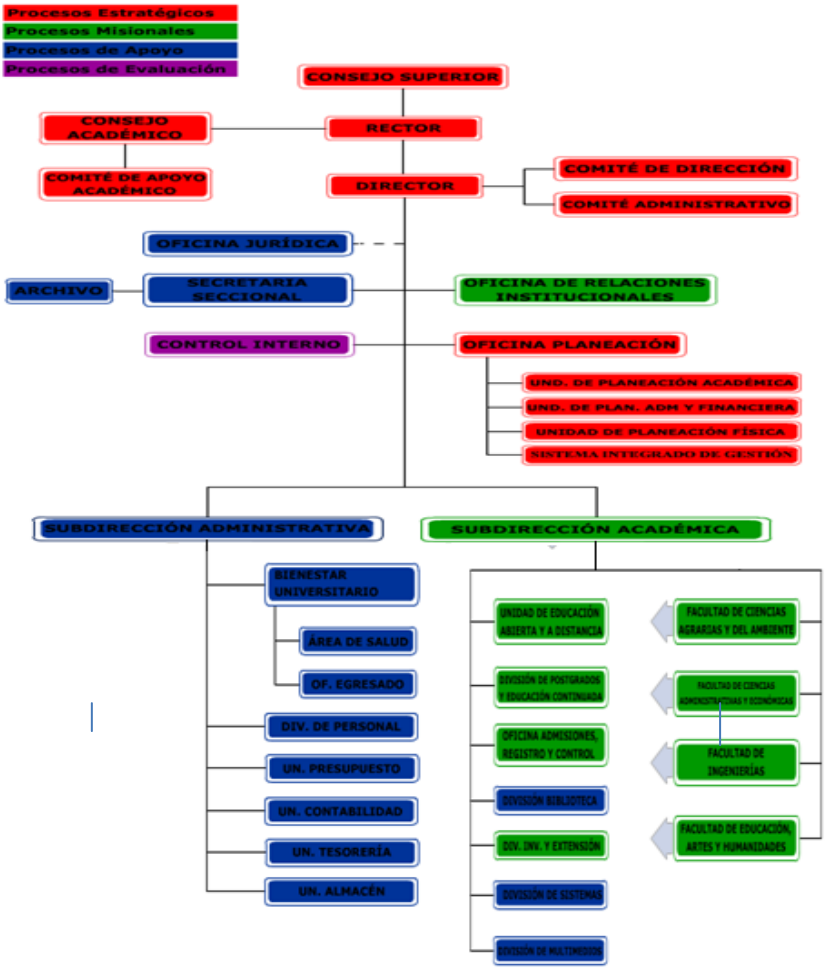
Servicio. El servicio es una responsabilidad de todos los miembros de la institución y compromete a todos por igual; este servicio debe darse en la relación humana, la gestión administrativa y todos los procesos de la universidad, mediante el ofrecimiento a sus clientes tanto internos como externos.

Compromisos. El trabajo en equipo, la lealtad, la transparencia y el sentido de pertenencia por la institución son características indispensables de nuestros colaboradores.

Estructura Orgánica de la Universidad Francisco de Paula Santander Ocaña. Según Acuerdo No. 084 de septiembre 11 de 1995, el Consejo Superior Universitario, con base en

las atribuciones legales y estatutarias que le confieren la ley 30 de 1992 y el Acuerdo No. 029 del 12 de Abril de 1994, aprueba La Estructura Orgánica de la Universidad Francisco de Paula Santander Seccional Ocaña.

Figura 4. Estructura orgánica de la Universidad Francisco de Paula Santander Ocaña



Fuente: http://www.ufpso.edu.co/ufpso/general.html#estructura

4.1.2 Modelo de negocios para la Unidad de Almacén de la Universidad Francisco de Paula Santander Ocaña

Modelo de Objetivos. 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.

Misión. La Unidad de Almacén de la Universidad Francisco de Paula Santander Ocaña, tiene como misión canalizar los diferentes requerimientos solicitados por la Institución, para de esta forma lograr los objetivos Institucionales.

Visión. La Unidad de Almacén de la Universidad Francisco de Paula Santander Ocaña, tendrá como visión velar que en las diferentes dependencias sepan dar un buen manejo de los diferentes elementos que le son entregados.

Principios. La Unidad de Almacén de la Universidad Francisco de Paula Santander Seccional Ocaña se fundamenta en los siguientes principios:

Responsabilidad Social. La institución y quienes la integran tienen como responsabilidad contribuir, al desarrollo de la zona de influencia apoyando a la comunidad en la solución de problemas, mediante proyectos de investigación y la entrega de profesionales con alta formación integral en lo humanístico y académico.

Productividad. La Universidad afronta como uno de sus grandes retos, el logro de niveles óptimos de productividad que hagan de su actividad una labor eficiente y eficaz que le permita el cumplimiento de sus objetivos y responsabilidades para con su personal y la comunidad en general.

Respeto por la persona. Las actividades se fundamentan en el respeto por las personas, sus valores, sus creencias, respeto por los derechos y excelencias de las responsabilidades mutuas.

Servicio. El servicio es una responsabilidad de todos los miembros de la institución y compromete a todos por igual; este servicio debe darse en la relación humana, la gestión administrativa y todos los procesos de la universidad, mediante el ofrecimiento a sus clientes tanto internos como externos.

Compromisos. El trabajo en equipo, la lealtad, la transparencia y el sentido de pertenencia por la institución son características indispensables de nuestros colaboradores.

Objetivos

General. Permanecer en contacto directo con la Subdirección Administrativa para analizar y suministrar los elementos necesarios requeridos por las diferentes dependencias de nuestra Institución.

Específicos. Establecer con el Subdirector Administrativo las necesidades prioritarias de la Institución.

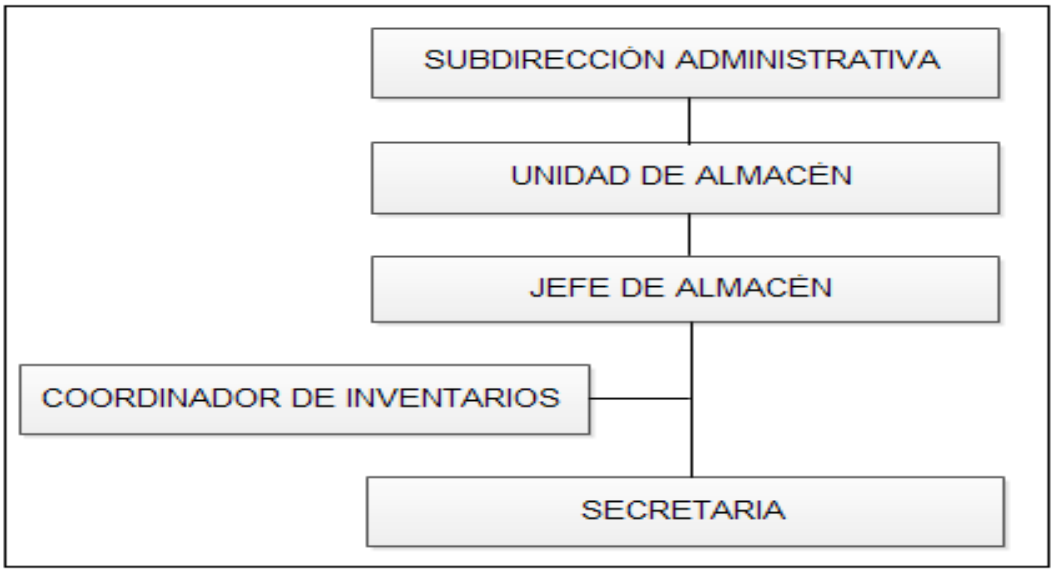
Verificar que los diferentes proveedores cumplan con los requisitos legales.

Sistematizar los inventarios de la Institución.

Evaluar las solicitudes realizadas por las diferentes dependencias para verificar, si colmaron las expectativas requeridas.

Estructura Orgánica de la Unidad de Almacén

Figura 5. Estructura orgánica de la Unidad de Almacén



Fuente. Autores del Proyecto.

Descripción de Funciones del Jefe de Almacén

Atender las solicitudes de suministros y consumibles de los diferentes dependencias.
Revisar la conformidad, calidad y cantidad exacta de los elementos que ingresan al almacén.
Llevar un riguroso control de los elementos a su cuidado mediante el registro en el kárdex de las adquisiciones, ingresos y egresos, baja de inservibles y venta de productos del almacén.
Ordenar y supervisar el despacho de elementos a las dependencias que lo requieran, de acuerdo con lo autorizado presupuestalmente y en el acuerdo de gastos.
Entregar y controlar mediante inventario físico los elementos, equipos y enseres que requieran las distintas dependencias de la Universidad.
Llevar los libros de inventarios, kárdex y demás registros, en las formas establecidas por la Universidad.
Clasificar y codificar los artículos y elementos para la elaboración de inventarios periódicos parciales.
Informar y remitir diariamente a la Unidad de Contabilidad y Presupuesto los comprobantes de ingresos y egresos que se causen y los comprobantes correspondientes al movimiento de bienes.

Gestionar las cotizaciones para adquisición de bienes que requiere la Universidad con base en el registro de proveedores.
Firmar y entregar los paz y salvos a los estudiantes.
Firmar salidas de consumo y entrega de los elementos solicitados por las diferentes dependencias.
Asistir a las reuniones programadas por los diferentes comités a la cual se hace parte.
Mantener adecuadamente clasificados y almacenados los elementos que ingresan al almacén de acuerdo al inventario.
Asegurar la correcta implementación de los procedimientos del área.
Las demás relacionadas con el cargo que le sean asignadas por el Jefe inmediato.

Descripción de Funciones del Coordinador de Inventarios

Prepara la toma de inventario físico de los bienes de la Institución y/o mantiene actualizado el inventario sistematizado existente.
Registrar en forma ordenada y detallada los bienes devolutivos que tiene la universidad, con anotación de las especificaciones de código contable, descripción, costo de compra, fecha, cantidad, serial, modelo, marca, clasificándolos de acuerdo a su naturaleza, uso y destino.
Mantener actualizada la base de datos en cuanto a existencias físicas reales.
Mantener informado al Jefe de División de Almacén, sobre el control y manejo de los inventarios de los bienes de la institución, y a su ve suministrar la información que este solicite.
Realizar formatos de Traslados y baja de elementos cuando el funcionario con inventario de elementos devolutivos lo solicite y sea necesario.
Efectuar conjunto con la unidad de convalidad la depreciación de los activos de la institución.
Atender las consultas y reclamos formulados por los funcionarios responsables de bienes.
Crear la responsabilidad que atañe a cada funcionario por la pérdida o hurto de bienes.
Administrar en la herramienta tecnológica el software o el aplicativo correspondiente a éste, en el cual se registran o procesa la información, de acuerdo con los movimientos y rotación de los bienes muebles de propiedad de la Universidad.

Descripción de Funciones de la Secretaria de Almacén

Asistir administrativamente al jefe para facilitar la ejecución de las actividades propias de la dependencia.

Redactar comunicaciones, producir a computadora correspondencia de rutina y ocasional, y encargarse de asuntos generales, con el fin de colaborar permanentemente en la realización del trabajo de oficina.

Tomar decisiones que le sean específicamente delegadas por el jefe.

Recibir, revisar, clasificar, radicar, distribuir y controlar documentos, datos y elementos y/o correspondencia relacionados con los asuntos de competencia de la Universidad, de acuerdo con las normas y los procedimientos respectivos

Llevar y mantener actualizados los registros de carácter técnico, administrativo o financiero, verificar la exactitud de los mismos y presentar los informes correspondientes.

Adelantar labores relacionadas con el recibo, el pago y el manejo de valores y de fondos institucionales, de conformidad con las disposiciones, los trámites y las instrucciones pertinentes.

Tomar dictados, colaborar en su redacción y presentación, transcribir en equipos de oficina correspondencia y otros documentos que le indique el superior, con base en manuscritos, grabaciones y otros medios o instrucciones.

Orientar a los usuarios y suministrar información, documentos o elementos que sean solicitado de conformidad con los trámites, las autorizaciones y los procedimientos establecidos.

Informar al jefe inmediato, en forma oportuna, sobre las inconsistencias o anomalías relacionadas con los asuntos, elementos o documentos y/o correspondencia encomendados.

Colaborar en el diseño de formas y cuestionarios para la recolección de datos, en la verificación de información y revisión de tabulados y en la obtención de promedio o proposiciones sencillas.

Coordinar, de acuerdo con instrucciones, reuniones y eventos que deba atender el jefe inmediato, llevando la agenda correspondiente y recordando los compromisos adquiridos.

Llevar controles periódicos sobre consumo de elementos, con el fin de determinar su necesidad real y presentar el programa de requerimientos correspondientes.

Colaborar en la disposición y organización de materiales, equipos, instalaciones y demás aspectos que requieran para la elaboración de los eventos da carácter institucional.
Garantizar la correcta aplicación de las normas y los procedimientos

Elaborar, de acuerdo con las instrucciones del jefe inmediato, actas, registros y relaciones sencillas.

Responder por la calidad y oportunidad de los trabajos asignados conforme a las normas, procedimientos establecidos e instrucciones dadas.

Velar por la organización y aseo de las oficinas e instalaciones de la dependencia.

Atender los teléfonos de la oficina y establecer las comunicaciones que le solicite el Jefe inmediato.

Firmar inventario individual y responsabilizarse por todos los elementos devolutivos asignados a su cargo.

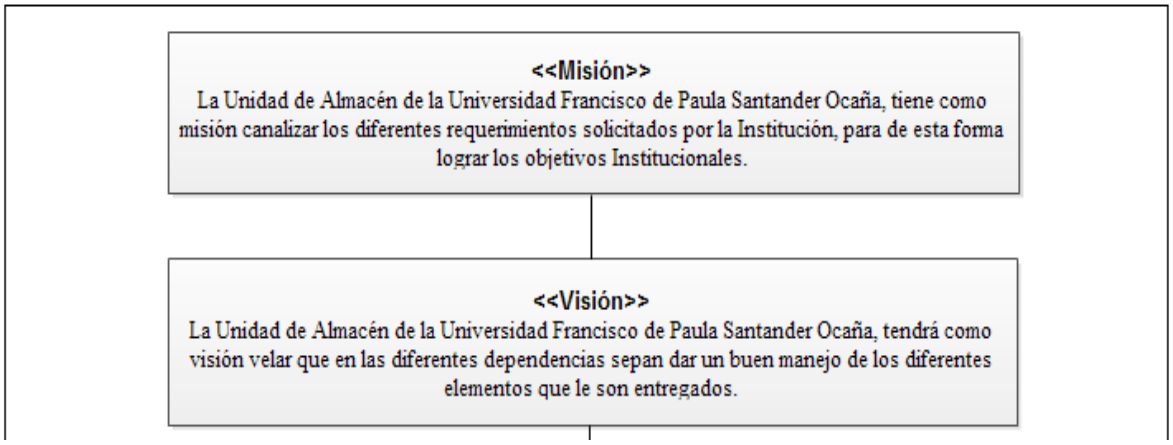
Planear, organizar, dirigir, ejecutar, controlar y evaluar con eficiencia el desarrollo de los proyectos y las actividades propias de su trabajo.

Participar con su labor diaria en la misión, visión, objetivos, políticas, propósitos y principios de la Universidad

Coordinar y participar directamente con actividades referentes a sus responsabilidades y desempeño de sus funciones, con el desempeño y funciones de los otros cargos o entidades internas y/o externas, relacionadas con el desarrollo de su labor de manera efectiva.

Desempeñar las demás funciones asignadas por la autoridad competente, de acuerdo con el nivel, la naturaleza y el área de desempeño del empleo.

Figura 6. Misión, visión y objetivos de la Unidad de Almacén



Fuente. Autores del Proyecto.

4.1.3 Modelado de procesos del negocio. En el modelado de procesos del negocio de la Unidad de Almacén de la Universidad Francisco de Paula Santander Ocaña se describen las actividades que permiten cumplir los objetivos especificados en la jerarquía de objetivos de negocio, las condiciones y reglas que deben se deben cumplir y la definición de los responsables o roles de la ejecución del mismo.

Procesos Principales.

Suministro. Proceso que se lleva a cabo para satisfacer las necesidades de consumo de la Universidad Francisco de Paula Santander Ocaña.

Inventario. Es un proceso de control, que consiste en confrontar los registros implementados para registrar el movimiento y ubicación de los bienes, con el recuento físico total o parcial de los mismos.

Procesos de Apoyo

Archivo (Ventanilla Única). La ventanilla única de documentos se encargará de su recepción, radicación y distribución interna; y cada una de las dependencias serán las responsables de dar respuesta oportuna y en el menor tiempo posible a las comunicaciones, de acuerdo a la normatividad interna de cada dependencia.

Infraestructura y Mantenimiento. Coordinar y supervisar las actividades correspondientes a la proyección, construcción y mantenimiento de la infraestructura física de la Universidad Francisco de Paula Santander Ocaña, en sus diferentes sedes; asegurando que las condiciones de los espacios físicos, sean las adecuadas para la prestación de los servicios ofrecidos.

Sistemas de Información de Comunicaciones y Tecnología. Administrar y mantener de manera eficaz los sistemas de información, las telecomunicaciones y la infraestructura tecnológica utilizados para el desarrollo de los procesos de la Universidad en el cumplimiento de su Misión.

Adquisición de Bienes y Servicios. Suplir las necesidades de bienes y servicios a los diferentes procesos institucionales y administrar de forma oportuna y eficaz los recursos económicos y financieros de la Universidad Francisco de Paula Santander Ocaña.

Seguimiento y Evaluación de Proveedores. Establecer las medidas de control y actividades a seguir para realizar el seguimiento y evaluación de proveedores inscritos, requeridos por la institución.

Diagrama de Actividades. La Unidad de Almacén ejecuta sus procesos utilizando las cadenas de valor diseñadas para el suministro y manejo de inventarios. (Ver Figura 5).

Figura 7. Cadena de valor

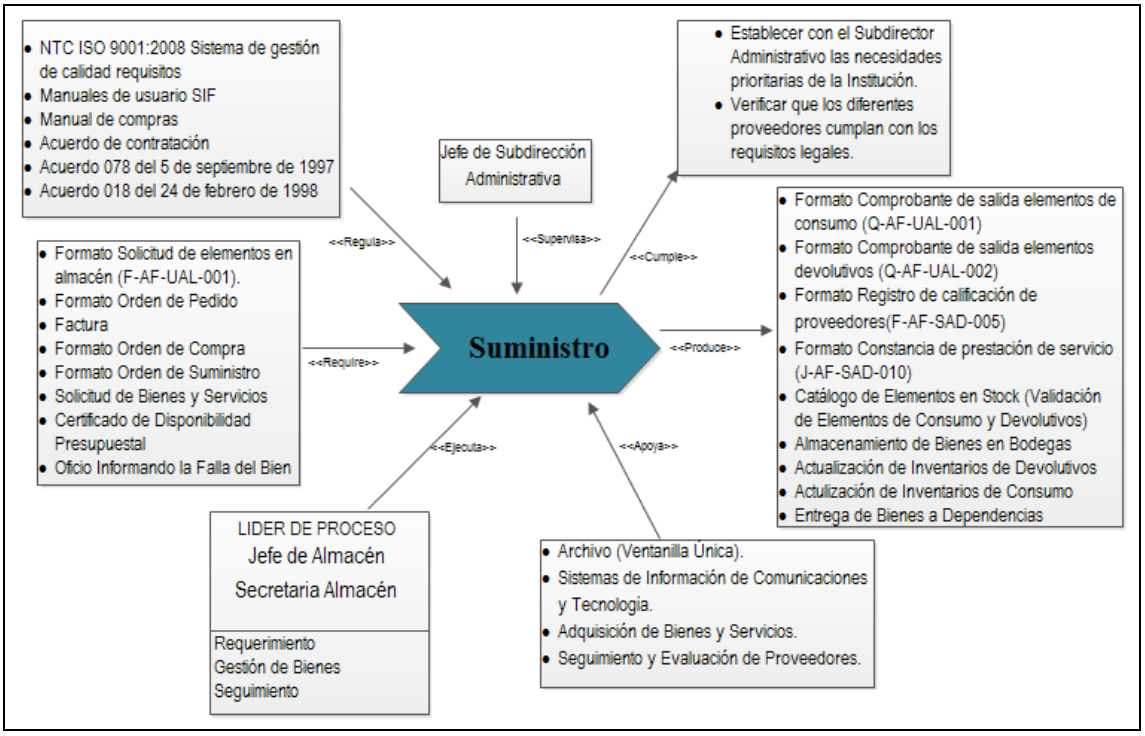
Fuente. Autores del Proyecto.

La descripción de cada uno de estos procesos se presenta en el Diagrama de Descripción de Procesos de manera jerárquica.

Modelo de descripción de procesos

PF Suministro. Proceso que se lleva a cabo para satisfacer las necesidades de consumo de la Universidad Francisco de Paula Santander Ocaña.

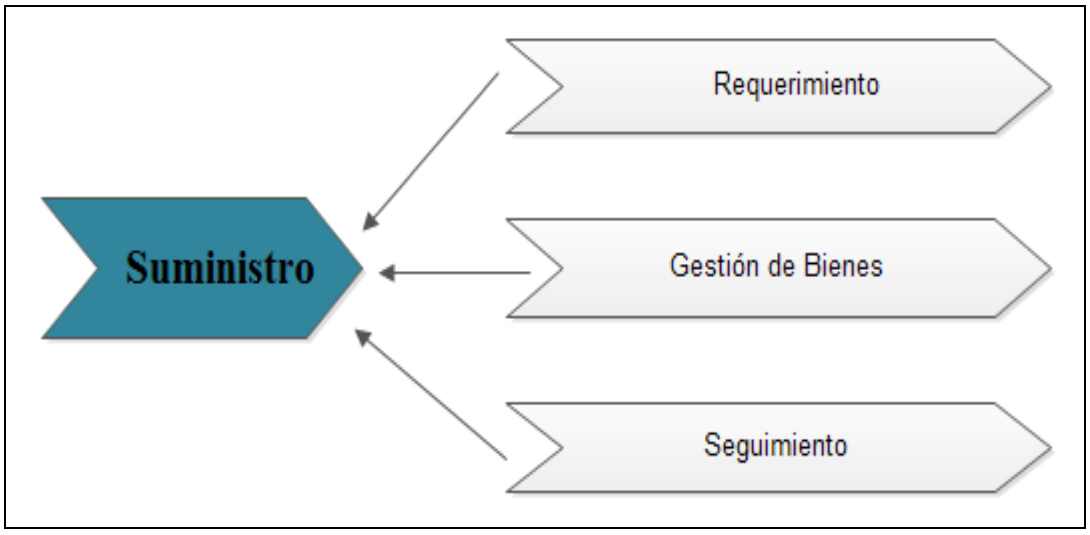
Figura 8. Proceso principal suministro



Fuente. Autores del Proyecto.

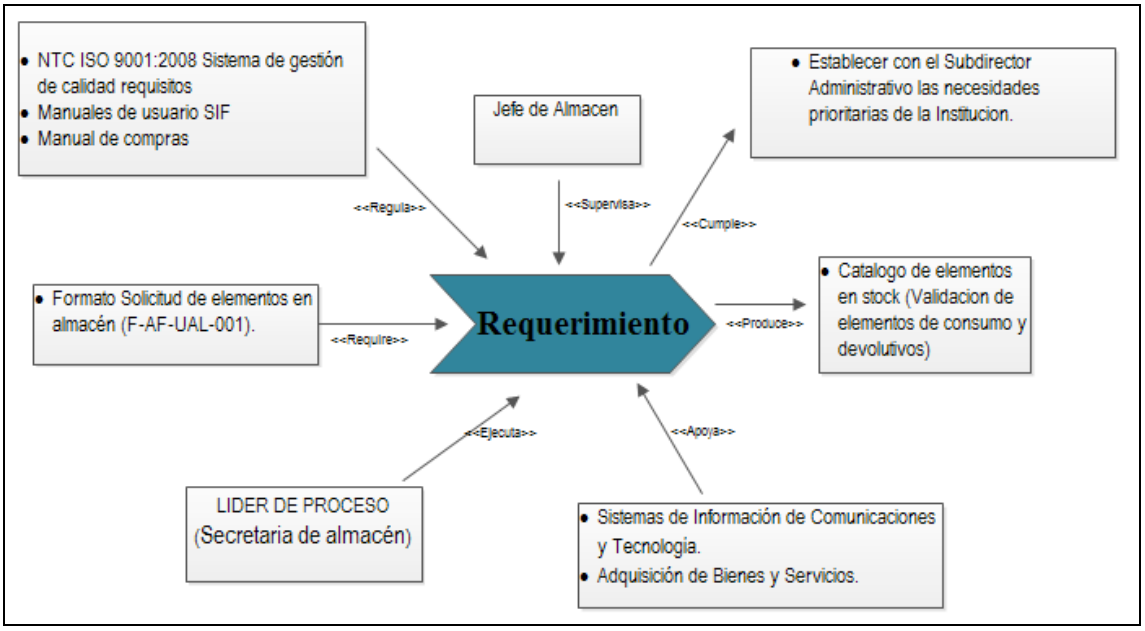
La descripción de subprocesos está compuesta por:

Figura 9. Subprocesos del proceso suministro



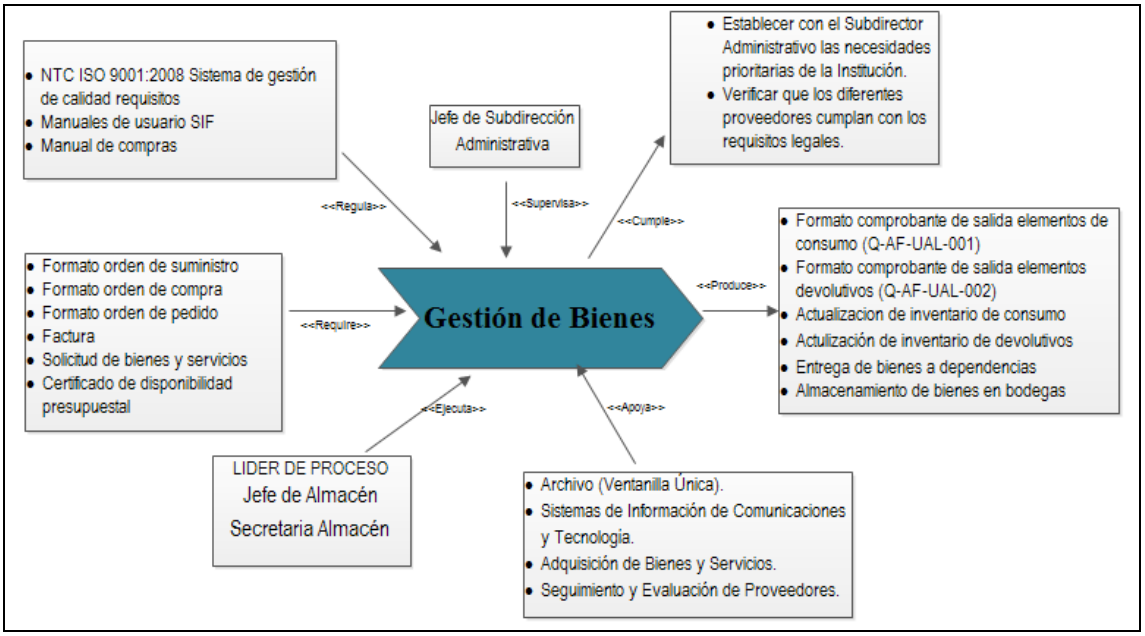
Fuente. Autores del Proyecto.

Figura 10. Subproceso requerimiento.



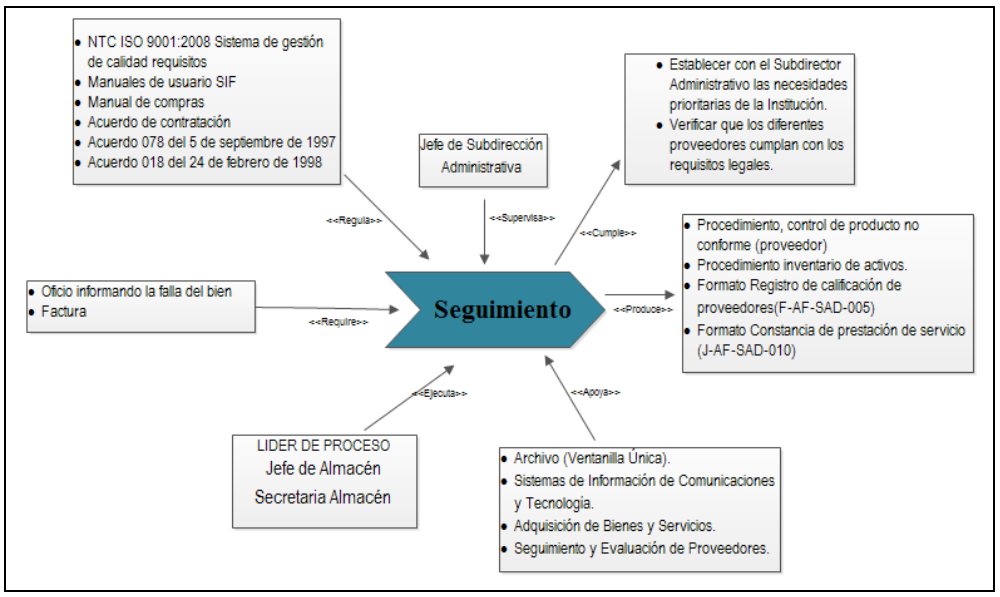
Fuente. Autores del Proyecto.

Figura 11. Subproceso gestión de bienes.



Fuente. Autores del Proyecto.

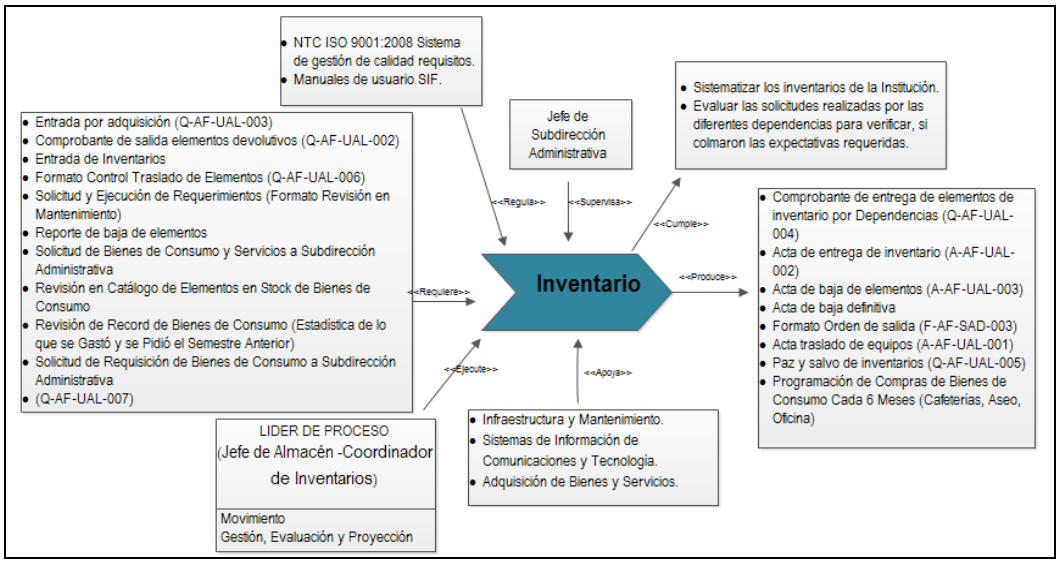
Figura 12. Subproceso seguimiento.



Fuente. Autores del Proyecto.

PF Inventario. Es un proceso de control, que consiste en confrontar los registros implementados para registrar el movimiento y ubicación de los bienes, con el recuento físico total o parcial de los mismos.

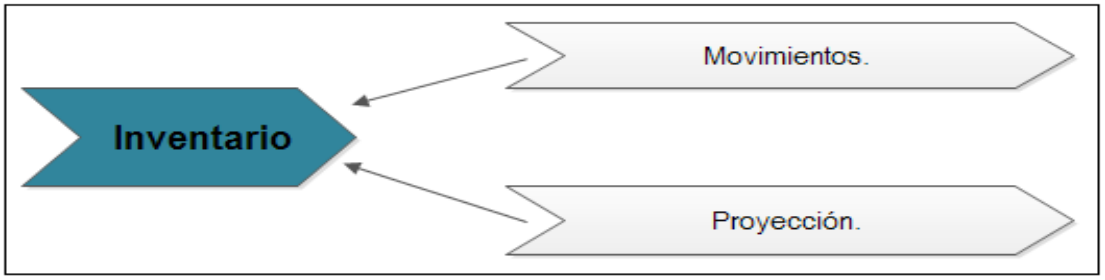
Figura 13. Proceso principal inventario



Fuente. Autores del Proyecto.

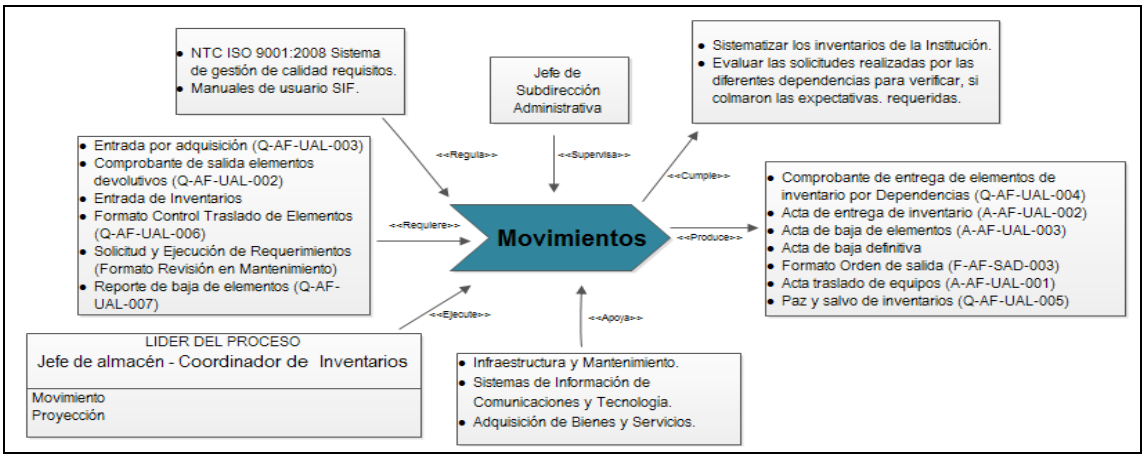
La descripción de subprocesos está compuesta por:

Figura 14. Subproceso del proceso inventario



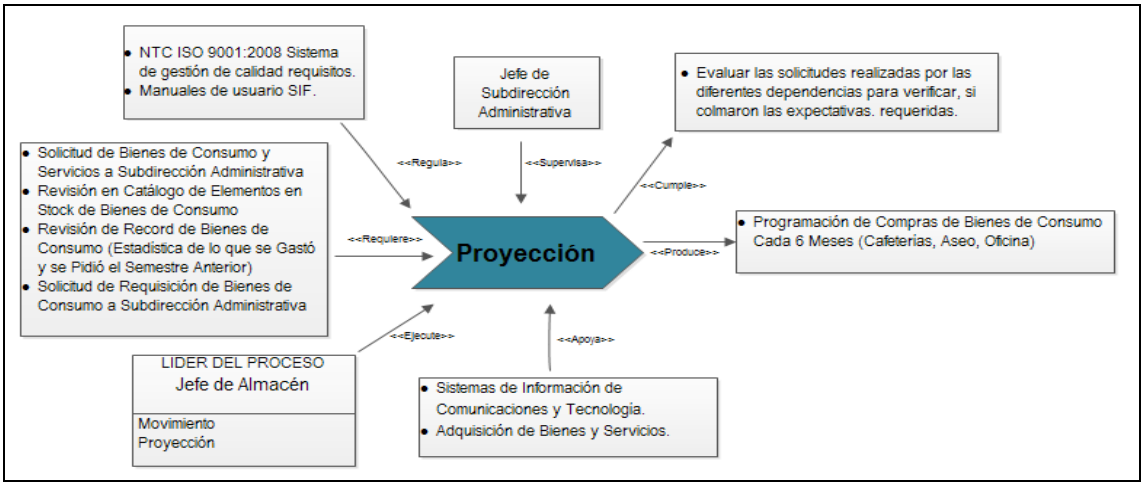
Fuente. Autores del Proyecto.

Figura 15. Subproceso movimiento.



Fuente. Autores del Proyecto.

Figura 16. Subproceso proyección.



Fuente. Autores del Proyecto.

4.1.4 Infraestructura tecnológica. La Unidad de Almacén de la Universidad Francisco de Paula Santander Ocaña, cuenta con equipos de cómputo en los espacios de trabajo. Se relaciona las características de los dispositivos para la ejecución de los procesos de la misma.

Dispositivos de cómputo y comunicaciones

Tabla 4. Equipos de cómputo de la Unidad de Almacén y sus características

Dispositivo	**Características y/o especificaciones**
PC Escritorio All in One (AIO) Coordinador(a) de Inventario	Hardware: - Procesador Intel® Core™ I3 3220, Velocidad 3.3 GHz -RAM 4GB -Disco Duro 500 GB -Monitor de 22 pulgadas -Tarjeta de Red incorporada Software: -Sistema Operativo Windows 7 32 bits -Microsoft Office 2010 -Sistema de Información Financiero (SIF). Módulo Almacén (Web)
PC Escritorio HP All in One (AIO) Secretario(a) Unidad de Almacén	Hardware: -Procesador Intel® Core™ I3-2120, Velocidad 3.3GHz -RAM 4GB -Disco Duro 500 GB -Monitor de 20 pulgadas -Tarjeta de Red 802.11 BGN Mini Card Software: -Sistema Operativo Windows 7 32 bits -Microsoft Office 2010 -Sistema de Información Financiero (SIF). Módulo Almacén (Web)
PC Escritorio HP All in One (AIO) Jefe de Unidad de Almacén	Hardware: -Procesador Intel® Core™ I3-2120, Velocidad 3.3GHz -RAM 4GB -Disco Duro 500 GB -Monitor de 20 pulgadas -Tarjeta de Red 802.11 BGN Mini Card Software: -Sistema Operativo Windows 7 32 bits -Microsoft Office 2010

	-Sistema de Información Financiero (SIF). Módulo Almacén (Web)
Impresora Láser Jet Pro	Modelo M1132 MFP -Marca HP -Serial CNG9C3WP4P
Teléfono	-Modelo KX-TS500LXB -Marca PANASONIC -Serial 31BAAA005966
Impresora de Código de Barras.	Modelo R-400K -Marca Argox

Fuente. Autores del Proyecto.

En cuanto a conectividad, se relaciona los dispositivos de comunicaciones.

Tabla 5. Dispositivos de comunicaciones y sus características

Dispositivo	**Características**
Servidor **HP ProLiant DL380 G5**	**Procesador:** -Tipo de procesador Intel Xeon, Upgradeable to 2 processors (8 cores). -Bus del sistema 1333 MHz. -Cache de 2° nivel 12 MB. -Placa base Intel 5000P. **Video:** -Tarjeta gráfica ES1000 -Características del adaptador de video Integrated ATI ES1000 1280 x 1024 x 16 M color -RAM de video 32 MB SDRAM Video Memory **Características técnicas:** Network Controller: Two embedded NC373i Multifunction Gigabit Network Adapters with TCP/IP Offload Engine, including support for Accelerated iSCSI through an optional Licensing Kit Internal Drive Support: (8) small form factor (SFF) hot-plug drive bays t **Posibilidades de almacenamiento interno** 2.0 TB SATA; 1.168 TB SAS (with optional hard drives) **Almacenamiento de disco:** -Capacidad 144GB -Interfaz Serial Attached SCSI (SAS) -Numero 2 y Tamaño 2.5” -Tipo 2 x 72 GB SAS Hot Plug 2.5" Hard Drive -Velocidad 10000 RPM **Memoria:** -RAM 64GB – 2048MB -Ranuras 8 DIMM -Tipo de memoria interna DDR2 -Velocidad del reloj 667MHz **Control de Energia:** -Tipo de fuente 800 Watt, CE Mark Compliant; Optional Hot Plug AC

	Redundant Power Supply; Optional 48 Volt DC Power Supply Kit (Factory integration not available) **Conectividad:** -N° de conexiones 2 -N° de puertos VGA 1 -N° de puertos USB 4 -N° puerto de ratón PS/2 2 -Puerto serie 1 -Puertos de E/S Serial - 1; Pointing Device (Mouse) - 1; Graphics - 1; Keyboard - 1; VGA - 2 (1 front, 1 back); Network RJ-45 - 2; iLO 2 remote management port - 1; USB 2.0 ports - 5 (2 front, 2 back, 1 internal)
Switch	**General** -Tipo de Dispositivo Conmutador - 24 puertos - Gestionado – apilable -Puertos 24x10/100 -Protocolo de gestión remota SNMP, RMON -Características Control de flujo, diseño modular, capacidad duplex, activable, apilable -Cumplimiento de normas IEEE 802.3, IEEE 802.3u, IEEE 802.1Q, IEEE 802.1p -Voltaje necesario CA 120/230 V (50/60 Hz) -Consumo eléctrico 75 vatios. **Expansión / Conectividad** -Interfaces 24 x 10Base-T/100Base-TX - RJ-45 - 24 1 x RS-232C - D-Sub de 9 espigas (DB-9) - 1 – gestión -Ranura de expansión 2 (total) / 2 (libre) x Ranura de expansión
Router	**Especificaciones Técnicas** -Puertos: Uno 10/100BASE-T, uno serie de alta velocidad (Sínc./Asínc.), uno de consola, uno serie AUX; una ranura para MIM y dos ranuras para SIC -Interfaces WAN: RDSI, ADSL, E1, T1, serie de alta velocidad, X.25, PPP, PPPoE, MP, Frame Relay, HDLC/SDLC -Interfaces de LAN: Ethernet 10/100, 10/100/1000 -Routing de WAN: IP, IPX, OSPF, BGP-4, IS-IS Integrado, RIP V1/V2, Routing Estático, VPN MPLS L2 y L3 -Seguridad: Stateful Firewall, VPN (L2TP, GRE, IPSec), ACLs, NAT, RADIUS, PAP/CHAP, TACACS+, certificados X.509 -Convergencia: QoS, Multicast IGMP, PIM-SM, PIM-DM, VLAN IEEE 802.1q, Routing Inter-VLAN, Multi-links -Resistencia ante fallos: VRRP, Centro de Backup (configuración / Puerto), Centro de Control de Marcación, multilink, soporte de imágenes duales -SDRAM: 128 MB -Flash: 32 MB -Dimensiones: Altura: 43,0 mm Anchura: 440,0 mm Fondo: 315,0 mm -Peso: 6 kg -Tensión de entrada: De 90 a 240 VAC -Consumo máximo de potencia: 60 W

Fuente. Autores del Proyecto.

La universidad se encuentra interconectada por medio de fibra óptica en los 4 edificios principales (casona, anexos, salas de cómputo y edificio del bloque B). La casona, anexos y las salas de cómputo con fibra óptica de 4 hilos y el edificio del bloque B con fibra óptica de 6 hilos.

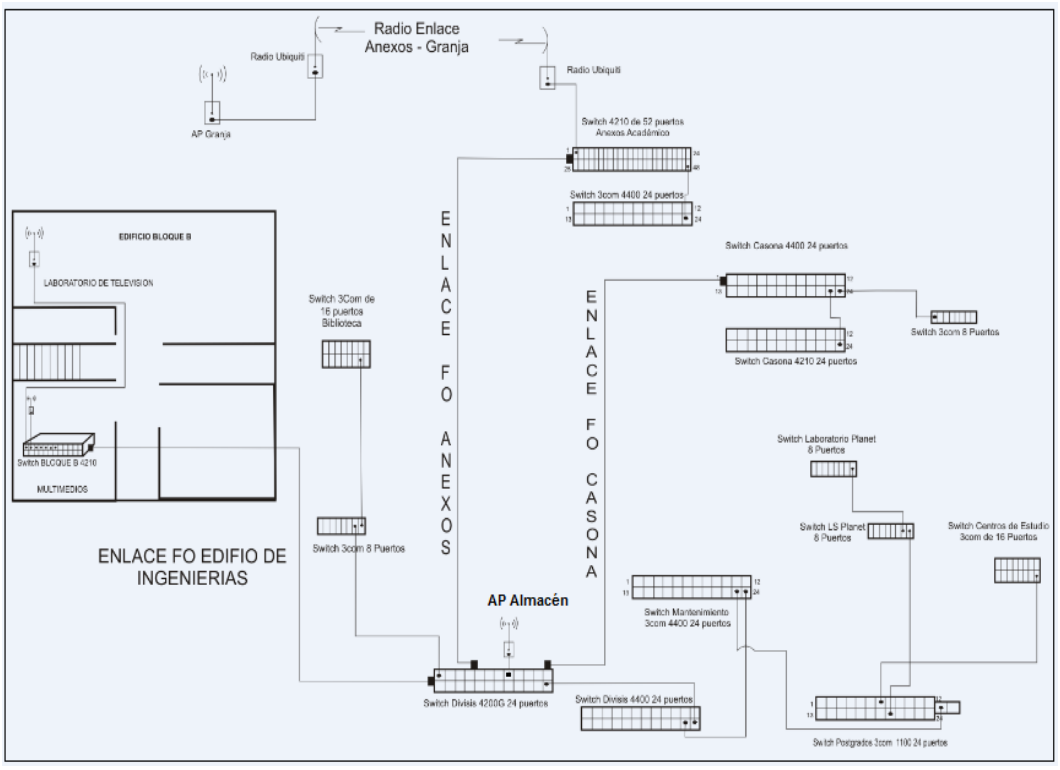
Anexos se encuentra cableado con categoría 7, las salas de cómputo se encuentran cableadas con categoría 7 y 5e, el edificio del bloque B se encuentra cableada con categoría 5e y la casona con categoría 5e.

EL cuarto de telecomunicaciones principal se encuentra ubicado en la Sistema de Información, Telecomunicaciones y Tecnología de la UFPSO, de este se desprende el cableado hacia los rack ubicados en la casona, anexos, salas de cómputo y edificio del bloque B respectivamente.

Hay actualmente tres redes separadas física y lógicamente.

Red Administrativa.

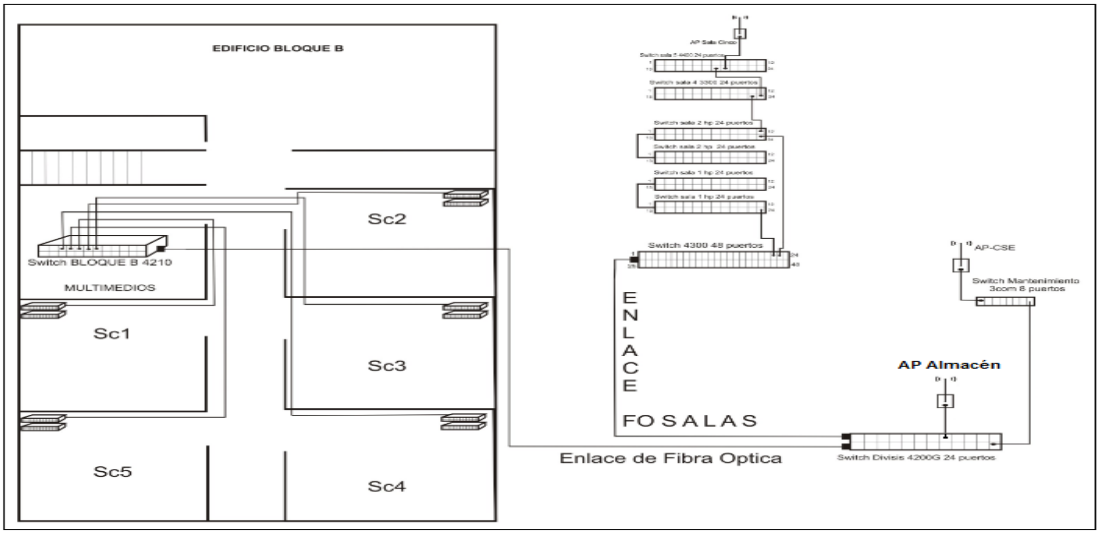
Figura 17. Plano de conectividad red administrativa – 2012.



Fuente: Sistema de Información, Telecomunicaciones y Tecnología

Red Académica.

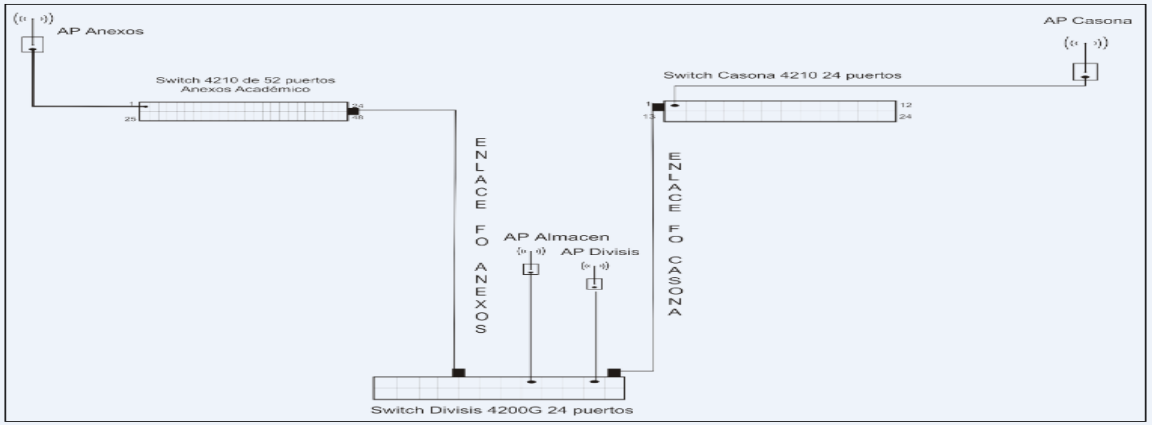
Figura 18. Plano de conectividad red académica – 2012.



Fuente: Sistema de Información, telecomunicaciones y tecnología

Red inalámbrica.

Figura 19. Plano de red inalámbrica – 2012.



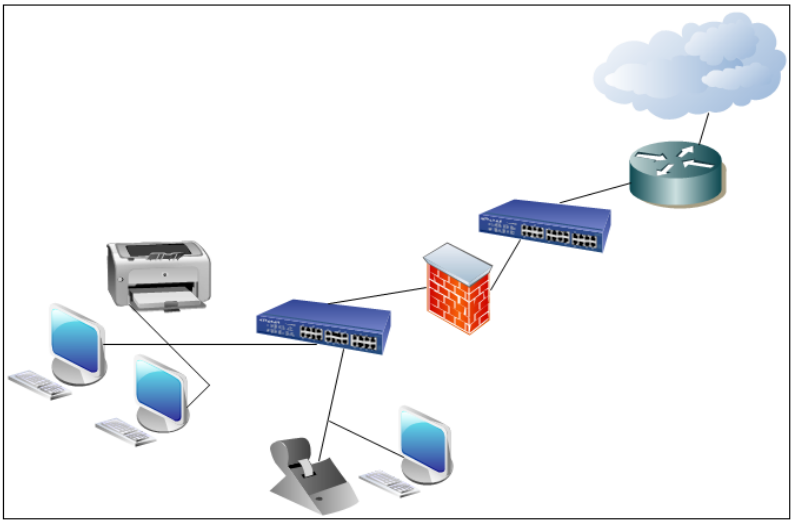
Fuente: Sistema de Información, telecomunicaciones y tecnología

Tipo de red. Referente al tipo de red, la Unidad de Almacén se encuentra inmersa en la red LAN de la UFPS Ocaña. La cual cuenta con un cableado de voz y datos.

LAN Ethernet 100/1000

Topología. La topología presente en la UFPS Ocaña es estrella-árbol extendida.

Figura 20. Esquema de red de datos de la Unidad de Almacén.



Fuente. Autores del Proyecto.

El proveedor de servicio de internet es ETB donde presta un canal de 20 MBytes. Para conectar las diferentes dependencias se utiliza cable UTP categoría 5e o 6 para exteriores.

Sistemas operativos. Los sistemas operativos de los equipos de cómputo de la Unidad de Almacén son Windows 7, y el servidor tiene sistema operativo Linux.

Tabla 6. Sistemas operativos

Dispositivo	**Sistema Operativo**
Equipo de cómputo Unidad de Almacén	Windows 7
Equipo de Cómputo Servidor	**Compatible.** Microsoft® Windows® Server 2000; Microsoft® Windows® Small Business Server 2003 R2; Microsoft® Windows® Server 2003; Microsoft® Windows® Server 2008; Microsoft® Windows® Server 2008 Hyper-V; Red Hat Enterprise Linux; SUSE Linux Enterprise Server

Fuente. Autores del Proyecto.

Sistemas de información

Sistema de Información Financiero (SIF). Módulo Almacén. Descripción: El módulo de Almacén, el cual pertenece al sistema de información financiero (SIF), de la Universidad Francisco de Paula Santander Ocaña, donde la información contenida permite que el

usuario pueda realizar entradas a elementos de una orden de compra teniendo en cuenta las facturas correspondientes, realizar además las requisiciones y posteriormente las salidas de los artículos dependiendo si corresponde a consumo o devolutivos. Además, permite hacer ingreso de artículos nuevos a sistemas y la manipulación de dependencias de acuerdo a los jefes de cada una para la asignación de los artículos solicitados por ellos.

Requisitos. Con el fin de garantizar el óptimo funcionamiento de la aplicación, es necesario contar con la disponibilidad de los siguientes requerimientos mínimos preliminares.

Técnicos (**Herramientas Tecnológicas).** La aplicación está desarrollada en Developer 2000, herramienta que permite la presentación y manipulación de los datos, a través de la inserción, consulta, actualización y borrado. En las aplicaciones de estos módulos se utilizan menús integrados para mayor navegabilidad. La base de datos es Oracle 10g que es una herramienta cliente/servidor.

Forms And Reports (Embebido en Oracle 10g).
Herramienta de Programación: PL/SQL.
Sistema Operativo Windows XP.
512 Mb Memoria RAM.

Usuario. Para la gestión del módulo de almacén, el usuario debe tener conocimientos sobre el manejo de editores de texto, hojas de cálculo.

A nivel de la información sobre los procesos que se realizan en el módulo el usuario debe tener conocimientos básicos de contabilidad.

En el Sistema de Información se encontrarán varias secciones que inician desde el ingreso al sistema hasta la forma de navegación, manipulación de reportes y formularios.

Componentes del Módulo de almacén.

Ingreso al Sistema. Este es un sistema que permite realizar las entradas de las distintas compras que se realizan en la institución así como la asignación de los artículos de consumo y devolutivos que se necesitan para el correcto funcionamiento de la entidad. El usuario se conectará a la unidad de red a través de una contraseña dada por el administrador del sistema, especificando la unidad de red.

Luego el usuario se conecta directamente al módulo principal con su nombre de usuario, contraseña y la base de datos, también asignadas por el administrador del sistema. Si el usuario ingresa por primera vez el sistema pedirá cambiar la clave de ingreso pues la que se asigna inicialmente es general.

Funciones. Son aquellas que permiten al usuario comunicarse con el sistema.

Descripción. Este marco de página permite modificar, agregar, eliminar o consultar artículos (entradas, salidas y traspasos), dependencias, funcionarios, proveedores, edificaciones, reportes, requisiciones, stock.

Análisis de Seguridad de las Oficinas. La Unidad de Almacén cuenta con dos bodegas, ambas situadas en la UFPS Ocaña, en las cuales se almacenan bienes de consumo y bienes devolutivos.

Las funciones de seguridad y de control de accesos a la oficina y las bodegas están delegadas al Jefe de Almacén y su Secretaria.

Número de Oficinas	2
Número de Bodegas	2
Número de Puertas	3
Tipo de Puertas	Metálicas
Estado de Puerta Oficinas	Abierta
Estado de Puerta Bodegas	Cerradas
Número de Personas Trabajando	3
Tipo de Actividad de Negocio	Almacén e Inventario
Acceso Independiente a la Zona de Oficina	Sí
Horario de Apertura	7 a.m. y 2 p.m.
Horario de Cierre	12 m. y 5 p.m.
Vigilancia Contratada Externa	Entrada a la Universidad
Extintores	No
Detectores de Humo	No
Medidas Contraincendios	No
Alarmas	No
Cámaras de Vigilancia	No
¿Plan de Evacuación de Oficina?	No
Central Telefónica Independiente	Sí
Número de Líneas Disponibles	1
Línea de Datos	Sí
Alimentación Eléctrica Independiente	No
Toma a Tierra	Si

Plan de Copias de Seguridad. Actualmente existen dos tipos de procedimientos de backup que se realizan sobre el Sistema de Información Financiera (SIF) Módulo Almacén:

Servidor (Interno).
Datacenter ETB (Externo).

A continuación se describirán con detalle cada uno de estos procedimientos, indicando en qué sistema se realizan, con qué frecuencia y que recursos son utilizados:

Servidor (Interno). Permite la recuperación de datos en caso de pérdida o destrucción de los mismos. La ejecución de las copias se hace exclusivamente en una ventana de tiempo nocturna que no interfiera la explotación normal del sistema. La ejecución de las copias de manera absolutamente planificada, se realizan automáticamente en el Servidor a las 12 de la noche diariamente. Este procedimiento obtiene una copia total de la máquina (servidor y base de datos), que puede ser utilizada no sólo para la recuperación total o parcial de ficheros, sino para el arranque del sistema con la configuración actual en que se encuentra. Semanalmente estas copias de seguridad son almacenadas en un CD, debidamente rotulado (con la fecha, hora y el responsable de la realización de la copia de seguridad).

Datacenter ETB (Externo). El proveedor del servicio de Internet, también presta el servicio de copias de seguridad por medio de un Datacenter que se encuentra ubicado en la ciudad de Bogotá, las copias se realizan diariamente a las 3 p.m.

Los dos procedimientos para hacer copias de respaldo son eficientes, válidos, están bien documentados y llevan funcionando correctamente desde hace tiempo. Sin embargo con el proceso de las copias de seguridad que se llevan en el servidor (Interna) y en los CD's, es que permanecen en el Centro de Procesamiento de Datos, por lo tanto, en caso de ocurrir cualquier catástrofe se perdería toda la información referente al Sistema de Información Financiera (SIF) Módulo Almacén. La solución a este problema es compleja, ya que exigiría tener un CPD alternativo configurado para poder realizar las replicaciones de los datos en lugares remotos.

4.1.5 Direccionamiento Estratégico Propuesto.

Durante la realización de la auditoria de sistemas al personal de la dependencia de la Unidad de Almacén de la Universidad Francisco de Paula Santander, se pudo evidenciar que el personal no conoce el Direccionamiento Estratégico del proceso, los funciones no tienen claro la Misión, Visión y objetivo; por esta razón se realizó un análisis los tópicos de la planeación estratégica, con el objeto de verificar si cumple con las características o requisitos de cada una de estas. Lo anterior permitirá crear estrategias que contribuyan a la eficiencia, eficacia y efectividad del proceso.

Evaluación de la Misión

Tabla 7. Evaluación de la Misión

EVALUACION DE LA MISION **Misión Actual:** La Unidad de Almacén de la Universidad Francisco de Paula Santander Ocaña, tiene como misión canalizar los diferentes requerimientos solicitados por la Institución, para de esta forma lograr los objetivos Institucionales.				
NO.	**CRITERIOS**	**PREGUNTA**	**SI**	**NO**
1	Clientes	¿Quiénes son los clientes?		X
2	Productos y Servicios	¿Cuáles son los servicios o productos		X

		más importantes?		
3	Mercados	¿Compite geográficamente?		X
4	Tecnología	¿Cuál es la tecnología básica?		X
5	Preocupación por supervivencia, crecimiento y rentabilidad	¿Cuál es la actitud de la organización en relación con metas económicas?		X
6	Filosofía	¿Cuáles son las creencias básicas, los valores, las aspiraciones, las prioridades éticas de la organización?		X
7	Concepto de sí misma	¿Cuáles son las ventajas competitivas claves?		X
8	Preocupación por la imagen pública	¿Cuál es la imagen pública a que aspira?, ¿Es responsable socialmente, ante la comunidad y el medio ambiente?		X
9	Preocupación por los empleados.	¿Son los empleados un valor activo para la organización? ¿Pone atención a los deseos de las personas claves, de los grupos de interés?		X

Fuente. Autores del Proyecto.

Realizado el análisis de la misión podemos concluir que: La Misión de la Unidad de Almacén no cumple con los criterios de evaluación.

No hace un detalle de los servicios que ofrece a sus clientes.
No tiene en cuenta el talento humano, las tecnologías y la responsabilidad ambiental.

Misión que se propuesta para la dependencia:

La Unidad de Almacén apoya a los diferentes procesos de la Universidad Francisco de Paula Santander Ocaña, con el suministro e inventario de bienes, Inmuebles, bienes de consumo y devolutivos, utilizando la Tecnología de la Información y Comunicaciones, para brindar un buen servicio con eficacia, eficiencia, confiabilidad y cumplimiento, con un personal idóneo, comprometido con el mejoramiento continuo y con responsabilidad ambiental.

Evaluación de la Visión

Tabla 8. Evaluación de la Visión

No.	EVALUACION DE LA VISION **Visión Actual:** La Unidad de Almacén de la Universidad Francisco de Paula Santander Ocaña, tendrá como visión velar que en las diferentes dependencias sepan dar un buen manejo de los diferentes elementos que le son entregados.	SI	NO
1	Orientado al futuro incluso en su redacción		X
2	Es integradora	X	
3	Es corta		X
4	Es positiva y alentadora		X
5	Es realista – posible		X
6	Es consistente con los principios y valores de la organización		X
7	Orienta la transición de los que es a lo que debe llegar a ser		X
8	Expresa claramente los logros que se esperan en el periodo		X
9	Cubre todas las áreas actuales y futuras de la organización		X
10	Está redactada en términos que signifiquen acción		X
11	Tienen fuerza e impulsa a la acción		X
12	Contiene el futuro visualizado		X
13	Es el sueño alcanzable a largo plazo		X

Fuente. Autores del Proyecto.

Realizado el análisis de la visión podemos concluir que: La visión no cumple con los criterios de evaluación de la misma, excepto que es integradora porque incluye las dependencias de la UFPSO

Visión que se propuesta para la dependencia:
Para el año 2017 la Unidad de Almacén de la UFPSO logrará confiabilidad en el registro, ubicación, clasificación, características, estado, cantidad y valor de los bienes de propiedad de la universidad, con un mejoramiento continuo, asumiendo los retos tecnológicos, cumpliendo con el plan institucional de gestión ambiental.

Perfiles del Personal a Cargo de los Procesos de la TIC

Tabla 9. Personal a Cargo de las TIC

PERSONAL A CARGO DE LAS TIC		
DEPENDENCIA UNIDAD DE ALMACEN DE LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDEROCAÑA		
	ENCARGADO	
PERFIL	CARGO	RESPONSABLE
Director Ejecutivo (CEO)	Director UFPSO	Edgar Antonio Sánchez Ortiz

Director Financiero (CFO)	Subdirector Administrativo	Jorge de Jesús Cañizares Arévalo
Ejecutivos del Negocio	Planeación	Luis Augusto Jácome
Director de Información (CIO)	División de Sistemas	Antón Garcia Barreto
Propietario del Proceso del Negocio	Jefe de la dependencia de la Unidad de Almacén	Nahún Lobo
Jefe de Operaciones	Profesionales responsable de los inventarios	Maylin Barbosa Navarro
Arquitecto en Jefe	Encargados Sistemas de Información financiero	Byron Cuesta Quintero
Jefe de Desarrollo	Encargados Sistemas de Información financiero	Byron Cuesta Quintero
Jefe de Administración de TI	Encargado de la División de Sistemas	Antón García Barreto
La Oficina de Administración de Proyectos (PMO)	Oficina de Planeación	Luis Augusto Jácome
Cumplimiento, auditoria, riesgo y seguridad	Oficina de Calidad y control interno	Yurley Constanza Medina Claudia Pilar Quintero

Fuente. Autores del Proyecto.

4.2 MANUAL DE GESTIÓN O PLAN DE CONTINUIDAD DEL NEGOCIO PARA LA UNIDAD DE ALMACÉN CON BASE EN LA NORMA ISO/IEC 27002

Aspectos de la Seguridad de la Información de la Gestión de Continuidad del Negocio. En este paso se deben 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. Por tanto, la seguridad de la información debe ser una parte integral del proceso general de continuidad del negocio, y otros procesos gerenciales dentro de la Unidad de Almacén.

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.

4.2.1 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 la Unidad de Almacén, para tratar los requerimientos de seguridad de la información necesarios para la continuidad comercial de la misma.

Este apartado se trata en el **Capítulo 4.1.** El proceso debe reunir los siguientes elementos claves de la gestión de continuidad del negocio:

Reconocimiento de la Filosofía Institucional y del Modelo de Procesos de Negocio de la Unidad de Almacén.
Identificación y priorización de los procesos comerciales críticos de la Unidad de Almacén.
Identificar todos los activos involucrados en los procesos comerciales críticos de la Unidad de Almacén: Infraestructura Tecnológica (Dispositivos de Cómputo y Comunicaciones, Sistema de Información Financiero – Módulo Almacén), Infraestructura, Bienes Muebles y de Consumo.

4.2.2 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.

El análisis de riesgos es fundamental en cualquier Plan de Continuidad de Negocio. Mediante este análisis, se reconocen todas aquellas amenazas a las que se enfrenta la Unidad de Almacén. De esta manera, se pueden conocer los potenciales problemas que pueden surgir y el grado de seguridad existente para poder evitarlos.

Una vez conocidas aquellas amenazas que pueden ocurrir sobre la Unidad de Almacén, se podrán estudiar los mecanismos de prevención y recuperación existente y poder determinar si éstos son válidos o necesitan ser corregidos.

Los conceptos que van a ser utilizados en el Análisis de Riesgos son los siguientes:

Activo: Componente del sistema al que la Organización le asigna un valor.
Amenaza: Ocurrencia de un evento que cause un impacto no deseado.
Riesgo: Posibilidad de que una amenaza se realice.
Vulnerabilidad: Debilidad o ausencia de medidas de salvaguarda.
Salvaguarda: Medida de control para reducir el riesgo asociado a una determinada amenaza.

El Análisis de Riesgos va a constar de tres fases:

Matriz de riesgos. Matriz con las posibles amenazas, el riesgo asociada a éstas para cada grupo de activos, la valoración de las medidas de control existentes para cada amenaza y el riesgo residual resultante de las medidas de control para cada amenaza. El valor del riesgo residual determina de manera relativa las vulnerabilidades existentes respecto a las distintas amenazas.

Medidas de prevención y control. Se estudia, para cada amenaza, las causas que pueden causar la ocurrencia de éstas, las medidas de prevención y control existentes y se proponen otras medidas para su implantación.

Estudio de Vulnerabilidades. A partir de la fase anterior, se determinan los puntos débiles de la Unidad de Almacén para cada amenaza existente, se analizan las posibles medidas de salvaguarda a implantar y se determinan cuáles deben de ser implantadas finalmente.

Matriz de Riesgos. El propósito general de la identificación de los peligros y la valoración de los riesgos en la Unidad de Almacén, es entender los peligros que se pueden generar en el desarrollo de las actividades con el fin que ésta pueda establecer los controles necesarios al punto de asegurar que cualquier riesgo sea aceptable.

La valoración de los riesgos es la base para la gestión proactiva de la Unidad de Almacén, liderada por la alta dirección como parte de la gestión integral del riesgo, con la participación y compromiso de todos los niveles de la Institución y otras partes interesadas. Independientemente de la complejidad de la valoración de los riesgos, éste debería ser un proceso sistemático que garantice el cumplimiento de su propósito (Ver Anexo).

Para que Sirve. Identificar los peligros asociados a las actividades en el lugar de trabajo y valorar los riesgos derivados de estos peligros para poder determinar las medidas de control necesarias.

Tomar decisiones en cuanto a la selección de infraestructura tecnológica, materiales, herramientas, métodos, procedimientos, equipo y organización del trabajo con base en la información recolectada en la valoración de los riesgos.

Comprobar si las medidas de control existentes en el lugar de trabajo son efectivas para reducir los riesgos.

Priorizar la ejecución de acciones de mejora resultantes del proceso de valoración de los riesgos.

Demostrar a las partes interesadas que se han identificado todos los peligros asociados al trabajo y que se han dado los criterios para la implementación de las medidas de control necesarias para proteger la seguridad y la salud de los trabajadores.

Actividades de Identificación de Peligros y Valoración de Riesgos. Definir el instrumento para recopilar la información.

Clasificar los procesos, actividades y las tareas.
Identificar los peligros.
Identificar los controles existentes.
Valorar riesgo.
Definir los criterios para determinar la aceptabilidad del riesgo.
Definir si el riesgo es aceptable.
Elaborar el plan de acción para el control de los riesgos con el fin de mejorar los controles existentes si es necesario, o atender cualquier otro asunto que lo requiera.
Revisar la conveniencia del plan de acción.
Mantener y actualizar: Realizar seguimiento a los controles nuevos y existentes y asegurar que sean efectivos; asegurar que los controles implementados son efectivos y que la valoración de los riesgos está actualizada.
Documentar el seguimiento a la implementación de los controles establecidos en el plan de acción.

Identificación de Peligros. Descripción y Clasificación de Peligros

Para identificar los peligros, se recomienda plantear una serie de preguntas como las siguientes:

¿Existe una situación que pueda generar daño?
¿Quién (o qué) puede sufrir daño?
¿Cómo puede ocurrir el daño?
¿Cuándo puede ocurrir el daño?

Efectos Posibles. Para establecer los efectos posibles de los peligros sobre la integridad o salud de los trabajadores, se debe tener en cuenta preguntas como las siguientes:

¿Cómo puede ser afectado el trabajador o la parte interesada expuesta?
¿Cuál es el daño que le(s) puede ocurrir?

Se debería tener en cuenta el nivel de daño que puede generar en las personas.

Identificación de los Controles Existentes

Las organizaciones deberían identificar los controles existentes para cada uno de los peligros identificados y clasificarlos en:

Fuente
Medio
Individuo

Valorar el Riesgo. La valoración del riesgo incluye:

La evaluación de los riesgos teniendo en cuenta la suficiencia de los controles existentes.

La definición de los criterios de aceptabilidad del riesgo.

La decisión de si son aceptables o no, con base en los criterios definidos.

Definición de los Criterios de Aceptabilidad del Riesgo

Para determinar los criterios de aceptabilidad del riesgo, la Unidad de Almacén debería tener en cuenta entre otros aspectos, los siguientes:

Cumplimiento de los requisitos legales aplicables y otros.
Aspectos operacionales, técnicos, financieros, sociales y otros.
Opiniones de las partes interesadas.

Evaluación de los Riesgos

La evaluación de los riesgos corresponde al proceso de determinar la probabilidad de que ocurran eventos específicos y la magnitud de sus consecuencias, mediante el uso sistemático de la información disponible.

Para evaluar los riesgos inherentes a la Unidad de Almacén, se tienen en cuenta los siguientes aspectos en la identificación y valoración de riesgos; activo, tipo de activo, descripción y el propietario del mismo:

Activos de TI (Hardware y Software).
Información (SIF).
Medio Ambiente e Infraestructura (Oficinas Administrativas, Bodegas y CPD).
Personas (Personal Administrativo y Personal Operativo).
Comunicaciones (Red Local e Internet).

Luego se realiza la evaluación de impacto potencial adverso en el negocio, teniendo en cuenta las dimensiones como la confidencialidad, integridad y disponibilidad de la información, con unos rangos establecidos para esta evaluación.

0- Muy bajo
1- Bajo
2-Medio
3- Alto
4- Crítico

La valoración del activo promedio se halla sumando el valor dado a las dimensiones y luego dividiéndolas entre 3.

Se identifican las distintas amenazas que van a ser tenidas en consideración para hacer el estudio de las vulnerabilidades del sistema son:

Incendio [Inc]
Inundación [Inn]
Cortes de corriente [Crt.]
Cortes de comunicación [CdC]
Sabotaje [Sbt]
Terrorismo [Trr]
Fallo de Hardware [FdH]
Fallo de Software [FdS]
Robo [Rbo]
Virus [Vrs]

Se han contemplado estas amenazas por ser las más probables en el ámbito que se está tratando.

Para las amenazas y las vulnerabilidades se clasifican con una valoración en un rango establecido para esta evaluación:

Baja
Media
Alta

La probabilidad de que ocurra la amenaza está definida en los siguientes rangos:

Muy Raro
Poco Probable
Probable
Muy Probable
Prácticamente Seguro

El impacto de la amenaza es igual a la valoración activo promedio. Para cada uno de los tipos de activos a proteger, se establece una valoración de la pérdida media que ocasionaría esa amenaza en todos los activos clasificados según ese tipo.

Por último la medida del riesgo es igual a la probabilidad por el impacto.
Después de calcular la medida del riesgo total, se establece el porcentaje de la efectividad del control.

Esto es el porcentaje del riego total que se mitigaría con la medida o medidas de control y prevención que existen para reducir los efectos probables de la ocurrencia de una amenaza.

Medidas de Prevención y Control. A continuación, se enumeran las medidas existentes actualmente en funcionamiento y propuestas para las distintas amenazas estudiadas.

Incendio. Un incendio puede provocar la destrucción o inutilización total de los activos que se ven afectados por él.

Las causas que pueden provocar un incendio pueden ser:

Eléctricas (cortocircuitos, líneas recalentadas).
Roces y fricciones.
Chispas mecánicas de aparatos y cables en mal estado.
Cigarrillos y fósforos.
Incendio espontáneo.
Superficies calientes.
Chispas de combustión.
Llamas abiertas.
Soldadura.
Materiales recalentados.
Electricidad estática.

Las medidas que existen en la actualidad para prevención y control de inundaciones son:

Existen 2 extintores situados en la Unidad de Almacén, se recargan anualmente, pero al momento de la revisión no cuentan con las fechas en orden.
Dentro del plan de emergencia existe el plan operativo normalizado sobre situaciones de incendio.
Se realiza formación, capacitación, entrenamiento y simulacros al personal sobre situaciones de emergencia con el apoyo de Positiva ARL.
Se realizan revisiones periódicas de las instalaciones eléctricas existentes (enchufes, aparatos eléctricos obsoletos) en compañía de Positiva ARL utilizando el formato J-GH-DRH-003 y se realizan informes para su respectivo control.
Materiales de seguridad antiincendios almacenados en un lugar estratégico. Existen extintores en cada piso, el grupo de brigadas cuenta con cada uno de los elementos de seguridad.

Las medidas de prevención y control antiincendios que no están actualmente contempladas en la Unidad de Almacén son:

Aparatos de detección de humo situados en el techo de la oficina de Almacén y la Coordinación de Inventario, además de las dos bodegas.
No existen extintores situados en las dos bodegas.
Responsable de Seguridad con formación antiincendios y manejo de extintores.
Sistemas de detección y extinción automática de incendios (sistemas de aspersión).
Señalización y almacenamiento de recipientes con materiales inflamables.

Estas medidas, aunque correctas y necesarias, no son suficientes para evitar o minimizar el riesgo de un incendio dentro las oficinas y bodegas de la Unidad de Almacén. Por tanto se ha valorado la efectividad de los controles antiincendios con un 40%.

Inundación. Las inundaciones en el lugar de trabajo pueden causar daños graves en los activos de la Unidad de Almacén. Las causas más frecuentes suelen ser:

Rotura de cañerías.
Humedades.
Filtraciones.
Lluvias torrenciales.

Las medidas que existen en la actualidad para prevención y control de inundaciones son:

Normas sobre situaciones de inundación. Existe dentro del plan de emergencias, un plan operativo normalizado, en donde se establece el procedimiento según la normatividad vigente.
Formación del personal para casos de emergencia. Se realiza capacitación y entrenamiento 2 veces al año por parte de Positiva ARL.
Revisión cada cierto tiempo del estado de desagües y sumideros. Se realiza por parte de Infraestructura y Mantenimiento con el asesoramiento del Coordinador de Sistema de Gestión Ambiental.

Las medidas de prevención y control de inundaciones que no están actualmente contempladas en la Unidad de Almacén son:

Mantener bombas hidráulicas en caso de emergencia.
Crear muros de con tensión o barricadas en caso de desbordamiento del río.

La Unidad de Almacén corre riesgo en caso de inundaciones, ya que está situada en la planta baja de la Universidad, cerca de los baños de la Institución. Además, el Río Algodonal pasa de forma limítrofe a la Institución donde existe un riesgo medio de sufrir inundaciones. Por tanto, se han considerado que el porcentaje de la efectividad de los controles para las inundaciones es del 50%.

Cortes de Corriente. Los cortes de corriente pueden dejar parados los procesos de negocio de la Unidad de Almacén durante el tiempo que estos duran. Además, pueden producir otros efectos colaterales, como la pérdida de información o inestabilidad en los sistemas.

Las causas más comunes que suelen provocar este tipo de contingencias son:

Conmutaciones en la red eléctrica (picos de tensión).
Fluctuaciones de tensión.
Averías en el suministro eléctrico.
Tormentas Eléctricas.

Existen una serie de medidas preventivas instaladas y otras medidas para debilitar los posibles efectos de la ocurrencia de una incidencia de este tipo, que son:

Sistema de alimentación ininterrumpida (SAI), para los servidores situados en el Centro de Procesamiento de Datos de la Universidad.
Mantenimiento del SAI con revisiones periódicas (Personal de Mantenimiento).

Estabilizadores de corriente repartidos en la Unidad de Almacén y la Coordinación de Inventarios.
Uso de pararrayos (1).
Se realizan revisiones periódicas de las instalaciones eléctricas existentes (enchufes, aparatos eléctricos obsoletos) en compañía de Positiva ARL utilizando el formato J-GH-DRH-003 y se realizan informes para su respectivo control.

Normalmente, los cortes de corriente en la Unidad de Almacén se han dado por averías, tormentas o fallos del suministro eléctrico, y nunca han sido de larga duración. Por tanto, se ha considerado que el porcentaje de eficacia de las medidas protectoras contra los cortes de corriente son del 80%, ya que la mayor parte de cortes de corriente de corta duración se resuelven mediante el uso de los sistemas de alimentación ininterrumpida.

Cortes de comunicaciones. Los cortes de comunicaciones son aquellas contingencias que impiden o interrumpen de forma más o menos prolongada la transmisión de datos o de voz. Dado que en la Institución existen diferentes redes (alámbricas e inalámbricas), es crítico para los procesos de negocio de la Unidad de Almacén la pérdida de comunicación eventual ya que paraliza el manejo de los inventarios de la misma.

Las causas que suelen provocar este tipo de contingencias son la destrucción total o parcial de las infraestructuras de las compañías de suministro telefónico y/o de los proveedores de los servicios de internet (ISP).

Actualmente existen medidas preventivas o de control en la Institución para evitar o minimizar los daños de este tipo.

Planificación de rutas de comunicación alternativas entre las diferentes redes (actualmente la comunicación entre las diferentes redes de la Institución se hace por medio de Internet e Intranet). Uso de fibra óptica, inalámbrica, cable categoría 7A y restricción por direccionamiento IP.

Por tanto, se ha estimado que el porcentaje de eficacia de las medidas de control es del 50%.

Existen ciertas medidas cuya implantación en los sistemas de transmisión de datos de la Institución se ha de estudiar a fin de prevenir los cortes de comunicación o reducir el impacto que éstos pueden tener:

Implantación de centralitas de voz alternativas para casos de emergencia.

Sabotaje. Sabotaje incluye todo tipo de daños intencionados realizados a los activos o procesos de la Universidad, realizados normalmente por alguna persona propia de la misma, a fin de perjudicar sus intereses.

Las causas más comunes suelen ser actos de venganza o de reivindicación por parte de trabajadores despedidos o descontentos con la propia Institución.

En cuanto a las medidas de protección y control que existen a este respecto, se han identificado las siguientes:

Existencia de una política de gestión de identidades, para el acceso a la información Institucional. Asignación de perfiles de usuarios a los trabajadores.

Existencia de una política para la prevención de pérdida de datos sensibles. Medidas de control para el acceso a la información de tipo sensible (Protocolos, privilegios, usuarios y roles).

Acceso al Centro Procesamiento de Datos restringido únicamente al Responsable de Sistemas de Información, Telecomunicaciones y Tecnología, Soporte de Comunicaciones y Soporte de Servidores.

Publicar un código o protocolo de buen uso de las herramientas informáticas dentro de la Unidad de Almacén, que delimite el uso que pueden hacer de éstas los empleados.

Existencia de una cláusula contractual que deben firmar los trabajadores de la Institución por la cual se comprometen a hacer un buen uso de los materiales y tecnologías de la misma.

Estas medidas aseguran en un alto porcentaje la inexistencia de contingencias provocadas por actos de sabotaje, sin embargo, no se puede asegurar que estas medidas eviten con total seguridad la posibilidad de ocurrencia del mismo, ya que en la Universidad se presentó un caso de sabotaje en el cambio de notas a estudiantes por parte de un empleado de la misma. Por tanto, se ha estimado en un 85% la eficacia de estas medidas.

Terrorismo. Son acciones llevadas a cabo por personas ajenas a la Institución que atentan contra la integridad de los empleados y de los activos de la misma.

Las causas de las acciones terroristas suelen ser políticas e inconformidades sociales.

Actualmente, hay implantadas una serie de medidas y políticas preventivas y de control para evitar y/o minimizar los posibles daños que podrían producirse como efecto de un atentado terrorista, que son las siguientes:

Control de acceso a las oficinas: Las empresa de seguridad que vigila la Universidad está ubicada en la entrada para el control del acceso a ésta, evitando el ingreso de personas que no estén autorizadas. Existe un registro para las personas que van a hacer una visita puntual, y se les concede un acceso limitado y temporal.

Sistemas de entrada/salida: Puertas de madera y metálicas en los accesos a las oficinas. Puertas metálicas también para el acceso a la Unidad de almacén y bodegas. Deberían ser blindadas o de cierre automático.

Estas medidas aseguran en un alto porcentaje la posibilidad de ser objetos de ataques externos. El hecho de tener una empresa subcontratada (Viprioriente) para asegurar la integridad tanto de los empleados como de los activos de la Institución asegura un tratamiento profesional de la seguridad y evita el gasto de recursos excesivos. Se ha valorado en un 50% la eficacia de las medidas de control contra el terrorismo.

Aun así, se proponen una serie de medidas complementarias para hacer un estudio de su implantación para reforzar la eficacia de las medidas anteriores:

Sistemas de seguridad: No existen una serie de cámaras conectadas en circuito cerrado, que vigilan y controlan el acceso a la oficina de Almacén, Inventario y Bodegas.

Instalación de sistemas anti intrusión en los complejos de la Institución. Estos sistemas no están incluidos en los contratos con la empresa de seguridad encargada de la vigilancia de los inmuebles de la Universidad. Por tanto, debería hacerse aparte y probablemente con una segunda empresa de seguridad.

Implantación de un sistema de control de acceso al Centro de Procesamiento de Datos mediante lectores de tarjetas unipersonales, distribuidas únicamente a los encargados del Proceso de Apoyo de Sistemas de Información, Comunicaciones y Tecnología.

Fallo de Hardware. Un fallo de hardware es una de las contingencias más críticas que puede darse, ya que en caso de avería de un servidor podrían paralizarse varios de los procesos más importantes para el negocio, además de consecuencias secundarias graves como la pérdida de información de las bases de datos.

En caso de avería de equipos para el personal, sería menos grave, pero podría impedir el trabajo de un empleado durante un tiempo determinado. Si se diese un error de hardware en periféricos también se retrasarían algunas funciones y podría rebajarse el nivel de servicio.

Para evitar estas situaciones y contrarrestar el posible efecto de la ocurrencia de un fallo de hardware actualmente se tienen dispuestas una serie de medidas:

Se cuenta con personal de mantenimiento de equipos informáticos, servidores, impresoras, escáneres, monitores, switches y otros periféricos hardware.

Provisión de recursos de hardware para usuario final, para poder trabajar en el caso si la reparación de un recurso es de larga duración.

Replicación diaria de la información de los PCs en discos de los servidores con frecuencia semanal.

Realización de copias de seguridad de los discos de los servidores fuera de la Universidad (Servicio de Datacenter con ETB en Bogotá y estos a su vez en Estados Unidos).

La Universidad cuenta con un proveedor de recursos hardware que le ofrece garantía y la sustitución de los equipos en caso de salir defectuosos o en mal estado. Sin embargo, se ha constatado que no existen medidas efectivas que ayuden a prever los fallos de hardware, por tanto se valora en un 50% la efectividad de los controles.

Fallo de Software. Los fallos de software pueden afectar a aplicaciones y datos de la Unidad de Almacén, pudiendo paralizar incluso procesos críticos del negocio. Hay una amplia gama de errores de software, entre los que destacan:

Errores de programación: Aplicaciones, normalmente internas, con fallos graves de programación que son detectados en algún momento de la ejecución de éstas.

Errores del sistema operativo: Son errores que suelen causar una interrupción involuntaria de la actividad en un PC o incluso en servidores.

Errores en la gestión de cambios de software: La gestión de cambios abarca todas aquellas operaciones y protocolos que se llevan a cabo cuando es necesario realizar cambios en algún software. Algunos ejemplos son:

Cambios evolutivos en las aplicaciones: Extensión o reducción de las funcionalidades de una aplicación.
Cambios correctivos en las aplicaciones: Pequeñas modificaciones realizadas en un software para corregir posibles errores o comportamientos.
Instalación de aplicaciones: Implantación de software de nuevo uso en el sistema.

Las medidas implantadas para la previsión y el control de los errores de software son:

Protocolo para la gestión de cambios: Existe un protocolo para poner en funcionamiento cualquier cambio en aplicaciones instaladas (actualización versiones, parches, instalación de aplicaciones nuevas). Antes de realizar la gestión de cambios directamente en un entorno de producción, se realizará un simulacro en un entorno de pruebas. Se aplican los parches cada vez que hay un cambio para seguridad de la máquina.

Entorno de pruebas fiable, con una configuración similar al entorno de producción.

Utilizar únicamente software de confianza. Control de licencias.

Política de administración de máquinas: El perfil de los empleados en las máquinas, no podrán instalar aplicaciones en sus PCs. Únicamente el responsable del proceso de apoyo de Sistemas de Información, Comunicaciones y Tecnología o a quien delegue pueden acceder como administrador local a todos los ordenadores e instalar aplicaciones nuevas.

Establecer un procedimiento para controlar los accesos a los servidores de aplicaciones, mediante ficheros de log, que deberán ser revisados periódicamente por el encargado del proceso de apoyo de Sistemas de Información, Comunicaciones y Tecnología.

Poner en funcionamiento un departamento de calidad, o al menos un encargado, que realice las funciones de control de las aplicaciones instaladas, supervisión de la gestión de cambios y de la documentación de todas las aplicaciones instaladas en la Institución.

Estas medidas aseguran en un buen porcentaje la prevención de errores de software. Se ha estimado en un 85% la eficacia de las medidas de control para estas contingencias.

Robo. Los robos son aquellas acciones perpetradas por empleados o por personas ajenas a la Institución para quedarse en propiedad activos pertenecientes a la misma.

El mayor peligro de este tipo de amenazas son los robos de datos sensibles de la Universidad y de la Unidad de Almacén, ya que esto no sólo supondría una pérdida económica inmediata, sino que además supondría una pérdida de prestigio muy importante.

En la actualidad, se han constatado una serie de medidas para evitar y minimizar los riesgos y efectos de un posible robo:

Seguro por robo de equipos hardware.
Inventario de equipos hardware de cada dependencia. Repuestos suficientes para hacer una sustitución rápida.
Control de accesos: La empresa de seguridad se encarga del control y supervisión de los accesos a los inmuebles de la Institución.
Control de acceso al Centro de Procesamiento de Datos: La sala donde está ubicado tiene una puerta de acceso semiautomática, que permanece habitualmente cerrada y cuenta con una secretaria que autoriza el ingreso a esa zona restringida.
Seguridad en el almacén y las bodegas: El almacén cuenta con una puerta metálica que todo el tiempo se encuentra abierta y el ingreso se hace sin la respectiva identificación, además no se lleva a cabo una política de escritorios limpios. Las bodegas cuentan con puertas metálicas que todo el tiempo se encuentran cerradas y el ingreso se hace con la autorización del Jefe de Almacén.

Estas medidas parecen razonables para evitar en gran medida los robos o hurtos de equipos hardware, dadas las dimensiones de las oficinas de la Institución y la cantidad de empleados existentes. Sin embargo, existen algunas carencias en la prevención en cuanto a robos de datos o información. Se estima en un 70% la efectividad de las medidas de control para este tipo de amenazas.

Se proponen las siguientes medidas para mejorar el sistema de prevención y control de robos:

Instalar sistemas de prevención de robos de datos en los equipos por medio de USB.

Existen herramientas software que impiden que se ejecute el auto arranque de los dispositivos USB.

Establecer una política de seguridad antirrobos: Para garantizar la seguridad de la información de la Institución, se debería establecer una serie de protocolos y normas para evitar robos de información. Unos ejemplos serían:

Distribución de contraseñas de bases de datos únicamente a los responsables de dichas bases de datos.
Restringir los accesos a información de tipo sensible a personas que estrictamente sean necesarias.
Protocolo de actuación en caso de abandono de empleado: En caso de despido o baja voluntaria de un empleado, establecer una serie de actuaciones a realizar respecto a su equipo de trabajo y usuarios asignados. Se propone una serie de pasos a seguir en estos casos:

Reclamar al empleado saliente todo aquél material de la Institución que pudiera tener prestado para realizar sus funciones (móvil de empresa, material de oficina).

Eliminar claves de acceso del usuario, contraseñas, cuentas de correo, cuenta de usuario en el dominio.

Hacer una copia de seguridad de los discos duros del equipo de trabajo del empleado y guardarla en sitio seguro.

Formatear PC del empleado y realizar un clonado con una maqueta para dejarlo disponible a una nueva incorporación.

Virus. Se considera virus todo código malicioso insertado en el código fuente de cualquier aplicación. Un virus normalmente se introduce en el sistema cuando es ejecutado en éste al menos una vez, provocando alteraciones, pérdida de información o errores graves.

Un virus siempre necesita un programa portador para poder cargarse en memoria y ejecutarse. Algunas características más comunes de un virus son:

Son de carácter malicioso, su objetivo es alterar o destruir algunas funciones del sistema infectado.
Suelen tener la capacidad para crear copias de sí mismo.
Suelen ocultar su presencia para evitar ser detectados.

Una clasificación primaria de los tipos de virus que se encuentran en todo el mundo, por su finalidad y por las acciones que realizan podría ser la siguiente:

Virus de macro o de código fuente: Son aquellos que van incorporados o bien en las macros utilizadas por algunas aplicaciones o bien directamente en el código fuente.

Virus mutantes: Tipo de virus caracterizado por cambiar su propio código al infectar un sistema, para evitar ser reconocidos.

Gusanos: Son virus que se auto reproducen en un sistema sin necesidad de ser transportados por un programa, y van eliminando sus anteriores posiciones, lo que puede ocasionar pérdida de datos.

Caballos de Troya: Son virus camuflados que se introducen en un sistema bajo una apariencia nada maliciosa.

Bomba de tiempo: Son programas ocultos (normalmente ligados a ejecutables de tipo COM o EXE), que esperan un determinado tiempo para ejecutarse.

Auto - replicables: Son virus que se auto reproducen e infectan a los programas ejecutables que se encuentran en el sistema.

Para evitar el contagio de virus, existen una serie de medidas preventivas:

Herramienta centralizada antivirus: NOD 32 instalado en el servidor de base de datos y la red de desarrollo. Es una herramienta centralizada que permite controlar y administrar la protección contra amenazas de toda la red. Permite la monitorización en tiempo real de todos los elementos de esta red para poder controlar en cualquier momento las posibles infecciones de malware.

Actualizaciones antivirus: La herramienta anterior actualiza cada hora su catálogo de malware de forma automática.

Normas y procedimientos antivirus:

No está permitida la ejecución de programas que no vengan de una fuente de confianza.
No está permitida la instalación de aplicaciones en los equipos. Será el Responsable de Mantenimiento quién realice esta función para todos los equipos.
Bloqueo de los controles Active X en los navegadores de todos los PCs.
Uso de software certificado, con licencia y actualizado.

Se ha constatado que los canales de comunicación de datos entre las distintas redes de la Institución aseguran un alto porcentaje de seguridad contra las intrusiones externas. Esta medida no sólo permitiría bloquear el acceso de los usuarios a algunas páginas web no recomendadas, por tanto, se ha estimado en un 90% la efectividad de estas medidas.

Estudio de Vulnerabilidades. En el Estudio de Vulnerabilidades se analizará, para cada amenaza, el riesgo residual resultante. Posteriormente, se valorarán aquellas medidas de prevención y control propuestas en el Estudio de medidas preventivas y de control, y se decidirá cuáles de éstas medidas han de implantarse en los sistemas de tecnologías de

información de la Unidad de Almacén para mejorar la seguridad sin comprometer la economía de la Institución innecesariamente.

La finalidad de este método es conseguir mejorar la política de seguridad de la Universidad de una forma sostenible y responsable.

A nivel global se ha detectado una estructura organizativa respecto a la gestión de la seguridad de los Sistemas de Información, ya que existe la figura del Responsable de Sistema de Información, Telecomunicaciones y Tecnología y en el caso de Almacén el Responsable del SIF (Modulo Almacén).

Por ello el Jefe de Sistema de Información, Telecomunicaciones y Tecnología es el responsable de supervisar y organizar todas aquellas tareas destinadas a prevenir, controlar y poner en marcha los planes de acción en caso de emergencia. Sus competencias serían:

Realizar una evaluación de riesgos.
Asesorar sobre medidas de seguridad.
Desarrollar procedimientos.
Supervisar la administración y las políticas de seguridad.
Ser el contacto con consultores y proveedores externos en materia de seguridad.

A continuación se detallan las vulnerabilidades en los sistemas para cada amenaza y las medidas a implantar:

Incendio. Aunque la posibilidad de que se produzca un incendio grave es algo remoto, las pérdidas que se producirían como consecuencias de éste serían muy cuantiosas, por lo tanto siempre es conveniente estar preparado ante una situación de tan grandes consecuencias.
Más probable de llegar a producirse sería el caso de un incendio de pequeñas consecuencias o una concentración alta de humos.

Dado el riesgo residual estipulado, se concluye que se han de efectuar las siguientes medidas correctoras:

Revisión periódica de las instalaciones eléctricas existentes. Esta labor ha de ser coordinada y supervisada por el Responsable de Seguridad.

Formación del Responsable de Seguridad en prevención y control de incendios. El Responsable de Seguridad debe añadir a su formación sobre situaciones de emergencia un conocimiento específico sobre las situaciones de incendio.

Señalización y almacenamiento de recipientes con materiales inflamables. Esta tarea también debe ser asignada al Responsable de Seguridad.

Inundaciones. El riesgo de una inundación a gran escala que pueda dañar gravemente los activos de la Unidad de Almacén, aunque también tiene una escasa probabilidad, debe ser tenido en cuenta dado los daños potenciales que puede causar.

También se ha de poner especial hincapié en otros tipos de pequeñas inundaciones y humedades en algunas estancias de las oficinas.

Las siguientes medidas, se han seleccionado, de acuerdo al gasto que ocasionaría su puesta en funcionamiento y el riego residual resultante en el análisis anterior:

Revisión cada cierto tiempo del estado de desagües y sumideros. Esta tarea corresponde al Responsable de Seguridad.
Adquirir bombas hidráulicas en caso de emergencia. Esta tarea corresponde igualmente al Responsable de Seguridad.

Cortes de corriente. Los cortes de corriente suponen una parada temporal de los servicios de la Unidad de Almacén durante el tiempo que dura éste.

Pueden ocasionar, además, la pérdida de datos y fallos graves de los procesos de negocio. Sin embargo, las pérdidas estimadas que podrían ocasionarse en relación a la probabilidad de que el riego se materialice y a las medidas preventivas existentes no son muy altas.

Cortes de comunicación. Los cortes de comunicación que más pueden afectar al funcionamiento correcto de las actividades de negocio y a los servicios prestados por la Unidad de Almacén sería el corte de las comunicaciones de datos, especialmente el canal de comunicación existente entre la red de la Institución, ya que existen procesos críticos dependientes de este canal de comunicación.

De las dos medidas adicionales propuestas anteriormente, se concluye que la única medida efectiva y eficiente que ha de implantarse para esta amenaza es:

Planificación de rutas de comunicación alternativas entre las diferentes redes. La planificación de esta tarea corresponde al jefe del Proceso de Sistemas de Información, Comunicaciones y Tecnología.

Dado que una caída de los servicios de Internet en la Unidad de Almacén afectaría los procesos existentes en la red, se ha de establecer un canal de comunicación alternativo en caso de un corte de comunicación.

Sabotaje. El sabotaje, normalmente ocasionado por empleados de la propia Institución como actos de venganza o reivindicación, pueden ocasionar daños muy graves a los activos de los sistemas de información.

Además de las políticas actuales actualmente implantadas, se recomiendan las siguientes medidas adicionales:

Publicar un código o protocolo de buen uso de las herramientas informáticas dentro de la Institución, que delimite el uso que pueden hacer de éstas los empleados. La redacción y publicación deben ser llevadas a cabo por el Responsable de Seguridad.

Existencia de una cláusula contractual que deben firmar los trabajadores de la Universidad por la cual se comprometen a hacer un buen uso de los materiales y tecnologías de la Institución. Esta tarea debe ser llevada a cabo por el Departamento de Recursos Humanos en colaboración con el Responsable de Seguridad.

Terrorismo. Este tipo de amenazas suponen una serie de daños potenciales muy graves para la Institución, si bien es cierto que la probabilidad de que lleguen a producirse es muy remota.

Las medidas de seguridad actual, llevada a cabo en su mayoría por la empresa de seguridad contratada por la Universidad, así como una política de restricciones de accesos a lugares críticos como el CPD, aseguran una protección eficiente aunque sencilla contra estos tipos de ataques.

Las dos medidas propuestas en el capítulo anterior, aunque aumentarían de manera considerable la protección contra estos ataques, supondría una inversión proporcionalmente muy superior al coste que supondría el proceso de reparación de procesos de negocio tras la ocurrencia de un atentado terrorista, teniendo en cuenta la probabilidad de que éste llegue a producirse. Por tanto, no se recomiendan ninguna de las dos.

Fallos de Hardware. Los fallos de hardware pueden ser críticos si se trata de averías que dejan sin funcionamiento a servidores o a dispositivos de comunicaciones de la Institución.

La mejor manera para prevenir este tipo de contingencias es una labor periódica y continua de supervisión del estado de los equipos hardware, así como un control de las garantías de éstos.

Los contratos con el proveedor de equipos hardware aseguran la garantía de estos equipos durante el tiempo que dura la misma, así como un contrato de sustitución de equipos con averías que no puedan ser reparadas.

Se recomienda poner en práctica la medida propuesta anteriormente:

Almacenamiento de las copias de seguridad de los servidores en un lugar alejado del CPD, a ser posible, incluso en otras oficinas alejadas de la Universidad. Además de las copias que se realizan en el Datacenter ETB (Bogotá y Estados Unidos). Esta tarea deberá ser coordinada por el Responsable de Seguridad.

El procedimiento de realización y almacenamiento de las copias de seguridad será estudiado y evaluado en el apartado dedicado a backups.

Fallos de Software. Existe una amplia variedad de errores ligados a fallos de software. Desde errores cometidos en la programación en las aplicaciones propias a fallos del sistema operativo instalado en un equipo.

Los procedimientos que actualmente están en funcionamiento y las políticas que se siguen a la hora de implantar nuevos elementos software son bastante útiles y están bien dimensionadas.

Sin embargo, se recomienda la implantación de las medidas propuestas en el capítulo anterior:

Establecer un procedimiento para controlar los accesos a los servidores de aplicaciones, mediante ficheros de log, que deberán ser revisados periódicamente por el encargado del Proceso de Sistemas de Información, Comunicaciones y Tecnología.

Poner en funcionamiento un departamento de calidad, o al menos un encargado, que realice las funciones de control de las aplicaciones instaladas, supervisión de la gestión de cambios y de la documentación de todas las aplicaciones instaladas en la Institución.

Con la aplicación de estas medidas, cualquier cambio que se realice en alguna aplicación o cualquier aplicación nueva que vaya a ser instalada, estará supervisado por un Responsable de Calidad.

Robo. Como se ha mencionado anteriormente, el tipo de robo más sensible para la Institución es el robo de información.

A las medidas descritas que ya están implantadas, se recomienda la implantación de la siguiente medida:

Establecer una política de seguridad antirrobos: Para garantizar la seguridad de la información de la Unidad de Almacén, se debería establecer una serie de protocolos y normas para evitar robos de información.

Estas medidas deben ser puestas en práctica por el Responsable de Seguridad y aprobadas por la dirección de la Institución.

Virus. La forma más sencilla de contraer un virus en los sistemas informáticos es mediante periféricos infectados que son conectados a los equipos.

La probabilidad de recibir un ataque exterior es menor, ya que los cortafuegos instalados, las reglas de entrada/salida de los routers y la configuración de las redes de la organización están bien preparados para este tipo de ataques.

Sin embargo, se mejoría la eficacia de las medidas ya implantadas con estas medidas adicionales:

Implantación de la herramienta McAfee Protection Pilot para las redes 2,3 y 4.
Implantación de un servidor proxy en las redes. Esta medida no sólo permitiría bloquear el acceso de los usuarios a algunas páginas web no recomendadas, sino que mejoraría la opacidad del sistema.

La planificación y puesta en marcha de estas medidas en los sistemas deberá corresponder al jefe del Proceso de Sistemas de Información, Comunicaciones y Tecnología, con la supervisión y el control del Responsable de Seguridad.

Análisis de Impacto del Negocio. El Análisis del Impacto en el Negocio es la base para cualquier Plan de Continuidad del Negocio. Este documento también es conocido como BIA (Business Impact Analysis).

El BIA indica qué procesos o áreas de negocio son críticos, además de valorar cuáles son las aplicaciones, datos o procesos que han de ser trasladados a un CPD remoto en caso de que ocurra una catástrofe, siempre que la opción del CPD remoto sea factible.

Al especificar que procesos y servicios son los más críticos, se podrá establecer la base para poder realizar en consecuencia una estrategia de recuperación adecuada.

Es la fase más importante del plan ya que identifica los riesgos asociados a las funciones críticas del negocio, determina el impacto de los mismos y los prioriza para establecer posteriormente las estrategias de recuperación mediante la determinación de los tiempos de recuperación.

El BIA tiene que especificar, para cada proceso, dos conceptos:

RTO (Recovery Time Objective u Objetivo de Tiempo Recuperación): Es el máximo tiempo permitido que un proceso puede estar caído como consecuencia de una catástrofe.

RPO (Recovery Point Objective u Objetivo de Punto Recuperación): Es el punto de partida desde el cual se tiene que iniciar la recuperación del proceso. Es necesario indicar si es necesario disponer de la información que se tenía justo antes de la catástrofe, o se puede utilizar información previa (hasta qué momento: horas, días, semanas, entre otros).

Estos dos parámetros referentes a procesos o actividades de negocio determinarán los procesos de negocio críticos. Estos procesos son aquellos que permiten entregar los servicios y productos clave para que la Unidad de Almacén alcance sus objetivos más importantes y sensitivos en tiempo.

Para poder analizar los casos de contingencias y la criticidad de los procesos de negocio se han definido una serie de situaciones que constituyen el escenario de peor caso, aplicables de forma distinta para cada proceso:

Falta de acceso a la oficina de Almacén y bodegas.

Falta de acceso a la información almacenada dentro de la Unidad de Almacén.
Falta de acceso a los sistemas de información.
Falta de información acerca de cuánto puede durar una interrupción.
La interrupción ocurre en el peor momento posible.

Estos escenarios son la hipótesis de partida para evaluar las posibles respuestas que se han de producir en las diferentes áreas de negocio o procesos de negocio.

Además, se han definido una serie de tiempos establecidos para poder establecer una serie de niveles para los Objetivos de Tiempo Respuesta (RTO). Estos niveles serán utilizados para clasificar los procesos de negocio.

Tabla 10. Niveles para Intervalos de Recuperación

NIVEL RTO	INTERVALO DE RECUPERACIÓN
1	0-24 Horas
2	24-48 Horas
3	48-72 Horas
4	3-7 Días
5	7-14 Días
6	Más de 2 Semanas

Fuente. Autores del Proyecto.

Para poder clasificar los niveles de los Objetivos de Punto Recuperación (RPO), se han definido también una serie de niveles estableciendo los puntos de partida para la restauración de los datos de las funciones de negocio.

Tabla 11. Niveles de Datos de Recuperación

NIVEL RPO	DATOS DE RECUPERACIÓN
1	Datos justo antes de contingencia
2	Máximo 24 horas antes de contingencia
3	Máximo 72 horas antes de contingencia
4	Máximo 1 semana antes de contingencia
5	Máximo 2 semanas antes de contingencia
6	Más de 2 semanas

Fuente. Autores del Proyecto.

Para la realización del Análisis de Impacto del Negocio, se realizó una entrevista al Jefe de Almacén, la Coordinadora de Inventario y la Secretaria de Almacén.

Resultados del BIA. Los resultados obtenidos de las entrevistas realizadas al Jefe de Almacén, la Coordinadora de Inventario y la Secretaria de Almacén determinaron la existencia de dos procesos de negocio generales.

Tabla 12. Resultado BIA Proceso de Suministro

Proceso de Negocio	Suministro
Criticidad	Normal
Nivel RTO	3
Nivel RPO	2
Recursos Humanos Necesarios para Recuperación	Jefe de Unidad Almacén Secretaria de Unidad de Almacén
Aplicaciones y Datos que Soportan el Proceso	Sistema de Información Financiera (Módulo Almacén) -Solicitud de Elementos en Almacén -Orden de Pedido -Orden de Compra -Orden de Suministro -Factura -Solicitud de Bienes y Servicios -Salida Elementos de Consumo -Certificado de Disponibilidad Presupuestal -Oficio Informando la Falla del Bien
Recursos Hardware que Soportan el Proceso	Servidor de Aplicaciones Servidor de Bases de Datos PC Escritorio Jefe Unidad de Almacén PC Escritorio Secretaria Unidad de Almacén Impresora

Fuente. Autores del Proyecto.

Tabla 13. Resultados BIA del Proceso de Inventario

Proceso de Negocio	Inventario
Criticidad	Critica
Nivel RTO	1
Nivel RPO	2
Recursos Humanos Necesarios para Recuperación	Jefe de Unidad Almacén Coordinadora de Inventario
Aplicaciones y Datos que Soportan el Proceso	Sistema de Información Financiera (Módulo Almacén) -Entrada por Adquisición -Salida de Elementos Devolutivos -Entrada de Inventarios -Control de Traslado de Elementos -Solicitud y Ejecución de

	Requerimientos -Baja de Elementos -Catálogo de Elementos en Stock -Programación de Compras de Bienes de Consumo y Devolutivos -Paz y Salvo de Inventarios
Recursos Hardware que Soportan el Proceso	Servidor de Aplicaciones Servidor de Bases de Datos PC Escritorio Jefe Unidad de Almacén PC Escritorio Coordinadora de Inventario Impresora de Código de Barras Impresora

Fuente. Autores del Proyecto.

4.2.3 Desarrollar e implementar los planes de continuidad incluyendo la seguridad de la información

Control. Se deberían desarrollar e implementar planes para mantener y 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.

El desarrollo de un Plan de Continuidad del Negocio el cual contiene procedimientos y guías, que puede utilizar la Unidad de Almacén durante una crisis para minimizar los impactos del negocio.

Objetivos. Los objetivos del plan de continuidad del negocio en caso de desastre son:

Reducir las consecuencias de un desastre a un nivel aceptable mediante procedimientos preestablecidos de recuperación y continuidad.

Recuperar las actividades de los procesos críticos identificados en el BIA (Business Impact Analysis).

Alcance. El plan no contempla todas las áreas de la Universidad, solo la Unidad de Almacén, Coordinación de Inventarios y las dos bodegas.

El plan considera los siguientes aspectos:

Restablecimiento de equipos y el Sistema de Información Financiero (SIF).
Instalaciones alternas de recuperación TI, áreas de trabajo y del centro de dirección del negocio.

Comité de Continuidad del Negocio. En el caso de un desastre u otra circunstancia la Unidad de Almacén deberá cambiar a una situación de emergencia. La Unidad de Almacén deberá centrarse en cambiar, la estructura actual y funciones de un día normal de trabajo, a la estructura y funciones requeridas por la contingencia trabajando en conjunto para la restauración en tiempo de las operaciones de la misma. Una estructura propuesta es la que se presenta a continuación:

Comité de Dirección.

Jefe Unidad de Almacén
Jefe de Sistema de Información, Telecomunicaciones y Tecnología
Jefe de Sistema de Información Financiero (SIF)

Comité Responsable de Recuperación.

Jefe de Sistema de Información, Telecomunicaciones y Tecnología
Jefe de Soporte de Comunicaciones
Jefe de Soporte de Servidores

Comité de Logística.

Coordinadora de Inventarios
Jefe de Mantenimiento y Soporte
Secretaria Almacén

Comité de Dirección. Máximo responsable del Plan de Continuidad del Negocio, de este comité, dependen todos los demás comités y grupos de trabajo.

Está conformado por el Coordinador del Comité Nahúm Lobo Pacheco y los Coordinadores de los Comités de Recuperación y Logística, Antón García Barreto y Maylin Barbosa Nvarro respectivamente.

Coordinador del Comité de Dirección

Funciones y Responsabilidades. Dirigir la ejecución de las fases del Plan de Continuidad las cuales son: respuesta inicial y notificación, evaluación del problema, declaración de desastre, implementación del plan de logística, recuperación y reanudación, y normalización.

Coordinar las actividades y proporcionar un vínculo de comunicación importante entre los equipos.
Comunicar a las autoridades respectivas en caso de alguna emergencia o eventualidad.
Es responsable del desarrollo, pruebas y mantenimiento del plan.

Comité Responsable de Recuperación. Es responsable de la recuperación del servicio degradado, de la solución de la causa que originó la contingencia, y del retorno a la situación normal.

Coordinador del Comité Responsable de Recuperación

Funciones y Responsabilidades

Coordinar las acciones de recuperación junto al coordinador del comité de dirección.
Dirigir el equipo evaluador de la crisis.
Generar el reporte preliminar y final del problema hacia el comité de dirección.
Generar el reporte de daños al personal debido al problema o emergencia.

Comité de Logística

Es responsable de la logística del plan de continuidad del negocio.
Notifica a proveedores y clientes acerca de la emergencia.
Realizar compras y preparación de los recursos necesarios.
Genera el reporte de daños al personal debido al problema o emergencia.
Esta encargado de la contratación de los servicios de respaldo.

Información de Contactos de Comités de Continuidad. Para localizar y notificar de manera rápida y oportuna a los miembros de los Comités de Continuidad del Negocio contamos con una tabla en la cual detallamos el cargo y los números de teléfonos de la casa y celular.

Tabla 14. Información de Contactos de Comités de Continuidad

Nombres	Apellidos	Cargo	Teléfono	Celular

Fuente. Autores del Proyecto.

Procesos de Recuperación. Una vez realizados tanto el Análisis de Riegos como el Análisis de Impacto del Negocio, es necesario estudiar qué acciones hay que realizar y cómo hay que realizarlas en caso de que, por efecto de una catástrofe o contingencia, se paralicen uno o varios de los procesos de negocio de la Unidad de Almacén.

Para ello, se deben analizar y estudiar aquellas alternativas de recuperación apropiadas para lograr la recuperación de los sistemas en el tiempo necesario indicado en el Análisis de

Impacto del Negocio. Para ello se propondrán diferentes alternativas y se elegirá la más adecuada.

Una vez escogida la estrategia de recuperación, se establecerán una serie de procedimientos de recuperación. Estos procedimientos serán un compendio de acciones a llevar a cabo para una serie de situaciones de contingencias en los sistemas.

Finalmente, se especificarán aquellos perfiles que deben intervenir en los procesos de recuperación, así como los responsables de las tareas y los actores que van a intervenir de alguna manera en estos procedimientos.

Estrategia de Recuperación. Las estrategias de recuperación son una serie de alternativas cuyo objetivo es conseguir recuperar los recursos críticos de la información, entre las cuales se elige aquella que sea aceptable en el coste de recuperación y razonable en el impacto que se determinó en el BIA.

Para ello, se contemplan una serie de alternativas de instalaciones de procesamiento (CPDs alternativos), que se analizarán, y entre las cuales se elegirá una de ellas:

Hot site
Warm site
Cold site
Mirror site
Sitios móviles
Acuerdos recíprocos con otras organizaciones
Alternativas de Recuperación

Hot Site. Es una segunda ubicación de procesamiento que está configurado y suficientemente actualizado como para poder restaurar los servicios correctamente tan sólo unas pocas horas después de la ocurrencia de la interrupción de dichos servicios.

Los costes son elevados, pero permiten alcanzar los tiempos establecidos en el BIA casi con seguridad.

Los costes podrían ser:

Coste básico de suscripción.
Cuotas mensuales.
Cargos de pruebas.
Costes de activación (emergencia real).
Cargos por uso por hora o por día (dependiendo del proveedor).

Warm Site. Es una segunda ubicación de procesamiento, con una configuración adecuada pero que no está suficientemente actualizada como para poder restaurar los servicios sin

perder datos. Por tanto, sería necesaria una actualización antes de proceder a una restauración de los servicios en este centro de procesamiento.

Los costes son elevados, pero menores que para el Hot Site, ya que el mantenimiento y las pruebas se realizan con menor frecuencia.

Cold Site. Es una segunda ubicación que contiene los elementos físicos para establecer un centro de procesamiento si fuera necesario (cableado eléctrico, aire acondicionado, etc.), pero que no contiene ni las máquinas ni los componentes hardware necesarios para poder levantar los servicios en caso de desastre.

Los costes serían netamente inferiores a los costes para las estrategias anteriores.

Mirror Site. Es una segunda ubicación con los recursos necesarios, correctamente configurados y actualizados, donde se realizan las distintas transacciones de cada servicio en paralelo con el centro de procesamiento principal.

Esta alternativa supone la necesidad de realizar pruebas periódicas que garanticen la sincronía entre el centro principal y el de respaldo. Debe existir también una correspondencia equitativa de capacidad de trabajo entre ambos centros.

Se trata de una alternativa muy costosa, además de ser muy necesario el uso de recursos informáticos y de personal que garanticen la viabilidad de este método.

Sitios móviles. Es una segunda ubicación móvil, por ejemplo un remolque, que contiene los elementos necesarios para instalar un centro de procesamiento alternativo.

Pueden ser útiles en caso de desastre expandido para constituir áreas de trabajo donde situar PCs y terminales de trabajo.

Acuerdos recíprocos con otras organizaciones. Son acuerdos suscritos con otra organizaciones (normalmente cuyas sedes se encuentren cerca geográficamente) para proveerse mutuamente de tiempo de CPU e incluso de espacio para poder instalar a algunos trabajadores de forma temporal después de una catástrofe.

Este método supone una dificultad de conseguir una configuración y actualización adecuadas para poder reanudar los servicios críticos al poco de producirse dicho desastre.
El coste de esta alternativa sería el más bajo de todas las presentadas.

Estrategia de Recuperación Elegida. Las alternativas de recuperación anteriores sólo serán ejecutadas en caso de desastre en los sistemas cuya recuperación sea de larga duración y afecte a las funciones principales de negocio. En caso de contingencia de sistemas cuya recuperación sea de menor duración, se aplicarán los procesos de recuperación descritos en el apartado siguiente.

Se propone la elección de un Cold Site como lugar de recuperación alternativo. Es decir, una ubicación alternativa con los elementos físicos necesarios para poder instalar un CPD, pero sin contar ni con los equipos de procesamiento ni de comunicación.

Esta alternativa supondría:

Un coste relativamente poco elevado.
Los equipos de procesamiento y de comunicación están soportados por los proveedores de hardware. Por lo tanto, en caso de destrucción de éstos, los proveedores tendrían que transportar e instalar estos equipos al lugar de procesamiento alternativo.
La intervención de las siguientes personas o departamentos:

Dirección de la Institución: Aprobar el traslado del CPD al lugar alternativo.
Responsable de Sistema de Información, Telecomunicaciones y Tecnología: Coordinar y supervisar el traslado e instalación de equipos. Evaluar los tiempos de recuperación. Coordinación de personal encargado de la recuperación de los sistemas.
Administrador de Soporte de Comunicaciones: Configuración de los sistemas de procesamiento y comunicación. Ejecución de tareas de recuperación de datos mediante las copias de seguridad.
Responsables de Soporte de Servidores: Aprobar y supervisar las tareas de configuración de aplicaciones y la recuperación de datos mediante copias de seguridad.

Según la criticidad de las funciones de negocio, definidas en el BIA, se estudiará el traslado a un CPD alternativa siempre que se den las siguientes situaciones:

Situación de desastre que afecte al CPD: Incendios, inundaciones, que afecten al CPD y a sus componentes.
Averías en sistemas de larga duración: Si los sistemas que soportan las funciones de negocio críticas no se pueden reparar en menos de 24 horas. Este sistema es:

Servidor del Sistema de Información Financiero (Modulo Almacén).

Procedimientos de Recuperación. Una vez elegida la estrategia de recuperación para casos de desastres, es necesario diseñar una serie de protocolos de actuación para las situaciones de contingencias. Para cada situación, se propondrán unas medidas a seguir para proceder a la restauración del sistema.

Se han diferenciado las siguientes situaciones de contingencias:

Fallo de hardware (Sin daños para la información).
Dañado o borrado lógico de datos.
Dañado o borrado de software.
Dañado físico de los soportes de la información.
Destrucción total de alguno de los sistemas.

Fallo de Hardware (sin daños para la información). Se describen los procedimientos a seguir en caso de averías o destrucción de los siguientes equipos de hardware:

Switch
Router
Firewall

El procedimiento a seguir debe ser el siguiente:

Se avisa a Mantenimiento y Soporte de la avería.
Si el equipo está en garantía o tiene contrato suscrito de sustitución:
Mantenimiento y Soporte da parte de avería al proveedor.
Si el equipo no está en garantía o no tiene contrato suscrito de sustitución:
Mantenimiento y Soporte elabora petición de compra al Departamento de Compras.
Si la sustitución o reparación del equipo es de larga duración, se procede a la sustitución del equipo por otro que esté disponible, siempre y cuando sea posible.

Dañado o Borrado Lógico de Datos. Se describen los procesos a seguir en caso de que resulten dañados los ficheros o las bases de datos que soportan a las aplicaciones.

El procedimiento sería el siguiente:

El Responsable Técnico de la aplicación valora, en función de la aplicación y la cantidad de datos perdidos, si se debe proceder a una replicación de la copia de la base de datos en la base de datos original.

Si el Responsable Técnico da el visto bueno a la replicación, se continúa el proceso.

Si la aplicación requiere una parada en producción:
Se informa a los usuarios de la aplicación de la detención y la duración de esta. Se procede a la parada de la aplicación.
Si la aplicación no requiere una parada en producción:
Se continúa el proceso de replicación, haciendo el proceso "en caliente".

El Responsable de Soporte de Servidores inicia la replicación desde la copia de la base de datos.
Cuando finaliza, avisa al Responsable Técnico para que compruebe si la réplica se ha hecho correctamente.

Si el Responsable Técnico aprueba la réplica:
El Responsable de Soporte de Servidores da por finalizado el proceso guardando los cambios y reportando dicho cambio. Se reinicia la aplicación si fuera necesario.
Si el Responsable Técnico no está conforme con la réplica:

El Responsable de Soporte de Servidores da marcha atrás en la réplica, volviendo al estado anterior del comienzo de dicho proceso. En función de la decisión del Responsable Técnico, el proceso quedaría en espera o cancelado.

Dañado o Borrado de Software. Se describen aquellos procesos que sería necesario realizar en caso de que existan daños más o menos graves en las aplicaciones o en el sistema operativo de las máquinas o de los servidores de la organización.

Se van a diferenciar los siguientes casos, cada uno con un tratamiento diferente:

Daños o borrado en el software de un PC. En caso de daño o borrado de alguna aplicación de un PC, se comunicará a Mantenimiento y Soporte, para que proceda a instalar o reinstalar las aplicaciones necesarias en el PC.

Si se trata de daños en el Sistema Operativo de un PC, se comunicará a Mantenimiento y Soporte el cual valorará la gravedad de los daños y efectuará las siguientes medidas:

Se intenta la recuperación del sistema. Si el daño es suficientemente grave (no se puede iniciar el Sistema Operativo):

Se procede al formateado de los discos duros del PC. Posteriormente, se realiza un clonado de PC a partir de una maqueta con las aplicaciones estándar para cada PC, con el programa Norton Ghost.

Daño o borrado en el software de aplicaciones de uno de los servidores. En caso de daños o borrado en el software de alguno de los servidores, se comunicará al Responsable de Soporte de Servidores, este procederá a instalar o reinstalar los productos o aplicaciones necesarias en el servidor, siempre con el permiso del Jefe de Sistemas de Información, Telecomunicaciones y Tecnología.

Dañado Físico de los Soportes de Información. Este procedimiento se seguirá sólo en caso de fallo del disco instalado en el servidor donde se encuentra el SIF (Modulo Almacén).

Esto es debido a que este servidor tiene, dos discos replicados en espejo, por lo tanto, en caso de fallo de uno de los discos, el sistema continúa trabajando. Se sabe que un disco está averiado cuando aparece una luz roja “fija”.

El procedimiento a seguir sería el siguiente:

Se comunica a Mantenimiento y Soporte que uno de los discos está averiado.
Mantenimiento y Soporte da aviso al proveedor de la avería. El proveedor envía un disco de repuesto.
Una vez recibido el disco de repuesto, se extrae el disco dañado y se inserta el nuevo.

Se sigue el mismo proceso usado para la creación de discos imagen. De esta manera, el disco nuevo contendrá una copia imagen del disco que ya estaba funcionando.

Si los discos existentes en uno de los servidores mencionados fallasen simultáneamente, se trataría como destrucción total del sistema, y habría que proceder de distinta manera.

Destrucción Total de Alguno de los Sistemas. Son los procedimientos a seguir en caso de que alguno de los servidores esté gravemente dañado, sin posibilidad de arranque.

Procedimiento. Este procedimiento se seguirá en caso de destrucción de ambos discos de los servidores que realizan periódicamente la creación de discos imagen.

El procedimiento a seguir sería el siguiente:

Se comunica a Mantenimiento y Soporte la avería del servidor.

Mantenimiento y Soporte da aviso al proveedor de la avería.

El proveedor determina el hardware que debe ser sustituido para restaurar el sistema.

Se sustituye el hardware necesario.

Se procede a la recuperación del sistema a partir del último disco imagen de seguridad almacenada. Esta tarea corresponde al Responsable de Soporte de Servidores.

Se introduce el disco imagen de seguridad en la ranura principal del servidor y se inicia el modo de recuperación del servidor.
Se introduce un disco nuevo en la ranura secundaria del servidor. El sistema duplica el disco imagen de seguridad sobre el disco nuevo.
Se extrae el disco imagen de seguridad y se introduce otro disco nuevo en su lugar. Se sigue el mismo proceso descrito para la creación de discos imagen para duplicar el disco en la ranura secundaria sobre el disco en la ranura principal.
Se reinicia el sistema.

A partir del Libro de Registro de Actuaciones, se realizan de forma manual y secuencial todos aquellos cambios posteriores a la creación del disco imagen de seguridad que se han realizado sobre el sistema. Esta tarea corresponde al Responsable de Soporte de Servidores.

Se procede a la recuperación de los datos de la aplicación. Para ello, se podrán utilizar:

La cinta de seguridad del día anterior.
Las réplicas de las bases de datos, actualizadas el día anterior.

Se notifica en el Libro de Registro de Actuaciones los cambios realizados, si fuera necesario.

Equipo de Recuperación. Hasta ahora se han visto las personas responsables de la realización de las tareas de recuperación. Sin embargo, se tienen que definir también las personas encargadas de desarrollar, implantar, probar y mantener las políticas de seguridad y los procedimientos de recuperación que se han de seguir en el Plan de Continuidad de Negocio.

Estas personas forman el Equipo de Recuperación, y según su rol dentro del grupo, van a ser los encargados de diseñar y ejecutar todas aquellas medidas de seguridad. El Equipo de Recuperación debe ser designado por el Departamento de Gerencia de la Institución. Los diferentes roles que deben conformarlo son:

Coordinador del equipo

Las responsabilidades del Coordinador deben ser:

Coordinar y supervisar el traslado e instalación de equipos al CPD alternativo.
Evaluar tiempos de recuperación.
Desarrollar la organización de los procedimientos de recuperación.
Desarrollar el plan de evacuación.
Desarrollar el plan de formación para los empleados.
Desarrollo del Plan de Pruebas. Supervisión de los resultados.
Desarrollo del Plan de Mantenimiento.

El rol del Coordinador del equipo será asumido por el Responsable de Sistema de Información, Telecomunicaciones y Tecnología.

Mantenimiento y Soporte

Las responsabilidades de Soporte deben ser:

Diseñar y desarrollar los procedimientos de Mantenimiento y Soporte.
Recibir incidencias, documentarlas y ser enlace de los distintos departamentos si fuera necesario.
Contactar con los proveedores necesarios en caso de contingencia.
Revisar contratos de mantenimiento durante la fase de mantenimiento.

El rol de Soporte será asumido por el Responsable de Mantenimiento y Soporte.

Sistemas Informáticos

Las responsabilidades de Sistemas Informáticos deben ser:

Ejecución de procedimientos de recuperación de datos.
Diseñar y desarrollar los procedimientos de recuperación de Sistemas.
Desarrollo y ejecución de los procesos de backup.

Configuración y mantenimiento de los servidores.
Control del rendimiento de los sistemas.

El rol de Sistemas Informáticos será asumido por el Responsable de Soporte de Servidores.

4.2.4 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.

Este apartado se trata en el **Capítulo 4.3.** Se relacionan a continuación los procedimientos a seguir para la Gestión de Continuidad del Negocio:

Procedimiento para la formulación de acciones correctivas y preventivas para el suministro de energía eléctrica en la Unidad de Almacén.
Procedimiento para la formulación de acciones correctivas y preventivas para cuidar la integridad del personal en la Unidad de Almacén.
Procedimiento para la coordinación administrativa de las TIC.
Procedimiento de evacuación de la Unidad de Almacén.

Prueba, mantenimiento y re-evaluación de los planes de continuidad del negocio

Una vez realizado el Plan de Continuidad del Negocio, es necesario que dicho plan sea presentado a la Dirección de la Institución para su aprobación. Si el plan es aprobado, sería necesaria su implantación. La implantación en la Unidad de Almacén supondría:

Modificación de aquellas políticas de seguridad que hayan sido modificadas en el Plan de Continuidad del Negocio.

Formación de los responsables directos de los procedimientos de seguridad descritos en el Plan de Continuidad del Negocio.

Formación de los empleados en aquellas normas y procedimientos de seguridad en los que estén involucrados.

Implantación de medidas de prevención y medidas correctoras recomendadas en el Plan de Continuidad del Negocio en la Unidad de Almacén.

Un Plan de Pruebas que sirva para evaluar los procedimientos de recuperación descritos en el Plan de Continuidad del Negocio, midiendo tiempos de respuesta, daños en la Organización y coordinación de empleados en el desempeño de dichos procedimientos.

Un Plan de Mantenimiento que realice aquellas correcciones necesarias en el Plan de Continuidad del Negocio, en función de los cambios de tecnologías o en las funciones de negocio que son utilizadas por la Institución. También debe realizar correcciones en función de los resultados del Plan de Pruebas.

Para el Plan de Pruebas y el Plan de Mantenimiento, es indispensable concretar los objetivos que éstos deben cumplir, las personas que deben llevarlo a cabo, las tareas que se deben realizar y los resultados que se deben obtener.

Plan de Pruebas. El Plan de Pruebas es una parte esencial del Plan de Continuidad de Negocio. Los objetivos que tiene que cumplir son:

Medir la habilidad y capacidad del lugar de respaldo.
Evaluar la capacidad de recuperación de funciones críticas de negocio.
Evaluar estado y cantidad de equipos y suministros en el lugar de recuperación.
Medir el desempeño general de actividades operativas y de sistemas relacionados con el negocio.
Verificar si el Plan de Continuidad del Negocio es completo y preciso.
Evaluar el desempeño del personal involucrado.
Evaluar el entrenamiento y conocimiento del personal que no pertenece al negocio.
Evaluar la coordinación entre el equipo de continuidad y los proveedores externos.

La primera prueba debe realizarse antes de aprobarse el Plan de Continuidad de Negocio.
De esta manera, los resultados obtenidos servirán para que la Dirección de la Institución valore la viabilidad de dicho plan.

Se propone una frecuencia anual para la realización de las pruebas del Plan de Continuidad del Negocio. Esta frecuencia deber ser aprobada por la Dirección de la Organización, ya que implica un simulacro de parada de los sistemas.

Definición de la Prueba. La prueba consistirá en un simulacro de diversas situaciones de desastre, que serán las siguientes:

Caída del servidor de SIF.

Fallo del switch de la red.

Fallo del router de la red.

Fallo de la línea telefónica en la Unidad de Almacén.

Destrucción de servidores existentes en el CPD.

Estas pruebas se realizarán de forma independiente, aislando cada caso de los demás, para analizar la respuesta dada para cada una de las situaciones.

La prueba quedará finalizada con la elaboración de un informe que evaluará, para cada situación de desastre:

Tiempo empleado para la reanudación de cada una de las funciones críticas afectadas por el desastre.

Problemas de aplicación de los procedimientos de recuperación en los desastres.

Evaluación del personal encargado de realizar los procedimientos de recuperación.

Coordinación del equipo encargado de realizar los procedimientos de recuperación.

Recursos necesarios para la reanudación de los procesos de negocio.

Plan de Mantenimiento. El Plan de Mantenimiento es un seguimiento de la eficacia y los resultados del Plan de Continuidad del Negocio a lo largo del tiempo. No se trata de la realización puntual y periódica de una serie de procedimientos, sino que es un proceso cíclico de mejora y revisión del Plan de Continuidad del Negocio según los cambios tecnológicos, de personal o de funciones críticas.

El Plan de Mantenimiento debe llevarse a cabo especialmente en dos circunstancias del ciclo de vida del Plan de Continuidad del Negocio:

Errores localizados en el Plan de Continuidad del Negocio durante la fase de pruebas: Si en el informe realizado posteriormente a la fase de pruebas se encuentran fallos en los procedimientos, en la coordinación del equipo de recuperación o en los tiempos de respuesta ante las situaciones de desastre, se deben analizar estos fallos para hacer las correspondientes modificaciones sobre el Plan de Continuidad del Negocio.

Cambios en el entorno del Plan de Continuidad del Negocio: Si se producen cambios que afectan al modo de recuperación ante desastres, se deben hacer las correcciones necesarias en el Plan de Continuidad del Negocio para adaptarse a las nuevas situaciones. Estos cambios pueden ser:

Renovaciones tecnológicas: Cambios evolutivos en las tecnologías utilizadas en los procesos de negocio. Estos cambios requieren una modificación en las respuestas a las situaciones de desastre.

Cambios estructurales en la Unidad de Almacén: Si se producen modificaciones que afectan a la organización estructural de la Unidad de Almacén, como nuevos perfiles de empleados o nuevas áreas de negocio se debe actualizar el Plan de Continuidad del Negocio para asignar o desasignar tareas en función de la nuevas jerarquías implantadas en la misma.

Contratos con los proveedores: Si cambian los proveedores que van a dar soporte técnico a los sistemas de información, o bien cambian los contratos de soporte, se deben corregir los procedimientos de recuperación para adaptarse a las nuevas condiciones.

Si durante la fase de mantenimiento del Plan de Continuidad del Negocio se realizan cambios sobre éste, estos cambios deben llevarse a la Dirección de la Institución para ser aprobados. Si estos cambios son aprobados, se deberá reemplazar el Plan de Continuidad del Negocio actual por el Plan de Continuidad del Negocio modificado con los cambios y proceder a la formación de los responsables de las tareas de recuperación y de los empleados involucrados.

El Plan de Mantenimiento es responsabilidad del equipo de recuperación.

4.3 DOCUMENTAR PROCEDIMIENTOS QUE PERMITAN LA PREVENCIÓN Y PROTECCIÓN DE LAS PERSONAS, INSTALACIONES, EQUIPOS Y DOCUMENTOS DE LA UNIVERSIDAD EN CASO DE EMERGENCIAS O AMENAZAS QUE LO PONGAN EN PELIGRO.

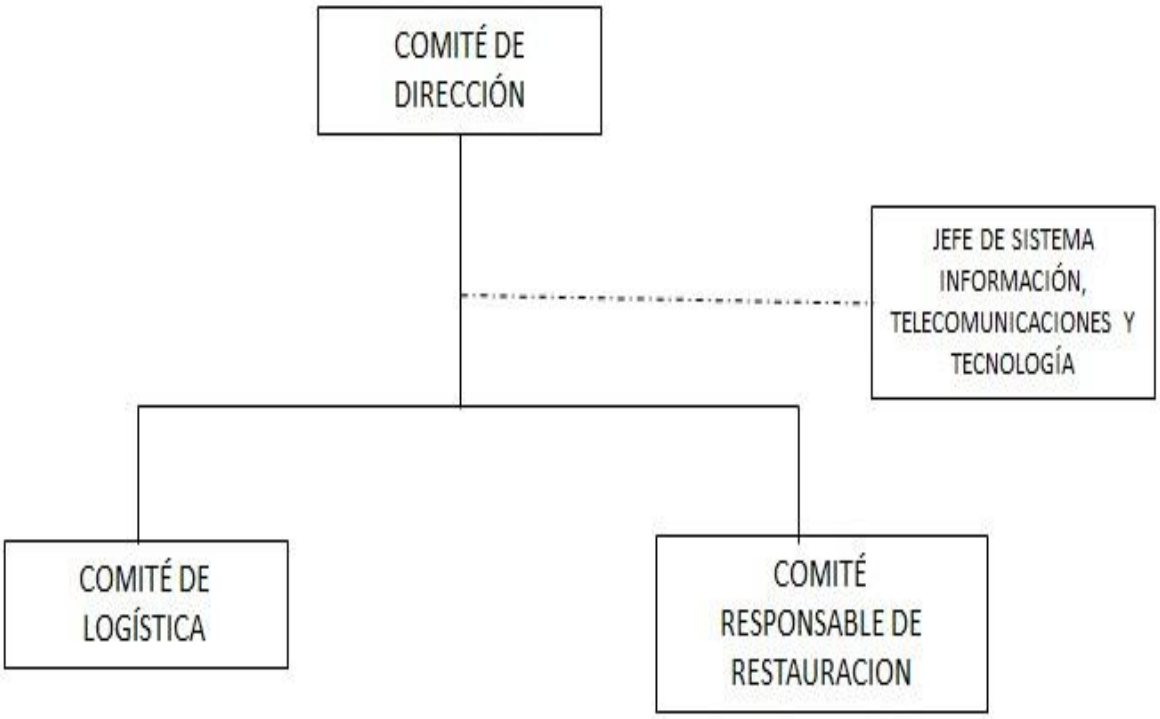
En la actualidad los cambios tecnológicos adquieren cada vez mayor importancia al interior de las organizaciones, no menos importante es también el cuidado de la integridad del recursos humanos, tecnológicos y físicos, por lo cual se hace necesario o indispensable contar con un plan de continuidad del negocio, que garantice el restablecimiento del correcto funcionamiento de los servicios en el menor tiempo posible, ante cualquier eventualidad.

Según la Resolución 1016 de marzo 31 de 1989, Artículo 11, numeral 18, de la legislación colombiana en materia de Salud ocupacional establece la obligatoriedad que tienen las empresas de organizar y desarrollar un plan de emergencias.

La Gestión de Continuidad del Negocio para la Unidad de Almacén de la Universidad Francisco de Paula Santander Ocaña, podrá servir como un repositorio centralizado para la información, tareas y procedimientos que puedan ser necesarios para facilitar la toma de decisiones a la administración del almacén, así como de desarrollar procesos y definir sus tiempos de respuesta ante cualquier interrupción extendida de las operaciones normales y servicios de la institución.

En el caso de un desastre u otra circunstancia que conlleve la necesidad de operaciones de contingencia, la organización normal de la Unidad de Almacén, deberá cambiar a una organización de contingencia. La Unidad de Almacén deberá centrarse en cambiar, la estructura actual y funciones de un "día normal de trabajo", a la estructura y funciones requeridas por la contingencia trabajando en conjunto para la restauración en tiempo de las operaciones de la misma.

Una estructura propuesta es la que se presenta en el siguiente diagrama:



1.NOMBRE	2.PROCESO
GESTIÓN DE CONTINUIDAD DEL NEGOCIO PARA LA UNIDAD DE ALMACÉN	**GESTION ADMINISTRATIVA Y FINANCIERA**

3. OBJETIVO: Identificar los riesgos y realizar acciones de prevención y mitigación para evitar que estos se materialicen, y en caso de presentarse una situación de emergencia, establecer las acciones que se deben desarrollar para atender de manera adecuada la situación presentada y atender los afectados y de esta manera reducir el impacto generado durante la situación de emergencia.

4. ALCANCE: El presente plan, tiene una cobertura de atención y coordinación que permitan la atención al personal de la Unidad de Almacén.

5. RESPONSABLE: Comité de Dirección.

6. DEFINICIONES

- **Accidente:** Suceso extraño al normal desenvolvimiento de las actividades de una organización que produce una interrupción generando daños a las personas, patrimonio o al medio ambiente.
- **Accidente de trabajo:** Lesión ocurrida durante el desempeño de las labores encomendadas a un trabajador.
- **Desastre:** Una interrupción grave en el funcionamiento de una comunidad causando grandes pérdidas a nivel humano, material o ambiental, suficientes para que la comunidad afectada no pueda salir adelante por sus propios medios, necesitando apoyo externo. Los desastres se clasifican de acuerdo a su origen (natural o tecnológico).
- **Emergencia**: Estado de daño sobre la vida, el patrimonio y el medio ambiente ocasionado por la ocurrencia de un fenómeno natural o tecnológico que altera el normal desenvolvimiento de las actividades de la zona afectada.

- **Medios Técnicos:** Descripción detallada de los medios técnicos necesarios y que se dispongan para la protección. Se describirá las instalaciones de detección, alarmas, de los equipos contra incendio, luces de emergencia, señalización, indicando características, ubicación, adecuación, cantidad, estado de mantenimiento,

- **Medios Humanos:** Número de personas que sean necesarias y se disponga, quienes participaran en las acciones de protección.

- **Densidad de ocupación de la edificación**.- Dificulta el movimiento físico y la correcta percepción de las señales existentes, modificando el comportamiento de los ocupantes. A su vez, condiciona el método para alertar a los ocupantes en caso de emergencia y agudiza el problema.

- **Existencia de personas ajenas**.- Aquellas edificaciones, instalaciones o recintos ocupados en su totalidad por personas que no los usan con frecuencia, y por ello no están familiarizados con los mismos. Ello dificulta la localización de salidas, de vías que conducen a ellas o de cualquier otra instalación de seguridad que se encuentre en dichos locales.
- **Condiciones de Iluminación**.- Da lugar a dificultades en la percepción e identificación de señales, accesos a vías de escape, y a su vez incrementa el riesgo de caídas, golpes o empujones.

Nº	ACTIVIDADES	RESPONSABLE	REGISTRO
1	**ACCIONES ANTES DE LA CONTINGENCIA** • Programar dos fumigaciones anuales, en periodos vacacionales. • Programas 2 simulacros al año. • Contar con botas, batas, guantes y cubre bocas e impermeables para poder entrar y salir de la Unidad de Almacén. • Conocer el manejo de los extintores. • Contar con botiquines de primeros auxilios en áreas estratégicas de la Unidad de Almacén y su respectiva capacitación. • Implementar alarmas de emergencia en lugares estratégicos dentro de la Unidad Almacén. • Establecer puntos de reunión dentro y fuera de la Unidad Almacén. • Difundir las rutas de evacuación, así como los sitios de localización de alarmas, extintores. • Establecer procedimientos de evacuación. • Capacitación permanente y actualizada sobre Seguridad e Higiene a los funcionarios del área. • Contar con un directorio del personal.	Comité de Dirección.	Formato seguimiento en el uso de los elementos de protección personal (F-GH-DRH-031) Formato asistencia a eventos (F-SI-SIG-011)

2	**ACCIONES DURANTE LA CONTINGENCIA** • Accionar las alarmas de emergencia • Utilizar las botas e impermeables para poder salir o ingresar a la Unidad de Almacén. • En caso de inundación. • Dirigir a los usuarios en la evacuación e información de salidas de emergencia. • Priorizar la evacuación.	Comité de Logística.	Formato seguimiento en el uso de los elementos de protección personal (F-GH-DRH-031) Formato asistencia a eventos (F-SI-SIG-011)
3	**ACCIONES DESPUÉS DE LA CONTINGENCIA** • Brindar los primeros auxilios a las personas que lo requieran. Realizar un recuento de los daños causados. • Realizar un informe con los hallazgos y emitir a la Dirección. Tomar acciones de acuerdo al informe emitido. • Retroalimentar los planes de contingencia con lo aprendido en la ultima contingencia	Comité Responsable de Recuperación.	Formato seguimiento en el uso de los elementos de protección personal (F-GH-DRH-031) Formato asistencia a eventos (F-SI-SIG-011)

8. DOCUMENTOS REFERENCIALES:

Norma ISO/IEC 27002 dominio gestión continuidad del negocio. Objetivo de control marco referencial.
Gerencia Estratégica Planeación y Gestión - Teoría y Metodología.
Propuesta de Mejoramiento y Contingencia de Sistemas Informáticos en la Empresa. RAMÍREZ ROBAYO, Maritza Yohana,
VARGAS DAZA, Freddy H. Plan de Emergencias Corporación Educativa Minuto De Dios.

9. ANEXOS:

Formato Evaluación de Emergencias Ambientales F-DP-SGA-014
Formato Entrega de Elementos de Protección Persona F-GH-DRH-016
Formato Inspección Planeada F-GH-DRH-026
Formato Inspección de Extintores F-GH-DRH-030
Formato Seguimiento en el Uso de los Elementos de Protección Personal F-GH-DRH-031
Formato Asistencia de Eventos F-SI-SIG-011
Formulario de Inscripción Brigada de Emergencias J-GH-DRH-001

REVISÓ:	APROBO:
COORDINADOR SIG	REPRESENTANTE DE LA DIRECCIÓN

FECHA	CONTROL DE CAMBIOS	REVISIÓN
06-12-2013	Creación del Documento	A

1.NOMBRE	2.PROCESO
GESTIÓN DE CONTINUIDAD DEL NEGOCIO PARA LA UNIDAD DE ALMACÉN	GESTION ADMINISTRATIVA Y FINANCIERA

3. OBJETIVO Garantizar la continuidad de las operaciones de los elementos considerados Críticos que componen los Sistemas de Información, definiendo acciones y procedimientos a ejecutar en caso de fallas de los elementos que lo componen.

4. ALCANCE: El plan de contingencia informático cubre específicamente los eventos o incidentes de seguridad que comprometan total o parcialmente la operación informática de la Unidad de Almacén estableciendo los procedimientos necesarios para restablecer la prestación de los servicios informáticos de forma eficaz y oportuna.

5. RESPONSABLE: Coordinador Plan de Contingencia

6. DEFINICIONES

- **Datos**: En general se consideran datos tanto los estructurados como los no estructurados, las imágenes, los sonidos, etc.
- **Aplicaciones**: Se incluyen los manuales y las aplicaciones informáticas.
- **Tecnología**: El software y el hardware; los sistemas operativos; los sistemas de gestión de bases de datos; los sistemas de red, etc.
- **Instalaciones**: En ellas se ubican y se mantienen los sistemas de información.
- **Personal**: Los conocimientos específicos que ha de tener el personal de los sistemas de información para planificarlos, organizarlos, administrarlos y gestionarlos.

- **Acceso**: Es la recuperación o grabación de datos que han sido almacenados en
- un sistema de computación. Cuando se consulta a una base de datos, los datos son primeramente recuperados hacia la computadora y luego transmitidos a la pantalla del terminal.

- **Ataque:** Término general usado para cualquier acción o evento que intente interferir con el funcionamiento adecuado de un sistema informático, o intento de obtener de modo no autorizado la información confiada a una computadora.

- **Ataque Activo:** Acción iniciada por una persona que amenaza con interferir el funcionamiento adecuado de una computadora, o hace que se difunda de modo no autorizado información confiada a una computadora personal.

- **Ataque Pasivo:** Intento de obtener información o recursos de una computadora
- personal sin interferir con su funcionamiento, como espionaje

7. DESCRIPCIÓN DEL PROCEDIMIENTO

Nº	ACTIVIDADES	RESPONSABLE	REGISTRO
1	**ACCIONES PREVENTIVAS.** **INFRAESTRUCTURA:** En caso de tormenta o inundaciones, seguir las siguientes medidas de prevención: • Realizar mantenimiento general de la planta eléctrica de emergencia. • antener tanque de la planta de emergencia lleno de diesel. • ener un tanque de combustible lleno • omprar pilas para lámpara de emergencia • ar servicio de impermeabilizante a los techos y paredes, • ontar con impermeables. • Encintar ventanas y sellar puerta trasera y delantera de la coordinación donde se pueda filtrar agua. • Tener a la mano el mapa eléctrico de la Coordinación.	Comité de Dirección.	Formato asistencia a eventos (F-SI-SIG-011) Formato inspección planeada (F-GH-DRH-026)

	EQUIPOS DE TELECOMUNICACIONES • Mantenimiento anual de las torres de comunicaciones. • Aislar equipos que estén en riesgo en el piso. • Dejar en funcionamiento el servicio RAS **SERVIDORES** • Sacar relación de servicios prioritarios: DNS, correo electrónico, Real Audio, Web, Conmutada e Internet. • Apagar Servidores no prioritarios • Tapar con bolsas de plástico servidores que pueden mojarse. • Poner sobre mesas los UPS de servidores • Generar los últimos respaldos • Poner en un lugar distante los respaldos de información	COMITÉ DE DIRECCION	FORMATO EVALUACIÓN DE EMERGENCIAS F-DP-SGA-014
	TELECOMUNICACIONES • Sacar relación de equipos prioritarios • Apagar equipos no prioritarios. • Tapar con bolsas de plástico equipos de comunicaciones que pueden mojarse. • Poner sobre mesas los UPS de equipos de comunicaciones. • Generar respaldos de configuraciones e imprimirlos.	COMITÉ DE DIRECCION	Formato asistencia a eventos (F-SI-SIG-011) Formato inspección planeada (F-GH-DRH-026)

	DURANTE LA CONTINGENCIA **INFRAESTRUCTURA** • Si la planta se encuentra en funcionamiento no se deberán conectar equipos con motor como refrigerador y no se proporcionará el servicio de carga de teléfonos celulares. • Contar con mangueras y embudo para poner diesel, llevando extinguidor por si se requiere. • En caso de que la planta haya trabajado más de 72 horas sin parar, se recomienda hablar a proveedor para mantenimiento.	Comité de Logística.	Formato asistencia a eventos (F-SI-SIG-011) Formato inspección planeada (F-GH-DRH-026)
	TELECOMUNICACIONES • Verificación de enlaces hacia Internet Conmutadas y servidores, paulatinamente verificación de enlaces a DES, generando relación de los que ya están en funcionamiento. • Verificación de estado de los equipos y secado de los mismos en caso necesario • Levantamiento de reportes de DES con problemas y establecimiento de prioridades	Comité de Logística	FORMATO ASISTENCIA A EVENTOS F-SI-SIG-011
	SERVIDORES • Verificación de servicios prioritarios de la Unidad de Almacén. • Verificación de estado de los equipos y secado de los mismos en caso necesario. • Levantamiento todos los servicios adicionales.	Comité de Logística	FORMATO ASISTENCIA A EVENTOS F-SI-SIG-011
	ACCIONES DESPUÉS DE LA CONTINGENCIA • Realizar un reporte de daños. • Que el personal encargado del área de contingencia se reúna para analizar el plan de continencias y realizar las modificaciones correspondientes, así como las funciones o acciones del personal de contingencias	Comité Responsable de Recuperación.	Formato asistencia a eventos (F-SI-SIG-011) Formato inspección planeada (F-GH-DRH-026)

8. DOCUMENTOS REFERENCIALES:

Norma ISO/IEC 27002 dominio gestión continuidad del negocio. Objetivo de control marco referencial.
Gerencia Estratégica Planeación y Gestión - Teoría y Metodología. Propuesta de Mejoramiento y Contingencia de Sistemas Informáticos en la Empresa. RAMÍREZ ROBAYO, Maritza Yohana, VARGAS DAZA, Freddy H. Plan de Emergencias Corporación Educativa Minuto De Dios.

9. ANEXOS:

Formato Evaluación de Emergencias Ambientales F-DP-SGA-014
Formato Entrega de Elementos de Protección Persona F-GH-DRH-016
Formato Inspección Planeada F-GH-DRH-026
Formato Inspección de Extintores F-GH-DRH-030
Formato Seguimiento en el Uso de los Elementos de Protección Personal F-GH-DRH-031
Formato Asistencia de Eventos F-SI-SIG-011

REVISÓ:	APROBO:
COORDINADOR SIG	REPRESENTANTE DE LA DIRECCIÓN

FECHA	CONTROL DE CAMBIOS	REVISIÓN
06-12-2013	Creación del Documento	A

1.NOMBRE	2.PROCESO
GESTIÓN DE CONTINUIDAD DEL NEGOCIO PARA LA UNIDAD DE ALMACÉN	GESTION ADMINISTRATIVA Y FINANCIERA

3. OBJETIVO Ejecutar acciones oportunas de evacuación ante cualquier contingencia que se pudiera presentar como consecuencia de un siniestro para salvaguardar a las personas, bienes y el entorno de los mismos que se encuentren dentro de la Unidad de Almacén.

4. ALCANCE: Para todas las personas que laboren, utilicen y / o se encuentren dentro de las Instalaciones de la Unidad de Almacén.

5. RESPONSABLE: Comité de Dirección.

6. DEFINICIONES

- **AMENAZA**: Condición latente derivada de la posible ocurrencia de un fenómeno físico de origen natural, socio - natural o antrópico no intencional, que puede causar daño a la población y sus bienes, la infraestructura, el ambiente y la economía pública y privada. Es un factor de riesgo externo.
- **ATENCIÓN DE EMERGENCIAS**: Medidas y acciones de respuesta a la ocurrencia de un evento tendientes a auxiliar a las víctimas, reducir el daño derivado del mismo y facilitar la recuperación, mediante la acción coordinada de distintas entidades públicas, el sector privado y la comunidad.
- **ESCENARIO DE GESTIÓN:** Es el nivel de análisis e intervención del riesgo que corresponde a un espacio físico de la ciudad caracterizado por: a) procesos territoriales o económicos similares de generación de riesgo. b) Una red de actores sociales con niveles similares de desarrollo, relacionados con procesos comunes de ocupación y transformación del territorio o con una cadena de producción e intercambio de bienes o servicios. c) Similitud en el tipo, naturaleza y expresión de las amenazas naturales, socio - naturales o antrópicas.
- **EVACUACION:** Entendido como el conjunto de actividades y procedimientos tendientes a conservar la vida y la integridad física de las personas en el evento de verse afectadas por amenazas naturales y/o antrópicas no intencionales, mediante el traslado hacia una construcción segura, y localización segura.
- **GESTIÓN DEL RIESGO**: Es un proceso social complejo que tiene como objetivo la reducción o la previsión y control permanente del riesgo en la sociedad, en consonancia con, e integrada al logro de pautas de desarrollo humano, económico, ambiental y territorial sostenibles.

- **PLAN DE ATENCIÓN MÉDICA:** Componente del Plan de Emergencia y Contingencias orientado a prestar a las víctimas atención pre-hospitalaria en el lugar del incidente (ya sea en Emergencia o Desarrollo Normal del Incidente) y a posibilitar la derivación de las que así lo requieran a centros de atención especializada. En caso de Emergencia este plan opera mientras llega la ayuda institucional (principalmente Secretaría de Salud), y sirve de apoyo a esta cuando se haga presente en el lugar.
- **PLAN DE EVACUACIÓN:** Este Plan se refiere a todas las acciones necesarias para detectar la presencia de un riesgo que amenace la integridad de las personas, y como tal comunicarles oportunamente la decisión de abandonar las instalaciones y facilitar su rápido traslado hasta un lugar que se considere seguro, desplazándose a través de lugares también seguros.
- **PREVENCIÓN**: Políticas y acciones que buscan evitar la generación de nuevos riesgos. Está asociada a la gestión prospectiva del riesgo
- **RECUPERACIÓN:** Proceso de recuperación de las áreas y/o funciones afectadas por una emergencia, calamidad o desastre para el restablecimiento de condiciones socialmente aceptables y sostenibles de vida de la población, la reducción de las vulnerabilidades existentes antes de la emergencia y la intervención de procesos territoriales o sectoriales generadores de nuevos riesgos.
- **VULNERABILIDAD:** Característica propia de un elemento o grupo de elementos expuestos a una amenaza, relacionada con su incapacidad física, económica, política o social de anticipar, resistir y recuperarse del daño sufrido cuando opera dicha amenaza. Es un factor interno.
- **RIESGO PÚBLICO:** El daño potencial que, sobre la población y sus bienes, la infraestructura, el ambiente y la economía pública y privada, pueda causarse por la ocurrencia de amenazas de origen natural, socio - natural o antrópico no intencional, que se extiende más allá de los espacios privados o actividades particulares de las personas y organizaciones y que por su magnitud, velocidad y contingencia hace necesario un proceso de gestión que involucre al Estado y a la sociedad.
- **PROCESO DE GENERACIÓN DEL RIESGO:** Es una cadena de acciones dentro de los procesos generales de la ocupación y transformación del territorio, o de la producción y distribución de bienes y servicios, que por su localización, por las características de los medios empleados o por su forma de operar, incrementan las amenazas o la vulnerabilidad. Tales procesos relacionan variables biofísicas, sociales, económicas y culturales que deben ser tener en cuenta en la gestión de cada escenario.
- **PROGRAMA:** Es el conjunto de líneas de acción, proyectos y metas que se deben adelantar en cada escenario de gestión para la consecución de los objetivos del plan.

7. DESCRIPCIÓN DEL PROCEDIMIENTO

Nº	ACTIVIDADES	RESPONSABLE	REGISTRO
1	**EN CASO DE PRESENTARSE UN INCENDIO** • Informe a vigilancia y/o al Jefe de Brigada y al Coordinador de Evacuación quienes asumirán el control de la situación. • Si el fuego se encuentra en etapa incipiente y ninguno de los brigadistas o coordinadores de evacuación se encuentra cerca del lugar, haga uso del extintor si sabe cómo hacerlo, de lo contrario evacue la zona junto con las demás personas. • Si es un incendio declarado, no se deje llevar por el pánico y desaloje en orden el sitio dirigiéndose al punto de encuentro más cercano al área.	Comité de Dirección Comité de Logística Comité Responsable de Recuperación	Formato asistencia a eventos (F-SI-SIG-011) Formato inspección planeada (F-GH-DRH-026) Formato Evaluación De Emergencias (F-DP-SGA-014) Formato Entrega De Elementos de Protección Persona (F-GH-DRH-
2	**EN CASO DE SISMO O TERREMOTO** • No se deje llevar por el pánico, mantenga la calma. • Aléjese de las estructuras y objetos que se puedan caer, si se encuentra en un parqueadero no utilice vehículo. • Ubíquese cerca de una columna, esquina, a un lado de un escritorio o de alguna estructura firme (en posición fetal.) • No intente salir hasta cuando el sismo ó terremoto haya cesado. • Inicie evacuación cuando lo ordene el jefe de emergencia o jefe de la brigada si las condiciones del área ofrecen peligro. • Ayude a quien lo necesite y no regrese por ningún motivo. Diríjase a algún punto de encuentro de reunión asignado y espere. instrucciones	Comité de Dirección Comité de Logística Comité Responsable de Recuperación	Formato asistencia a eventos (F-SI-SIG-011) Formato inspección planeada (F-GH-DRH-026) Formato Evaluación De Emergencias (F-DP-SGA-014) Formato Entrega De Elementos de Protección Persona (F-GH-DRH-016)

3	**EN CASO DE ATENTADOS- EXPLOSION** • Evacue inmediatamente por la salida más próxima. Comunique la alarma a los teléfonos de emergencia como:(Vigilancia, Bienestar universitario y Salud Ocupacional) para que se inicie el procedimiento operativo. • Impida el regreso de personas. Mantenga contacto verbal con su grupo, repita en forma calmada las consignas especiales (No corran, Conserven la calma, etc.) • Inicie evacuación cuando lo ordene el jefe de emergencia si las condiciones del área ofrecen peligro. • Si se encuentra bloqueada la vía de evacuación busque una salida alterna. En caso de no poder salir lleve al personal a un sitio seguro. Solicite inmediatamente auxilio por los medios que tenga a su alcance.	Comité de Dirección Comité de Logística Comité Responsable de Recuperación	Formato asistencia a eventos (F-SI-SIG-011) Formato inspección planeada (F-GH-DRH-026) Formato Evaluación De Emergencias (F-DP-SGA-014) Formato Entrega De Elementos de Protección Persona (F-GH-DRH-016)
4	**EN CASO DE SOSPECHA O AMENAZA DE ATENTADO** • No mueva o toque ningún material sospechoso • Comunique inmediatamente, por alguno de los medios disponibles de la Universidad al Jefe de Emergencias (Bienestar Universitario) o Jefe de Brigada.(Salud Ocupacional) • Suspenda actividades en el área. Espere instrucciones para iniciar la búsqueda de elementos o materiales extraños, en coordinación con el Grupo de Vigilancia. • Apague celulares, radios, y todo equipo que pueda admitir ondas electromagnéticas • Cuide que no se muevan elementos sospechosos. Inicie los procedimientos de evacuación. • Impida el regreso de personas. • Espere la orden de regreso a las actividades	Comité de Dirección Comité de Logística Comité Responsable de Recuperación	Formato asistencia a eventos (F-SI-SIG-011) Formato inspección planeada (F-GH-DRH-026) Formato Evaluación De Emergencias (F-DP-SGA-014) Formato Entrega De Elementos de Protección Persona (F-GH-DRH-016)

5	**EN CASO DE ASONADA O ATAQUE** • No se deje llevar por el pánico, no grite, no corra y mantenga la calma. • Resguárdese en un lugar seguro, al lado de un escritorio, mesa o cerca de una columna y ubíquese en posición fetal lejos de las ventanas hasta cuando pueda salir. • Evalué las diferentes posibilidades de salir por un lugar diferente a donde se encuentra el problema principal. • Inicie evacuación cuando lo ordene el jefe de emergencias o jefe de brigadas si las condiciones del área ofrecen peligro. • Preste ayuda a quien lo requiera	Comité de Dirección Comité de Logística Comité Responsable de Recuperación	Formato asistencia a eventos (F-SI-SIG-011) Formato inspección planeada (F-GH-DRH-026) Formato Evaluación De Emergencias (F-DP-SGA-014) Formato Entrega De Elementos de Protección Persona (F-GH-DRH-016)
6	**EN CASO DE ASONADA O ATAQUE** • No se deje llevar por el pánico, no grite, no corra y mantenga la calma. • Resguárdese en un lugar seguro, al lado de un escritorio, mesa o cerca de una columna y ubíquese en posición fetal lejos de las ventanas hasta cuando pueda salir. • Evalué las diferentes posibilidades de salir por un lugar diferente a donde se encuentra el problema principal. • Inicie evacuación cuando lo ordene el jefe de emergencias o jefe de brigadas si las condiciones del área ofrecen peligro. • Preste ayuda a quien lo requiera	Comité de Dirección Comité de Logística Comité Responsable de Recuperación	Formato asistencia a eventos (F-SI-SIG-011) Formato inspección planeada (F-GH-DRH-026) Formato Evaluación De Emergencias (F-DP-SGA-014) Formato Entrega De Elementos de Protección Persona (F-GH-DRH-016)

7	**EN CASO DE INUNDACIÓN O ANEGACION** • Reporte el evento que se presenta a Jefe de Vigilancia, emergencias y/o brigada. • Apague equipos eléctricos que puedan ser objeto de corto circuito. • Evacue a las personas que están en el lugar. • Controle con barreras y baldes plásticos mientras recibe apoyo de seguridad y brigadistas. • Si la situación es grave, evacue a los sitios de reunión y espere la llegada de los organismos de apoyo: (Cruz Roja, Defensa Civil, etc.)	Comité de Dirección Comité de Logística Comité Responsable de Recuperación	Formato asistencia a eventos (F-SI-SIG-011) Formato inspección planeada (F-GH-DRH-026) Formato Evaluación De Emergencias (F-DP-SGA-014) Formato Entrega De Elementos de Protección Persona (F-GH-DRH-016)
8	**EN CASO DE LLAMADA TELEFONICA POR AMENAZA DE BOMBA.** • Espere a que la persona que llama cuelgue, no cuelgue primero; Trate de obtener la mayor información posible. • Tome atento nota y entere a otra por escrito o por señas para que reporte lo sucedido de la amenaza a vigilancia y jefe de emergencias y/o jefe de brigadas. • Sí se conoce el posible lugar, no toque ni mueva ningún objeto y alerte calmadamente a las personas del lugar, mientras asume el control el comité de emergencias. • Todo el personal está obligado a despejar los pasillos para facilitar la correcta acción del personal de seguridad y control. • De acuerdo con lo que determine el Comité de Emergencia, evacue a las personas del lugar hasta el punto de encuentro, indíqueles no usar ningún tipo aparato eléctrico o electrónico.	Comité de Dirección Comité de Logística Comité Responsable de Recuperación	Formato asistencia a eventos (F-SI-SIG-011) Formato inspección planeada (F-GH-DRH-026) Formato Evaluación De Emergencias (F-DP-SGA-014) Formato Entrega De Elementos de Protección Persona (F-GH-DRH-016)

9	• **EN CASO DE DETECTAR PRESENCIA DE OBJETOS SOPECHOSOS** • Reportar inmediatamente al Jefe de Vigilancia, jefe de Emergencias o de la brigada sobre la situación. • No toque ni trate de remover el objeto. Deje la curiosidad a un lado. • Elimine fuentes de explosión, mantenga apagados equipos eléctricos y electrónicos (radios, celulares u otros) • Manténgase usted y demás miembros de la comunidad Universitaria a una distancia a 300 metros del lugar donde está el paquete u objeto • Profesores, estudiantes, funcionarios y visitantes no autorizados NO deben empezar por su cuenta la búsqueda de artefactos explosivos.	Comité de Dirección Comité de Logística Comité Responsable de Recuperación	Formato asistencia a eventos (F-SI-SIG-011) Formato inspección planeada (F-GH-DRH-026) Formato Evaluación De Emergencias (F-DP-SGA-014) Formato Entrega De Elementos de Protección Persona (F-GH-DRH-016)

. DOCUMENTOS REFERENCIALES:

Norma ISO/IEC 27002 dominio gestión continuidad del negocio. Objetivo de control marco referencial.
Gerencia Estratégica Planeación y Gestión - Teoría y Metodología. Propuesta de Mejoramiento y Contingencia de Sistemas Informáticos en la Empresa. RAMÍREZ ROBAYO, Maritza Yohana,
VARGAS DAZA, Freddy H. Plan de Emergencias Corporación Educativa Minuto De Dios.

9. ANEXOS:

Formato Evaluación de Emergencias Ambientales F-DP-SGA-014
Formato Entrega de Elementos de Protección Persona F-GH-DRH-016
Formato Inspección Planeada F-GH-DRH-026
Formato Inspección de Extintores F-GH-DRH-030
Formato Seguimiento en el Uso de los Elementos de Protección Personal F-GH-DRH-031
Formato Asistencia de Eventos F-SI-SIG-011

REVISÓ:	APROBO:
COORDINADOR SIG	REPRESENTANTE DE LA DIRECCIÓN

FECHA	CONTROL DE CAMBIOS	REVISIÓN
06-12-2013	Creación del Documento	A

1.NOMBRE	2.PROCESO
GESTIÓN DE CONTINUIDAD DEL NEGOCIO PARA LA UNIDAD DE ALMACÉN	**GESTION ADMINISTRATIVA Y FINANCIERA**

3. OBJETIVO: Coordinar el trabajo de reposición de la energía eléctrica en la Unidad de Almacén de la Universidad Francisco de Paula Santander Ocaña, mediante un plan estructurado que resuelva, en el menor tiempo posible la discontinuidad del suministro de energía eléctrica producida por cortes originados por la compañía de energía o por siniestro o falla de los sistemas de distribución interna.

4. ALCANCE: Comprende todas las actividades y procesos de la Unidad de Almacén que involucren el suministro el eléctrico.

5. RESPONSABLE: Coordinador Plan de Contingencia

6. DEFINICIONES

- **Sistema alternativo de red eléctrica**: red privada de energía eléctrica generada por grupo electrógeno.
- **Grupo electrógeno:** máquina que mueve un generador eléctrico a través de un motor de combustión interna.
- **Transferencia electrónica**: encendido automático de motor generador de electricidad.
- **Encendido manual:** puesta en marcha de motor a través de comandos manuales por un operario.
- **Acción Correctiva:** Es la acción tomada para eliminar la causa de una no conformidad detectada u otra situación no deseable.
- **Acción Preventiva**: Es la acción tomada para eliminar la causa de una no conformidad potencial.

- **Riesgos**: Toda posibilidad de ocurrencia de aquella situación que pueda entorpecer el desarrollo normal de las funciones de la entidad y le impidan el logro de sus objetivos.
- **Eficacia**: Grado en el que se realizan las actividades planificadas y se alcanzan los resultados planificados.
- **Eficiencia:** Relación entre el resultado alcanzado y los recursos utilizados.

7. DESCRIPCIÓN DEL PROCEDIMIENTO

Nº	ACTIVIDADES	RESPONSIBLE	REGISTRO
1	**Acciones preventivas a la contingencia** • Contar con una planta de emergencia que suministre energía regulada a toda la Unidad de Almacén. • Supervisar semanalmente el nivel óptimo de combustible, agua, baterías, etc. • Contar con un plan de mantenimiento semestral con supervisiones mensuales • Supervisar el combustible de respaldo en el área de servicios generales. • Contar con equipo de emergencia contra incendios en el local de la planta. • Contar con el mapa eléctrico del área en la planta y archivado, identificando los contactos respaldados y regulados. • Contar con polo a tierra independientes a los servicios de telecomunicaciones • Contar con una UPS con capacidades necesarias (40% superiores) en todos los sitios y centros de cableado	Comité de Dirección.	Formato asistencia a eventos (F-SI-SIG-011) Formato inspección planeada (F-GH-DRH-026)

	• Contar con un directorio de los responsables del suministro eléctrico en la Unidad de Almacén. • Reportar el incidente a las áreas involucradas (Servicios Generales, Proveedores de mantenimientos) • Notificar a los usuarios afectados la probable baja de los servicios de comunicación. • Ejecutar respaldos de emergencia a la información del servidor Web, mail, DNS, configuraciones de Equipo activo principales y centrales. • Contar con una tabla de claves de prioridades para dar aviso a los usuarios prioritarios con el fin de optimizar tiempo y recursos • Solicitar revisión periódica (semestral) del estado y óptimo		
2	**En caso de interrupción del suministro eléctrico en lapsos cortos consecutivos** • Comunicarse con servicios generales para la supervisión de la Planta de emergencia • Monitorear el UPS cada 20 min. para programar acciones mayores • Valorar la decisión de dar de baja los equipo activos y/o servicios para evitar daños y/o pérdida de información y de equipos.	Comité de Logística.	Formato asistencia a eventos (F-SI-SIG-011) Formato inspección planeada (F-GH-DRH-026)

3	**En caso de una interrupción del suministro eléctrico no mayor a una hora:** • Comunicarse con servicios generales para la supervisión de la Planta de emergencia. • Monitorear el UPS cada 10 min. para programar acciones mayores. • Apagar los equipos no prioritarios como impresoras, monitores o PC que no demanden su uso. • Desconectar electrodomésticos (cafeteras, equipo de sonido, refrigerador, horno de microondas, ventiladores, etc.) • Dar de baja a los equipos que cumplieron con su vida útil. • Contar con radios de comunicación cargados	Comité de Logística	Formato inspección planeada (F-GH-DRH-026)
4	**En caso de una interrupción del suministro eléctrico mayor a una hora** • Dar aviso de la contingencia a los usuarios prioritarios (Almacén) • Preparar el apagado de los equipos prioritarios (equipo activo) Comunicarse con servicios generales para la supervisión de la planta de emergencia con mayor énfasis. • Monitorear el UPS cada 5 min. para programar acciones mayores. • Dar de baja equipo activo y servicios con mediana prioridad con respecto a las fases definidas.	Comité de Logística	FORMATO INSPECCIÓN PLANEADA F-GH-DRH-026

5	**Acciones después de la contingencia** • Brindar un tiempo de gracia (depende de la magnitud de la contingencia) para restablecer los equipos activos y servicios • Restablecer los equipos activos y servicios que se dieron de baja, en forma paulatina. • Validar el correcto funcionamiento de los equipos activos y servicios. • Identificar los posibles daños de los equipos activos • Notificar a los usuarios afectados el restablecimiento de los servicios y su condición • Evaluar los daños de los equipos activos, planta de emergencia, UPS y canalizarlos a las áreas involucradas.	Comité Responsable de Recuperación.	Formato asistencia a eventos (F-SI-SIG-011) Formato inspección planeada (F-GH-DRH-026)

8. DOCUMENTOS REFERENCIALES:

Norma ISO/IEC 27002 dominio gestión continuidad del negocio. Objetivo de control marco referencial.
Propuesta de Mejoramiento y Contingencia de Sistemas Informáticos en la Empresa. RAMÍREZ ROBAYO, Maritza Yohana,
VARGAS DAZA, Freddy H. Plan de Emergencias Corporación Educativa Minuto De Dios.

9. ANEXOS:

Formato Evaluación de Emergencias Ambientales F-DP-SGA-014
Formato Entrega de Elementos de Protección Persona F-GH-DRH-016
Formato Inspección Planeada F-GH-DRH-026
Formato Inspección de Extintores F-GH-DRH-030
Formato Seguimiento en el Uso de los Elementos de Protección Personal F-GH-DRH-031
Formato Asistencia de Eventos F-SI-SIG-011

REVISÓ:	APROBO:
COORDINADOR SIG	REPRESENTANTE DE LA DIRECCIÓN

FECHA	CONTROL DE CAMBIOS	REVISIÓN
06-12-2013	Creación del Documento	A

5. CONCLUSIONES

Se realizó el reconocimiento de la Unidad de Almacén dentro del contexto de la Universidad, identificando la cadena de valor de la dependencia, modelando sus procesos a través del BMM (Business Motivation Model), creando su estructura orgánica e identificando la Tecnología de Información (TI) presente en la Unidad de Almacén. Al realizar el diagnóstico se detectaron amenazas a nivel Natural y Humanas (Como Incendios, Inundaciones, Robos, Sabotajes, entre otros) que pueden afectar los activos de la Universidad y la Unidad de Almacén, clasificados en: Medio Ambiente e Infraestructura (En las oficinas y bodegas), Activos de TI (Hardware y Software), Información (SIF), Personas (Personal Administrativo y Operativo), Comunicaciones (Internet y Local) en la Gestión de Continuidad del Negocio. Como aspecto positivo se cuenta con un sistema de información que cumple con los procesos identificados dentro de la dependencia.

Se creó un Manual de Gestión de Continuidad del Negocio según la Norma ISO/IEC 27002 (Teniendo en cuenta sus cinco objetivos de control: Incluir la Seguridad de la Información en el Proceso de Gestión de Continuidad del Negocio, Continuidad del Negocio y Evaluación del Riesgo, Desarrollar e Implementar los Planes de Continuidad Incluyendo la Seguridad de la Información, Marco Referencial de la Planeación de la Continuidad del Negocio y Prueba, Mantenimiento y Re-Evaluación de los Planes de Continuidad del Negocio), los cuales especifican los controles que se deberán aplicar para reducir los riesgos en materia de seguridad de la información y continuidad del negocio en la Unidad de Almacén.

La creación de procedimientos para la Gestión de Continuidad del Negocio en la Unidad de Almacén permite acciones básicas de respuesta a tomar 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.

6. RECOMENDACIONES

Presentar a las directivas de la Universidad esta propuesta para su implementación y llegado el caso se debe contar con un rubro presupuestal para el desarrollo de la misma, además se deben realizar campañas de concientización y capacitación dirigida al personal de la Unidad de Almacén, en la Gestión de Continuidad del Negocio según la norma ISO/IEC 27002.

Se deben elaborar convenios de compromiso y responsabilidad del personal de la Unidad de Almacén, al buen uso de los activos de la información a su cargo.

Incluir dentro de la planeación estratégica de la Universidad los requerimientos de mejoramiento de la infraestructura física de la Unidad de Almacén y de la bodega, incluyendo la creación de un puesto de trabajo en esta área.

La bodega debe contar con una estantería para la clasificación adecuada de los elementos de consumo y devolutivos, que permita el fácil acceso a ellos. Así mismo una bodega exclusiva para los bienes devolutivos dados de baja.

Las Oficinas de Almacén y las bodegas deben estar dotadas de detectores de humo, alarmas, cámaras de seguridad, extintores y demás instrumentos de seguridad industrial.

BIBLIOGRAFIA

BELTRAN, Gustavo. Consultoría Estratégica y coachig de negocios. [en línea] [Citado el: 28 de 01 de 2013.] http://gustavobeltran.com/%C2%BFque-se-entiende-por-direccionamiento-estrategico/.

GARCÍA FORT, Javier. Plan de Continuidad del Negocio de una TIC. Madrid, España. 2010. 173h. Trabajo de Grado (Ingeniero Técnico en Informática de Gestión). Universidad Pontificia Comillas. Escuela Técnica superior de Ingeniería. [en línea]. http://www.iit.upcomillas.es/pfc/resumenes/4c2474cf9a017.pdf

GÓMEZ, Humberto. Gerencia Estratégica Planeación y Gestión - Teoría y metodología. Santa Fé de Bogotá : 3R Editores, 1994.

GUEVARA, Alberto y LÓPEZ, Diana. Diseñar un modelo de contingencia de sistemas y Telecomunicaciones para las entidades bancarias del Ecuador. Guayaquil, Ecuador. 2012. 198h. Trabajo de Grado (Ingeniero en Sistemas Computacionales). Universidad de Santiago de Guayaquil. Facultad de Ingeniería. [en línea]. http://repositorio.ucsg.edu.ec/bitstream/123456789/181/1/T-UCSG-PRE-ING-CIS-7.pdf

INSTITUTO ECUATORIANO DE CRÉDITO EDUCATIVO Y BECAS. Plan de Continuidad de Negocios. Quito, Ecuador. 2012. 39h. Fecha de Última Revisión: 11/09/2012. [en línea]. http://www.iece.fin.ec/docs/lotaip/planes_programas_en_ejecucion/2012/plan_de_continuidad_de_negocios.pdf

INSTITUTO DEL MAR DEL PERÚ (IMARPE). Plan de Contingencia Informático 2012-2015. Callao, Perú. 2012. 78h. [en línea]. http://www.imarpe.pe/imarpe/archivos/informes/imarpe_resol_de_158_2012_conting.pdf

ISO/IEC 27002:2005 Tecnología de la información - Técnicas de seguridad - Código de buenas prácticas para la gestión de seguridad de la información. [en línea]. http://www.iso.org/iso/home/search.htm?qt=iso+27002&sort=rel&type=simple&published=on

LEON LÓPEZ, Diana Rocío. Plan de Contingencia para el archivo de la Universidad de la Salle como parte de la implantación del sistema integrado de Conservación. Bogotá, Colombia. 2007. 186h. Trabajo de grado (Profesional en Sistemas de Información, bibliotecología y archivística). Universidad La Salle. Facultad de sistemas de Información y Documentación. [en línea]. http://repository.lasalle.edu.co/bitstream/10185/12680/2/33021222.pdf

MARTINEZ FAJARDO, Humberto. Plan Local de Emergencia y Contingencias (PLEC´s) Municipio de Manaure Departamento de La Guajira. Manaure, Colombia. 2011. 95h. [en línea]. http://www.sigpad.gov.co/sigpad/archivos/03_PLEC_MANAURE2011.pdf

MESSINO SOZA, Alexis. Módulo Auditoria al Desarrollo de Proyectos de Ingenieria. Universidad Francisco de Paula Santander, Ocaña. 2012. 97h. Especialización en Auditoría de Sistemas.

MINISTERIO DEL INTERIOR Y DE JUSTICIA DE COLOMBIA. Dirección Nacional del Derecho de Autor. Unidad Administrativa Especial. [en línea]. http://www.propiedadintelectualcolombia.com/Site/LinkClick.aspx?fileticket=yDsveWsCdGE%3D&tabid=

PACHECO SOLANO, Andrés Alfonso y TORO RUEDA, Mileidy. Políticas de Seguridad de la Información para la Unidad de Almacén de la Universidad Francisco de Paula Santander Ocaña. Ocaña, Colombia. 2013. 232h. Trabajo de Grado. Universidad Francisco de Paula Santander Ocaña. Facultad de Ingenierías. Plan de Estudios de Ingeniería de Sistemas. [en línea].

RODRIGUEZ GALEZO, Lorencita y RINCON PARADA. Isbelia. Módulo Técnicas y Herramientas para Auditoría de Sistemas. Universidad Francisco de Paula Santander, Ocaña. 2012. 56h. Especialización en Auditoría de Sistemas.

SUPERINTENDENCIAS DE SOCIEDADES. Manual Manejo y Control Administrativo de los Bienes de Propiedad. Bogotá D.C., Colombia, 2009. 29h. [en línea]. http://www.supersociedades.gov.co/web/Ntrabajo/SISTEMA_INTEGRADO/Documentos%20Infraestructura/DOCUMENTOS/GINF-M-001%20MANUAL%20ADMINISTRATIVO.pdf

TAPIA PIEDRA, Jonathan Oswaldo y ZAPATA CHORRA, Jorge Eduardo. Plan de Contingencia y Continuidad Dirigido a la Universidad Técnica de Babahoyo. Babahoyo, Ecuador. 2013. 173h. Trabajo de Grado. Universidad Técnica de Babahoyo. Escuela de Sistemas y Tecnología. [en línea]. http://190.63.130.199:8080/handle/123456789/2087

TRUJILLLO, Freddy. C.E Soft Colombia. [en línea] [Citado el: 28 de enero de 2013.] http://cesoftco.net/2cmc/PAPER.htm.

TUMBACO MIELES, Ingrid Tatiana y YÉPEZ MANOSALVAS, Daniela Margarita. Desarrollo de un Plan de Continuidad del Negocio para el Área de Producción de una Empresa dedicada a la Producción y Comercialización de Helados para el año 2009. Guayaquil, Ecuador. 2009. 132 h. Trabajo de grado (Ingeniería en auditoría y control de gestión, especialización calidad de procesos). Escuela Superior Politécnica del Litoral. Instituto de Ciencias Matemáticas. [en línea]. http://www.dspace.espol.edu.ec/bitstream/123456789/16711/2/Tesina%20BCP%20FINAL.pdf

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER. Consejo Superior Universitario. Acuerdo No. 126. Diciembre 9 de 1994. [en línea]. http://www.ufpso.edu.co/ftp/pdf/acuerdos/acuerdo_126.pdf

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA. Gerencia de Innovación y Desarrollo Tecnológico. Última actualización el Lunes, 22 de Abril de 2013 09:05. [en línea]. http://www.unad.edu.co/gidt/index.php/leyesinformaticas

VARGAS DAZA, Freddy H. Plan de Emergencias Corporación Educativa Minuto De Dios. Bogotá, Colombia. 2009. 82h. [en línea]. http://colegios.minutodedios.org/saludocupacionalcemid/imagenes/plan.pdf

VELASQUEZ PEREZ, Torcoroma y PUENTES VELASQUEZ, Mauricio. Módulo Gobernabilidad de TI. Universidad Francisco de Paula Santander, Ocaña. 2012. 58h. Especialización en Auditoría de Sistemas.

ANEXOS

Anexo A.

ENCUESTA DIRIGIDA AL PERSONAL ADMINISTRATIVO DE LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

1- ¿Existe en la Universidad un Plan de Contingencia?
SI_____ NO_____
Cual?_____
_____
_

2- ¿Recibió usted Capacitación o socialización de este Plan de Contingencia?
SI_____ NO_____

3- ¿Actualmente este Plan de Contingencia se está aplicando en la Universidad?
SI_____ NO_____

GRACIAS.

Anexo B.

ENCUESTA DIRIGIDA AL JEFE DE SISTEMAS DE INFORMACIÓN, TELECOMUNICACIONES Y TECNOLOGÍA DE LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

1- ¿Existe en la Universidad un Plan de Contingencia?
SI_____ NO_____
Cual?_____
_____
_

2- ¿Recibió usted Capacitación o socialización de este Plan de Contingencia?
SI_____ NO_____

3- ¿Actualmente este Plan de Contingencia se está aplicando en la Universidad?
SI_____ NO_____

4- ¿En qué año fue creado el Plan de Contingencia?
_____

5- ¿Este Plan de Contingencia ha sido actualizado?

SI_____ NO_____

6- ¿Cuántas versiones?
_____

7- ¿Cuál fue la ultima?_____

GRACIAS.

Anexo C. Auditoria en la Unidad de Almacén e Inventario de la Universidad Francisco de Paula Santander

Ver archivo adjunto

Anexo D. Elementos protección personal

Ver archivo adjunto

Anexo E. Asistencia a eventos

Ver archivo adjunto

Anexo F. Evaluación emergencias

Ver archivo adjunto

Anexo G. Inspección de extintores

Ver archivo adjunto

Anexo H. Lista chequeo

Ver archivo adjunto

Anexo I. Seguimiento uso de los elementos de protección personal

Ver archivo adjunto

Anexo J. Inscripción de brigadas emergencia

Ver archivo adjunto

Anexo K. Inspección planeada

Ver archivo adjunto

Anexo L. Formato UFPS procedimiento

Ver archivo adjunto

Anexo M. Matriz riesgo 1

Ver archivo adjunto