RESUMEN – TRABAJO DE GRADO

AUTORES DEL PROYECTO	JAVIER ALEXANDER BLANCO LINDARTE LINA FERNANDA MARTÍNEZ VEGA CLAUDIA DEL PILAR QUINTERO PRADO JORGE FRANCISCO RINCÓN ANGARITA
FACULTAD	FACULTAD DE INGENIERÍAS
PLAN DE ESTUDIOS	ESPECIALIZACIÓN EN AUDITORIAS DE SISTEMAS
DIRECTOR	ANDRÉS MAURICIO PUENTES VELÁSQUEZ
TÍTULO DE LA TESIS	PLAN DE CONTINUIDAD PARA EL CENTRO DE DESARROLLO E INOVACCIÓN TECNOLOGIA DE LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA.

RESUMEN
(70 palabras aproximadamente)

EL PLAN DE CONTINUIDAD DEL NEGOCIO ES UNA HERRAMIENTA QUE MITIGA EL RIESGO DE NO DISPONIBILIDAD DE LOS RECURSOS NECESARIOS PARA EL NORMAL DESARROLLO DE LAS OPERACIONES, OFRECIENDO COMO ELEMENTOS DE CONTROL LA PREVENCION, ATENCION DE EMERGENICAS Y ADMINISTRACION DE LA CRISIS.

EL PRESENTE TRABAJO DESCRIBE SITUACIONES EN LA CUALES SE PUEDE APLICAR UN PLAN DE CONTINUIDAD DEL NEGOCIO QUE GARANTICE LA SEGURIDAD DE LA INFORMACION, POR LO QUE SE HACE NECESARIO QUE SE DEFINAN OBJETIVAMENTE LAS ETAPAS QUE CONLLEVAN A LA ELABORACIÓN DEL PLAN, ESTABLECIENDO UNOS PROCEDIMIENTOS, CONSTRUYENDO ACCIONES CORRECTIVAS Y PREVENTIVAS QUE GARANTICEN LA CONTINUIDAD DE LAS ACTIVIDADES A SU QUEHACER INSTITUCIONAL, ESTRUCTURANDO PLANES ADECUADOS PARA QUE LA MISIÓN, LA VISIÓN Y LOS OBJETIVOS SE CUMPLAN.

CARACTERÍSTICAS

PÁGINAS:	PLANOS:	ILUSTRACIONES:	CD-ROM:

PLAN DE CONTINUIDAD PARA EL CENTRO DE DESARROLLO E INNOVACIÓN TECNOLÓGICA DE LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

JAVIER ALEXANDER BLANCO
LINA FERNANDA MARTINEZ VEGA
CLAUDIA DEL PILAR QUINTERO PRADO
JORGE FRANCISCO RINCÓN ANGARITA

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
FACULTAD DE INGENIERIAS
ESPECIALIZACION EN AUDITORIA DE SISTEMAS
OCAÑA
2015

PLAN DE CONTINUIDAD PARA EL CENTRO DE DESARROLLO E INNOVACIÓN TECNOLÓGICA DE LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

JAVIER ALEXANDER BLANCO LINDARTE
LINA FERNANDA MARTINEZ VEGA
CLAUDIA DEL PILAR QUINTERO PRADO
JORGE FRANCISCO RINCÓN ANGARITA

Proyecto presentado como requisito para optar al título de Especialista en Auditoria de Sistemas

Director
ANDRES MAURICIO PUENTES VELASQUEZ

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
FACULTAD DE INGENIERIAS
ESPECIALIZACION EN AUDITORIA DE SISTEMAS
OCAÑA
2015

DEDICATORIA

*Dedico este logro principalmente a **Dios** por darme la sabiduría para alcanzar cada una de las metas y objetivos propuestos, por gene siempre en mí ese sentimiento de alegría, tranquilidad y serenidad en cada momento de mi vida, por permitirme culminar esta etapa y de la cual espero ser digno por tan valioso esfuerzo.*

*A mi Madre **Miryam Vega Sánchez**, y a mi Padre **Luis Eduardo Martínez** (Q.E.P.D), no hay un día en el que no le agradezca a Dios por el haberme colocado entre ustedes, por hacerme sentir la fortuna más grande y en especial por tenerte conmigo, y por inculcarme cada uno de los valores que tiene la vida.*

*A mis hermanos, **José Luis Martínez Vega, Diana Milena Martínez Vega y Kelly Johanna Vega Bacca**, por acompañarme siempre en todas mis metas.*

A mis Sobrinos, porque hoy soy un ejemplo para ellos de esfuerzo, entrega, dedicación y superación, para que nunca desmayen y alcancen sus sueños.

A mi novio, por estar en los momentos más difíciles de mi vida, por su amor, dedicación y comprensión.

*Si algo me enseño esta carrera es que existen personas valiosas, mis compañeros **Claudia del Pilar Quintero Prado, Jorge Francisco Rincón Angarita, Javier Alexander Blanco Lindarte**, valió la pena luchar juntos por una meta, queda la satisfacción de haber compartido con personas tan valiosas como ustedes, les doy las gracias por su apoyo y afecto.*

Por último deseo dedicarles este trabajo especial a todas las personas que siempre creyeron en mi capacidad, es grato saber la fuerza y determinación que poseemos cuando queremos alcanzar algo.

"El éxito debe medirse no por la posición a que una persona ha llegado, sino por su esfuerzo por triunfar".

Booker T. Washington.

LINA FERNANDA MARTINEZ VEGA

DEDICATORIA

Dedico este nuevo triunfo principalmente a Dios todopoderoso por darme la sabiduría y la actitud para alcanzar cada una de los objetivos propuestos.

*A mi madre **BERTHA MARINA LINDARTE RAMIREZ** por su apoyo y ser el motor que día a día me impulsa a seguir adelante, gracias por permitir que mis sueños se hagan una realidad.*

*A mi esposa **NANCY TERESA BLANCO MONTAÑEZ** por su amor, dedicación y comprensión por darme las fuerzas para seguir adelante.*

*A mi hija hermosa **LAURA SOFIA BLANCO BLANCO** por ser el angelito que se suma a nuestra familia llenándonos de emoción y de esperanza, pues no existe mejor regalo del cielo que un hijo.*

*A mi hermana **SANDRA MILENA BLANCO LINDARTE** por apoyarme incondicionalmente y compartir conmigo cada momento de mi vida.*

*A mi sobrina **MARIA GABRIELA TORRES PEREZ** porque hoy soy un ejemplo para ella de esfuerzo, entrega, dedicación y superación, para que nunca flaquee y alcance siempre sus sueños.*

Y demás familiares y amigos quienes han compartido conmigo en este largo camino y hoy ven este sueño hecho realidad.

JAVIER ALEXANDER BLANCO LINDARTE

DEDICATORIA

*El presente trabajo está dedicado a la memoria de mi padre "**Pacho Rincón**", quien desde el cielo guía mis pasos junto con el DIOS Celestial; a mi madre, Esp. **Fabiola Angarita**, y a mis hermanos. Pero de manera muy especial, quiero dedicar esta tesis a mi amada esposa, **Genny Magdely**, quien con cariño, comprensión y estímulo me ha brindado su apoyo cuando lo he necesitado; a mi hija **Genny Andrea**, quien es mi fuente de inspiración y el motivo por el cual he aprendido, con esfuerzo y perseverancia, a encontrarle el sentido y darle la suficiente importancia a las cosas buenas que tiene la vida, es por eso que todos mis logros, y este en especial, los dejo como un legado de motivación a ella, razón por la cual lucho día a día, no solo para ser el mejor papá, sino el mejor amigo.*

*A mis suegros, **Luis Arides** y **Elida** "**Mamá Lelo**", amigos y familiares, por su motivación de "¡VAMOS, TÚ PUEDES!", "¡HAZLO Y NO TE ARREPENTIRÁS!", no podía dejar de rendirles tributo sincero, en especial a mi amigo y jefe, Mag. **Wilmar González**, por su estímulo y su confianza hacia lo que aspiro. Pero sobre toda las cosas, quiero ofrecerle este logro a **Dios**, que es quien tiene el don de guiar nuestros pasos cada día. Gracias, y que DIOS derrame todas sus bendiciones sobre ustedes.*

JORGE FRANCISCO RINCÓN ANGARITA

DEDICATORIA

*A **DIOS**, por darme el don de la vida, la salud, la sabiduría y el camino para encontrar a mi esposo J**osé Gregorio**, con el cual me permitió construir una familia llena de amor y me bendijo con mis angelitas; **María José**, **María Lucia** y **María Paz**, convirtiéndose ellos en la fuente que me impulsa a superarme, y me animan cuando siento desfallecer, llenándome de sueños, esperanzas y amor, por esas razones y muchas más los adoro, los amo y pido a la Madre de DIOS que no se aparte de mí y sola nunca me deje para junto a ella educar a mis hijas y me ilumine para ser mejor esposa, madre e hija.*

A mis padres, mis hermanos y a mi sobrina por estar siempre conmigo de una manera incondicional apoyándome en todo lo que me propongo conseguir.

Bendiciones y mil gracias a todos para seguir creciendo en la gracia y el amor de DIOS.

CLAUDIA DEL PILAR QUINTERO PRADO

AGRADECIMIENTOS

Agradezco a Dios todopoderoso por darme la sabiduría y el entendimiento que me permiten alcanzar cada una de mis metas propuestas y hacer realidad este gran sueño.

A mi madre ***BERTHA MARINA LINDARTE RAMIREZ Y MI TIA MARIA ELIDALINDARTE RAMIREZ*** *por haberme brindado la oportunidad de optar a la realización de una carrera con esfuerzo y dedicación.*

A la Msc. ***TORCOROMA VELÁSQUEZ PÉREZ*** *por el gran apoyo que me brindó durante la especialización.*

A mis suegros ***DON JOAQUIN Y DOÑA GRACIELA*** *por su apoyo, colaboración y estar ahí cuando los necesite.*

Al Ingeniero ***ANDRÉS MAURICIO PUENTES VELÁSQUEZ*** *por su colaboración, tiempo y aportes que nos brindó para hacer de este logro una realidad.*

A mis compañeros ***CLAUDIA DEL PILAR QUINTERO PRADO****,* ***LINA FERNANDA MARTINEZ VERA Y JORGE FRANCISCO RINCON ANGARITA****, a ustedes mil y mil gracias por ser un grupo selecto y comprometido, por su apoyo y entrega en este proyecto que hace unos meses emprendimos y que hoy nos permite una vez más, alcanzar este nuevo triunfo.*

.

JAVIER ALEXANDER BLANCO LINDARTE

AGRADECIMIENTOS

*Profundo agradecimiento a **Dios**, por darme la fortaleza y la constancia necesaria para cumplir con los objetivos propuestos. A mi madre, por estar siempre al lado brindándome su apoyo; a mi familia; a la Universidad Francisco de Paula Santander Ocaña, por acogerme y darme la oportunidad de formarme como especialista y, especialmente, a la División de Post grados – Especialización en Auditoria de Sistemas, cuyas directivas y docentes me dieron una sólida formación como especialista y lograron que culmine con éxito tan importante etapa académica.*

*Al Ing. **Andrés Mauricio Puentes Velásquez**, mi Director de Tesis, y a los Jurados Ing. **Isbelia Rincón** e Ing. **Torcoroma Velásquez**, quienes me orientaron y guiaron en este proyecto que sella y da cuenta de un testimonio de trabajo, entrega y voluntad; deseo dejar constancia de mi sincero sentimiento de gratitud y amistad.*

*A mis compañeros de especialización, **Lina**, **Claudia** y **Javier**; quienes me acogieron con mucho cariño y amabilidad.*

A todas aquellas personas que de una u otra manera me brindaron su apoyo y cooperación moral y espiritual y me aconsejaron por mi bienestar. Gracias, mil gracias a todos ellos.

JORGE FRANCISCO RINCÓN ANGARITA

RESUMEN

La información es uno de los activos más importantes que se encuentra presente en una organización, por esto se hace necesario que los procesos y sistemas que la gestionan a diario deban ser protegidos de amenazas que afectan la continuidad del negocio; para ello se debe establecer unos procedimientos adecuados que permitan la continuidad de las actividades del CEDIT.

Este documento se presenta como una serie de recomendaciones, que orientan la implementación de un Plan de Continuidad del Negocio que determina las acciones a tomar en caso de una contingencia.

TABLA DE CONTENIDO

pág.

INTRODUCCIÓN 17

1. PLAN DE CONTINUIDAD PARA EL CENTRO DE DESARROLLO E INNOVACIÓN TECNOLÓGICA DE LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA. 18
1.1 PLANTEAMIENTO DEL PROBLEMA 18
1.2 FORMULACIÓN DEL PROBLEMA 20
1.3 OBJETIVOS 20
1.3.1 Objetivo general 20
1.3.2 Objetivos específicos 20
1.4 JUSTIFICACIÓN 20
1.5 HIPÓTESIS 21
1.6 DELIMITACIONES 21
1.6.1 Geográficas 21
1.6.2 Temporales 21
1.6.3 Conceptuales 21

2. MARCO REFERENCIAL 22
2.1 MARCO HISTÓRICO 22
2.2 MARCO CONCEPTUAL 24
2.2.1 Acceso 25
2.2.2 Ataque 25
2.2.3 Amenaza 25
2.2.4 Datos 25
2.2.5 Equipos de cómputo 25
2.2.6 Incidente 25
2.2.7 Integridad 25
2.2.8 Plan de contingencia 26
2.2.9 Privacidad 26
2.2.10 Seguridad 26
2.2.11 Sistema de Información 26
2.3 MARCO LEGAL 26
2.3.1 Constitución Política de Colombia 26
2.3.2 Ley 1289 de 2009 26
2.3.3 Resolución 1286 de 2012 – Colciencias 26
2.3.4 Acuerdo 084 de 1995 – Consejo Superior Universitario – Universidad Francisco de Paula Santander 26
2.3.5 Acta 003 de 2013 – Comité de Apoyo Académico - Universidad Francisco de Paula Santander Ocaña 26
2.3.6 Resolución 0260 de 2013 - Universidad Francisco de Paula Santander Ocaña 27

pág.

2.3.7 Ley 1341 de 2009 27

3 DISEÑO METODOLÓGICO 28
3.1 TIPO DE INVESTIGACIÓN 28
3.2 POBLACIÓN 28
3.3 MUESTRA 28
3.4 TÉCNICAS DE RECOLECCIÓN DE LA INFORMACIÓN 28

4. PRESENTACIÓN DE RESULTADOS 29
4.1 ETAPAS PARA LA ELABORACIÓN DEL PLAN DE CONTINUIDAD 29
4.2 IDENTIFICACIÓN DE LOS RIESGOS A QUE ESTÁ EXPUESTO EL CEDIT 44
4.3 ACCIONES PREVENTIVAS 46

CONCLUSIONES 50

RECOMENDACIONES 51

REFERENCIA BIBLIOGRÁFICA 52

ANEXOS 53

LISTA DE TABLAS

pág.

Tabla 1. Etapas ISO 22301 29
Tabla 2. Rol, funciones y responsabilidades 31
Tabla 3. Análisis e Impacto del negocio 44
Tabla 4. Recomendaciones 47

LISTA DE ANEXOS

pág.

Anexo A. Registro de entrevista 54
Anexo B. Encuesta 57
Anexo C. Lista de chequeo 59
Anexo D. Registro de observación 62
Anexo E. Auditoría Externa 63
Anexo F. Guía telefónica UFPS Ocaña 77
Anexo G. Informe de Auditoría Interna 79
Anexo H. Plan de Mejoramiento 81
Anexo I. Recursos materiales 83
Anexo J. Situaciones detectadas 84
Anexo K. Matriz de riesgos 85
Anexo L. Plan de continuidad del negocio para el CEDIT 87

INTRODUCCIÓN

En el mundo de hoy existen eventos tales como el terrorismo, terremotos, fallas de la tecnología, entre otros, que pueden generar interrupciones en la entrega de productos y servicios[1]. Estos generan desde hace muchos años la necesidad de establecer lineamientos para la gestión de continuidad del negocio, que permitan a las empresas seguir entregando sus productos y servicios a un nivel aceptable.

En el presente anteproyecto se abordan los conceptos más relevantes respecto de la continuidad del negocio, se realiza una breve revisión de la literatura desde sus orígenes y se describen los modelos de gestión de continuidad del negocio más recientes. Además, se presenta como delimitación objeto de estudio al Centro de Desarrollo e Innovación Tecnológica de la Universidad francisco de Paula Santander Ocaña.

El presente documento comienza por un planteamiento del problema en donde se describen los factores que llevaron a realizar dicha investigación. Luego con las herramientas dadas en el planteamiento del problema se procede a formular de manera sistemática el problema. Estando ya definida la pregunta a resolver se exponen los objetivos (general y específicos); los cuales permiten enunciar las hipótesis que posiblemente resuelvan la incógnita planteada.

Estos parámetros sirven como base para delimitar la investigación dentro de un marco geográfico, temporal y conceptual; el cual, necesariamente conlleva a un marco referencial que se construye a partir de marcos o bases históricas, conceptuales y legales. Propiciando un diseño metodológico que incluye a su vez el tipo de investigación, la población, la muestra y las técnicas necesarias para la recolección de la información. No debemos olvidar que para conseguir culminar la investigación se hace imprescindible mostrar los resultados del mismo culminando con unas conclusiones y recomendaciones.

Invitamos al lector a revisar el presente trabajo, con el propósito de que se ilustre al respecto de la investigación en curso.

[1] SHARP, John. The route map to Business Continuity Management, Meeting the requirements of BS 25999; British Standards Institution, Londres Reino Unido, 2008. p.57

1. PLAN DE CONTINUIDAD PARA EL CENTRO DE DESARROLLO E INNOVACIÓN TECNOLÓGICA DE LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

1.1 PLANTEAMIENTO DEL PROBLEMA

Desde una perspectiva global encontramos que las actividades terroristas, los climas extremos, la falla de las herramientas, la interrupción en la cadena de suministro y las pandemias son ejemplos de grandes eventos que pueden derivar en interrupciones y falla de las organizaciones que entregan productos y servicios. Los terremotos, las erupciones volcánicas y las huelgas industriales, son sólo algunos de los incidentes que han llevado a una mayor sensibilización de las empresas sobre lo que significa la continuidad en toda América[2].

Como consecuencia de ello aparecieron los sitios de recuperación de desastres en EE.UU. a finales de los 70's y el concepto de Planeamiento de Recuperación de Desastres (Disaster Recovery Planning- DRP)[3]. El primer uso conocido del término "Continuidad del Negocio" fue hecho por Ron Ginn en 1986, después de haber investigado el tema en los EE.UU. y de haber entrevistado a muchos destacados profesionales. Él escribió un libro titulado "Planificación de la Continuidad", que sugiere la aplicación de un conjunto de habilidades de DRP a un rango más amplio de riesgos de negocio e interrupciones operativas potenciales. Uno de los problemas iníciales fue la dificultad de convencer a la Alta Dirección de la justificación para hacer una importante inversión en algo que probablemente nunca iba a suceder. Esto llevó al concepto de Análisis de Impacto en el Negocio (BIA) para añadir más atención a los procesos de negocio. En 1994 se fundó el BCI, como un grupo de trabajo encargado de definir el conjunto de habilidades para medir y juzgar la capacidad de aquellos que buscaban el reconocimiento como profesionales de continuidad del negocio.[3] En el 2003 el British Standard Institute (BSI) publicó la Guía para la Gestión de Continuidad del Negocio PAS56, que muestra las mejores prácticas en gestión de continuidad del negocio y que fue adoptado por muchas organizaciones alrededor del mundo. En el 2006 PAS56 fue remplazada por el estándar británico BS 25999-1: Código de Prácticas, donde se establece el modelo para la gestión de continuidad del negocio; y en 2007 el BSI publicó la especificación para que las organizaciones puedan certificarse, llamada BS 25999- 2.[4]

En algunos países se están implementando normas específicas sobre la gestión de la continuidad del negocio, como es el caso del Perú, en el cual la Superintendencia de Banca, Seguros y Asociación de Fondo de Pensiones (SBS), mediante Circular N° G-139-2009,

[2] BIRD, Larry. Good Practice Guidelines A Management Guide to Implementing Global Good Practice in Business Continuity Management, Business Continuity Institute, Berkshire Reino Unido, 2010. p.12
[3] Ibid. p. 121
[4] Ibid. p.122

aprueba las normas sobre gestión de la continuidad del negocio de manera obligatoria para las empresas del sector financiero[5].

Respecto de la gestión de continuidad del negocio se han desarrollado modelos derivados del estándar BS 25999, tales como el Modelo de Buenas Prácticas de implementación de Sharp, y el modelo para la implementación de prácticas globales de Gestión de Continuidad del Negocio. Asimismo se han generado aquellos modelos orientados a un tipo de respuesta específico como el NIST1800-34 Planeamiento de Contingencia para Sistemas de Información Federales para la recuperación de desastres, el NFPA2 1600 Gestión de Emergencias y Desastres y Programas de Continuidad del Negocio para la gestión de emergencias, el Modelo para el Planeamiento de Gestión de Crisis e Incidentes, o el Modelo de Madurez de Continuidad del Negocio. En mayo de este año el estándar británico ha sido actualizado a través del estándar ISO 22301 Sociedad de Seguridad – Requerimientos para un Sistema de Gestión de Continuidad del Negocio, el cual brinda un mayor énfasis en la definición de los objetivos, el seguimiento, el rendimiento y la métrica; más claras expectativas sobre la gestión, y mejor y más cuidadosa planificación y preparación de los recursos necesarios para garantizar la continuidad del negocio.[6]

Debido a que existen varios esfuerzos orientados a establecer un modelo para la gestión de la continuidad del negocio desde diferentes aspectos (organizacional, tecnológico, crisis, incidentes, emergencia) y que todos ellos son relevantes para las realidades en las cuales fueron creadas y han sido aplicadas (Reino Unido, EE.UU.), se hace necesario realizar la revisión detallada de dichos modelos y establecer sus puntos de convergencia y divergencia, así como las fortalezas de cada uno.

Esto con el propósito de llegar a nuestro punto álgido que exige una revisión además del entorno local específico denominado Universidad Francisco de Paula Santander Ocaña; el cual presenta en su Plan de Contingencia de TI acorde con su misión; pos procedimientos relevantes con relación a protocolos y políticas de seguridad, backup, lineamientos para el desarrollo y actualización de los sistemas de información que son vitales para orientar las acciones ante una contingencia a la infraestructura informática en la Universidad Francisco de Paula Santander Ocaña[7]. Que plantea que se entenderá como infraestructura informática al hardware, software y elementos complementarios que soportan la información o datos críticos para la función de los procesos misionales y de apoyo. Siendo el **CEDIT** un proceso misional de la Universidad Francisco de Paula Santander Ocaña.

Dadas estas pautas, debemos plantearnos el interrogante de si: ¿las medidas plasmadas en dicho Plan de Contingencia en lo referente a la FASE II - Recuperación y Restauración,

[5] SWANSON, Mike. BOWEN, Peter. WOHL PHILLIPS, Amy. Contingency Planning Guide for Federal Information Systems Special Publication 800-34 Rev. 1, National Institute of Standards and Technology NIST, EE.UU. 2010. p.56

[6] SCHMIDT, Douglas. NFPA 1600 Standard on Disaster/ Emergency Management and Business Continuity Programs‖, National Fire Protection Association, EE.UU. 2010. p.95

[7] WITTY, Robert. Preplanning for plan invocation, Continuity Magazine, ISSN 14601451, 2011. p. 19-20.

(http://www.ufpso.edu.co/ftp/doc/otrospro/sitt/L-TT-DSS-002A.pdf), determinan los pasos apropiados para garantizar la continuidad de las actividades del CEDIT? [8]

La negativa a la respuesta nos lleva a soportar el planteamiento del problema indicando que no se menciona dicha dependencia poniendo en evidencia la necesidad de elaborar un Plan de Continuidad para el Centro de Desarrollo e Innovación Tecnológica de la Universidad Francisco de Paula Santander Ocaña.

1.2 FORMULACIÓN DEL PROBLEMA

Si bien es cierto que en los últimos años la información se ha convertido en un activo muy valioso para las organizaciones y que la seguridad de la información tiene como fin la protección y de los sistemas de información en cuanto acceso, uso, divulgación, interrupción o destrucción no autorizada. Se hace necesario contar con unos lineamientos que permitan consultar que acción o acciones realizar en caso de una contingencia para garantizar la continuidad de las actividades normales de dichas organizaciones.

En razón a esto el CEDIT debe implementar una serie de estrategias para elaborar el plan de continuidad, identificando las posibles amenazas al interior y al exterior del centro que le permitan recuperar en un nivel aceptable después de una interrupción no prevista sus sistemas de información buscando minimizar el tiempo de respuesta ante la perturbación.

1.3 OBJETIVOS

1.3.1 Objetivo general. Elaborar un plan de continuidad para el Centro de Desarrollo e Innovación Tecnológica de la Universidad Francisco de Paula Santander Ocaña.

1.3.1 Objetivos específicos. Listar las etapas para la elaboración del plan de continuidad y aplicarlas al CEDIT.

Determinar los riesgos a los cuales están expuestas las operaciones que desarrolla el CEDIT

Documentar las acciones preventivas para evitar la pérdida de información ante un desastre o siniestro.

1.4 JUSTIFICACIÓN

El Centro de Desarrollo e Innovación Tecnológica de la Universidad Francisco de Paula Santander Ocaña, por su ubicación geográfica requiere establecer acciones preventivas y correctivas que garanticen que los procedimientos están debidamente custodiados para dar continuidad a su quehacer institucional, por lo que es preciso estructurar planes adecuados para que la misión, la visión, los objetivos y los requisitos del cliente se cumplan.

[8] Ibid. p. 19-20

Para desarrollar el plan de continuidad del CEDIT se requiere de una metodología que tenga buenas prácticas de gestión inmersas en las Normas Técnicas Colombiana adoptadas en la institución, las cuales deben ser congruentes con la misión, visión y con la cultura de riesgos de la Institución, además con la capacidad de operar en forma continua y minimizar las perdidas ante la ocurrencia de eventos manteniendo activo todos los procedimientos de tal forma que los servicios que ofrece el centro no se vean interrumpidos ante hechos que alteren la normalidad de las operaciones.

En relación a la anterior, las ventajas de desarrollar una metodología para desarrollar un plan de continuidad en el CEDIT son las siguientes:

Proporcionar fortalezas a la vulnerabilidad que puede ser afectado por los diferentes eventos.

Analizar los factores críticos de riesgo que pueden afectar el desarrollo de las actividades del CEDIT.

Proteger la imagen y credibilidad del CEDIT

Cumplimiento de los requisitos de las Normas Técnicas Colombianas
Integración y certificación con otros sistemas adoptados en la institución

Desarrollar resistencia a las interrupciones no planificadas para garantizar la continuidad de los requisitos de los clientes internos y externos.

1.5 HIPÓTESIS

El plan de continuidad para el Centro de Desarrollo e Innovación Tecnológica de la Universidad Francisco de Paula Santander Ocaña, ¿disminuye la posible pérdida de conectividad con el sistema central que causa la caída del mismo?, ¿cuenta con el apoyo de la Dirección?, ¿identifica los requisitos necesarios?, ¿cuenta con los documentos que respaldan el sistema de gestión?, ¿realiza la evaluación y el tratamiento de riesgos?, ¿implementa programas de capacitación y concienciación?

1.6 DELIMITACIONES

1.6.1 Geográficas. El CEDIT tiene sus oficinas geográficamente en la sede La Primavera de la UFPS Ocaña, las cuales se encuentran ubicadas en la calle 7 29-285 Avenida Francisco Fernández de contreras, Barrio La Primavera, Municipio de Ocaña - Norte de Santander – Colombia.

1.6.2 Temporales. El proyecto de investigación se desarrolló en un periodo de cuatro meses.

1.6.3 Conceptuales. La propuesta se enmarca dentro de los lineamientos de la norma ISO 22301.

2. MARCO REFERENCIAL

2.1 MARCO HISTÓRICO

El primer uso conocido del término "Continuidad del Negocio" fue hecho por Ron Ginn (posteriormente Presidente del Instituto de Continuidad del Negocio - BCI) en 1986, después de haber investigado el tema en Estados Unidos y de haber entrevistado a muchos destacados profesionales. Él escribió un libro titulado "Planificación de la Continuidad", que sugiere la aplicación de un conjunto de habilidades de DRP a un rango más amplio de riesgos de negocio e interrupciones operativas potenciales.[9]

El Concejo de Estándares NFPA, de Estados Unidos, estableció el Comité de Gestión de Desastres en enero de 1991, con la responsabilidad de desarrollar documentos relacionados a la preparación, respuesta, y recuperación de desastres resultados de eventos naturales, humanos o tecnológicos.

En 1994 se fundó en el Reino Unido el Instituto de Continuidad del Negocio, como un grupo de trabajo encargado de definir el conjunto de habilidades para medir y juzgar la capacidad de aquellos que buscaban el reconocimiento como profesionales de continuidad del negocio, las cuales se desarrollaron en un esfuerzo cooperativo con el Instituto de Recuperación de Desastres (ahora DRII).

En 1995 se realiza el lanzamiento de la Norma Británica para la Seguridad de Información BS 7799 y su posterior versión americana ISO/IEC 17799 Código de Buenas Prácticas para la Gestión de la Seguridad de la Información. Esto incluye en sus principios básicos la necesidad de la GCN, que se define en términos de disponibilidad de datos. Esto añadió más confusión al debate y dio lugar a que muchos profesionales de TI afirmaran que la GCN era simplemente un subconjunto de seguridad de la información. Ese año también se lanza el NFPA 1600 Prácticas recomendadas para la Gestión de Desastres, presentado en la Reunión Anual de los miembros en Estados Unidos[10]

Knight y Pretty de Templeton College, Oxford, realizaron una investigación en fines de los 90's que mostró que la falta de confianza en la habilidad de los directores para actuar rápida y profesionalmente en el momento de un desastre lleva a la reducción del valor de las acciones. La GCN efectiva integra la gestión de crisis/incidentes para asegurar que si un incidente mayor ocurre, la organización no está solo preparada para mantener la continuidad de sus operaciones, sino para asegurar a la comunidad que todo está bajo control.

En el 2000 el comité de NFPA incorpora en el NFPA 1600 la aproximación a la gestión de desastres/emergencias y programas de continuidad del negocio [6]. En el 2003 el BSI publicó la Especificación Disponible al Público PAS56 Guía para la Gestión de Continuidad del Negocio, que muestra las mejores prácticas en GCN, que fue adoptado por muchas organizaciones alrededor del mundo.

[9] Op.Cit.SCHMIDT. p. 96

En el 2004 el comité NFPA actualizó la terminología y el formato del NFPA 1600 de acuerdo al Manual de Estilo para los documentos técnicos del NFPA emitido en el 2003.

En el 2006 PAS56 fue remplazada por un nuevo están- dar británico para la GCN: BS 25999-1. Este es un código de prácticas para la GCN e incorpora las mejores prácticas de PAS56, las guías de GCN que soporta el Acta de Contingencias Civiles del Reino Unido del 2004 y otros recursos de todo el mundo[11].

En el 2007 el BSI publicó la segunda parte del nuevo estándar que es una especificación de GCN para las organizaciones que desean certificarse: BS 25999-2, Gestión de Continuidad del Negocio Parte 2 – Especificación. Este último se basa en el ciclo de la ISO 9000 ―Planear-Hacer-Verificar-Actuar‖, estableciéndose como el ciclo de vida de la continuidad del negocio las fases de: entendimiento de la organización, determinación de la estrategia, desarrollo e implementación de la respuesta, ejercicio, mantenimiento y revisión, y forjamiento de la cultura organizacional de continuidad del negocio. El mismo año se actualiza el NFPA 1600, identificando la prevención como un as- pecto adicional a la mitigación, preparación, respuesta y recuperación, identificado en versiones anteriores. Así mismo, reconoce la colaboración del Departamento de Seguridad interna de los Estados Unidos (DHS), IAEM3 y NEMA4.

En el 2008, John Sharp, auspiciado por el BCI, elabora un libro para la implementación de la BS 25999-2, indicando lineamientos más específicos, casos y plantillas del cómo y quiénes implementan el SGCN.

En el 2010 se lanza la actualización de la norma NFPA 1600 de Gestión de Emergencias y Desastres y Pro- gramas de Continuidad del Negocio, alineada al ciclo PDCA. El capítulo Gestión del Programa fue expandido para enfatizar la importancia del liderazgo y el compromiso, incluyendo nuevos requerimientos para definir los objetivos de desempeño y gestión de registros. Se conforman otros cuatro capítulos de Planeación, Implementación, Pruebas y Ejercicios, y Mejora del Programa. El análisis de impacto al negocio y la evaluación de riesgos ahora están separados. En el capítulo de implementación se incluye una sección de asistencia al empleado y soporte. Paralelamente, el NIST publica la Especificación Pública NIST 800-34 Rev. 1 Guía de Planificación de Contingencia para Sistemas de Información Federales, tomando en consideración los requerimientos del estándar FIPS 199 Categorización de Seguridad para Información Federal y Sistemas de Información, y de la publicación NIST 800-53 Controles de Seguridad recomendados para Sistemas de Información y Organizaciones Federales. Este estándar establece siete etapas del ciclo de vida del desarrollo del sistema de contingencias: desarrollo de la política, análisis de impacto al negocio, identificación de controles preventivos, creación de estrategias de contingencia, desarrollo de planes de contingencia, pruebas, entrenamiento y ejercicio del plan, y mantenimiento del plan.

[11] BAIN, George. UK Cabinet Office, Emergency Preparedness, Guidance on Part 1of the Civil Contingences Act 2004, HM Government, Londres – Reino Unido, 2005. p.114

En el 2011 la empresa Virtual Corporation publica la segunda versión del Modelo de Madurez de Continuidad del Negocio, publicado originalmente en 2003 para dirigir a la organización a que sean capaces de evaluar y mejorar su programa de continuidad del negocio, como un mecanismo de medición de la efectividad del mismo. Ese mismo año Roberta Witty establece los componentes principales de un programa efectivo de gestión de crisis e incidentes, los cuales son: marco de referencia, equipo de gestión de crisis/incidentes, centro de operaciones de comando/emergencia, software de GCN, y ejercitación de los procedimientos de gestión de crisis.[12]

En mayo de este año se publica la norma ISO/IEC 22301 Sociedad de Seguridad – Sistema de Gestión de Continuidad del Negocio – Requerimientos, en reemplazo de la BS 25999-2, que manteniendo el ciclo de vida del SGCN y alineado al modelo PDCA establece nuevas consideraciones y mejoras respecto a su predecesor. Esta norma es certificable. Finalmente como complemento, John Sharp actualiza su libro de Mapa de Ruta, alineado en esta oportunidad a la ISO 22301.

2.2 MARCO CONCEPTUAL

La literatura que se considera pertinente para determinar aspectos claves para la elaboración de un plan de continuidad para el CEDIT de la UFPS Ocaña tienen como base teórica temas de investigación expuestos por algunos Autores del Proyecto como:

Toigo (1989), que manifiesta que el termino desastre significa la interrupción del negocio debido a la pérdida o incapacidad de acceso a los activos que contienen la información requeridos para la operación normal los cuales pueden ser causados por fenómenos naturales o inducida por el factor humano. Los cuales pueden impactar en la organización teniendo un efecto negativo sobre los objetivos de la misma.

Además, Gaspar (2004) quien menciona que el Plan debe ser fiel reflejo de la organización y esta es un organismo vivo que evoluciona para responder a las necesidades del entorno. Por ello. El Plan debe mantenerse vivo mediante un programa adecuado de actualizaciones.

Según, (Business Continuity Plan –BCP), la planificación de la continuidad del negocio, es el proceso mediante el cual las instituciones de servicios y financieras se aseguran de mantener o recuperar sus operaciones, incluyendo servicios al cliente, cuando confrontan eventos adversos tales como desastres naturales, fallas tecnológicas, errores humanos o terrorismo.

Siguiendo este orden, iniciaremos con el Análisis de Impacto en el Negocio, respetando el nivel de apetito al riesgo. De esta forma se pueden definir los requerimientos de recursos y la estructura para responder a incidentes.

[12] EVANS, Donald. International Organization for Standardization, ISO 22301:2012 Societal Security Business Continuity management systems Requirements, Primera Edición, Suiza, 2012. p.78.

El resultado de estos análisis deben quedar plasmados en el Plan de Continuidad del Negocio (**BCP, Business Continuity Planning**), uno de los requisitos documentales fundamentales de la ISO 22301:2012, debe contemplar las acciones que la organización debe seguir para recuperar y restaurar las actividades críticas del negocio en un tiempo prudencial y de manera progresiva regresar a la normalidad; garantizando en todo momento la integridad, confidencialidad y disponibilidad de la información.

Lo más importante dentro de la gestión de la continuidad del negocio es que los planes de continuidad sean probados. De nada sirve tener todo documentado, definidos los responsables, contar con la tecnología de respaldo si no se hacen pruebas para determinar que las actividades definidas para responder ante una emergencia son las adecuadas para la organización. Si bien el estándar es único, la forma en que se desarrolla y se aplica es única y debe estar en concordancia con los procesos más críticos del negocio.

Estos conceptos tomados del Plan de Contingencia para la División de sistemas de la UFPS Ocaña son:

2.2.1 Acceso. Es la recuperación o grabación de datos que han sido almacenados en un sistema de computación.

2.2.2 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 un computador.

2.2.3 Amenaza. Cualquier agente que pueda interferir con el funcionamiento adecuado de un computador o causar la difusión no autorizada de información confiada en un servidor.

2.2.4 Datos. Los datos son hechos y cifras que al ser procesados constituyen una información, sin embargo, muchas veces datos e información se utilizan como sinónimos. En su forma más amplia los datos pueden ser cualquier forma de información: campos de datos, registros, archivos y bases de datos, texto, hojas de cálculo, imágenes, vídeo, etc.

2.2.5 Equipos de cómputo. Elementos o dispositivos de hardware, software, redes y telecomunicaciones interconectados que son utilizados para lleva a cabo las actividades operativas sistematizadas de la Institución.

2.2.6 Incidente. Cuando se produce un ataque o se materializa una amenaza, como por ejemplo las fallas de suministro eléctrico o un intento de borrado de un archivo protegido.

2.2.7 Integridad. Se refiere a que los valores de los datos se mantengan tal como fueron puestos intencionalmente en un sistema. Las técnicas de integridad sirven para prevenir que existan valores errados en los datos provocados por el software de la base de datos, por fallas de programas, del sistema, hardware o errores humanos.

2.2.8 Plan de contingencia. Estrategia planificada con una serie de procedimientos que faciliten u orienten a tener una solución alternativa que permita restituir rápidamente los servicios de la Institución ante la eventualidad de todo lo que la pueda paralizar, ya sea de forma parcial o total.

2.2.9 Privacidad. Se define como el derecho que tienen los individuos y organizaciones para determinar, ellos mismos, a quién, cuándo y qué información referente a ellos serán difundidos o transmitidos a otros.

2.2.10 Seguridad. Se refiere a las medidas tomadas con la finalidad de preservar los datos o información que en forma no autorizada, sea accidental o intencionalmente, puedan ser modificados, destruidos o simplemente divulgados.

2.2.11 Sistema de Información. Organización sistemática para almacenar los datos de una organización y ponerlos a disposición de su personal. Los sistemas están estrechamente relacionados entre usuarios, equipos y rutinas o procedimientos automatizados; estos elementos son necesarios entre sí, por lo tanto es imprescindible tomar medidas que permitan una continuidad en la operatividad de los sistemas para no ver afectados los objetivos y no perder la inversión de costos y tiempo.

2.3 MARCO LEGAL

2.3.1 Constitución Política de Colombia. El Estado creará incentivos para personas e instituciones que desarrollen y fomenten la ciencia y la tecnología y las demás manifestaciones culturales y ofrecerá estímulos especiales[13].

2.3.2 Ley 1289 de 2009. Por la cual se modifica la Ley 29de 1990, se transforma a Colciencias[14].

2.3.3 Resolución 1286 de 2012 - Colciencias. Por la cual se deroga la Resolución 504de 2010 y se establecen definiciones y requisitos para el reconocimiento de los Centros de Investigación o Desarrollo Tecnológico[15].

2.3.4 Acuerdo 084 de 1995 – Consejo Superior Universitario – Universidad Francisco de Paula Santander. Se aprueba la estructura orgánica de la Universidad Francisco de Paula Santander Ocaña.[16].

2.3.5 Acta 003 de 2013 – Comité de Apoyo Académico - Universidad Francisco de Paula Santander Ocaña. Estructura de la División de Investigación y Extensión.[17].

[13] Constitución Política de Colombia, 1991.
[14] Ley 1289 de 2009.
[15] Resolución 1286 de 2012 - Colciencias.
[16] Acuerdo 084 de 1995, Consejo Superior Universitario – Universidad Francisco de Paula Santander.
[17] Acta 003 de 2013, Comité de Apoyo Académico - Universidad Francisco de Paula Santander Ocaña

2.3.6 Resolución 0260 de 2013 - Universidad Francisco de Paula Santander Ocaña. Creación del CEDIT[18].

2.3.7 Ley 1341 de 2009. Por la cual se define 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[19].

[18] Resolución 0260 de 2013 - Universidad Francisco de Paula Santander Ocaña
[19] Ley 1341 de 2009

3. DISEÑO METODOLÓGICO

3.1 TIPO DE INVESTIGACIÓN

El presente estudio se encamina dentro del tipo de investigación descriptiva con enfoque cuantitativo. Como también se encuentra dentro del marco de la Investigación Aplicada, dado que utiliza los conocimientos obtenidos en las investigaciones en la práctica, y con ello traer beneficios a la entidad.

3.2 POBLACIÓN

La población objeto de investigación se tomó como tal los funcionarios pertenecientes al CEDIT cuantificados en 15 personas.

3.3 MUESTRA

Por tratarse de una población finita y medible se trabajó con el 100% de la misma.

3.4 TÉCNICAS DE RECOLECCIÓN DE LA INFORMACIÓN

Las técnicas de recolección de la información han sido seleccionadas con el propósito de reunir los datos necesarios para poder cumplir los objetivos trazados en el presente estudio. Estas son: entrevistas (Ver Anexo A. Registro de entrevista), encuestas (Ver Anexo B. Encuesta), lista de chequeo (Ver Anexo C. Lista de chequeo), y observación directa (Ver Anexo D. Registro de observación). Todas enmarcadas dentro de un plan de auditoría sistemático y ordenado. (Ver Anexo E. Auditoría Externa).

4. PRESENTACIÓN DE RESULTADOS

Para realizar el Plan de Continuidad para el CEDIT de la UFPS Ocaña, se hace necesario realizar una revisión documental basada en:

Norma ISO 22301

Plan de Contingencia – División de sistemas – UFPS Ocaña.

Auditoria externa aplicada al CEDIT por los responsables del proyecto (Ver Anexo E. Auditoría externa).

Auditoria interna realizada al CEDIT por Control Interno de la UFPS Ocaña (Ver Anexo G. Informe de auditoría interna).

Plan de mejoramiento (Ver Anexo H. Plan de mejoramiento).

Después de revisada la documentación se encuentra que las etapas para la elaboración del respectivo Plan de Continuidad para el CEDIT de la UFPS Ocaña, se describe a continuación:

4.1 ETAPAS PARA LA ELABORACIÓN DEL PLAN DE CONTINUIDAD

Las etapas para la elaboración del plan de continuidad, según la ISO 22301 son:

Tabla 1. Etapas ISO 22301

ETAPA	DESCRIPCIÓN
a	Objeto, ámbito de aplicación y usuarios
b	Documentos de referencia
c	Supuestos
d	Funciones y responsabilidades
e	Contactos clave
f	Plan de activación y desactivación
g	Comunicación
h	Respuesta a incidentes
i	Sitios físicos y transporte
j	Orden de recuperación para las actividades
k	Los planes de recuperación para las actividades
l	Plan de recuperación de desastres
m	Recursos necesarios
n	La restauración y la reanudación de las actividades de medidas temporales

Fuente: Autores del Proyecto

ETAPA a. OBJETO, ÁMBITO DE APLICACIÓN Y USUARIOS

Por qué se desarrolla este plan, sus objetivos, a que partes de la organización se aplica, y quienes deberían leerlo.

El Plan de continuidad del negocio se desarrolla porque permite establecer las actividades que el CEDIT debe seguir, en caso de que la UFPS Ocaña, ante una contingencia, active su Plan de Contingencia, además de: Garantizar la seguridad de la información, Identificar los documentos esenciales para darles prioridad ante una emergencia, Ayudar a evacuar los documentos para evitarles algún tipo de daño, y Coordinar actividades tendientes a la atención de una emergencia.

ESTAPA b. DOCUMENTOS DE REFERENCIA

¿Qué documentos se relacionan en este plan? Normalmente, se trata de la Política de Continuidad de Negocios, Análisis de Impacto de Negocios, Estrategia de Continuidad de Negocio, etc.

Los documentos que se relacionan para el plan de continuidad se basan en el Sistema Integrado de Gestión, que es una filosofía adoptada por la Universidad Francisco de Paula Santander Ocaña para dirigir y evaluar el desempeño institucional orientado al mejoramiento de los productos y/o servicios que se ofrecen al estudiante y a la sociedad. El cual se encuentra debidamente documentado para consulta y de fácil acceso a través del portal web http://www.ufpso.edu.co/sig/. Estos documentos son: Guía para la administración del riesgo, y Plan de contingencia de TI - División de Sistemas.

ETAPA c. SUPUESTOS

Los requisitos previos que deben existir para que este plan sea eficaz.

Los requisitos previos que deben existir para que el Plan de continuidad del Negocio para el CEDIT sea eficaz son: Apoyo de la alta dirección de la **UFPS Ocaña**, existencia del plan de contingencia, reservas financieras, socialización previa del Plan de Continuidad para distribuir funciones y responsabilidades, establecer y mantener comunicación con contactos clave.

ETAPA d. FUNCIONES Y RESPONSABILIDADES

¿Quiénes serán responsables de la gestión del incidente perturbador?, y ¿quién está autorizado para realizar ciertas actividades en caso de un incidente perjudicial?

Los responsables de la gestión del incidente en el CEDIT, basados en el Plan de Contingencia de la División de sistemas de la UFPS Ocaña, se establecen como un equipo de trabajo con las funciones y responsabilidades que deberán ejecutar en caso de presentarse una eventualidad identificada. Es importante tener en cuenta, que los roles pueden ser asumidos

por una o más personas de acuerdo al grado de conocimiento y responsabilidad. Estos son: Responsable de la ejecución del Plan, Coordinador de Servidores, Coordinador de Redes y Comunicaciones, Coordinador de Soporte Técnico, Coordinador de Sistemas, y Personal Clave.

Estos a su vez asumen sus roles así:

Tabla 2. Rol, funciones y responsabilidades.

ROL	FUNCIONES Y RESPONSABILIDADES
Responsable de la ejecución del Plan de Contingencia – Director Dependencia	Es el responsable de aprobar la realización del Plan, dirigir los comunicados de concientización y solicitud de apoyo a los jefes y/o directivos de las diferentes áreas involucradas. Una vez concluida la realización del Plan, el Responsable tendrá como función principal, verificar que se realicen reuniones periódicas, cuando menos cada seis meses, en donde se informe de los posibles cambios que se deban efectuar al plan original y de que se efectúen pruebas del correcto funcionamiento, cuando menos dos veces al año o antes si se presentan circunstancias de cambio que así lo ameriten. Al declararse una contingencia, deberá tomar las decisiones correspondientes a la definición de las ubicaciones para instalar los equipos de cómputo alternos y comunicará a las directivas los costos para los gastos necesarios y el cronograma para la restauración del ambiente de trabajo.
Coordinador de Servidores	Tendrá como función principal asegurar que se lleven a cabo todas las fases para la realización del Plan, registrará las reuniones que se realicen y mantendrá actualizadas las bitácoras de monitoreo a servidores. Durante la realización del plan, una de sus actividades principales será la coordinación de la realización de las pruebas de los equipos de cómputo alternos, la restauración de datos e instalación de BD. Una vez que se encuentre aprobado el Plan, será el Coordinador General quien lleve a cabo formalmente la declaración de una contingencia grave y de inicio formal de la aplicación del Plan, cuando así lo considere conveniente, propiciando que la contingencia desaparezca con el objeto de continuar normalmente con las actividades; será el responsable de dar por concluida la declaración de contingencia. En conjunto con el responsable del Plan llevarán a cabo la toma de decisiones.
Coordinador de Redes y Comunicaciones	Es el responsable de determinar los procedimientos a seguir en caso de que se presente una contingencia que afecte las comunicaciones, servicios de internet, intranet, correo electrónico y red, mantener actualizados dichos procedimientos en el Plan,

	determinar los requerimientos mínimos necesarios, tanto de equipo como de software, servicios, líneas telefónicas, cuentas de acceso a Internet, enlaces dedicados, dispositivos de comunicación (ruteadores, switchs, antenas etc). Asimismo, deberá mantener actualizado el inventario de equipo de telecomunicaciones y redes, efectuar los respaldos correspondientes y llevar a cabo las pruebas de operatividad necesarias, para asegurar la continuidad del servicio, en caso de que se llegara a presentar alguna contingencia, ya sea parcial, grave o crítica. El coordinador de comunicaciones es el responsable de mantener el directorio de contactos, proveedores y usuarios de los servicios antes descritos y mantenerlo permanentemente actualizado e incluirlo dentro del Plan. Deberá realizar los procedimientos correspondientes para la emisión de los respaldos de cada uno de los servidores o equipos críticos y asegurar la actualización de datos. Coordinará las actividades correspondientes a los servicios de comunicaciones al declararse una contingencia, hasta su restablecimiento total.
Coordinador de Soporte Técnico	Es el responsable de llevar a cabo el inventario de equipo, software y equipos periféricos, como impresoras, escáneres, fotocopiadoras, etc.; mantener los equipos en óptimas condiciones de funcionamiento; determinar la cantidad mínima necesaria de equipo y sus características para dar continuidad a las operaciones de la Institución; es responsable de elaborar o coordinar con los usuarios los respaldos de información. Efectuar y mantener actualizado el directorio de proveedores de equipos, garantías, servicio de mantenimiento y reparaciones, suministros, en su caso, e incluirlo dentro del Plan. En caso de que se declare alguna contingencia que afecte a los equipos y al software, sea cual fuere su grado de afectación, es el responsable de restablecer el servicio a la brevedad, con el objeto de que no se agrave el daño o se llegara a tener consecuencias mayores. Para tal efecto debe participar en pruebas del Plan en conjunto con los demás participantes, con el objeto de estar permanentemente preparado para actuar en caso de contingencia.
Coordinador de Sistemas	Será el responsable de determinar los sistemas de información, módulos y procedimientos críticos de la Institución, que en caso de presentarse alguna contingencia como corte de energía eléctrica prolongada, temblor, incendio, falla del sistema de cómputo, pérdida de documentación, o alguna otra causa determinada, se llegara a afectar sensiblemente la continuidad de

	las operaciones en las áreas que utilicen dichos sistemas. En caso de cambiar a otras instalaciones alternas, el Coordinador de sistemas deberá definir cuáles serían las actividades que se deberán seguir para la configuración o instalación de los sistemas desarrollados, optimizando los recursos con los que se cuente, realizando las pruebas necesarias hasta su correcto funcionamiento en las terminales destinadas para su operación. Deberá mantener actualizados los Manuales de Usuario, resguardándolos fuera de las instalaciones para su consulta y utilización al momento de requerirse.
Personal clave	Es el responsable de la aplicación de los procedimientos, instructivos y actividades que describa el Plan para cada una de las diferentes circunstancias o contingencias previstas y de reportar con la periodicidad que se indique en el plan, al Coordinador de su área y al jefe de la división, los resultados de la aplicación de alguna de las fases del plan. Coordinarán con el personal de la Institución involucrado, la realización de las actividades contenidas en el Plan para la situación que se hubiera presentado y tratar por todos los medios que les sea posible el logro de los objetivos y asegurar la continuidad de las operaciones, disminuyendo el impacto de la contingencia al mínimo. Darán aviso al Coordinador de su área, cuando a su juicio, las circunstancias que provocaron la activación del plan hubieran desaparecido y se estuviera en condiciones de continuar normalmente con las actividades. En caso de requerir de actividades complementarias para regresar a las actividades normales, especialmente cuando se trate de los sistemas de información, deberán incluir el plan de actividades que se deberá seguir para retornar a la situación normal, prestar el apoyo técnico, operativo y toda la colaboración necesaria.
Usuarios (funcionarios) de la UFPS Ocaña	El personal usuario en general, al verse afectado por una situación de contingencia, deberá en primera instancia apoyar para salvaguardar las vidas propias y de sus compañeros de trabajo, cuando la situación que se estuviera presentado sea grave (incendio, temblor, etc.); posteriormente, y en la medida en que la situación lo permita, deberá coadyuvar a salvaguardar los bienes de la Universidad (el propio inmueble, equipos, documentación importante, etc.). Con posterioridad a la crisis inicial, deberá apoyar a solicitud del Coordinador de su área y/o del personal clave del Plan, en la toma del inventario de daños, para lo cual deberá seguir las instrucciones generales que se indiquen.

	En forma alterna, deberá dar cumplimiento a las instrucciones que se incluyan en el Plan para darle continuidad a las funciones informáticas críticas, siguiendo los procedimientos establecido, con la salvedad de que deberá, en forma creativa y responsable, adaptarlos a las circunstancias de limitación que represente el cambio de ubicación de las diferentes áreas involucradas en los procesos y la utilización de recursos de cómputo, mensajería, comunicaciones, etc., limitados. Al declararse concluida la contingencia, deberá participar activamente en la restauración de las actividades normales, esto es, apoyar en la movilización de documentación, mobiliario, etc., a las instalaciones originales o al lugar que le sea indicado, hasta la estabilización de las actividades. Cuando sea necesario, deberá participar en la capacitación del personal eventual que hubiera sido necesario.

Fuente: Plan de Contingencia – División de Sistemas – UFPS Ocaña

ETAPA e. CONTACTOS CLAVE

Datos de contacto de las personas que participarán en la ejecución del plan de continuidad del negocio.

Los datos de contacto de las personas que participarán en la ejecución del plan de continuidad del negocio para el CEDIT son en primera instancia el directorio de la UFPS Ocaña (Ver Anexo F. Guía telefónica UFPS Ocaña), y por otra parte los números de las autoridades y entidades de emergencias tales como: Policía Nacional (5611128), Hospital (5611940), Bomberos (119 – 5611002), Defensa Civil, Cruz Roja, Ejercito Nacional; entre otras.

ETPA f. PLAN DE ACTIVACIÓN Y DESACTIVACIÓN

¿En qué casos se pueden activar el plan, y el método de activación?; ¿qué condiciones deben existir para desactivar el plan?

Para activar el Plan de continuidad del negocio del **CEDIT** en necesario detectar una situación que represente un riesgo, dentro de los riesgos descritos en el numeral 4.2 del presente capitulo.

De igual manera es responsabilidad de todos los miembros de la organización (Personal Clave) informar el momento en el cual a su juicio las circunstancias que provocaron la activación del plan hubieran desaparecido y se estuviera en condiciones de continuar normalmente con las actividades. Después de evaluar la situación, el Director del CEDIT debe decidir si se puede desactivar el Plan.

ETAPA g. COMUNICACIÓN

¿Qué medios de comunicación se utilizarán entre los diferentes equipos y con otras partes interesadas durante el incidente perturbador?, ¿Quién está a cargo de la comunicación con cada parte interesada?, y las normas especiales de comunicación con los medios de comunicación y agencias de gobierno.

Los medios de comunicación utilizados por el CEDIT, durante el incidente perturbador, entre los miembros de la organización y los entes externos son: primero la comunicación directa, segundo el servicio de chat institucional, tercero el correo institucional, cuarto el servicio telefónico, quinto los servicios de telefonía celular, sexto portal web, séptimo la correspondencia escrita, octavo el servicio de mensajero.

Para cada caso, los responsables son todos los miembros de la organización dentro de su rol.

ETAPA h. RESPUESTA A INCIDENTES

¿Cómo reaccionar inicialmente a un incidente con el fin de reducir el daño?

En todas las situaciones de emergencia hay que controlar el pánico. Dada una situación de emergencia, la prioridad es asegurar la seguridad de las personas y alertar a las entidades pertinentes (Bomberos, Defensa Civil, Policía, etc.).

De ser posible hay que localizar el origen del siniestro y tratar de neutralizarlo sin tomar riesgos que puedan atentar contra la vida, esto se puede lograr a través del correcto uso de extintores, la suspensión de las redes de agua, de electricidad y de datos entre otros. Una vez controlada la situación, se procederá a determinar la magnitud de los daños.
Los incidentes identificados en el CEDIT se especifican en los siguientes grupos: Movimiento Telúrico, Incendio, Inundación y Humedad, Corte de Energía, Fallas en la red de Voz y Datos, Fallas en Hardware o Software, Sabotaje o Daño Accidental, Vandalismo, y Paro o Manifestaciones. Estas situaciones se describen a continuación:

MOVIMIENTO TELÚRICO.

Sin pérdida o daños menores del edificio: El siniestro puede afectar únicamente parte de la estructura del edificio, en cuyo caso no se verían afectados los datos, sin embargo, podría ser necesario evacuar las instalaciones trasladando al personal fuera del edificio; el impacto que provocaría sería menor, puesto que las actividades se interrumpirían por unas horas o a hasta por un día completo.

Con pérdida del edificio: La pérdida de las instalaciones afectaría gravemente a las operaciones de la Sede y los datos pueden verse dañados seriamente. En esta parte de la contingencia es donde se requiere que todas las medidas de emergencia y de recuperación funcionen adecuada y oportunamente.

INCENDIO.

Área de sistemas: Se tiene gran impacto en la información ya que los sistemas utilizados residen en los Servidores y dispositivos de comunicación localizados en la División y en caso de sufrir algún daño, se requerirá adquirir nuevos equipos, así como de instalar nuevamente los sistemas, configurar los servidores y restaurar los respaldos para continuar trabajando.

Áreas distintas al sitio de cómputo: Un incendio dependiendo de su magnitud, puede afectar desde las estaciones de trabajo o periféricos y dispositivos de comunicación (racks) localizados en las áreas administrativas. En el caso de las primeras el impacto que tendría es medio alto, puesto que la información o tiempo de operación que se pierde no tiene gran repercusión en las operaciones generales, ya que puede restablecerse en un tiempo relativamente corto, pero en el caso de las comunicaciones si pueden afectar en gran medida la operación del servicio.

INUNDACIÓN Y HUMEDAD.

Puesto que es equipo electrónico el que se maneja dentro de la institución, una inundación severa dañaría los dispositivos irremediablemente deteniendo las operaciones de la misma totalmente.

Un daño grave correspondería a una inundación en la División de Sistemas, en tanto que una inundación parcial o limitada a parte de las instalaciones (no al Centro de Cómputo) podría sólo ocasionar un daño medio sí no va seguido de corto circuito. Por otro lado, teniendo en cuenta el datacenter la recuperación de los datos sería relativamente rápido aunque no sería lo mismo para los equipos servidores.

CORTE DE ENERGÍA

Las operaciones informáticas se detendrían, puesto que los dispositivos en los que se trabaja dependen de la corriente eléctrica para su desempeño. Si el corte eléctrico dura poco tiempo las operaciones no se ven afectadas gravemente, pero si el corte se prolongara por tiempo indefinido se provocaría un trastorno en las operaciones del día, sin afectar los datos. Actualmente no se cuenta con una planta eléctrica, de manera que la capacidad de restablecer la energía inmediatamente después de la perdida de luz es nula.

Los equipos servidores cuentan con una UPs, para entrar inmediatamente después del corte de energía y evitar daños en los equipos.

FALLAS EN LA RED DE VOZ Y DATOS.

Red: Representa la columna vertebral de las operaciones, si la red falla en su totalidad, las operaciones se detienen con la consecuente falta del servicio informático.

Aplicaciones: La falla en los sistemas utilizados, representa un impacto medio en las operaciones totales, ya que pueden ser reinstalados casi de inmediato.

FALLAS EN HARDWARE O SOFTWARE

Las alteraciones que sufran los servidores tanto en Hardware y Software pueden ser corregidas en la mayoría de los casos, sin embargo si las alteraciones llegan a ser tan grandes que el tiempo requerido para el inicio de las operaciones normales puede extenderse hasta por días.

Sabotaje o Daño Accidental.

La alteración de la información requiere de la restauración de los respaldos y de pruebas posteriores para contar con la integridad de los datos. Es posible que se requieran re procesos de captura de datos, dependiendo de las fechas de los respaldos que se tengan disponibles y del volumen de transacciones realizadas manualmente.

Vandalismo, Paro o Manifestaciones.

Un intento de vandalismo ya sea menor o mayor, podría afectar a las PC's, periféricos y servidores así como las comunicaciones. Si el intento de vandalismo es mayor, se presenta un grave riesgo dentro del área de la División ya que puede dañar los dispositivos y por consecuencia las actividades se verían afectadas en su totalidad, así como el servicio proporcionado.

ETAPA i. SITIOS FÍSICOS Y TRANSPORTE

Son los sitios primarios y alternativos, en los puntos de concentración, y cómo llegar de los primarios a sitios alternativos.

Para el CEDIT los sitios primarios se encuentran situados en el parqueadero de la sede La Primavera, mientras que los alternos para continuar las labores de forma normal, son las sedes de la UFPS Ocaña; las cuales se describen así:

Sede Principal. Vía Acolsure, Sede el Algodonal - Ocaña Norte de Santander.
Sede Bellas Artes. Calle 10 # 13-64, Centro - Ocaña Norte de Santander.

Sede La Primavera. Calle 7 # 29-235, Piso 1 Avenida Francisco Fernández de contreras, Ocaña Norte de Santander.

En cuanto al transporte, se debe contar con los recursos necesarios y los contactos para la respectiva contratación de los medios de transporte para trasladar los equipos necesarios para dar continuidad a las actividades del **CEDIT**. Se estipula un 10% del salario mínimo como valor de referencia a cancelar por recorrido. El valor del transporte depende de los materiales a transportar y ello se deriva del incidente a resolver.

ETAPA j. ORDEN DE RECUPERACIÓN PARA LAS ACTIVIDADES

Lista de todas las actividades, con precisión Objetivo de Tiempo de Recuperación (RTO) para cada uno.

Las actividades de recuperación para el **CEDIT** de la **UFPS Ocaña**, se encuentran descritas en las acciones a tomar en caso de presentarse una situación de riesgo y se describe en el numeral 4.2 del presente capitulo, al igual que la descripción, causa y consecuencia.

ETAPA k. LOS PLANES DE RECUPERACIÓN PARA LAS ACTIVIDADES

Descripción del paso a paso de las acciones y responsabilidades de mano de obra en recuperación, instalaciones, infraestructura, software, información y procesos, incluyendo las interdependencias e interacciones con otras actividades y partes interesadas externas.

Los planes de recuperación para las actividades del CEDIT se describen como:

Valoración de las necesidades materiales y recursos económicos necesarios para efectuar el plan de recuperación.

Organización de brigadas de trabajo, operaciones de salvaguarda.

Preparación de un informe describiendo los sucesos acontecidos, costos y requerimientos.

Es importante anexar evidencias de los documentos e instalaciones afectadas. Estos datos serán necesarios para el expediente de la aseguradora en el caso de que exista un seguro.

Adecuación de espacios para el almacenamiento de la documentación afectada y para adelantar acciones de recuperación y descarte.

Elección de los métodos de tratamiento de la documentación de acuerdo al tipo de daño y tipo de documentos a tratar.

ETAPA l. PLAN DE RECUPERACIÓN DE DESASTRES

Esto es normalmente un tipo de plan de recuperación que se centra en la recuperación de la infraestructura de tecnología de la información y la comunicación.
Para el Plan de recuperación de desastres se hacen relevantes aspectos como: Seguridad Física y Seguridad Lógica. Estas se describen a continuación:

SEGURIDAD FÍSICA

Garantiza la integridad de los activos lógicos y materiales de un sistema de información y de su infraestructura. Desde el edificio en donde se encuentran ubicados los dispositivos el

enfoque debe ser a cubrir las amenazas ocasionadas tanto por el hombre como por la naturaleza del medio físico del entorno.

El nivel adecuado de seguridad física, o grado de seguridad, es un conjunto de acciones utilizadas para evitar el fallo o para aminorar las consecuencias que de él se puedan derivar. Algunos aspectos a considerar son: Ubicación del Centro de Procesamiento de Datos dentro del edificio, Potencia eléctrica, Sistemas contra Incendios, Control de accesos, Selección de personal, Medidas de protección.

Las principales amenazas que se prevén en la seguridad física son: 1. Desastres naturales, incendios accidentales e inundaciones, 2. Amenazas ocasionadas por el hombre, 3. Disturbios, sabotajes internos y externos deliberados.

A continuación se analizan los peligros más importantes que se corren en un centro de procesamiento; con el objetivo de mantener una serie de acciones a seguir en forma eficaz y oportuna para la prevención, reducción, recuperación y corrección de los diferentes tipos de riesgos.

Incendios. Los incendios son causados por el uso inadecuado de combustibles, fallas de instalaciones eléctricas defectuosas y el inadecuado almacenamiento y traslado desustancias peligrosas.

Es considerado el enemigo número uno de los equipos de cómputo ya que puede destruir fácilmente los archivos de información y programas. Algunos factores a contemplar para reducir los riesgos de incendio: No debe estar permitido fumar en el área de proceso, Deben emplearse muebles incombustibles y cestos metálicos para papeles, El piso y el techo en el recinto del centro de cómputo y de almacenamiento de los medios magnéticos deben ser impermeables.

Es necesario proteger los equipos de cómputo instalándolos en áreas en las cuales el acceso a los mismos sólo sea para personal autorizado. Además, es necesario que estas áreas cuenten con los mecanismos de ventilación y detección de incendios adecuados.

Para protegerlos se debe tener en cuenta que: 1. La temperatura no debe sobrepasar los 18º C y el límite de humedad no debe superar el 65% para evitar el deterioro, 2. El centro de cómputo debe estar provisto de equipo para la extinción de incendios en relación al grado de riesgo y la clase de fuego que sea posible en ese ámbito, 3. Deben instalarse extintores manuales (portátiles) y/o automáticos (rociadores).

RECOMENDACIONES

El personal designado para usar extinguidores de fuego debe ser entrenado en su uso.

Implementar paredes protectoras de fuego alrededor de las áreas que se desea proteger del incendio que podría originarse en las áreas adyacentes (cuarto de servidores).

Proteger el sistema contra daños causados por el humo. Este, en particular la clase que es principalmente espeso, negro y de materiales especiales, puede ser muy dañino y requiere una lenta y costosa operación de limpieza.

Mantener procedimientos planeados para recibir y almacenar abastecimientos de papel

Inundaciones**.** Se las define como la invasión de agua por exceso de escurrimientos superficiales o por acumulación en terrenos planos, ocasionada por falta de drenaje ya sea natural o artificial.

Instalaciones Eléctricas. Esta es una de las principales áreas a considerar en la seguridad física. En la medida que los sistemas se vuelven más complicados se hace más necesaria aplicar las soluciones que estén de acuerdo con una norma de seguridad industrial.

Las subidas (picos) y caídas de tensión no son el único problema eléctrico al que se han de enfrentar los usuarios. También está el tema del ruido que interfiere en el funcionamiento de los componentes electrónicos. El ruido interfiere en los datos, además de favorecer la escucha electrónica.

Los cables que se suelen utilizar para construir las redes locales van del cable telefónico normal al cable coaxial o la fibra óptica. Es importante supervisar su disposición con los cables instalados para evitar el tiempo y el gasto posterior, y de forma que se minimice el riesgo de un corte, rozadura u otro daño accidental.

Los riesgos más comunes para el cableado se pueden resumir en los siguientes:

Interferencia. Estas modificaciones pueden estar generadas por cables de alimentación de maquinaria pesada o por equipos de radio o microondas. Los cables de fibra óptica no sufren el problema de alteración (de los datos que viajan a través de él) por acción de campos eléctricos, que si sufren los cables metálicos.

Corte del cable. La conexión establecida se rompe, lo que impide que el flujo de datos circule por el cable.

Daños en el cable. Los daños normales con el uso pueden dañar el recubrimiento que preserva la integridad de los datos transmitidos o dañar al propio cable, lo que hace que las comunicaciones dejen de ser fiables.

Sistema de aire acondicionado. Se debe proveer un sistema de calefacción, ventilación y aire acondicionado separado, que se dedique al cuarto de servidores y equipos de proceso de datos en forma exclusiva. Teniendo en cuenta que los aparatos de aire acondicionado son causa potencial de incendios e inundaciones, es recomendable instalar redes de protección en todo el sistema de cañería al interior y al exterior, detectores y extinguidores de incendio, cámaras de vigilancia y alarmas efectivas.

Amenazas ocasionadas por el hombre. Los componentes de la infraestructura tecnológica son posesiones valiosas de la Institución y pueden estar expuestas. Es frecuente que los usuarios utilicen los equipos de cómputo de la institución para realizar trabajos privados y de esta manera, utilicen tiempo de máquina.

La información importante o confidencial puede ser fácilmente copiada. El software, es una propiedad muy fácilmente de sustraer y los discos o cintas son fácilmente transportados y llevados fuera del recinto.

RECOMENDACIONES

Todos los equipos que componen la infraestructura tecnología de la institución deben estar instalados de manera no fácil de sustraer o acceder. Su posicionamiento y ubicación se debe registrar y auditar de manera frecuente.

El uso que los funcionarios de la institución dan a los diferentes componentes de la infraestructura tecnológica debe estar registrado y se deben comunicar las políticas de buen uso y responsabilidad.

Disturbios, Sabotajes internos y externos deliberados. Para el control de acceso al cuarto de servidores a cualquier personal ajeno a la institución y/o División de sistemas se le tomarán los datos y se registrará el motivo de la visita, hora de ingreso y de salida.

El uso de carnés de identificación es uno de los puntos más importantes del sistema de seguridad, a fin de poder efectuar un control eficaz del ingreso y egreso del personal a los distintos sectores de la Institución. En este caso la persona se identifica por algo que posee, por ejemplo un documento de identificación para los externos.

Otro mecanismo de seguridad, es el circuito cerrado de televisión; herramienta útil para el control y monitoreo de los espacios libres y algunos cerrados a fin de chequear el curso normal de actividades.

SEGURIDAD LÓGICA

Es importante recalcar que la mayoría de los daños que puede sufrir un centro de cómputo no será sobre los medios físicos sino contra información por él almacenada y procesada.

El activo más importante que se posee la institución es la información, y por lo tanto deben existir técnicas, más allá de la seguridad física, que la aseguren.

La Seguridad Lógica consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo.

Los objetivos que se plantean son:

Restringir el acceso a los programas y archivos de acuerdo al tipo de usuario.

Asegurar que los usuarios puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.

Asegurar que se estén utilizados los datos, archivos y programas correctos en y por el procedimiento correcto.

Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro.

Que la información recibida sea la misma que ha sido transmitida.

Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos. Por ejemplo: un buen canal de comunicación físico, por correo o telefónico.

Que se disponga de pasos alternativos de emergencia para la transmisión de información. Por ejemplo: servidores de respaldo.

Controles de Acceso. Estos controles pueden implementarse en el Sistema Operativo, sobre los sistemas de aplicación, en bases de datos, en un paquete específico de seguridad o en cualquier otro utilitario.

Constituyen una importante ayuda para proteger al sistema operativo de la red, al sistema de información y demás software de la utilización o modificaciones no autorizadas; para mantener la integridad de la información (restringiendo la cantidad de usuarios y procesos con acceso permitido) y para resguardar la información confidencial de accesos no autorizados.

Los siguientes, son los requisitos mínimos de seguridad en cualquier sistema: Identificación y Autentificación, Roles, Transacciones, Limitaciones a los Servicios, Modalidad de Acceso, Ubicación y Horario, Control de Acceso Interno, Control de Acceso Externo, y Administración.

En este punto es necesario resaltar que los sistemas de información son de tipo cliente / servidor, su acceso es local y no se accede vía Web. Solo en el caso de módulos de manejo por estudiantes, algunas funcionalidades han sido desarrolladas para acceder por Internet.

Las actividades para la creación de roles, privilegios y administración de usuarios, se encuentran definidas en los procedimientos de la división. SIA Sistema de Información Académico: Es una aplicación elaborada para facilitar la administración de los diferentes procesos académicos que se llevan a cabo en la Universidad.

Desarrollos Web del Sistema de Información Académico: Digitación de Notas, Inclusiones y/o Cancelación, Registro de Hora Cátedra, Peticiones, quejas y Reclamos, Sistema de Información Académico de la Escuela de Artes, y Evaluación Docente.

SIB Sistema de Información de Biblioteca: El SIB cuenta con una Base de Datos diseñada en el Formato MARC para Datos Bibliográficos, que permite manejar información de cualquier tipo de material bibliográfico como lo son libros, tesis, publicaciones seriadas, archivos de computadora y material audiovisual y definir diferentes políticas propias de la Biblioteca Argemiro Bayona Portillo.

Desarrollos Web del Sistema de Información Bibliográfico: Consulta de Bibliografía.

SIF Sistema de Información Financiero: El Sistema de Información Financiera SIF, es una aplicación elaborada para facilitar la administración de los diferentes procesos contables y presupuestales que se llevan a cabo en la Universidad.

ETAPA m. RECURSOS NECESARIOS

Una lista de todos los empleados, los servicios de terceros, instalaciones, infraestructura, información, equipamiento, etc., que son necesarios para llevar a cabo la recuperación, y quién es el responsable de proporcionar a cada uno de ellos.

Los recursos necesarios para poner en marcha la aplicación del Plan son:

Recursos humanos. En la Tabla 2. Rol, funciones y responsabilidades, se describen los recursos humanos necesarios con sus roles, responsabilidades y funciones.

Recursos materiales. Los materiales necesarios para la adecuación se enumeran en el Anexo I. Recursos materiales.

Recursos financieros. Los recursos de inversión necesarios en caso de una contingencia dependen directamente del incidente a enfrentar, para lo cual se derivan del costo de cubrir los recursos materiales y el transporte necesario para llevarlos al sitio indicado. Para resolver esta situación se estipula que la organización debe proveer una reserva que cubra dichos recursos.

ETAPA n. LA RESTAURACIÓN Y LA REANUDACIÓN DE LAS ACTIVIDADES DE MEDIDAS TEMPORALES

¿Cómo restaurar las actividades de nuevo una vez que el incidente perturbador se ha resuelto.

En ningún caso las actividades normales del CEDIT se deben interrumpir por un lapso de tiempo considerable.

Para ello se dispone de las medidas adecuadas que permitan el restablecimiento de las mismas. Estas son, en caso de ser necesarias:

Traslado de los equipos de cómputo y oficina a la sede del CEDIT ubicada en el barrio La Primavera.
Adecuación de los espacios físicos.

Reinstalación y adaptación de los servicios de acueducto, alcantarillado, energía eléctrica, internet, y telefonía fija.

4.2 IDENTIFICACIÓN DE LOS RIESGOS A QUE ESTA EXPUESTO EL CEDIT

En la siguiente tabla se presentan algunas de las implicaciones que se podrían generar en la ocurrencia de una emergencia si no se establece un plan de acción preventivo.

Tabla 3. Análisis e Impacto del Negocio

FACTORES DE RIESGO	RIESGO	COSTO
Riesgo Físico Los que afectan a la seguridad del edificio	Sismos/ terremotos Temperatura y humedad relativa del aire Inundación y/o anegación Incendio Rayos Iluminación	Reconstrucción de la edificación en general o de los sectores afectados. Pérdida total o parcial de información clave. Reparación de equipos de cómputo o adquisición de nuevos equipos para suplir las necesidades. Pérdida total o parcial de soportes. Pérdida total o parcial de soportes por incendio o explosión. Retraso en la ejecución de operaciones por daño en las instalaciones o equipos. Pérdida total o parcial de soportes.
Riesgo Biológico	Insectos, Roedores Microorganismos	Perdida de la documentación.
Riesgo Social	Hurto, Vandalismo Huelga, Motín Asonada, Entorno y vecinos	Cuando ocurre un impacto de este tipo, la imagen institucional se puede ver afectada ante entidades externas y en general en la comunidad académica, debido a la evidencia de fallas en la seguridad.
Riesgo Tecnológico Riesgos que afectan la integridad de los datos	Corte de energía eléctrica Riesgos Tecnológicos	Perdida de información que no se halla salvado en los computadores, costos por el retraso de las actividades propias del CEDIT.

	Virus informáticos Seguridad en la Información de tipo tecnológico	Adquisición de nuevos equipos, reparación de instalaciones físicas. Perdida de información clave, daño de los equipos. Problemas de carácter jurídico y/o legal. Perdida de la integridad de la información, deterioro de la imagen institucional.

Fuente: Autores del Proyecto.

A continuación se listan las emergencias más comunes y las indicaciones a seguir:

Avisar de la emergencia. Avisar al jefe de área y/o brigadistas quienes se encuentran entrenados para enfrentar la emergencia.

Alertar a los servicios públicos oportunos, suministrar la mayor cantidad de información posible.

De ser posible intervenir con las herramientas con que se cuenta, siempre y cuando no esté en peligro la seguridad personal.
Si las magnitudes de la emergencia lo ameritan, evacuar.

¿Cómo evacuar?

Al oír la señal de evacuación, prepárese para abandonar el centro.

Procurar llevar siempre consigo los objetos personales (no voluminosos).

Desconectar los objetos eléctricos a su cargo.

Si se encuentra junto a alguna visita, acompáñela hasta el exterior.

Evacuar el edificio con rapidez, pero sin correr.

No volver al Centro de trabajo a recoger objetos personales.

Durante la evacuación seguir las siguientes instrucciones:

Realizar la evacuación de forma rápida y ordenada.

Tranquilizar a las personas que durante la evacuación, hayan podido perderla calma.

Ayudar a las personas impedidas o disminuidas.

No permitir el ingreso al Centro de trabajo a ninguna persona que pretenda ir a buscar algún objeto o a otra persona.

Abandonar el Centro, dirigirse al punto de reunión y no detenerse inmediatamente después de la salida del edificio.

Permanecer en el punto de reunión y seguir las instrucciones del jefe de área y los brigadistas.

En caso de que la evacuación se realice por amenaza de bomba, dejar las puertas y ventanas del Centro abiertas.

De igual manera, analizando las situaciones detectadas (Ver Anexo J. Situaciones detectadas) se concluyó mediante la aplicación de una matriz de riesgos (Ver Anexo K. Matriz de riesgos) que la calificación del riesgo general es alta, al encontrarse un valor de 0,26; como promedio. Hecho que lleva a aplicar estrategias y acciones al respecto tales como:

Transferir: Capacitar al personal en la formación requerida.

Aceptar - Mitigar: Evidenciar controles, políticas, procesos y procedimientos de la seguridad de la información de manera independiente y objetiva.

Eliminar: Definir políticas que permita definir nuevos roles que admitan la oportuna y rápida toma de decisiones.

Aceptar - Mitigar: Plantear políticas que permitan la independencia.

4.3 ACCIONES PREVENTIVAS

Las acciones preventivas para evitar la pérdida de información ante un desastre o siniestro se resumen en:

Seguridad física y ambiental, incluye el control de equipos y áreas (servidores, PCs, medios magnéticos, información impresa, etc.)

Control de acceso de acuerdo a los perfiles de cada usuario.

Control de los recursos físicos incluida la actualización de hardware y software.

Capacitación y entrenamiento del personal, esta tarea es apoyada por el departamento de personal. Además del suministro de instructivos y manuales con el fin de trabajar de forma unificada y conjunta garantizando de esta forma la seguridad e integridad de la información y su adecuado uso y manipulación.

Protección de la información en redes y de la infraestructura de soporte.

Desarrollo y mantenimiento de los sistemas, incluye la protección de archivos, bases de datos, políticas de cifrado, etc.

Evitar daños a los recursos de información e interrupciones en las actividades de la Universidad.

Con base en el análisis efectuado, a continuación se presentan recomendaciones importantes para tener en cuenta antes, durante y después de la ocurrencia de algunas de las emergencias que se pueden llegar a producir.

Tabla 4. Recomendaciones

TIPO DE EMERGENCIA	DAÑOS QUE PUEDE LLEGARA OCASIONAR	¿QUÉ HACER ANTES DE LA EMERGENCIA ?	¿QUÉ HACER DURANTEDE LA EMERGENCIA?	¿QUE HACER DESPUES DE LAEMERGENCIA?
INCENDIO	Proliferación de llamas Generación de Humo tóxico Derrumbamiento de estructuras	Es importante contar con los extintores adecuados de acuerdo al tipo de incendio y el área donde se presente el evento.	Mantenga la calma. Active las alarmas de incendios y avise al cuerpo de bomberos Si se encuentra atrapado en una oficina; cierre todas las puertas. Tape con trapos, de ser posible húmedos, todas las rendijas por donde penetre el humo. Haga saber de su presencia. Si se trata de un foco incipiente y posee formación en el manejo de sistemas de extinción, actúe sobre el foco con extintores portátiles o las mangueras interiores. Si es posible, corte la electricidad. Si el incendio es grave o no sabe apagarlo, desaloje la zona ayudando a las personas que lo precisen: ancianos, niños e impedidos.	Reúnase en una zona segura con el resto del personal. Localice al jefe de área y/o brigadistas. Espere las instrucciones y colabore sólo cuando se solicite su ayuda.

			No rompa las ventanas. Cierre las puertas sin llave. Toque las puertas y si están calientes o sale humo por las rendijas, tápelas con trapos húmedos, no las abra y busque otras salidas. Si el edificio está en llamas cúbrase la nariz con un pañuelo mojado, si hay mucho humo camine agachado o a gatas. Olvídese de salvar posesiones, lo importante es su vida y la del resto de las personas. Si se le prende la ropa, no corra, tiéndase en el suelo y échese a rodar.	
INUNDACIÓN	Incendios por cortocircuito Deterioro de la documentación por efectos del agua.	Revisión y reparación de los sitios por donde se pueda filtrar el agua. Revisión periódica de tuberías y desagües. Dejar estanterías y otros soportes de documentación a una altura mínima de 10 cm. para evitar que se afecten los documentos en sus diferentes soportes en caso de inundación.	Mantenga la calma. Avise al jefe de área y/o brigadistas. Dé prioridad a las zonas donde se encuentran los documentos esenciales. Avise al cuerpo de bomberos Corte la corriente eléctrica, para evitar cortocircuitos. Evite la descarga de agua cerrando las llaves de paso, si el derrame es interior, o cerrando puertas y taponando entradas, si la procedencia es exterior. Si no existe riesgo para su integridad, espere la llegada de los bomberos; en una zona segura.	No intente activar fuentes de calor para secar los documentos. No envuelva documentos en plástico Espere las instrucciones y colabore sólo cuando se solicite su ayuda. Abandone la zona cuando se le indique. Una vez extraída la documentación afectada por la inundación proceder a empacarla o proceder al secado manual o al secado asistido mecánicamente y efectuar una desinfección

Fuente: Autores del Proyecto

Todo el proceso debe ir acompañado de programas de capacitación y concienciación para garantizar que el mismo sea conocido por todos los miembros de la dependencia y la Universidad.

PROGRAMAS DE CAPACITACIÓN Y CONCIENCIACIÓN

Según la auditoría realizada por los Autores del Proyecto al CEDIT en los meses de abril y mayo de 2014(Ver Anexo E. Auditoría Externa), se evidenció que los programas de capacitación y concienciación se encuentran a cargo del director de la dependencia y de la división de personal.

PRUEBA Y VERIFICACIÓN

Para poder realizar pruebas y verificación es necesario que se presenten situaciones que afecten el normal funcionamiento de la UFPS Ocaña y específicamente el CEDIT. Como referencia se pueden aplicar las acciones de remodelación y adecuación de la infraestructura física de la Casona a finales del año pasado; en donde fue necesario aplicar el Plan de Contingencia para garantizar la continuidad del negocio. En lo concerniente al **CEDIT**, igualmente y debido a remodelaciones en la sede La Primavera de la UFPS Ocaña en el año 2014, se hizo necesario utilizar espacios anexos para poder continuar con las labores de dicha dependencia.

Además, con la instalación de la subestación en la sede de La Primavera de la UFPS Ocaña, se mejoró en parte los continuos cortes de energía que se presentaban. Demostrando que las recomendaciones dadas en el Plan de Contingencia son acertadas y resuelven la situación o situaciones detectadas.

REVISIONES POST INCIDENTES

El SIG identifica que la autoevaluación es implementada como un proceso de reflexión permanente y de obtención de información oportuna y eficaz para la toma de decisiones en pro del mejoramiento continuo y la obtención de la calidad esperada de los programas académicos y la Institución en su conjunto. Esta cultura es vista a la luz del Proyecto Educativo Institucional (PEI), el Plan de Desarrollo y los Proyectos Educativos de cada programa académico (PEP). Este principio genera en cada individuo de la organización un compromiso que permite revisiones durante y después de cualquier incidente. Siendo Control Interno la dependencia cumple un papel importante como responsable del Componente de Evaluación Independiente, y como asesor, evaluador, integrador y dinamizador del Sistema de Control Interno y el Sistema Integrado de Gestión con miras a mejorar la cultura organizacional y, por ende, a contribuir con la productividad de la Universidad.

Producto de este trabajo de investigación nos permitimos referenciar el Plan de continuidad para el CEDIT de la UFPS Ocaña (Ver Anexo L. Plan de continuidad del negocio para el CEDIT).

CONCLUSIONES

El desarrollo del Plan de continuidad para el Centro de Desarrollo e Innovación Tecnológica de la Universidad Francisco de Paula Santander permitió definir objetivamente tanto las etapas que conllevan a la elaboración del Plan, como también los procesos críticos de la dependencia que sirvió además de apoyo a la toma de decisiones en otros ámbitos.

No se evidencian controles, políticas, procesos y procedimientos de la seguridad de la información de manera independiente y objetiva evidenciando falta de adaptación e implementación de controles, políticas y procedimientos generando desconocimiento del proceso en cuanto a sus funciones.

No se cuenta en el proceso un plan de acción independiente que le permita subsanar situaciones detectadas mediante auditorias demostrando la falta de un plan de acción de auditoría independiente que conlleva al no logro de los objetivos y metas propuestas por el proceso.

Muchos procesos presentan dependencia absoluta centralizada mostrando que los procesos de revisión independiente de la seguridad de la información, dependen exclusivamente del departamento de sistemas. Siendo nula la iteración del CEDIT en este caso. Situación que lleva al Director de la UFPS Ocaña y al Jefe de la División de Sistemas a proponer una solución para el mes de septiembre del año en curso.

Se encontró que los roles están debidamente asignados y cada funcionario ejecuta su respectivo Rol, sin embargo esta situación retarda la toma de decisiones prioritarias para el buen desempeño de la dependencia en lo referente a seguridad de la información. Lo que evidencia una vez más que los procesos en la organización se encuentran centralizados; retardando la rápida toma de decisiones.

Estos riesgos conducen a tomar decisiones como: Transferir: Capacitar al personal en la formación requerida; Aceptar - Mitigar: Evidenciar controles, políticas, procesos y procedimientos de la seguridad de la información de manera independiente y objetiva; Eliminar: Definir políticas que permita defir uevos roles que admitan la oportuna y rápida toma de decisiones; y Aceptar - Mitigar: Plantear políticas que permitan la independencia.

RECOMENDACIONES

Las principales recomendaciones para la ejecución del Plan son:

Una vez establecido el Plan, este se debe difundir y dar a conocer al personal que tenga relación con el CEDIT. Este es un esfuerzo que debe liderar con la colaboración de la Oficina de Personal. Es importante que los funcionarios conozcan las medidas de prevención y las medidas correspondientes a la fase de respuesta.

Es importante inspeccionar las instalaciones físicas del CEDIT y cuantificar el impacto que un desastre podría tener en estas. Las instalaciones deben estar en conformidad con el Código de Construcción Colombiano, en caso contrario deben efectuarse las respectivas reestructuraciones para darle solidez a la estructura.

Se deben asignar responsabilidades para cada empleado en caso de que ocurra una emergencia, es recomendable emplear un lenguaje simple y sencillo de entender y seguir. Es primordial practicar los procedimientos establecidos para cada tipo de emergencia, esto se puede lograr a través de simulacros.

Es importante contar con una lista de direcciones y teléfonos importantes (Jefes de área, brigadistas, agentes de seguros, aseguradoras y otros empleados y de las entidades que atienden emergencias; bomberos, policía, Cruz Roja). Se recomienda seguir las instrucciones que se precisan en el Programa de Salud Ocupacional.

Es necesario considerar que herramientas se puede llegar a necesitar después de ocurrida la emergencia.

El personal de la Universidad en general debe saber cómo proceder en caso de que el CEDIT sufra un colapso, deben conocer donde se encuentran almacenadas copias de respaldo en especial de los documentos esenciales y cuáles son los procesos que deben seguir mient[illegible] se restablece la normalidad.

Es importante evaluar los costos e impacto que se puede llegar a generar sobre la información en caso de que ocurriese un siniestro. Es importante analizar las siguientes preguntas ¿Cuánto le costaría al CEDIT permanecer cerrado por un día, una semana o un período mayor? ¿Cuánto le costaría perder información clave para el desarrollo de sus actividades y trámites?

Una de las principales estrategias para asegurar la perdurabilidad de la información dada una emergencia consiste en mantener archivos por duplicado, es decir, archivos de respaldo actualizados (Tanto físicos como electrónicos), lo más aconsejable es que estos archivos estén ubicados fuera de la dependencia.

Resulta de gran utilidad asegurarse de que se posee suficiente cobertura de seguros para pagar los costos indirectos de un desastre, no solo de la instalación sino también de equipos y maquinaria. Igualmente es importante conocer los límites y deducibles de la(s) póliza(s).

REFERENCIA BIBLIOGRÁFICA

Acuerdo 084 de 1995, Consejo Superior Universitario – Universidad Francisco de Paula Santander.

Acta 003 de 2013, Comité de Apoyo Académico - Universidad Francisco de Paula Santander Ocaña

BAIN, George. UK Cabinet Office, Emergency Preparedness, Guidance on Part 1of the Civil Contingences Act 2004, HM Government, Londres – Reino Unido, 2005. p.114

BIRD, Larry. Good Practice Guidelines A Management Guide to Implementing Global Good Practice in Business Continuity Management, Business Continuity Institute, Berkshire Reino Unido, 2010. p.12

Constitución Política de Colombia, 1991.

EVANS, Donald. International Organization for Standardization, ISO 22301:2012 Societal Security Business Continuity management systems Requirements, Primera Edición, Suiza, 2012. p.78

Ley 1289 de 2009.

Ley 1341 de 2009

Resolución 1286 de 2012 - Colciencias.

Resolución 0260 de 2013 - Universidad Francisco de Paula Santander Ocaña

SCHMIDT, Douglas. NFPA 1600 Standard on Disaster/ Emergency Management and Business Continuity Programs‖, National Fire Protection Association, EE.UU. 2010. p.95

SHARP, John. The route map to Business Continuity Management, Meeting the requirements of BS 25999; British Standards Institution, Londres Reino Unido, 2008. p.57

SWANSON, Mike. BOWEN, Peter. WOHL PHILLIPS, Amy. Contingency Planning Guide for Federal Information Systems Special Publication 800-34 Rev. 1, National Institute of Standards and Technology NIST, EE.UU. 2010. p.56

WITTY, Robert. Preplanning for plan invocation, Continuity Magazine, ISSN 14601451, 2011. p. 19-20.

ANEXOS

ANEXO A. REGISTRO DE ENTREVISTA

FORMATO: REGISTRO DE ENTREVISTA	**AC-7**
EMPRESA: UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA	**FECHA:** 18 AL 21 DE ABRIL DE 2014
AREA AUDITADA:CENTRO DE DESARROLLO E INNOVACIÓN TECNOLÓGICA	
RESPONSABLE DEL PROCESO:PROFESIONAL DE APOYO CEDIT (JORGE FRANCISCO RINCÓN ANGARITA)	
AUDITOR LIDER: FERNANDA MARTINEZ VEGA……..…….AL **AUDITOR ACOMPAÑANTE 1:** CLAUDIA DEL PILAR QUINTERO PRADO…… AA1 **AUDITOR ACOMPAÑANTE 2:** JAVIER ALEXANDER BLANCO LINDARTE…… AA2	
REGISTRO	**OBSERVACIÓN**
MARCO REFERENCIAL GERENCIAL PARA INICIAR Y CONTROLAR LA IMPLEMENTACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN DENTRO DE LA ORGANIZACIÓN. 1. En la Universidad, ¿quién asigna los usuarios y las claves para cada cargo? 2. Cuándo se bloquea su cuenta de usuario ¿usted a quien se dirige?, o lo soluciona sin solicitar ayuda.	1. Los usuarios y las claves respectivas las asigna la división de sistemas. 2. El procedimiento a seguir es reportarlo al director del CEDIT, quien a su vez solicita la respectiva corrección a la división de sistemas.
CONTACTO CON ESPECIALISTAS O GRUPOS DE SEGURIDAD EXTERNO QUE PROPORCIONEN VINCULOS ADECUADOS PARA EL MANEJO DE LOS INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN. 1. ¿Cuentan con una empresa que les brinde el servicio de seguridad externa?	1. Sí.
ENFOQUE MULTIDISCIPLINARIO PARA LA SEGURIDAD DE LA INFORMACIÓN. 1. ¿Quién lo capacita para que usted maneje la información de una forma segura?	1. La capacitación está a cargo del director del CEDIT y de la división de personal.
CONTROL DE LA SEGURIDAD DE LA INFORMACIÓN. 1. ¿Sabe usted si se encuentran implementados los lineamientos (resoluciones, manuales, etc.) para la seguridad de la información? 2. Cuando realiza una consulta, ¿Qué tipo de consulta hace?	1. Si, los lineamientos se encuentran para su consulta en la página web www.ufpso.edu.co. Estos son: Manual Sistema de Información, Telecomunicaciones y Tecnología; Caracterización Sistemas de Información, Telecomunicaciones y Tecnología; Administración de los Recursos Informáticos; Gestión de los sistemas de TI; Plan de Contingencia de TI - División de Sistemas, entre otros. 2. Aclaración de dudas, descarga de formatos para solicitudes, consultas sobre caídas del sistema, entre las más comunes.
COORDINACION DE LA SEGURIDAD DE LA INFORMACIÓN. 1. ¿Quién coordina los lineamientos implementados para la seguridad de la información? 2. ¿De esos lineamientos cuales son aplicados por usted?	1. El Jefe de la división de sistemas. 2. Dentro de los lineamientos se aplican los procedimientos de: Administración de los Recursos

3. ¿Qué manejo le dan al tratamiento de las No-conformidades? 4. Cuándo usted va a aplicar un proceso con método a la seguridad de la información ¿Quién los aprueba? 5. ¿Quién identifica las amenazas a que está expuesta la información de la dependencia? 6. ¿Con que periodicidad recibe capacitaciones para un adecuado manejo de la seguridad de la información? 7. Ante los incidentes de seguridad de la información, ¿Quién monitorea y revisa dichos incidentes? 8. ¿Identifica usted el funcionario que recomienda las acciones apropiadas en respuesta a los incidentes identificados de seguridad de información?	Informáticos e Instructivos: Gestión de la Configuración, Servicio Técnico y Tecnológico, Soporte y Atención al usuario. 3. Se reportan al director del CEDIT, quien le da el reporte a la división de sistemas para su respectivo tratamiento. 4. El director del CEDIT con el visto bueno del jefe de la división de sistemas. 5. Cada profesional de apoyo, como el eslabón más pequeño dentro del CEDIT, pasando por el director del CEDIT y encabezado por el departamento de sistemas. 6. Como inducción, se dan los lineamientos a seguir en cuanto a seguridad de la información, pero no se da un manejo periódico para darle continuidad a las capacitaciones. 7. Cada profesional de apoyo, el director del CEDIT y la división de sistemas. 8. Si, estos son: el director del CEDIT y el jefe de la división de sistemas.
ASIGNACIÓN DE LAS RESPONSABILIDADES DE LA SEGURIDAD DE LA INFORMACIÓN. 1. ¿Quién es el responsable de la seguridad de la información en esta dependencia? 2. Ante una contingencia que involucre la seguridad de la información ¿Cómo garantizan la continuidad de sus labores? 3. ¿El responsable de la seguridad de la información de esta dependencia delega tareas de seguridad a terceros? 4. ¿Todas las personas que laboran en esta dependencia son responsables de la totalidad de la seguridad de la información? 5. ¿Qué procesos de seguridad de la información existen en esta dependencia? 6. De los procesos de seguridad de la información ¿cuáles están a su cargo? 7. ¿Documentan en detalle los procesos de seguridad de la información? 8. ¿Qué niveles de autorización manejan dentro de la seguridad de la información al interior de la dependencia? 9. ¿Están documentados los niveles de autorización?	1. El director del CEDIT y los profesionales de apoyo de cada unidad. 2. Siguiendo las recomendaciones e instrucciones del plan de contingencia de TI. 3. Si, dado que toda la organización es responsable de la seguridad de la información. 4. Si, dado que toda la organización es responsable de la seguridad de la información. 5. Los consignados en el instructivo: Administración de los Recursos Informáticos. 6. Los consignados en los lineamientos para el manejo de la información; según el ROL de usuarios como funcionarios de la UFPS Ocaña. 7. No todo el tiempo. 8. Coordinador de Servidores, Coordinador de Redes y Comunicaciones, Coordinador de Soporte Técnico, Coordinador de

	Sistemas, Personal Clave, y Usuarios (Funcionarios de la UFPS Ocaña). 9. Si, se pueden consultar en el instructivo: Administración de los Recursos Informáticos.
AUTORIZACIÓN DE PROCESO PARA FACILIDADES PROCESADORAS DE INFORMACIÓN. 1. ¿Qué proceso facilita el procesamiento de información sin afectar la seguridad del sistema de información? 2. ¿Quién autoriza dicho proceso? 3. ¿Se revisa la compatibilidad del hardware y software con otros componentes del sistema?	1. Se utilizan procesos en línea y algunos propios de cada unidad. 2. El director del CEDIT con la autorización de la división de sistemas. 3. Siempre.
ACUERDOS DE CONFIDENCIALIDAD 1. ¿Qué procedimiento tiene establecido para revisar los requerimientos de confidencialidad de la información? 2. ¿Muéstreme bajo que requisito legal se protege la confidencial de la información? 3. ¿Qué acciones desarrolla la institución en caso de que la información no se proteja? 4. ¿Se tiene identificado que tipo de información es confidencial dentro de la institución?	1. Los consignados en el Manual Sistema de Información, Telecomunicaciones y Tecnología. 2. Se cumplen con los estándares de la Norma Técnica de Calidad para la Gestión Pública NTC GP 1000:2009 y del Modelo Estándar de Control Interno MECI 1000:2008. 3. Acciones: Evitar el riesgo, Administración de cuentas y roles de usuario, Encriptamiento, Protocolo de interfaces de usuario y acceso a los SI, Monitoreo y control de accesos, Actualización permanente de programas y paquetes de seguridad. 4. Sí. En su mayoría es de tipo financiero (manejo de nómina, por ejemplo).
CONTACTO CON LAS AUTORIDADES 1. Para el manejo de incidentes de la dependencia ¿cuenta la organización con un procedimiento que permitan contactar a las autoridades para reportar dichos incidentes de la información de una manera oportuna, si se sospecha que se han incumplido las leyes? 2. ¿Su proveedor de servicio de internet toma alguna acción contra ataques desde la red, después de haber sido contactada? 3. ¿Cómo manejan la continuidad del negocio ante esta contingencia? 4. ¿Se mantiene en contacto con organismos reguladores que faciliten anticipar y prepararse ante cambios en la ley? 5. ¿Con que otras autoridades se comunican para garantizar la continuidad de las actividades de la dependencia (Bomberos, empresas de salud, defensa civil, empresa de servicios públicos)?	1. Sí. Consultar Plan de Contingencia de TI - División de Sistemas. 2. Si. Plan de Contingencia de TI - División de Sistemas. 3. Aplicando los lineamientos del Plan de Contingencia de TI - División de Sistemas, aunque en ocasiones se tarda un poco la continuidad del mismo por razones de autorizaciones tardías de parte de las directivas de la universidad. 4. Si, el director de la UFPS Ocaña es el secretario de la organización de universidades públicas de Colombia. 5. Con las necesarias. Estas se encuentran registradas en los

	planes de contingencia como procedimiento a ejecutar.
CONTACTO CON GRUPOS DE INTERES ESPECIAL 1. ¿Qué grupos de interés tiene identificados para compartir conocimiento acerca de la seguridad de la información? 2. ¿Con que periodicidad se intercambia conocimiento con los grupos de interés especial? 3. ¿Se reciben advertencias tempranas de alertas, asesorías y avisos relacionados con ataques y vulnerabilidades de parte de interés especial? 4. ¿Su dependencia proporciona vínculos adecuados cuando se tratan incidentes de seguridad de la información?	1. Universidades públicas en Colombia, Centros de desarrollo, SENA, entre otros. 2. Existe un contacto constante y las capacitaciones redundan en calidad. En resumen dos veces al año como mínimo. 3. Gracias a la comunicación constante, si se reciben alertas, asesorías y avisos. 4. Si, precisamente es una de las acciones que interesan en el CEDIT.
REVISION INDEPENDIENTE DE LA SEGURIDAD DE LA INFORMACIÓN 1. ¿Existe un plan de revisión de controles, políticas, procesos y procedimientos de seguridad de la información de manera independiente en esta dependencia? 2. ¿Tiene establecido un plan de acción para subsanar las situaciones detectadas en auditorías realizadas en su dependencia? 3. ¿Lleva un registro de las acciones tomadas para subsanar las situaciones que requieren un mejoramiento? 4. ¿Son reportadas a la dirección las situaciones detectadas y las acciones tomadas? 5. Las acciones que toma la dirección frente a las situaciones detectadas, ¿son correctivas?	1. No, todos los lineamientos están dados por la división de sistemas. 2. Directamente no, dado que dependemos de la división de sistemas y hasta el momento no se han efectuado auditorias en el CEDIT. 3. Por parte de control interno Si. 4. Si, primero se reporten al director del CEDIT y luego se sigue el conducto regular. 5. En algunos casos sí. Cuando la situación lo amerita.
ELABORÓ	**APROBÓ**

ANEXO B. ENCUESTA

ENCUESTA		**AC-8**
EMPRESA: UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA		**FECHA:** 18 AL 21 DE ABRIL DE 2014
AREA AUDITADA:CENTRO DE DESARROLLO E INNOVACIÓN TECNOLÓGICA		
RESPONSABLE DEL PROCESO:PROFESIONAL DE APOYO CEDIT (JORGE FRANCISCO RINCÓN ANGARITA)		
AUDITOR LIDER: LINA FERNANDA MARTINEZ VEGA……..……. AL **AUDITOR ACOMPAÑANTE 1:** CLAUDIA DEL PILAR QUINTERO PRADO…… AA1 **AUDITOR ACOMPAÑANTE 2:** JAVIER ALEXANDER BLANCO LINDARTE…… AA2		
PREGUNTA	**RESPUESTA**	
1. ¿Están documentadas las políticas de la seguridad de la información en la organización?	SI _X_ NO ___	
2. ¿Se garantiza la continuidad del negocio?	En parte, dado que ante una contingencia de fallo eléctrico general en la sede central de la UFPS Ocaña, no se pude garantizar la continuidad del negocio.	
3. ¿En qué porcentaje califica la disposición para el acceso a la información?	100%, siempre y cuando no se esté haciendo mantenimiento al sistema y exista continuidad en el fluido eléctrico en la sede central de la UFPS Ocaña porque es en este lugar en donde reposan los servidores.	
4. ¿Qué tanto es seguro el acceso a la información?	Muy seguro. Están establecidos los roles y controles de acceso con usuarios y contraseñas.	
5. ¿Quién es el responsable del manejo de la seguridad de la información en el CEDIT?	El Jefe De La División De Sistemas. Entendiéndose que a nivel de la dependencia, cada persona en su cargo es responsable por el manejo de la seguridad de la información.	
6. ¿Quién se encarga de la adquisición de nuevos equipos para el manejo de la información?	Lo hace el Director de la UFPS Ocaña bajo la solicitud del director del CEDIT.	
7. ¿Se tiene en cuenta que los nuevos equipos sean compatibles con los ya existentes?	Sí. El Jefe de la División de Sistemas y el Director del CEDIT poseen el perfil y el conocimiento para garantizar que se pueda recomendar la compatibilidad de los mismos.	
8. ¿Se garantiza la confidencialidad de la información?	Al tomar posesión del cargo se adquiere el compromiso de confidencialidad y al mismo tiempo se presentan los roles, la asignación de usuario del sistema y la contraseña. Dando así acceso a información confidencial solo a los usuarios autorizados para tal fin.	
ELABORÓ	**APROBÓ**	

ANEXO C. LISTA DE CHEQUEO

LISTA DE CHEQUEO		**AC-9**
EMPRESA: UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA		**FECHA:** 14 AL 29 DE ABRIL DE 2014
AREA AUDITADA:CENTRO DE DESARROLLO E INNOVACIÓN TECNOLÓGICA		
RESPONSABLE DEL PROCESO:PROFESIONAL DE APOYO CEDIT (JORGE FRANCISCO RINCÓN ANGARITA)		
AUDITOR LIDER: LINA FERNANDA MARTINEZ VEGA…..…….. AL **AUDITOR ACOMPAÑANTE 1:** CLAUDIA DEL PILAR QUINTERO PRADO…… AA1 **AUDITOR ACOMPAÑANTE 2:** JAVIER ALEXANDER BLANCO LINDARTE…… AA2		
CONCEPTO A EVALUAR. MARCO REFERENCIAL GERENCIAL PARA INICIAR Y CONTROLAR LA IMPLEMENTACION DE LA SEGURIDAD DE LA INFORMACIÓN DENTRO DE LA ORGANIZACIÓN		
	CUMPLE	
	SI	**NO**
En la Universidad, ¿quién asigna los usuarios y las claves para cada cargo?	✔	
Cuándo se bloquea su cuenta de usuario ¿usted a quien se dirige?, o lo soluciona sin solicitar ayuda.	✔	
CONCEPTO A EVALUAR. CONTACTO CON ESPECIALISTAS O GRUPOS DE SEGURIDAD EXTERNO QUE PROPORCIONEN VINCULOS ADECUADOS PARA EL MANEJO DE LOS INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN		
¿Cuentan con una empresa que les brinde el servicio de seguridad externa?	✔	
CONCEPTO A EVALUAR. ENFOQUE MULTIDICIPLINARIO PARA LA SEGURIDAD DE LA INFORMACIÓN		
¿Son capacitados para que manejo de la información se suministre de una forma segura?	✔	
CONCEPTO A EVALUAR. CONTROL DE LA SEGURIDAD DE LA INFORMACIÓN		
¿Sabe usted si se encuentran implementados los lineamientos (resoluciones, manuales, etc.) para la seguridad de la información?	✔	
Realiza consulta relacionadas con el manejo de la información, ¿Qué tipo de consulta hace?	✔	
CONCEPTO A EVALUAR. COORDINACION DE LA SEGURIDAD DE LA INFORMACIÓN		
¿Conoce quién coordina dentro de proceso los lineamientos implementados para la seguridad de la información?	✔	
¿Sabe cuántos de esos lineamientos son aplicados por usted dentro de su proceso?	✔	
¿Cuentan con un plan de tratamiento para las No-conformidades?	✔	
¿Qué manejo le dan al tratamiento de las No-conformidades?	✔	
Cuándo usted va a aplicar un proceso con método a la seguridad de la información ¿Quién los aprueba?	✔	
¿Quién identifica las amenazas a que está expuesta la información de la dependencia?	✔	
¿Con que periodicidad recibe capacitaciones para un adecuado manejo de la seguridad de la información?		✔
Ante los incidentes de seguridad de la información, ¿Quién monitorea y revisa dichos incidentes?	✔	
¿Identifica usted el funcionario que recomienda las acciones apropiadas en respuesta a los incidentes identificados de seguridad de información?	✔	

CONCEPTO A EVALUAR. ASIGNACIÓN DE LAS RESPONSABILIDADES DE LA SEGURIDAD DE LA INFORMACIÓN		
¿Quién es el responsable de la seguridad de la información en esta dependencia?	✔	
Ante una contingencia que involucre la seguridad de la información ¿Cómo garantizan la continuidad de sus labores?	✔	
¿El responsable de la seguridad de la información de esta dependencia delega tareas de seguridad a terceros?	✔	
¿Todas las personas que laboran en esta dependencia son responsables de la totalidad de la seguridad de la información?	✔	
¿Conoce los procesos de seguridad de la información existen en esta dependencia?	✔	
Conoce los procesos de seguridad de la información ¿De esos procesos cuáles están a su cargo?	✔	
¿Documentan en detalle los procesos de seguridad de la información?		✔
¿Qué niveles de autorización manejan dentro de la seguridad de la información al interior de la dependencia?	✔	
¿Están documentados los niveles de autorización?	✔	
CONCEPTO A EVALUAR. AUTORIZACIÓN DE PROCESO PARA FACILIDADES PROCESADORAS DE INFORMACIÓN		
¿Conoce el proceso que facilita el procesamiento de información sin afectar la seguridad del sistema de información?	✔	
¿Tiene identificado quien autoriza dicho proceso?	✔	
¿Se revisa la compatibilidad del hardware y software con otros componentes del sistema?	✔	
CONCEPTO A EVALUAR. ACUERDOS DE CONFIDENCIALIDAD		
¿Qué procedimiento tiene establecido para revisar los requerimientos de confidencialidad de la información?	✔	
¿Muéstreme bajo que requisito legal se protege la confidencial de la información?	✔	
¿La institución toma acciones en caso de que la información que se desarrolla no se protegida?	✔	
¿Se tiene identificados que tipo de información es confidencial dentro de la institución?	✔	
CONCEPTO A EVALUAR. CONTACTO CON LAS AUTORIDADES		
Para el manejo de incidentes de la dependencia ¿cuenta la organización con un procedimiento que permitan contactar a las autoridades para reportar dichos incidentes de la información de una manera oportuna, si se sospecha que se han incumplido las leyes?	✔	
¿Su proveedor de servicio de internet toma alguna acción contra ataques desde la red, después de haber sido contactada?	✔	
¿Cómo manejan la continuidad del negocio ante esta contingencia?		✔
¿Se mantiene en contacto con organismos reguladores que faciliten anticiparla y prepararse ante cambios en la ley?	✔	
¿Con que otras autoridades se comunican para garantizar la continuidad de las actividades de la dependencia (Bomberos, empresas de salud, defensa civil, empresa de servicios públicos)?	✔	
CONCEPTO A EVALUAR. CONTACTO CON GRUPOS DE INTERES ESPECIAL		
¿Tiene identificados los grupos de interés para compartir conocimiento acerca de la seguridad de la información?	✔	
¿Con que periodicidad se intercambia conocimiento con los grupos de interés especial?	✔	

¿Se reciben advertencias tempranas de alertas, asesorías y avisos relacionados con ataques y vulnerabilidades de parte de interés especial?	✔	
¿Su dependencia proporciona vínculos adecuados cuando se tratan incidentes de seguridad de la información?	✔	
CONCEPTO A EVALUAR. REVISION INDEPENDIENTE DE LA SEGURIDAD DE LA INFORMACIÓN		
¿Existe un plan de revisión de controles, políticas, procesos y procedimientos de seguridad de la información de manera independiente en esta dependencia?		✔
¿Tiene establecido un plan de acción para subsanar las situaciones detectadas en auditorías realizadas en su dependencia?		✔
¿Lleva un registro de las acciones tomadas para subsanar las situaciones que requieren un mejoramiento?	✔	
¿Son reportadas a la dirección las situaciones detectadas y las acciones tomadas?	✔	
Las acciones que toma la dirección frente a las situaciones detectadas, ¿son correctivas?	✔	
ELABORÓ	**APROBÓ**	

ANEXO D. REGISTRO DE OBSERVACIÓN

FORMATO: REGISTRO DE OBSERVACIÓN	**AC-10**
EMPRESA: UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA	**FECHA:** 14 AL 29 DE ABRIL DE 2014
AREA AUDITADA:CENTRO DE DESARROLLO E INNOVACIÓN TECNOLÓGICA	
RESPONSABLE DEL PROCESO:PROFESIONAL DE APOYO CEDIT (JORGE FRANCISCO RINCÓN ANGARITA)	
AUDITOR LIDER: LINA FERNANDA MARTINEZ VEGA…….…… AL **AUDITOR ACOMPAÑANTE 1:** CLAUDIA DEL PILAR QUINTERO PRADO…… AA1 **AUDITOR ACOMPAÑANTE 2:** JAVIER ALEXANDER BLANCO LINDARTE…… AA2	
REGISTRO	**OBSERVACIÓN**
POLITICA DE SEGURIDAD: ASIGNACION DE ROLES DE SEGURIDAD, COORDINACIÓN, Y REVISION DE LA IMPLEMENTACION DE LA SEGURIDAD EN TODA LA UFPS OCAÑA.	Se observa que los roles están debidamente asignados y cada funcionario ejecuta su respectivo Rol.
DISPOSICION DE UNA FUENTE DE CONSULTORIA SOBRE SEGURIDAD DE LA INFORMACIÓN DENTRO DE LA UFPS OCAÑA.	Se observa que la institución cuenta con el servicio de consultoría dentro de un horario establecido de lunes a viernes de 7:a.m. a 12:00 m. y de 2:00 p.m. a 5:00 p.m.
COORDINACION DE LA SEGURIDAD DE LA INFORMACIÓN	Se detecta que solo se imparten capacitaciones con respecto a la seguridad de la información en el proceso de inducción al cargo y se observa que no cuentan con un cronograma que verifique que se tienen programadas dichas formaciones.
REVISION INDEPENDIENTE DE LA SEGURIDAD DE LA INFORMACIÓN	Se evidencia que en el CEDIT, los procesos de revisión independiente de la seguridad de la información, dependen exclusivamente del departamento de sistemas. Siendo nula su iteración en este caso.
ELABORÓ	**APROBÓ**

ANEXO E. AUDITORÍA EXTERNA

INFORME DE AUDITORIA DEFINITIVO	**AC-1**
EMPRESA: UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA	**FECHA ELABORACIÓN:** 04 DE MAYO DE 2014
AREA AUDITADA:CENTRO DE DESARROLLO E INNOVACIÓN TECNOLÓGICA	
OBJETIVO: Evaluar la seguridad interna de la información en el Centro de Desarrollo e Innovación Tecnológica de la Universidad francisco de Paula Santander Ocaña en el periodo comprendido entre el 14 de abril de 2014 al 05 de mayo de 2014; basado en el estándar internacional ISO/IEC 17799 – Unidad 6, Numeral 6.1, Ordinal 6.1.1.	
ALCANCE: Revisar el compromiso de la gerencia con la seguridad de la información, la coordinación de la seguridad de la información, la asignación de las responsabilidades de la seguridad de la información, la autorización de procesos para facilidades procesadoras de información, el contacto con las autoridades, el contacto con grupos de interés especial y la revisión independiente de la seguridad de la información.	
RESPONSABLE DEL PROCESO:PROFESIONAL DE APOYO CEDIT (JORGE FRANCISCO RINCÓN ANGARITA)	
AUDITOR LIDER: LINA FERNANDA MARTINEZ VEGA……..…..……. AL **AUDITOR ACOMPAÑANTE 1:** CLAUDIA DEL PILAR QUINTERO PRADO…… AA1 **AUDI** AA2	

Dando cumplimiento al Programa de Trabajo, nos permitimos entregar el Informe de Auditoría Definitivo efectuado al Centro de Desarrollo e Innovación Tecnológica de la Universidad Francisco de Paula Santander Ocaña en lo referente a la Seguridad de la Información, ante lo cual nos permitimos indicar que ha sido un placer ejercer tan grandiosa labor y que hemos contado en todo momento con la colaboración de la de todo el equipo de trabajo, a todos ellos gracias por su aporte.

Ahora nos permitimos remitir las situaciones que se detectaron y que resumen evidentemente lo examinado en la presente auditoría. Comencemos por decir que los procesos se encuentran efectivamente documentados y están firmemente soportados en los archivos: Plan Ordenamiento Territorial campus POTU, Plan de desarrollo 2014-2019, Presentación Universidad Francisco de Paula Santander Ocaña, Presupuesto 2014, Resolución CEDIT, Gestión de los sistemas de TI, Plan acción investigación 2014, Plan de Contingencia de TI - División de Sistemas, Caracterización Sistemas de Información, Telecomunicaciones y Tecnología, Manual Sistema de Información, Telecomunicaciones y Tecnología, Parametrización de los Sistemas Informáticos, Plan de Mantenimiento Preventivo - División de sistemas, Servicio Técnico y Tecnológico. Soporte y Atención al usuario, Gestión de la Configuración, Convenio Red Colsi -UFPS Ocaña, Administración de los Recursos Informáticos.

De igual manera el acceso a los mimos es práctico pues se encuentran en el portal web de la Institución, que se pude acceder en cualquier momento y sin ninguna restricción.

Luego de analizar y utilizar como soporte dichos documentos se aplicaron las herramientas necesarias y encontramos que no existen capacitaciones para brindar un adecuado manejo de la seguridad de la información. Por otra parte, el proceso cuenta con un horario establecido para solucionar las consultas externas, pero no se tiene en cuenta si después del horario establecido se debe solucionar alguna consulta; lo que evidencia ausencia de horarios adicionales para ofrecer servicio de consultaría.
Además no todas las especificaciones funcionales y análisis de requisitos del sistema tienen un formato determinado presentándose registros incompletos o mal llevados. Así también no se evidencian controles, políticas, procesos y procedimientos de la seguridad de la información de manera independiente y objetiva evidenciando falta de adaptación e implementación de controles, políticas y procedimientos generando desconocimiento del proceso en cuanto a sus funciones.

También se detectó que no se ha tenido en cuenta en el proceso un plan de acción independiente que le permita subsanar situaciones detectadas mediante auditorias demostrando la falta de un plan de acción de auditoría independiente que conlleva al no logro de los objetivos y metas propuestas por el proceso.

Muchos procesos presentan dependencia absoluta centralizada mostrando que los procesos de revisión independiente de la seguridad de la información, dependen exclusivamente del departamento de sistemas. Siendo nula la iteración del CEDIT en este caso.

Para continuar encontramos que los roles están debidamente asignados y cada funcionario ejecuta su respectivo Rol, sin embargo esta situación retarda la toma de decisiones prioritarias para el buen desempeño de la dependencia en lo referente a seguridad de la información. Lo que evidencia una vez más que los procesos en la organización se encuentran centralizados; retardando la rápida toma de decisiones.

Cordialmente, **EQUIPO AUDITOR**

ELABORÓ	**APROBÓ**

INFORME DE AUDITORIA PRELIMINAR	**AC-2**
EMPRESA: UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA	**FECHA ELABORACIÓN:** 30 DE ABRIL DE 2014
AREA AUDITADA:CENTRO DE DESARROLLO E INNOVACIÓN TECNOLÓGICA	
OBJETIVO: Evaluar la seguridad interna de la información en el Centro de Desarrollo e Innovación Tecnológica de la Universidad francisco de Paula Santander Ocaña en el periodo comprendido entre el 14 de abril de 2014 al 05 de mayo de 2014; basado en el estándar internacional ISO/IEC 17799 – Unidad 6, Numeral 6.1, Ordinal 6.1.1.	
ALCANCE: Revisar el compromiso de la gerencia con la seguridad de la información, la coordinación de la seguridad de la información, la asignación de las responsabilidades de la seguridad de la información, la autorización de procesos para facilidades procesadoras de información, el contacto con las autoridades, el contacto con grupos de interés especial y la revisión independiente de la seguridad de la información.	
RESPONSABLE DEL PROCESO:PROFESIONAL DE APOYO CEDIT (JORGE FRANCISCO RINCÓN ANGARITA)	
AUDITOR LIDER: LINA FERNANDA MARTINEZ VEGA…….…… AL **AUDITOR ACOMPAÑANTE 1:** CLAUDIA DEL PILAR QUINTERO PRADO…… AA1 **AUDITOR ACOMPAÑANTE 2:** JAVIER ALEXANDER BLANCO LINDARTE…… AA2	

Dando cumplimiento al Programa de Trabajo, nos permitimos socializar el Informe de Auditoría Preliminar efectuado al Centro de Desarrollo e Innovación Tecnológica de la Universidad Francisco de Paula Santander Ocaña en lo referente a la Seguridad de la Información, ante lo cual nos permitimos indicar que ha sido un placer ejercer tan grandiosa labor y que hemos contado en todo momento con la colaboración de la de todo el equipo de trabajo, a todos ellos gracias por su aporte.

Ahora nos permitimos remitir las situaciones que se detectaron y que resumen evidentemente lo examinado en la presente auditoría. Comencemos por decir que los procesos se encuentran efectivamente documentados y están firmemente soportados en los archivos: Plan Ordenamiento Territorial campus POTU, Plan de desarrollo 2014-2019, Presentación Universidad Francisco de Paula Santander Ocaña, Presupuesto 2014, Resolución CEDIT, Gestión de los sistemas de TI, Plan acción investigación 2014, Plan de Contingencia de TI - División de Sistemas, Caracterización Sistemas de Información, Telecomunicaciones y Tecnología, Manual Sistema de Información, Telecomunicaciones y Tecnología, Parametrización de los Sistemas Informáticos, Plan de Mantenimiento Preventivo - División de sistemas, Servicio Técnico y Tecnológico. Soporte y Atención al usuario, Gestión de la Configuración, Convenio RedColsi-UFPS Ocaña, Administración de los Recursos Informáticos.

De igual manera el acceso a los mimos es práctico pues se encuentran en el portal web de la Institución, que se pude acceder en cualquier momento y sin ninguna restricción.

Luego de analizar y utilizar como soporte dichos documentos se aplicaron las herramientas necesarias y encontramos que no existen capacitaciones para brindar un adecuado manejo de la seguridad de la información. Por otra parte, el proceso cuenta con un horario establecido para solucionar las consultas externas, pero no se tiene en cuenta si después del horario establecido se debe solucionar alguna consulta; lo que evidencia ausencia de horarios adicionales para ofrecer servicio de consultaría.

Además no todas las especificaciones funcionales y análisis de requisitos del sistema tienen un formato determinado presentándose registros incompletos o mal llevados. Así también no se evidencian controles, políticas, procesos y procedimientos de la seguridad de la información de manera independiente y objetiva evidenciando falta de adaptación e implementación de controles, políticas y procedimientos generando desconocimiento del proceso en cuanto a sus funciones.

También se detectó que no se ha tenido en cuenta en el proceso un plan de acción independiente que le permita subsanar situaciones detectadas mediante auditorias demostrando la falta de un plan de acción de auditoría independiente que conlleva al no logro de los objetivos y metas propuestas por el proceso.

Muchos procesos presentan dependencia absoluta centralizada mostrando que los procesos de revisión independiente de la seguridad de la información, dependen exclusivamente del departamento de sistemas. Siendo nula la iteración del CEDIT en este caso.

Para continuar encontramos que los roles están debidamente asignados y cada funcionario ejecuta su respectivo Rol, sin embargo esta situación retarda la toma de decisiones prioritarias para el buen desempeño de la dependencia en lo referente a seguridad de la información. Lo que evidencia una vez más que los procesos en la organización se encuentran centralizados; retardando la rápida toma de decisiones.

Cordialmente, **EQUIPO AUDITOR**

ELABORÓ	**APROBÓ**

PLAN DE AUDITORIA				**AC-3**
EMPRESA: UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA				**FECHA ELABORACIÓN:** 14 DE ABRIL DE 2014
AREA AUDITADA:CENTRO DE DESARROLLO E INNOVACIÓN TECNOLÓGICA				
OBJETIVO: Evaluar la seguridad interna de la información en el Centro de Desarrollo e Innovación Tecnológica de la Universidad francisco de Paula Santander Ocaña en el periodo comprendido entre el 14 de abril de 2014 al 05 de mayo de 2014; basado en el estándar internacional ISO/IEC 17799 – Unidad 6, Numeral 6.1, Ordinal 6.1.1.				
ALCANCE: Revisar el compromiso de la gerencia con la seguridad de la información, la coordinación de la seguridad de la información, la asignación de las responsabilidades de la seguridad de la información, la autorización de procesos para facilidades procesadoras de información, el contacto con las autoridades, el contacto con grupos de interés especial y la revisión independiente de la seguridad de la información.				
RESPONSABLE DEL PROCESO:PROFESIONAL DE APOYO CEDIT (JORGE FRANCISCO RINCÓN ANGARITA)				
AUDITOR LIDER: LINA FERNANDA MARTINEZ VEGA……..…… AL **AUDITOR ACOMPAÑANTE 1:** CLAUDIA DEL PILAR QUINTERO PRADO…… AA1 **AUDITOR ACOMPAÑANTE 2:** JAVIER ALEXANDER BLANCO LINDARTE…….. AA2				
REFERENCIA	**ACTIVIDAD O FUNCION A EVALUAR**	**PROCEDIMIENTOS DE AUDITORIA**	**HERRAMIENTAS QUE SERAN UTILIZADAS**	**OBSERVACION**
AC-9	Estudio general del proceso, estructura organizacional y manual de funciones	Reglamento interno del proceso	Lista de Chequeo	
AC-9	Conocer cuáles son los instrumentos en los cuales se apoyan en el proceso (Manuales, instructivos, políticas, reglamentos)	Manuales Instructivos Políticas Reglamentos	Lista de Chequeo	
AC-9	Análisis a través del estudio de las entradas y salidas del proceso en cuanto a su sistema de seguridad de la información	Caracterización del proceso	Lista de Chequeo	
AC-9 **AC-7**	Identificación y evaluación de los riegos potenciales en cuanto a la seguridad de la información.	Entrevista-Lista de verificación	Lista de Chequeo Registro de Entrevista	

AC-9	Análisis y evaluación de controles y seguridades a través de las técnicas de evaluación aplicadas a la seguridad de la información.	Lista de Chequeo	Lista de Chequeo	
AC-7 **AC-9** **AC-10**	Aplicación de pruebas de auditoria y obtención de evidencias	Papeles de Trabajo	Registro de Entrevista	
	Documentación del trabajo y elaboración del informe final	Informe Final		
ELABORÓ		**APROBÓ**		

FORMATO: RESUMEN DE DESVIACIONES DETECTADAS			AC-4
EMPRESA: UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA		**FECHA :** 18 AL 21 DE ABRIL DE 2014	
AREA AUDITADA:CENTRO DE DESARROLLO E INNOVACIÓN TECNOLÓGICA			
RESPONSABLE DEL PROCESO:PROFESIONAL DE APOYO CEDIT (JORGE FRANCISCO RINCÓN ANGARITA)			
AUDITOR LIDER: LINA FERNANDA MARTINEZ VEGA…… AL **AUDITOR ACOMPAÑANTE 1:** CLAUDIA DEL PILAR QUINTERO PRADO……..…. AA1 **AUDITOR ACOMPAÑANTE 2:** JAVIER ALEXANDER BLANCO LINDARTE…… AA2			
REFERENCIA	**SITUACIONES**	**CAUSAS**	**SOLUCION**
AC-7 **AC-9**	No existen capacitaciones para brindar un adecuado manejo de la seguridad de la información.	No existe plan estratégico para identificar que se debe asegurar la seguridad de la información.	Crear un plan de capacitaciones para dar a conocer información que se genere sobre el aseguramiento de la Seguridad de la información en un tiempo establecido.
AC-7 **AC-9**	No se evidencia la documentación detallada del proceso.	No tener documentado genera desconocimiento de lo que se hace dentro del proceso.	Debido a que la información que maneja el proceso se sugiere documentar el procedimiento detallado de sus actividades más relevantes.
AC-10 **AC-9**	El proceso cuenta con un horario establecido para solucionar las consultas externas, pero no se tiene en cuenta si después de horario establecido se debe solucionar alguna consulta.	Que se presente consultas por fuera del horario establecido y que sean de solución inmediata.	Establecer unos mecanismos que den soluciones a esas consulta hechas por fuera del horario establecido.
AC-7 **AC-9**	No todas las especificaciones funcionales y análisis de requisitos del sistema tienen un formato determinado	Registros incompletos o mal llevados.	Relacionar cada uno de los requisitos para que estos sean documentados y el proceso cumpla con lo estipulado en el logro de los objetivos propuestos.
AC7 **AC-9**	No se evidencian controles, políticas, procesos y procedimientos de la seguridad de la información de manera independiente y objetiva.	La falta de adaptación e implementación de controles, políticas y procedimientos genera desconocimiento del proceso en cuanto a sus funciones.	Desligar el proceso del CEDIT, del proceso de sistemas para que exista mayor eficacia en la operaciones realizadas y puedan realizar sus debidos controles.

AC-7 **AC-9**	No se ha tenido en cuenta en el proceso un plan de acción independiente que le permita subsanar situaciones detectadas mediante auditorias.	La falta de un plan de acción de auditoría independiente conlleva al no logro de los objetivos y metas propuestas por el proceso.	Plantear al proceso de sistemas que dentro del plan de auditoria que se ejecute se lleve a cabo el proceso del CEDIT, para determinar con esto un Plan de Acción.
ELABORÓ		**APROBÓ**	

FORMATO: SITUACIONES ENCONTRADAS					**AC-5**
EMPRESA: UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA				**FECHA:** 18 AL 21 DE ABRIL DE 2014	
AREA AUDITADA:CENTRO DE DESARROLLO E INNOVACIÓN TECNOLÓGICA					
RESPONSABLE DEL PROCESO:PROFESIONAL DE APOYO CEDIT (JORGE FRANCISCO RINCÓN ANGARITA)					
AUDITOR LIDER: LINA FERNANDA MARTINEZ VEGA……..…….. AL **AUDITOR ACOMPAÑANTE 1:** CLAUDIA DEL PILAR QUINTERO PRADO……..…. AA1 **AUDITOR ACOMPAÑANTE 2:** JAVIER ALEXANDER BLANCO LINDARTE……. AA2					
REFERENCIA	**SITUACION**	**CAUSAS**	**SOLUCION**	**FECHA DE SOLUCION**	**RESPONSABLE**
AC-10	Los roles están debidamente asignados y cada funcionario ejecuta su respectivo Rol, sin embargo esta situación retarda la toma de decisiones prioritarias para el buen desempeño de la dependencia en lo referente a seguridad de la información.	Procesos centralizados.	Replantear funciones y roles.	Agosto de 2014	Director CEDIT
AC-10	La institución cuenta con el servicio de consultoría dentro de un horario establecido de lunes a viernes de 7:a.m. a 12:00 m. y de 2:00 p.m. a 5:00 p.m., pero por fuera de este horario no se atienden consultas.	Ausencia de horarios adicionales para ofrecer servicio de consultaría.	Ofrecer nuevos horarios para extender el servicio de consultoría 7 días/ 24 horas.	Julio de 2014	Director UFPS Ocaña Jefe División de Sistemas
AC-10	Se imparten capacitaciones con respecto a la seguridad de la información, sin embargo no cuentan con un cronograma que	No se ha planeado un plan de capacitaciones dirigido a la seguridad de la información.	Hacer un plan de capacitaciones sobre seguridad de la información.	Julio a diciembre de 2014	Jefe de personal Jefe División de Sistemas

	verifique que se tienen programadas dichas formaciones.				
AC-10	Los procesos de revisión independiente de la seguridad de la información, dependen exclusivamente del departamento de sistemas. Siendo nula la iteración del CEDIT en este caso.	Procesos centralizados.	Replantear los procesos para permitir más la iteración del CEDIT en este caso.	Septiembre de 2014.	Director de la UFPS Ocaña Jefe División de Sistemas
ELABORÓ		**APROBÓ**			

PROGRAMA DE TRABAJO DE AUDITORIA						AC-6
EMPRESA: UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA				**FECHA DE ELABORACIÓN:** 16 DE ABRIL DE 2014		
AREA AUDITADA:CENTRO DE DESARROLLO E INNOVACIÓN TECNOLÓGICA						
OBJETIVO: Evaluar la seguridad interna de la información en el Centro de Desarrollo e Innovación Tecnológica de la Universidad francisco de Paula Santander Ocaña en el periodo comprendido entre el 14 de abril de 2014 al 05 de mayo de 2014.						
ALCANCE: Revisar el compromiso de la gerencia con la seguridad de la información, la coordinación de la seguridad de la información, la asignación de las responsabilidades de la seguridad de la información, la autorización de procesos para facilidades procesadoras de información, el contacto con las autoridades, el contacto con grupos de interés especial y la revisión independiente de la seguridad de la información.						
RESPONSABLE DEL PROCESO:PROFESIONAL DE APOYO CEDIT (JORGE FRANCISCO RINCÓN ANGARITA)						
AUDITOR LIDER: LINA FERNANDA MARTINEZ VEGA……. AL **AUDITOR ACOMPAÑANTE 1:** CLAUDIA DEL PILAR QUINTERO PRADO…… AA1 **AUDITOR ACOMPAÑANTE 2:** JAVIER ALEXANDER BLANCO LINDARTE…….. AA2						
FASE	**DESCRIPCION**	**ACTIVIDAD**	**NUM. DEL PERSONAL PARTICIPANTE**	**PERIODO ESTIMADO INICIO**	**PERIODO ESTIMADO TERMINO**	**DIAS HAB. EST.**
I	Manuales, documentación, entrevistas, listas de chequeo	**Visita Preliminar** • Solicitud de manuales, y Documentaciones. • Elaboración de entrevista, lista de chequeo. • Recopilación de la información.	3	17 de abril de 2014	17 de abril de 2014	1
II	Entrevistas, estructura orgánica, funciones, desempeño capacitaciones, condiciones de trabajo	**Desarrollo de la Auditoria.** • Aplicación de la entrevista al personal • Evaluación de la estructura orgánica: Puestos, funciones, autoridad y responsables. • Evaluar el desempeño, capacitaciones, condiciones de trabajo y recursos.	1	18 de abril de 2014	21 de abril de 2014	4

		• Evaluación de los sistemas • Evaluación del proceso de datos y de los equipos de cómputo: Seguridad de los datos, control de operación, seguridad de la información y sus procedimientos respaldos.				
III	Diagnóstico, papeles de trabajo, pre-informe	**Revisión y Pre-Informe** • Revisión de los papeles de trabajo • Determinación del diagnostico • Elaboración de la carta de Gerencia • Elaboración del Borrador	3	14 de abril de 2014	29 de abril de 2014	16
IV	Informe Final	**Informe** Elaboración y presentación del informe.	3	01 de mayo de 2014	04 de mayo de 2014	4
ELABORÓ		**APROBÓ**				

OFICIO DE PRESENTACIÓN INFORME DE AUDITORIA PRELIMINAR	**AC-11**
EMPRESA: UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA	**FECHA:** 30 de abril de 2014
AREA AUDITADA:CENTRO DE DESARROLLO E INNOVACIÓN TECNOLÓGICA	
RESPONSABLE DEL PROCESO:PROFESIONAL DE APOYO CEDIT (JORGE FRANCISCO RINCÓN ANGARITA)	
AUDITOR LIDER: LINA FERNANDA MARTINEZ VEGA…….…. AL **AUDITOR ACOMPAÑANTE 1:** CLAUDIA DEL PILAR QUINTERO PRADO……. AA1 **AUDITOR ACOMPAÑANTE 2:** JAVIER ALEXANDER BLANCO LINDARTE……. AA2	

Miércoles, 30 de abril de 2014

Señor
JORGE FRANCISCO RINCÓN ANGARITA
Profesional de Apoyo
Centro de Desarrollo e Innovación Tecnológica
Universidad francisco de Paula Santander Ocaña
E. S. M.

Respetado señor Rincón,

Me permito remitir a Usted el informe de Resultados de la Auditoría practicada a las instalaciones del Centro de Desarrollo e Innovación Tecnológica de la Universidad francisco de Paula Santander Ocaña; que se realizó del 14 de abril de 2014 al 29 de abril de 2014.

Sin otro particular,

LINA FERNANDA MARTINEZ VEGA (AL)

ELABORÓ	**APROBÓ**

OFICIO DE SOLICITUD DE AUTORIZACIÓN	**AC-12**
EMPRESA: UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA	**FECHA:** 18 de abril de 2014
AREA AUDITADA:CENTRO DE DESARROLLO E INNOVACIÓN TECNOLÓGICA	
RESPONSABLE DEL PROCESO:PROFESIONAL DE APOYO CEDIT (JORGE FRANCISCO RINCÓN ANGARITA)	
AUDITOR LIDER: LINA FERNANDA MARTINEZ VEGA…… AL **AUDITOR ACOMPAÑANTE 1:** CLAUDIA DEL PILAR QUINTERO PRADO…….. ..AA1 **AUDITOR ACOMPAÑANTE 2:** JAVIER ALEXANDER BLANCO LINDARTE…… AA2	

Viernes, 18 de abril de 2014

Señor
JORGE FRANCISCO RINCÓN ANGARITA
Profesional de Apoyo
Centro de Desarrollo e Innovación Tecnológica
Universidad francisco de Paula Santander Ocaña
E. S. M.

Respetado señor Rincón,

Me permito solicitar a Usted autorización para comenzar las visitas necesarias para desarrollar la auditoria, labor que se realizaráen las instalaciones del Centro de Desarrollo e Innovación Tecnológica de la Universidad francisco de Paula Santander Ocaña; entre las fechas comprendidas desde el día 18 de abril hasta el 29 de abril de 2014.

Sin otro particular,

LINA FERNANDA MARTINEZ VEGA (AL)

ELABORÓ	**APROBÓ**

ANEXO F. GUÍA TELEFÓNICA UFPS OCAÑA.

Universidad Francisco de Paula Santander Ocaña - Colombia

GUÍA TELEFÓNICA (Registrada por Dependencias)

DEPENDENCIA	EXT
Subdirección Académica	
Secretaria	127
Oficina Subdirector	128
Profesional de Apoyo	427 424
Asesor Jurídico Académico	425
Auxiliar Administrativo	426
Subdirección Administrativa	
Subdirector Administrativo	140
Secretaria	142
Profesional de Apoyo	141 143
Pagaduria	138
Tesorería	139
Contratación	423
Secretaria General	
Secretario General	145
Secretaria	146
División Investigación y Extensión	
Secretaria	178
Director DIE	180
Admisiones y Registro	
Jefe Admisiones	129
Secretaria	130
Oficina de Planeación	
Jefe de Planeación	123
Ingenieros	125
Secretaria	121
Dirección	
Secretaria	103
Fax	104
División de Personal	
Secretaria	115
Contratos y Nominas	120
Apoyo Profesional	420
Salud Ocupacional	421
Presupuesto	
Jefe de Presupuesto	422
Secretaria	118-119
Contabilidad	
Jefe de Contabilidad	113
Secretaria	110
Control Interno	
Secretaria	114
Sistema Integrado de Gestión	
Secretaria	134
Bienestar Universitario	
Jefe de Bienestar Universitario	176
Secretario	175
Enfermería	276
Psicología	278
Trabajo Social	279
Deportes	281
Cultura	431
Egresado	428
Medico	430
Asesoría Espiritual	276
Archivo	
Secretaria	508

DEPENDENCIA	EXT
Almacén	
Jefe de Almacén	510
Profesional de Apoyo en Inventarios	511
Auxiliar de Almacén	512
Secretaria	170
Biblioteca	
Secretaria	251
Prestamo y Devolución	252
Centro de Investigación, Desarrollo y Fomento Empresarial	
Coordinadora del CIDFE	501
Area de Gestión, Proyectos y Ormet	504
Area de Investigación	503
CEISS	502
Secretaria	166
Ventanilla Única	
Profesional Universitario	506
Historias Laborales	507
Secretaria	158
Conmutador	101
Consultorio Empresarial	216
Departamento de Ciencias Administrativas y Economicas	
Laboratorio y Consultorio Contable y Tributario	477
División de Sistemas	
Jefe de Sistemas	156
Secretaria (Fax)	151 165
Administrador del Sistema de Investigación Financiero	157
Profesional de apoyo de los Sistemas de Información	153 159 154
Administrador de servidores	274
Mantenimiento de Hardware y Software	152
Control de Salas (Bloque A)	172
Control de Salas (Bloque B)	403
Centro de Idiomas	
Secretaria	135
Facultad de Ingenierías	
Secretaria	210
Director Plan de Estudios e Ingeniería Mecánica	211
Secretaria Plan de Estudios de Ingeniería de Sistemas	213
Ciclos Propedeuticos	225
Secretaria Plan de Estudios de Ingeniería Civil	218
Director de Departamento de Ingeniería de Sistemas	229
Director de Plan de Estudios de Ingeniería Civil	
Director de Departamento de Ingeniería Mecanica	221
Grupo de Investigación GIGMA	509
Grupo de Investigación GITYD	182
Facultad de Ciencias Agrarias y del Ambiente	
Secretaria	498
Secretaria Plan de Estudio de Ingeniería Ambiental	209
Director de Plan de Estudio de Ingeniería Ambiental	207
Decano Facultad de Ciencias Agrarias y del Ambiente	206
Profesional de Apoyo de Autoevaluación de la Facultad	208
Director del Plan de Estudios de Zootecnia y Tecnología Agropecuaria	204
Secretaria de Plan de Estudios de Zootecnia y Tecnología Agropecuaria	201
Director de Departamento Pecuario	205
Facultad de Educación Artes y Humanidades	
Secretaria	214
Decano FEAH	240

Universidad Francisco de Paula Santander Ocaña - Colombia

GUÍA TELEFÓNICA (Registrada por Dependencias)

DEPENDENCIA	EXT
Plan de Estudios de Comunicación Social	470
Coordinadores Plan de Estudios de Comunicación Social	131
Plan de Estudios de Derecho	217
Unidades Académicas de la Facultad de Educación Artes y Humanidades	231
Facultad de Ciencias Administrativas y Económicas	
Secretaria	241
Decana FCAE	260
Consultorio Empresarial	216
Laboratorio y Consultorio Contable y Tributario	277
Ciclos Propedeuticos	239
Secretaria De Plan de Estudio de Contaduría Pública Diurna y nocturna	
Director Plan de Estudios Tecnología Gestion Comercial y Financiera	463
Dirrector Plan de Estudios de Administración	464
Director Plan de Estudios de Contaduría Pública Diurna	462
Director Plan de Estudios de Contaduría Pública Nocturna	461
Director Departamento de Ciencias Contables y Administrativas	468
Granja	
Secretaria	285
Jefe de Granja	286
Caseta Celadores Granja	299
Coordinación de Pasantías	234
División de Postgrados y Educación a Distancia	
Secretaria de Distancia	147
Secretaria de Posgrados	181
Jefe de Divisón de Posgrados y Educación a Distancia	275
Facepruo	177
Multimedios	
Jefe de Multimedios	409
Secretaria	402
Diseñador Gráfico	407
Desarrollador web	408
Unidad de Televisión	404
Relaciones Institucionales	
Jefe de Relaciones Institucionales	406
Secretaria	401
Concejo Superior Estudiantil	189
Centros de Estudio	
Centro de Estudios de Ingeniería de Sistemas	183
Centro de Estudios Tecnología Agropecuaria	184
Centro de Estudios de Zootecnia	185
Centro de Estudios de Ingeniería Mecànica	186
Centro de Estudios de Ingeniería Civil	187
Centro de Estudios de Ingenieria Ambiental	188
Centro de Estudios de Administración de Empresas	195
Centro de Estudios de Contaduría Pública	197
Centro de Estudios de Comunicación Social	198
Departamento de Ingeniería Civil	227
Departamento de Ingeniería Mecánica	221

DEPENDENCIA	EXT
Departamento de Ingeniería de Sistemas	229
Departamento Ciencias Básicas	472
Dpto. Ciencias Contables y Financieras	488
Departamento de Ciencias Contables y Administrativas	216
Departamentos de Humanidades	471
Cubículos de Docentes	
Gustavo Guerrero G.	221
Iván Rodríguez Carrascal	473
Juan Carlos Hernández - Wilson Castilla	236
Mary Bohórquez	219
Martha Peñaranda - Dewar Rico	488
Marilce Pacheco - José G. Areválo - Jorge Cañizares	226
Marco A. Montaña	474
Nelson Afanador - Torcoroma Velásquez	222
Rómel Gallardo - Éder Flórez	227
Ramòn Bayona - Albeiro Rosado - Thomas Barbosa	229
Ramón J. Lobo - Carmen liceth García - Miriam Meza	224
Sir A. Suárez - Maribel Cárdenas - Blanca M. Velasco	228
Laboratorios	
Laboratorio de Ictiología	191
Laboratorio de Química	193
Laboratorio de Biología	148
Laboratorio y Consultorio Contable y Tributario	477
Laboratorio de Comunicación Social (Radio-Televisión-Fotografía)	405
Laboratorio de Cárnicos	223
Laboratorio de Nutrición	194
Restaurante	171
Sala de Juntas (La Casona)	108
Servicios Administrativos	277
SINETRAUFPS	174
Lineas Directas	
Conmutador	5690088
	5695052
	5690519
	5695148
	5691540
Dirección	5610066
Subdirección Administrativa	5610010
Admisiones y Registro	5694977
División de Sistemas	5693055
Subdirección Académica	5692199
Emisora UFM	5612952
	5613833
Escuela de Bellas Artes Jorge Pacheco Quintero	5696269
Centro de Desarrollo e Innovación Tecnológica (CEDIT)	5610550
Cafetería (Bloque B)	410
Caseta de Celadores	296
Entrada UFPS Ocaña	297

ANEXO G. INFORME DE AUDITORÍA INTERNA.

	UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA			
	Documento **FORMATO INFORME DE AUDITORIA INTERNA**	Código **F-CI-CIN-018**	Fecha **27-05-2014**	Revisión **C**
	Dependencia **CONTROL INTERNO**	Aprobado **JEFE DE CONTROL INTERNO**		Pág. **79(107)**

INFORME DE AUDITORIA INTERNA			
PROCESO AUDITADO		**LIDER DEL PROCESO**	
Centro de Desarrollo e Innovación Tecnológica		Wilmar Alirio González Peinado	
OBJETIVO DE LA AUDITORIA		**ALCANCE**	
Verificar y evaluar los requisitos del Modelo Estándar de Control Interno MECI:1000:2005 y la Norma Técnica de Calidad en la Gestión Pública, Requisitos Legales, Requisitos del Cliente, ISO 14001: 2004, OHSAS 18001:2007		Inicia con la planeación de la auditoría y finaliza con la presentación del informe.	
CRITERIO DE LA AUDITORIA:	NTCGP: 1000:2009 y MECI: 1000:2005, Requisitos Legales, Requisitos del Cliente, ISO 9001.ISO 14001: 2004-OHSAS 18001:2007		
EQUIPO AUDITOR:	Kely Johanna Vega Vacca		
FECHA DE AUDITORIA:	26//06/2014	**FECHA DE ENTREGA DEL INFORME:**	14/07/2014
NOMBRE DEL AUDITADO		**CARGO**	
Wilmar Alirio González Peinado		Jefe del CEDIT	
Elkin Rojas Picón		Profesional de apoyo	
Jorge Francisco Rincón		Profesional de apoyo	
Claudia Ximena Tovar		Profesional de apoyo	

RESULTADOS DE AUDITORIA		
DESCRIPCION DEL HALLAZGO	**N C**	**OBSERVACION**
No se observa control de riesgos identificados por el CEDIT		**X**
El CEDIT, no tiene planificado mecanismos de medición, análisis y mejora con respectos a indicadores, satisfacción y medición del cliente externo para demostrar la conformidad de los requisitos del producto y/o servicio que ofrecen.		**X**
No se evidencia actividades como socializaciones, informes para asegurar la comunicación interna con los procesos a los que pertenecen.		**X**

FORTALEZAS DEL AREA O PROCESO

- El proceso cuenta con Infraestructura adecuada permitiendo ejecutar sus actividades de desarrollo e innovación tecnológica.
- El proceso utiliza el cómputo en la nube (Dropbox) para almacenar información, garantizando acceso y conservación de la misma.
- El CEDIT cuenta con responsabilidades y funciones definidas por cada uno de los integrantes de mismo, permitiendo garantizar el cumplimiento del plan de acción.
- El proceso actualizó el normograma en el nuevo módulo implementado en el SID, permitiendo reconocer la normatividad que los rige.
- El proceso utiliza mecanismos de comunicación externa y cuenta con evidencias de capacitación y divulgación, permitiendo la participación de la comunidad en general en sus actividades.
- El proceso utiliza los medios de comunicación institucional permitiendo la divulgación de información propia de sus actividades.
- El proceso identifica e implementa estrategias de seguridad y salud ocupacional con el acompañamiento de la coordinadora del sistema permitiendo generar espacios de pausas activas.

OPORTUNIDADES DE MEJORA

➢ Mejorar el manual de funciones en conjunto con la oficina de personal para que el CEDIT esté acorde a la actualización de la nueva estructura orgánica de la UFPSO. ➢ Determinar la secuencia e interacción del CEDIT, con los procesos institucionales, para garantizar la implementación y control de los documentos y registros. ➢ Coordinar con el proceso de investigación y el proceso de extensión las actividades propias del CEDIT. ➢ Asegurarse que el CEDIT establece y cumple con los objetivos de calidad trazados por la institución.
RELACIÓN DE ANEXOS

Firma auditor	**Firma auditado**

ANEXO H. PLAN DE MEJORAMIENTO.

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA			
Documento: **FORMATO PLAN DE MEJORAMIENTO**	Código: **F-CI-CIN-006**	Fecha: **08-05-2012**	Revisión: **B**
Dependencia: **CONTROL INTERNO**	Aprobado: **JEFE DE CONTROL INTERNO**		Pág.: **81(107)**

PROCESO / AREA:		DIE/CEDIT									
TIPO DE PLAN DE MEJORAMIENTO:		Institucional:		Proceso: X			Individual:				
No.	FEHA DEL HALLAZGO DD-MM-AAAA	FUENTE	TIPO HALLAZGO PNC/ NC/ AM	DESCRIPCION DEL HALLAZGO	CAUSAS	DESCRIPCION DE LA ACCION DE MEJORA	TIPO C/P/A M	FECHA IMPLEMENTACIÓN		INVOLUCRADOS Y RESPONSABLES	RECURSOS NECESARIOS (FINANCIERO, HUMANO, TECNOLOGICO)	INDICADOR
								INICIO	FINAL			
1	27-05-2014	Resultado de auditorias internas y externas	AM	No se observa control de riesgos identificados por el CEDIT	Inicio o creacion de la nueva dependencia del CEDIT.	Identificar y Establecer Mecanismos de control sobre los riesgos identificados y valorados que puedan afectar la satisfacción del cliente y el logro de los objetivos de la dependencia, mediante el diligenciamiento del plan de tratamiento de los riesgos y el respectivo seguimiento.	AM	01-08 2014	30-06-2015	Director CEDIT Y profesionales universitarios de la dependencia	Financiero: salarios del personal del CEDIT Humano: personal del CEDIT y personal de apoyo de otros procesos Tecnológico: equipos de computo	Elaboracion del plan de tratamiento de los riesgos % de cumplimiento del plan de tratamiento de los riesgos
2	27-05-2014	Resultado de auditorías internas y externas	AM	El CEDIT, no tiene planificado mecanismos de medición, análisis y mejora con respectos a indicadores, satisfacción y medición del cliente externo para demostrar la conformidad de los	No se aplicaban instrumentos de recolección de información, que midiera la satisfacción de sus clientes externos e internos.	Realizar el respectivo seguimiento y medición según la norma NTCGP 1000:2009, parágrafo **8.2.1** Satisfacción del cliente, Mediante el diseño de instrumentos que	AM	01-08 2014	19-12-2014	Funcionarios del CEDIT	Financiero: Salarios del personal del CEDIT Humano: Personal del CEDIT y personal de apoyo de otros procesos Tecnológico: Equipos de	Elaboracion de Instrumentos de recolección de datos para medir la satisfacción del cliente. % de cumplimiento de aplicación

				requisitos del producto y/o servicio que ofrecen.		permitan obtener información relevante en cuanto a indicadores del servicio que ofrece el CEDIT.					computo	de instrumentos de recolección de datos para medir la satisfacción del cliente.
3	27-05-2014	Resultado de auditorías internas y externas	AM	No se evidencia actividades como socializaciones, informes para asegurar la comunicación interna con los procesos a los que pertenecen.	Falta de coordinación de reuniones periódicas con los procesos a los cuales pertenece el CEDIT.	Coordinar con los directores de las dependencias involucradas, reuniones periódicas, para retroalimentar información y presentación de informes. Enviar informes ejecutivos de las actividades realizadas en el CEDIT, al proceso al que pertenece.	AM	01-08 2014	19-12-2014	Director CEDIT, Director DIE y profesionales universitarios de la dependencia	Financiero: Salarios del personal del CEDIT Humano: Personal del CEDIT y personal de apoyo de otros procesos Tecnológico: Equipos de computo	Reuniones periódicas con las direcciones de los procesos internos involucrados. Envío de informes ejecutivos al proceso que pertenece el CEDIT. % de cumplimiento de reuniones programadas.

ANEXO I. RECURSOS MATERIALES

CANTIDAD	RECURSO MATERIAL	DESCRIPCIÓN
1	Espacio físico	Salón de 35 metros cuadrados aproximadamente con buena iluminación, piso en tableta, techo cubierto, puerta de acceso segura, aire acondicionado de 18.000 btu, baño, sala de recepción.
12	Computadores personales	Equipos de cómputo con procesador Intel celeron de 1.7 GHz, disco duro de 320 GB, Memoria ram de 2 GB, monitor de 17", Mouse, Teclado.
36	Tomas dobles	Toma regulados con conexión de polo a tierra y a 110 v.
18	Escritorios	Mesas modulares de 1,2 metros de altura, 0,6 metros de largo y 1,5 metros de ancho
18	Sillas	Sillas giratorias aprobadas por salud ocupacional
3	Impresoras	Impresoras laser
1	Red	Red inalámbrica con cobertura para 12 equipos de computo
5	Archivador	Archivador vertical de cinco módulos o gavetas
	Varios	Elementos de aseo (1 escoba, trapero, detergente, ambientador líquido, desinfectante, paños)

ANEXO J. SITUACIONES DETECTADAS

Las situaciones que se detectaron y que resumen evidentemente lo examinado en la presente auditoría al CEDIT de la Universidad Francisco de Paula Santander Ocaña son:

1. Se encontró que no existen capacitaciones para brindar un adecuado manejo de la seguridad de la información.

2. Además no todas las especificaciones funcionales y análisis de requisitos del sistema tienen un formato determinado presentándose registros incompletos o mal llevados.

3. No se evidencian controles, políticas, procesos y procedimientos de la seguridad de la información de manera independiente y objetiva evidenciando falta de adaptación e implementación de controles, políticas y procedimientos generando desconocimiento del proceso en cuanto a sus funciones.

4. No se cuenta en el proceso un plan de acción independiente que le permita subsanar situaciones detectadas mediante auditorias demostrando la falta de un plan de acción de auditoría independiente que conlleva al no logro de los objetivos y metas propuestas por el proceso.

5. Muchos procesos presentan dependencia absoluta centralizada mostrando que los procesos de revisión independiente de la seguridad de la información, dependen exclusivamente del departamento de sistemas. Siendo nula la iteración del CEDIT en este caso. Situación que lleva al Director de la UFPS Ocaña y al Jefe de la División de Sistemas a proponer una solución para el mes de septiembre del año en curso.

6. Se encontró que los roles están debidamente asignados y cada funcionario ejecuta su respectivo Rol, sin embargo esta situación retarda la toma de decisiones prioritarias para el buen desempeño de la dependencia en lo referente a seguridad de la información. Lo que evidencia una vez más que los procesos en la organización se encuentran centralizados; retardando la rápida toma de decisiones.

ANEXO K. MATRIZ DE RIESGOS

Código	Causa	Descripción del Riesgo	Referencia	Relación	Probabilidad	Impacto	Rango PxI
RPO10-01	Administración de proyectos - Control	**Si** no existen capacitaciones para brindar un adecuado manejo de la seguridad de la información **puede ocasionar** retrasos en el proyecto debido al entrenamiento de los mismos	Punto 1	RPO10-01	0,30	0,80	0,24
RPO10-02	Administración de proyectos - Control	**Si** no existen capacitaciones para brindar un adecuado manejo de la seguridad de la información **puede ocasionar** sobrecostos en el proyecto debido al entrenamiento de los mismos	Punto 1	RPO10-02	0,30	0,40	0,12
RPO10-03	Administración de proyectos - Planificación	**Si** no todas las especificaciones funcionales y análisis de requisitos del sistema tienen un formato determinado **puede ocasionar** retrasos en el proyecto al presentarse registros incompletos o mal llevados	Punto 2	RPO10-03	0,30	0,20	0,06
RPO10-04	Administración de proyectos - Planificación	**Si** no se evidencian controles, políticas, procesos y procedimientos de la seguridad de la información de manera independiente y objetiva **puede ocasionar** retrasos en el proyecto debido a falta de adaptación e implementación de controles, políticas y procedimientos generando desconocimiento del proceso en cuanto a sus funciones	Punto 3	RPO10-04	0,30	0,80	0,24
RPO10-05	Administración de proyectos - Control	**Si** no se cuenta en el proceso un plan de acción independiente que le permita subsanar situaciones detectadas mediante auditorias **puede ocasionar** retrasos en el proyecto debido a la falta de un plan de acción de auditoría independiente que conlleva al no logro de los objetivos y metas propuestas por el proceso	Punto 4	RPO10-05	0,50	0,80	0,40
RPO10-06	Administración de proyectos - Control	**Si** no se cuenta en el proceso un plan de acción independiente que le permita subsanar situaciones detectadas mediante auditorias **puede ocasionar** sobrecostos en el proyecto debido a la falta de un plan de acción de auditoría independiente que conlleva al no logro de los objetivos y metas propuestas por el proceso	Punto 4	RPO10-06	0,50	0,80	0,40
RPO10-07	Administración de proyectos - Control	**Si** muchos procesos presentan dependencia absoluta centralizada mostrando que los procesos de revisión independiente de la seguridad de la información, dependen exclusivamente del departamento de sistemas. Siendo nula la iteración del CEDIT **puede ocasionar** retrasos en el proyecto a causa de las decisiones del departamento de sistema y ka dirección de la UFPS Ocaña	Punto 5	RPO10-07	0,50	0,40	0,20
RPO10-07	Administración de proyectos - Control	**Si** se encontra que los roles están debidamente asignados y cada funcionario ejecuta su respectivo Rol **puede ocasionar** retrasos en el proyecto debido a que esta situación retarda la toma de decisiones prioritarias para el buen desempeño de la dependencia en lo referente a seguridad de la información	Punto 6	RPO10-07	0,50	0,80	0,40
					PROMEDIO		**0,26**
			CALIFICACION DEL RIESGO GENERAL DEL PROYECTO **ALTO**				

Estrategias y Acciones	Contingencias y Respaldos	Reservas
Tranferir: Capacitar al personal en la formación requerida	Realizar las capacitaciones necesarias para el personal	Se dispondrá de un 2% en tiempo para desarrollar las actividades que garanticen la idoneidad del personal
Tranferir: Capacitar al personal en la formación requerida	Capacitar al personal en la formación requerida	Disponer de un 2% del presupuesto para la contratación
Aceptar- Mitigar: Llevar los registros bajo los formatos determinados y completos	Llevar los registros bajo los formatos determinados y completos	Orientar un 2% en tiempo para mitigar los retrasos ocasionados en el proyecto
Aceptar- Mitigar: Evidenciar controles, politicas, procesos y procedimientos de la seguridad de la información de manera independiente y objetiva	Evidenciar controles, politicas, procesos y procedimientos de la seguridad de la información de manera independiente y objetiva	Planificar un 1% del tiempo para construir evidenciar controles, politicas, procesos y procedimientos de la seguridad de la información de manera independiente y objetiva
Eliminar: Construir un plan de acción de auditoría independiente que conlleva al logro de los objetivos y metas propuestas por el proceso		
Eliminar: Construir un plan de acción de auditoría independiente que conlleva al logro de los objetivos y metas propuestas por el proceso		
Aceptar- Mitigar: Plantear políticas que permitan la independencia	Plantear políticas que permitan la independencia	Planificar un 1% del tiempo para planear las políticas que lleven a la independencia
Eliminar: Definir politicas que permita definir nuevos roles que permitan la oportuna y rapida toma de decisiones		

ANEXO L. PLAN DE CONTINUIDAD DEL NEGOCIO PARA EL CEDIT

El Plan de continuidad para el CEDIT de la UFPS Ocaña, se basa en la Norma ISO 22301, el Plan de Contingencia – División de sistemas – UFPS Ocaña, una auditoria externa aplicada al CEDIT, una auditoria interna realizada al CEDIT por Control Interno de la UFPS Ocaña, y el plan de mejoramiento derivado de la oficina de Planeación de la UFPS Ocaña.

OBJETO, ÁMBITO DE APLICACIÓN Y USUARIOS

Por qué se desarrolla este plan, sus objetivos, a que partes de la organización se aplica, y quienes deberían leerlo.

El Plan de continuidad del negocio se desarrolla porque permite establecer las actividades que el **CEDIT** debe seguir, en caso de que la **UFPS Ocaña**, ante una contingencia, active su Plan de Contingencia, además de: Garantizar la seguridad de la información, Identificar los documentos esenciales para darles prioridad ante una emergencia, Ayudar a evacuar los documentos para evitarles algún tipo de daño, y Coordinar actividades tendientes a la atención de una emergencia.

DOCUMENTOS DE REFERENCIA

¿Qué documentos se relacionan en este plan? Normalmente, se trata de la Política de Continuidad de Negocios, Análisis de Impacto de Negocios, Estrategia de Continuidad de Negocio, etc.

Los documentos que se relacionan para el plan de continuidad se basan en el Sistema Integrado de Gestión, que es una filosofía adoptada por la Universidad Francisco de Paula Santander Ocaña para dirigir y evaluar el desempeño institucional orientado al mejoramiento de los productos y/o servicios que se ofrecen al estudiante y a la sociedad. El cual se encuentra debidamente documentado para consulta y de fácil acceso a través del portal web http://www.ufpso.edu.co/sig/. Estos documentos son: Guía para la administración del riesgo, y Plan de contingencia de TI - División de Sistemas.

SUPUESTOS

Los requisitos previos que deben existir para que este plan sea eficaz.

Los requisitos previos que deben existir para que el Plan de continuidad del Negocio para el CEDIT sea eficaz son: Apoyo de la alta dirección de la **UFPS Ocaña**, existencia del plan de contingencia, reservas financieras, socialización previa del Plan de Continuidad para distribuir funciones y responsabilidades, establecer y mantener comunicación con contactos clave.

FUNCIONES Y RESPONSABILIDADES

¿Quiénes serán responsables de la gestión del incidente perturbador?, y ¿quién está autorizado para realizar ciertas actividades en caso de un incidente perjudicial?

Los responsables de la gestión del incidente en el CEDIT, basados en el Plan de Contingencia de la División de sistemas de la UFPS Ocaña, se establecen como un equipo de trabajo con las funciones y responsabilidades que deberán ejecutar en caso de presentarse una eventualidad identificada. Es importante tener en cuenta, que los roles pueden ser asumidos por una o más personas de acuerdo al grado de conocimiento y responsabilidad. Estos son: Responsable de la ejecución del Plan, Coordinador de Servidores, Coordinador de Redes y Comunicaciones, Coordinador de Soporte Técnico, Coordinador de Sistemas, y Personal Clave.

Estos a su vez asumen sus roles así:

Rol, funciones y responsabilidades.

ROL	FUNCIONES Y RESPONSABILIDADES
Responsable de la ejecución del Plan de Contingencia – Director Dependencia	Es el responsable de aprobar la realización del Plan, dirigir los comunicados de concientización y solicitud de apoyo a los jefes y/o directivos de las diferentes áreas involucradas. Una vez concluida la realización del Plan, el Responsable tendrá como función principal, verificar que se realicen reuniones periódicas, cuando menos cada seis meses, en donde se informe de los posibles cambios que se deban efectuar al plan original y de que se efectúen pruebas del correcto funcionamiento, cuando menos dos veces al año o antes si se presentan circunstancias de cambio que así lo ameriten. Al declararse una contingencia, deberá tomar las decisiones correspondientes a la definición de las ubicaciones para instalar los equipos de cómputo alternos y comunicará a las directivas los costos para los gastos necesarios y el cronograma para la restauración del ambiente de trabajo.
Coordinador de Servidores	Tendrá como función principal asegurar que se lleven a cabo todas las fases para la realización del Plan, registrará las reuniones que se realicen y mantendrá actualizadas las bitácoras de monitoreo a servidores. Durante la realización del plan, una de sus actividades principales será la coordinación de la realización de las pruebas de los equipos de cómputo alternos, la restauración de datos e instalación de BD. Una vez que se encuentre aprobado el Plan, será el Coordinador General quien lleve a cabo formalmente la declaración de una contingencia grave y de inicio formal de la aplicación del Plan,

	cuando así lo considere conveniente, propiciando que la contingencia desaparezca con el objeto de continuar normalmente con las actividades; será el responsable de dar por concluida la declaración de contingencia. En conjunto con el responsable del Plan llevarán a cabo la toma de decisiones.
Coordinador de Redes y Comunicaciones	Es el responsable de determinar los procedimientos a seguir en caso de que se presente una contingencia que afecte las comunicaciones, servicios de internet, intranet, correo electrónico y red, mantener actualizados dichos procedimientos en el Plan, determinar los requerimientos mínimos necesarios, tanto de equipo como de software, servicios, líneas telefónicas, cuentas de acceso a Internet, enlaces dedicados, dispositivos de comunicación (ruteadores, switchs, antenas etc). Asimismo, deberá mantener actualizado el inventario de equipo de telecomunicaciones y redes, efectuar los respaldos correspondientes y llevar a cabo las pruebas de operatividad necesarias, para asegurar la continuidad del servicio, en caso de que se llegara a presentar alguna contingencia, ya sea parcial, grave o crítica. El coordinador de comunicaciones es el responsable de mantener el directorio de contactos, proveedores y usuarios de los servicios antes descritos y mantenerlo permanentemente actualizado e incluirlo dentro del Plan. Deberá realizar los procedimientos correspondientes para la emisión de los respaldos de cada uno de los servidores o equipos críticos y asegurar la actualización de datos. Coordinará las actividades correspondientes a los servicios de comunicaciones al declararse una contingencia, hasta su restablecimiento total.
Coordinador de Soporte Técnico	Es el responsable de llevar a cabo el inventario de equipo, software y equipos periféricos, como impresoras, escáneres, fotocopiadoras, etc.; mantener los equipos en óptimas condiciones de funcionamiento; determinar la cantidad mínima necesaria de equipo y sus características para dar continuidad a las operaciones de la Institución; es responsable de elaborar o coordinar con los usuarios los respaldos de información. Efectuar y mantener actualizado el directorio de proveedores de equipos, garantías, servicio de mantenimiento y reparaciones, suministros, en su caso, e incluirlo dentro del Plan. En caso de que se declare alguna contingencia que afecte a los equipos y al software, sea cual fuere su grado de afectación, es el responsable de restablecer el servicio a la brevedad, con el objeto de que no se agrave el daño o se llegara a tener consecuencias mayores.

	Para tal efecto debe participar en pruebas del Plan en conjunto con los demás participantes, con el objeto de estar permanentemente preparado para actuar en caso de contingencia.
Coordinador de Sistemas	Será el responsable de determinar los sistemas de información, módulos y procedimientos críticos de la Institución, que en caso de presentarse alguna contingencia como corte de energía eléctrica prolongada, temblor, incendio, falla del sistema de cómputo, pérdida de documentación, o alguna otra causa determinada, se llegara a afectar sensiblemente la continuidad de las operaciones en las áreas que utilicen dichos sistemas. En caso de cambiar a otras instalaciones alternas, el Coordinador de sistemas deberá definir cuáles serían las actividades que se deberán seguir para la configuración o instalación de los sistemas desarrollados, optimizando los recursos con los que se cuente, realizando las pruebas necesarias hasta su correcto funcionamiento en las terminales destinadas para su operación. Deberá mantener actualizados los Manuales de Usuario, resguardándolos fuera de las instalaciones para su consulta y utilización al momento de requerirse.
Personal clave	Es el responsable de la aplicación de los procedimientos, instructivos y actividades que describa el Plan para cada una de las diferentes circunstancias o contingencias previstas y de reportar con la periodicidad que se indique en el plan, al Coordinador de su área y al jefe de la división, los resultados de la aplicación de alguna de las fases del plan. Coordinarán con el personal de la Institución involucrado, la realización de las actividades contenidas en el Plan para la situación que se hubiera presentado y tratar por todos los medios que les sea posible el logro de los objetivos y asegurar la continuidad de las operaciones, disminuyendo el impacto de la contingencia al mínimo. Darán aviso al Coordinador de su área, cuando a su juicio, las circunstancias que provocaron la activación del plan hubieran desaparecido y se estuviera en condiciones de continuar normalmente con las actividades. En caso de requerir de actividades complementarias para regresar a las actividades normales, especialmente cuando se trate de los sistemas de información, deberán incluir el plan de actividades que se deberá seguir para retornar a la situación normal, prestar el apoyo técnico, operativo y toda la colaboración necesaria.
Usuarios (funcionarios) de la UFPS Ocaña	El personal usuario en general, al verse afectado por una situación de contingencia, deberá en primera instancia apoyar para salvaguardar las vidas propias y de sus compañeros de trabajo, cuando la situación que se estuviera presentado sea grave

	(incendio, temblor, etc.); posteriormente, y en la medida en que la situación lo permita, deberá coadyuvar a salvaguardar los bienes de la Universidad (el propio inmueble, equipos, documentación importante, etc.). Con posterioridad a la crisis inicial, deberá apoyar a solicitud del Coordinador de su área y/o del personal clave del Plan, en la toma del inventario de daños, para lo cual deberá seguir las instrucciones generales que se indiquen. En forma alterna, deberá dar cumplimiento a las instrucciones que se incluyan en el Plan para darle continuidad a las funciones informáticas críticas, siguiendo los procedimientos establecido, con la salvedad de que deberá, en forma creativa y responsable, adaptarlos a las circunstancias de limitación que represente el cambio de ubicación de las diferentes áreas involucradas en los procesos y la utilización de recursos de cómputo, mensajería, comunicaciones, etc., limitados. Al declararse concluida la contingencia, deberá participar activamente en la restauración de las actividades normales, esto es, apoyar en la movilización de documentación, mobiliario, etc., a las instalaciones originales o al lugar que le sea indicado, hasta la estabilización de las actividades. Cuando sea necesario, deberá participar en la capacitación del personal eventual que hubiera sido necesario.

Fuente: Plan de Contingencia – División de Sistemas – UFPS Ocaña

CONTACTOS CLAVE

Datos de contacto de las personas que participarán en la ejecución del plan de continuidad del negocio.

Los datos de contacto de las personas que participarán en la ejecución del plan de continuidad del negocio para el **CEDIT** son en primera instancia el directorio de la **UFPS Ocaña**, y por otra parte los números de las autoridades y entidades de emergencias tales como: Policía Nacional (5611128), Hospital (5611940), Bomberos (119 – 5611002), Defensa Civil, Cruz Roja, Ejercito Nacional; entre otras.

PLAN DE ACTIVACIÓN Y DESACTIVACIÓN

¿En qué casos se pueden activar el plan, y el método de activación?; ¿qué condiciones deben existir para desactivar el plan?

Para activar el Plan de continuidad del negocio del **CEDIT** en necesario detectar una situación que represente un riesgo.

De igual manera es responsabilidad de todos los miembros de la organización (Personal Clave) informar el momento en el cual a su juicio las circunstancias que provocaron la activación del plan hubieran desaparecido y se estuviera en condiciones de continuar normalmente con las actividades. Después de evaluar la situación, el Director del CEDIT debe decidir si se puede desactivar el Plan.

COMUNICACIÓN

¿Qué medios de comunicación se utilizarán entre los diferentes equipos y con otras partes interesadas durante el incidente perturbador?, ¿Quién está a cargo de la comunicación con cada parte interesada?, y las normas especiales de comunicación con los medios de comunicación y agencias de gobierno.

Los medios de comunicación utilizados por el **CEDIT,** durante el incidente perturbador, entre los miembros de la organización y los entes externos son: **primero** la comunicación directa, **segundo** el servicio de chat institucional, **tercero** el correo institucional, **cuarto** el servicio telefónico, **quinto** los servicios de telefonía celular, **sexto** portal web, **séptimo** la correspondencia escrita, **octavo** el servicio de mensajero.

Para cada caso, los responsables son todos los miembros de la organización dentro de su rol.

RESPUESTA A INCIDENTES

¿Cómo reaccionar inicialmente a un incidente con el fin de reducir el daño?
En todas las situaciones de emergencia hay que controlar el pánico. Dada una situación de emergencia, la prioridad es asegurar la seguridad de las personas y alertar a las entidades pertinentes (Bomberos, Defensa Civil, Policía, etc.).

De ser posible hay que localizar el origen del siniestro y tratar de neutralizarlo sin tomar riesgos que puedan atentar contra la vida, esto se puede lograr a través del correcto uso de extintores, la suspensión de las redes de agua, de electricidad y de datos entre otros. Una vez controlada la situación, se procederá a determinar la magnitud de los daños.

Los incidentes identificados en el **CEDIT** se especifican en los siguientes grupos: Movimiento Telúrico, Incendio, Inundación y Humedad, Corte de Energía, Fallas en la red de Voz y Datos, Fallas en Hardware o Software, Sabotaje o Daño Accidental, Vandalismo, y Paro o Manifestaciones. Estas situaciones se describen a continuación:

Movimiento Telúrico.

Sin pérdida o daños menores del edificio: El siniestro puede afectar únicamente parte de la estructura del edificio, en cuyo caso no se verían afectados los datos, sin embargo, podría ser necesario evacuar las instalaciones trasladando al personal fuera del edificio; el impacto que provocaría sería menor, puesto que las actividades se interrumpirían por unas horas o a hasta por un día completo.

Con pérdida del edificio: La pérdida de las instalaciones afectaría gravemente a las operaciones de la Sede y los datos pueden verse dañados seriamente. En esta parte de la contingencia es donde se requiere que todas las medidas de emergencia y de recuperación funcionen adecuada y oportunamente.

Incendio.

Área de sistemas: Se tiene gran impacto en la información ya que los sistemas utilizados residen en los Servidores y dispositivos de comunicación localizados en la División y en caso de sufrir algún daño, se requerirá adquirir nuevos equipos, así como de instalar nuevamente los sistemas, configurar los servidores y restaurar los respaldos para continuar trabajando.

Áreas distintas al sitio de cómputo: Un incendio dependiendo de su magnitud, puede afectar desde las estaciones de trabajo o periféricos y dispositivos de comunicación (racks) localizados en las áreas administrativas. En el caso de las primeras el impacto que tendría es medio alto, puesto que la información o tiempo de operación que se pierde no tiene gran repercusión en las operaciones generales, ya que puede restablecerse en un tiempo relativamente corto, pero en el caso de las comunicaciones si pueden afectar en gran medida la operación del servicio.

Inundación y Humedad.

Puesto que es equipo electrónico el que se maneja dentro de la institución, una inundación severa dañaría los dispositivos irremediablemente deteniendo las operaciones de la misma totalmente.

Un daño grave correspondería a una inundación en la División de Sistemas, en tanto que una inundación parcial o limitada a parte de las instalaciones (no al Centro de Cómputo) podría sólo ocasionar un daño medio sí no va seguido de corto circuito. Por otro lado, teniendo en cuenta el datacenter la recuperación de los datos sería relativamente rápido aunque no sería lo mismo para los equipos servidores.

Corte de Energía.

Las operaciones informáticas se detendrían, puesto que los dispositivos en los que se trabaja dependen de la corriente eléctrica para su desempeño. Si el corte eléctrico dura poco tiempo las operaciones no se ven afectadas gravemente, pero si el corte se prolongara por tiempo indefinido se provocaría un trastorno en las operaciones del día, sin afectar los datos. Actualmente no se cuenta con una planta eléctrica, de manera que la capacidad de restablecer la energía inmediatamente después de la perdida de luz es nula.

Los equipos servidores cuentan con una UPs, para entrar inmediatamente después del corte de energía y evitar daños en los equipos.

Fallas en la red de Voz y Datos.

Red: Representa la columna vertebral de las operaciones, si la red falla en su totalidad, las operaciones se detienen con la consecuente falta del servicio informático.

Aplicaciones: La falla en los sistemas utilizados, representa un impacto medio en las operaciones totales, ya que pueden ser reinstalados casi de inmediato.

Fallas en Hardware o Software.
Las alteraciones que sufran los servidores tanto en Hardware y Software pueden ser corregidas en la mayoría de los casos, sin embargo si las alteraciones llegan a ser tan grandes que el tiempo requerido para el inicio de las operaciones normales puede extenderse hasta por días.

Sabotaje o Daño Accidental.
La alteración de la información requiere de la restauración de los respaldos y de pruebas posteriores para contar con la integridad de los datos. Es posible que se requieran re procesos de captura de datos, dependiendo de las fechas de los respaldos que se tengan disponibles y del volumen de transacciones realizadas manualmente.

Vandalismo, Paro o Manifestaciones.

Un intento de vandalismo ya sea menor o mayor, podría afectar a las PC's, periféricos y servidores así como las comunicaciones. Si el intento de vandalismo es mayor, se presenta un grave riesgo dentro del área de la División ya que puede dañar los dispositivos y por consecuencia las actividades se verían afectadas en su totalidad, así como el servicio proporcionado.

SITIOS FÍSICOS Y TRANSPORTE

Son los sitios primarios y alternativos, en los puntos de concentración, y cómo llegar de los primarios a sitios alternativos.

Para el **CEDIT** los sitios primarios se encuentran situados en el parqueadero de la sede La Primavera, mientras que los alternos para continuar las labores de forma normal, son las sedes de la **UFPS Ocaña**; las cuales se describen así:

Sede Principal. Vía Acolsure, Sede el Algodonal - Ocaña Norte de Santander.
Sede Bellas Artes. Calle 10 # 13-64, Centro - Ocaña Norte de Santander.

Sede La Primavera. Calle 7 # 29-235, Piso 1 Avenida Francisco Fernández de contreras, Ocaña Norte de Santander.

En cuanto al transporte, se debe contar con los recursos necesarios y los contactos para la respectiva contratación de los medios de transporte para trasladar los equipos necesarios para

dar continuidad a las actividades del **CEDIT**. Se estipula un 10% del salario mínimo como valor de referencia a cancelar por recorrido. El valor del transporte depende de los materiales a transportar y ello se deriva del incidente a resolver.

ORDEN DE RECUPERACIÓN PARA LAS ACTIVIDADES

Lista de todas las actividades, con precisión Objetivo de Tiempo de Recuperación (RTO) para cada uno.

LOS PLANES DE RECUPERACIÓN PARA LAS ACTIVIDADES

Descripción del paso a paso de las acciones y responsabilidades de mano de obra en recuperación, instalaciones, infraestructura, software, información y procesos, incluyendo las interdependencias e interacciones con otras actividades y partes interesadas externas.

Los planes de recuperación para las actividades del CEDIT se describen como:

Valoración de las necesidades materiales y recursos económicos necesarios para efectuar el plan de recuperación.

Organización de brigadas de trabajo, operaciones de salvaguarda.

Preparación de un informe describiendo los sucesos acontecidos, costos y requerimientos.

Es importante anexar evidencias de los documentos e instalaciones afectadas. Estos datos serán necesarios para el expediente de la aseguradora en el caso de que exista un seguro.

Adecuación de espacios para el almacenamiento de la documentación afectada y para adelantar acciones de recuperación y descarte.

Elección de los métodos de tratamiento de la documentación de acuerdo al tipo de daño y tipo de documentos a tratar.

PLAN DE RECUPERACIÓN DE DESASTRES

Esto es normalmente un tipo de plan de recuperación que se centra en la recuperación de la infraestructura de tecnología de la información y la comunicación.

Para el Plan de recuperación de desastres se hacen relevantes aspectos como: Seguridad Física y Seguridad Lógica. Estas se describen a continuación:

Seguridad Física.

Garantiza la integridad de los activos lógicos y materiales de un sistema de información y de su infraestructura. Desde el edificio en donde se encuentran ubicados los dispositivos el

enfoque debe ser a cubrir las amenazas ocasionadas tanto por el hombre como por la naturaleza del medio físico del entorno.

El nivel adecuado de seguridad física, o grado de seguridad, es un conjunto de acciones utilizadas para evitar el fallo o para aminorar las consecuencias que de él se puedan derivar. Algunos aspectos a considerar son: Ubicación del Centro de Procesamiento de Datos dentro del edificio, Potencia eléctrica, Sistemas contra Incendios, Control de accesos, Selección de personal, Medidas de protección.

Las principales amenazas que se prevén en la seguridad física son: 1. Desastres naturales, incendios accidentales e inundaciones, 2. Amenazas ocasionadas por el hombre, 3. Disturbios, sabotajes internos y externos deliberados.

A continuación se analizan los peligros más importantes que se corren en un centro de procesamiento; con el objetivo de mantener una serie de acciones a seguir en forma eficaz y oportuna para la prevención, reducción, recuperación y corrección de los diferentes tipos de riesgos.

Incendios. Los incendios son causados por el uso inadecuado de combustibles, fallas de instalaciones eléctricas defectuosas y el inadecuado almacenamiento y traslado desustancias peligrosas.

Es considerado el enemigo número uno de los equipos de cómputo ya que puede destruir fácilmente los archivos de información y programas. Algunos factores a contemplar para reducir los riesgos de incendio: No debe estar permitido fumar en el área de proceso, Deben emplearse muebles incombustibles y cestos metálicos para papeles, El piso y el techo en el recinto del centro de cómputo y de almacenamiento de los medios magnéticos deben ser impermeables.

Es necesario proteger los equipos de cómputo instalándolos en áreas en las cuales el acceso a los mismos sólo sea para personal autorizado. Además, es necesario que estas áreas cuenten con los mecanismos de ventilación y detección de incendios adecuados.

Para protegerlos se debe tener en cuenta que: 1. La temperatura no debe sobrepasar los 18º C y el límite de humedad no debe superar el 65% para evitar el deterioro, 2. El centro de cómputo debe estar provisto de equipo para la extinción de incendios en relación al grado de riesgo y la clase de fuego que sea posible en ese ámbito, 3. Deben instalarse extintores manuales (portátiles) y/o automáticos (rociadores).

Recomendaciones

El personal designado para usar extinguidores de fuego debe ser entrenado en su uso.

Implementar paredes protectoras de fuego alrededor de las áreas que se desea proteger del incendio que podría originarse en las áreas adyacentes (cuarto de servidores).

Proteger el sistema contra daños causados por el humo. Este, en particular la clase que es principalmente espeso, negro y de materiales especiales, puede ser muy dañino y requiere una lenta y costosa operación de limpieza.

Mantener procedimientos planeados para recibir y almacenar abastecimientos de papel

Inundaciones. Se las define como la invasión de agua por exceso de escurrimientos superficiales o por acumulación en terrenos planos, ocasionada por falta de drenaje ya sea natural o artificial.

Instalaciones Eléctricas. Esta es una de las principales áreas a considerar en la seguridad física. En la medida que los sistemas se vuelven más complicados se hace más necesaria aplicar las soluciones que estén de acuerdo con una norma de seguridad industrial.

Las subidas (picos) y caídas de tensión no son el único problema eléctrico al que se han de enfrentar los usuarios. También está el tema del ruido que interfiere en el funcionamiento de los componentes electrónicos. El ruido interfiere en los datos, además de favorecer la escucha electrónica.

Los cables que se suelen utilizar para construir las redes locales van del cable telefónico normal al cable coaxial o la fibra óptica. Es importante supervisar su disposición con los cables instalados para evitar el tiempo y el gasto posterior, y de forma que se minimice el riesgo de un corte, rozadura u otro daño accidental.

Los riesgos más comunes para el cableado se pueden resumir en los siguientes:

Interferencia. Estas modificaciones pueden estar generadas por cables de alimentación de maquinaria pesada o por equipos de radio o microondas. Los cables de fibra óptica no sufren el problema de alteración (de los datos que viajan a través de él) por acción de campos eléctricos, que si sufren los cables metálicos.

Corte del cable. La conexión establecida se rompe, lo que impide que el flujo de datos circule por el cable.

Daños en el cable. Los daños normales con el uso pueden dañar el recubrimiento que preserva la integridad de los datos transmitidos o dañar al propio cable, lo que hace que las comunicaciones dejen de ser fiables.

Sistema de aire acondicionado. Se debe proveer un sistema de calefacción, ventilación y aire acondicionado separado, que se dedique al cuarto de servidores y equipos de proceso de datos en forma exclusiva. Teniendo en cuenta que los aparatos de aire acondicionado son causa potencial de incendios e inundaciones, es recomendable instalar redes de protección en todo el sistema de cañería al interior y al exterior, detectores y extinguidores de incendio, cámaras de vigilancia y alarmas efectivas.

Amenazas ocasionadas por el hombre. Los componentes de la infraestructura tecnológica son posesiones valiosas de la Institución y pueden estar expuestas. Es frecuente que los usuarios utilicen los equipos de cómputo de la institución para realizar trabajos privados y de esta manera, utilicen tiempo de máquina.

La información importante o confidencial puede ser fácilmente copiada. El software, es una propiedad muy fácilmente de sustraer y los discos o cintas son fácilmente transportados y llevados fuera del recinto.

Recomendaciones

Todos los equipos que componen la infraestructura tecnología de la institución deben estar instalados de manera no fácil de sustraer o acceder. Su posicionamiento y ubicación se debe registrar y auditar de manera frecuente.

El uso que los funcionarios de la institución dan a los diferentes componentes de la infraestructura tecnológica debe estar registrado y se deben comunicar las políticas de buen uso y responsabilidad.

Disturbios, Sabotajes internos y externos deliberados. Para el control de acceso al cuarto de servidores a cualquier personal ajeno a la institución y/o División de sistemas se le tomarán los datos y se registrará el motivo de la visita, hora de ingreso y de salida.

El uso de carnés de identificación es uno de los puntos más importantes del sistema de seguridad, a fin de poder efectuar un control eficaz del ingreso y egreso del personal a los distintos sectores de la Institución. En este caso la persona se identifica por algo que posee, por ejemplo un documento de identificación para los externos.

Otro mecanismo de seguridad, es el circuito cerrado de televisión; herramienta útil para el control y monitoreo de los espacios libres y algunos cerrados a fin de chequear el curso normal de actividades.

Seguridad Lógica

Es importante recalcar que la mayoría de los daños que puede sufrir un centro de cómputo no será sobre los medios físicos sino contra información por él almacenada y procesada.

El activo más importante que se posee la institución es la información, y por lo tanto deben existir técnicas, más allá de la seguridad física, que la aseguren.
La Seguridad Lógica consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo.

Los objetivos que se plantean son:

Restringir el acceso a los programas y archivos de acuerdo al tipo de usuario.

Asegurar que los usuarios puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.

Asegurar que se estén utilizados los datos, archivos y programas correctos en y por el procedimiento correcto.

Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro.

Que la información recibida sea la misma que ha sido transmitida.

Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos. Por ejemplo: un buen canal de comunicación físico, por correo o telefónico.

Que se disponga de pasos alternativos de emergencia para la transmisión de información. Por ejemplo: servidores de respaldo.

Controles de Acceso. Estos controles pueden implementarse en el Sistema Operativo, sobre los sistemas de aplicación, en bases de datos, en un paquete específico de seguridad o en cualquier otro utilitario.

Constituyen una importante ayuda para proteger al sistema operativo de la red, al sistema de información y demás software de la utilización o modificaciones no autorizadas; para mantener la integridad de la información (restringiendo la cantidad de usuarios y procesos con acceso permitido) y para resguardar la información confidencial de accesos no autorizados.

Los siguientes, son los requisitos mínimos de seguridad en cualquier sistema: Identificación y Autentificación, Roles, Transacciones, Limitaciones a los Servicios, Modalidad de Acceso, Ubicación y Horario, Control de Acceso Interno, Control de Acceso Externo, y Administración.

En este punto es necesario resaltar que los sistemas de información son de tipo cliente / servidor, su acceso es local y no se accede vía Web. Solo en el caso de módulos de manejo por estudiantes, algunas funcionalidades han sido desarrolladas para acceder por Internet.

Las actividades para la creación de roles, privilegios y administración de usuarios, se encuentran definidas en los procedimientos de la división. SIA Sistema de Información Académico: Es una aplicación elaborada para facilitar la administración de los diferentes procesos académicos que se llevan a cabo en la Universidad.

Desarrollos Web del Sistema de Información Académico: Digitación de Notas, Inclusiones y/o Cancelación, Registro de Hora Cátedra, Peticiones, quejas y Reclamos, Sistema de Información Académico de la Escuela de Artes, y Evaluación Docente

SIB Sistema de Información de Biblioteca: El SIB cuenta con una Base de Datos diseñada en el Formato MARC para Datos Bibliográficos, que permite manejar información de cualquier tipo de material bibliográfico como lo son libros, tesis, publicaciones seriadas, archivos de computadora y material audiovisual y definir diferentes políticas propias de la Biblioteca Argemiro Bayona Portillo.

Desarrollos Web del Sistema de Información Bibliográfico: Consulta de Bibliografía.

SIF Sistema de Información Financiero: El Sistema de Información Financiera SIF, es una aplicación elaborada para facilitar la administración de los diferentes procesos contables y presupuestales que se llevan a cabo en la Universidad.

RECURSOS NECESARIOS

Una lista de todos los empleados, los servicios de terceros, instalaciones, infraestructura, información, equipamiento, etc., que son necesarios para llevar a cabo la recuperación, y quién es el responsable de proporcionar a cada uno de ellos.

Los recursos necesarios para poner en marcha la aplicación del Plan son:

Recursos humanos. Describe los recursos humanos necesarios con sus roles, responsabilidades y funciones.

Recursos materiales. Enumera los materiales necesarios para la adecuación de las actividades ante una eventualidad.

Recursos financieros. Los recursos de inversión necesarios en caso de una contingencia dependen directamente del incidente a enfrentar, para lo cual se derivan del costo de cubrir los recursos materiales y el transporte necesario para llevarlos al sitio indicado. Para resolver esta situación se estipula que la organización debe proveer una reserva que cubra dichos recursos.

LA RESTAURACIÓN Y LA REANUDACIÓN DE LAS ACTIVIDADES DE MEDIDAS TEMPORALES

¿Cómo restaurar las actividades de nuevo una vez que el incidente perturbador se ha resuelto?

En ningún caso las actividades normales del CEDIT se deben interrumpir por un lapso de tiempo considerable.

Para ello se dispone de las medidas adecuadas que permitan el restablecimiento de las mismas. Estas son, en caso de ser necesarias:

Traslado de los equipos de cómputo y oficina a la sede del CEDIT ubicada en el barrio La Primavera.

Adecuación de los espacios físicos.

Reinstalación y adaptación de los servicios de acueducto, alcantarillado, energía eléctrica, internet, y telefonía fija.

IDENTIFICACIÓN DE LOS RIESGOS A QUE ESTA EXPUESTO EL CEDIT

En la siguiente tabla se presentan algunas de las implicaciones que se podrían generar en la ocurrencia de una emergencia si no se establece un plan de acción preventivo.

Análisis e Impacto del Negocio

FACTORES DE RIESGO	RIESGO	COSTO
Riesgo Físico Los que afectan a la seguridad del edificio	Sismos/ terremotos	Reconstrucción de la edificación en general o de los sectores afectados.
	Temperatura y humedad relativa del aire	Pérdida total o parcial de información clave.
	Inundación y/o anegación	Reparación de equipos de cómputo o adquisición de nuevos equipos para suplir las necesidades.
		Pérdida total o parcial de soportes.
	Incendio	Pérdida total o parcial de soportes por incendio o explosión.
	Rayos	Retraso en la ejecución de operaciones por daño en las instalaciones o equipos.
	Iluminación	Pérdida total o parcial de soportes.
Riesgo Biológico	Insectos, Roedores Microorganismos	Perdida de la documentación.
Riesgo Social	Hurto, Vandalismo Huelga, Motín Asonada, Entorno y vecinos	Cuando ocurre un impacto de este tipo, la imagen institucional se puede ver afectada ante entidades externas y en general en la comunidad académica, debido a la evidencia de fallas en la seguridad.
Riesgo Tecnológico Riesgos que afectan la integridad de los datos	Corte de energía eléctrica	Perdida de información que no se halla salvado en los computadores, costos por el retraso de las actividades propias del CEDIT.
	Riesgos Tecnológicos	Adquisición de nuevos equipos, reparación de instalaciones físicas.
	Virus informáticos	Perdida de información clave, daño de los equipos.
		Problemas de carácter jurídico y/o legal.
	Seguridad en la Información de tipo tecnológico	Perdida de la integridad de la información, deterioro de la imagen institucional.

Fuente: Autores del Proyecto.

A continuación se listan las emergencias más comunes y las indicaciones a seguir:

Avisar de la emergencia. Avisar al jefe de área y/o brigadistas quienes se encuentran entrenados para enfrentar la emergencia.

Alertar a los servicios públicos oportunos, suministrar la mayor cantidad de información posible.

De ser posible intervenir con las herramientas con que se cuenta, siempre y cuando no esté en peligro la seguridad personal.

Si las magnitudes de la emergencia lo ameritan, evacuar.

¿Cómo evacuar?

Al oír la señal de evacuación, prepárese para abandonar el centro.

Procurar llevar siempre consigo los objetos personales (no voluminosos).

Desconectar los objetos eléctricos a su cargo.

Si se encuentra junto a alguna visita, acompáñela hasta el exterior.

Evacuar el edificio con rapidez, pero sin correr.

No volver al Centro de trabajo a recoger objetos personales.

Durante la evacuación seguir las siguientes instrucciones:

Realizar la evacuación de forma rápida y ordenada.

Tranquilizar a las personas que durante la evacuación, hayan podido perderla calma.
Ayudar a las personas impedidas o disminuidas.

No permitir el ingreso al Centro de trabajo a ninguna persona que pretenda ir a buscar algún objeto o a otra persona.

Abandonar el Centro, dirigirse al punto de reunión y no detenerse inmediatamente después de la salida del edificio.

Permanecer en el punto de reunión y seguir las instrucciones del jefe de área y los brigadistas.

En caso de que la evacuación se realice por amenaza de bomba, dejar las puertas y ventanas del Centro abiertas.

ESTRATEGIAS Y ACCIONES

Transferir: Capacitar al personal en la formación requerida.

Aceptar - Mitigar: Evidenciar controles, políticas, procesos y procedimientos de la seguridad de la información de manera independiente y objetiva.

Eliminar: Definir políticas que permita definir nuevos roles que admitan la oportuna y rápida toma de decisiones.

Aceptar - Mitigar: Plantear políticas que permitan la independencia.

ACCIONES PREVENTIVAS

Las acciones preventivas para evitar la pérdida de información ante un desastre o siniestro se resumen en:

Seguridad física y ambiental, incluye el control de equipos y áreas (servidores, PCs, medios magnéticos, información impresa, etc.).

Control de acceso de acuerdo a los perfiles de cada usuario.

Control de los recursos físicos incluida la actualización de hardware y software.

Capacitación y entrenamiento del personal, esta tarea es apoyada por el departamento de personal. Además del suministro de instructivos y manuales con el fin de trabajar de forma unificada y conjunta garantizando de esta forma la seguridad e integridad de la información y su adecuado uso y manipulación.

Protección de la información en redes y de la infraestructura de soporte. Desarrollo y mantenimiento de los sistemas, incluye la protección de archivos, bases de datos, políticas de cifrado, etc.

Evitar daños a los recursos de información e interrupciones en las actividades de la Universidad.

Con base en el análisis efectuado, a continuación se presentan recomendaciones importantes para tener en cuenta antes, durante y después de la ocurrencia de algunas de las emergencias que se pueden llegar a producir.

Recomendaciones

TIPO DE EMERGENCIA	DAÑOS QUE PUEDE LLEGARA OCASIONAR	¿QUÉ HACER ANTES DE LA EMERGENCIA?	¿QUÉ HACER DURANTEDE LA EMERGENCIA?	¿QUE HACER DESPUES DE LAEMERGENCIA?
INCENDIO	Proliferación de llamas Generación de Humo tóxico Derrumbamiento de estructuras	Es importante contar con los extintores adecuados de acuerdo al tipo de incendio y el área donde se presente el evento.	Mantenga la calma. Active las alarmas de incendios y avise al cuerpo de bomberos Si se encuentra atrapado en una oficina; cierre todas las puertas. Tape con trapos, de ser posible húmedos, todas las rendijas por donde penetre el humo. Haga saber de su presencia. Si se trata de un foco incipiente y posee formación en el manejo de sistemas de extinción, actúe sobre el foco con extintores portátiles o las mangueras interiores. Si es posible, corte la electricidad. Si el incendio es grave o no sabe apagarlo, desaloje la zona ayudando a las personas que lo precisen: ancianos, niños e impedidos. No rompa las ventanas. Cierre las puertas sin llave. Toque las puertas y si están calientes o sale humo por las rendijas, tápelas con trapos	Reúnase en una zona segura con el resto del personal. Localice al jefe de área y/o brigadistas. Espere las instrucciones y colabore sólo cuando se solicite su ayuda.

			húmedos, no las abra y busque otras salidas. Si el edificio está en llamas cúbrase la nariz con un pañuelo mojado, si hay mucho humo camine agachado o a gatas. Olvídese de salvar posesiones, lo importante es su vida y la del resto de las personas. Si se le prende la ropa, no corra, tiéndase en el suelo y échese a rodar.	
INUNDACIÓN	Incendios por cortocircuito Deterioro de la documentación por efectos del agua.	Revisión y reparación de los sitios por donde se pueda filtrar el agua. Revisión periódica de tuberías y desagües. Dejar estanterías y otros soportes de documentación a una altura mínima de 10 cm. para evitar que se afecten los documentos en sus diferentes soportes en caso de inundación.	Mantenga la calma. Avise al jefe de área y/o brigadistas. Dé prioridad a las zonas donde se encuentran los documentos esenciales. Avise al cuerpo de bomberos Corte la corriente eléctrica, para evitar cortocircuitos. Evite la descarga de agua cerrando las llaves de paso, si el derrame es interior, o cerrando puertas y taponando entradas, si la procedencia es exterior. Si no existe riesgo para su integridad, espere la llegada de los bomberos; en una zona segura.	No intente activar fuentes de calor para secar los documentos. No envuelva documentos en plástico Espere las instrucciones y colabore sólo cuando se solicite su ayuda. Abandone la zona cuando se le indique. Una vez extraída la documentación afectada por la inundación proceder a empacarla o proceder al secado manual o al secado asistido mecánicamente y efectuar una desinfección

Fuente: Autores del Proyecto

Todo el proceso debe ir acompañado de programas de capacitación y concienciación para garantizar que el mismo sea conocido por todos los miembros de la dependencia y la Universidad.

Programas de Capacitación y Concienciación. Los programas de capacitación y concienciación se encuentran a cargo del director de la dependencia y de la división de personal.

Prueba y Verificación. Para poder realizar pruebas y verificación es necesario que se presenten situaciones que afecten el normal funcionamiento de la UFPS Ocaña y específicamente el CEDIT. Como referencia se pueden aplicar las acciones de remodelación y adecuación de la infraestructura física de la Casona a finales del año pasado; en donde fue necesario aplicar el Plan de Contingencia para garantizar la continuidad del negocio. En lo concerniente al **CEDIT**, igualmente y debido a remodelaciones en la sede La Primavera de la UFPS Ocaña en el año 2014, se hizo necesario utilizar espacios anexos para poder continuar con las labores de dicha dependencia.

Además, con la instalación de la subestación en la sede de La Primavera de la UFPS Ocaña, se mejoró en parte los continuos cortes de energía que se presentaban. Demostrando que las recomendaciones dadas en el Plan de Contingencia son acertadas y resuelven la situación o situaciones detectadas.

Revisiones Post Incidentes. El SIG identifica que la autoevaluación es implementada como un proceso de reflexión permanente y de obtención de información oportuna y eficaz para la toma de decisiones en pro del mejoramiento continuo y la obtención de la calidad esperada de los programas académicos y la Institución en su conjunto. Esta cultura es vista a la luz del Proyecto Educativo Institucional (PEI), el Plan de Desarrollo y los Proyectos Educativos de cada programa académico (PEP). Este principio genera en cada individuo de la organización un compromiso que permite revisiones durante y después de cualquier incidente. Siendo Control Interno la dependencia cumple un papel importante como responsable del Componente de Evaluación Independiente, y como asesor, evaluador, integrador y dinamizador del Sistema de Control Interno y el Sistema Integrado de Gestión con miras a mejorar la cultura organizacional y, por ende, a contribuir con la productividad de la Universidad.