RESUMEN – TRABAJO DE GRADO

AUTORES	**CARLOS ANDRES GOMEZ FLOREZ** **JOHAN SMITH RUEDA RUEDA** **CARLOS ANDRES SANCHEZ BECERRA** **NATALIA TORRADO PEÑARANDA**
FACULTAD	**INGENIERIAS**
PLAN DE ESTUDIOS	**ESPECIALIZACION AUDITORIA DE SISTEMAS**
DIRECTOR	**ESP. ING. YESICCA MARIA PEREZ PEREZ**
TÍTULO DE LA TESIS	**DISEÑO DE UN PLAN DE CONTINUIDAD PARA LA OFICINA DE ADMISIONES REGISTRO Y CONTROL DE LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA**

RESUMEN

(70 palabras aproximadamente)

ESTE TRABAJO TIENE COMO OBJETIVO PRINCIPAL EL DISEÑO DE UN PLAN DE CONTINUIDAD PARA LA OFICINA DE ADMISIONES REGISTRO Y CONTROL DE LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDER, TOMANDO COMO REFERENCIA EL ESTANDAR ISO 22301:2012. PARA LO CUAL SE REALIZO UNA AUDITORIA PASIVA A LA DEPENDENCIA POR LOS AUTORES DEL PROYECTO, UN ANALISIS DE RIESGOS Y UNA EVALUACION DE LAS POSIBLES AMENAZAS A LAS QUE SE PUEDE ENFRENTAR DICHA OFICINA.

CARACTERÍSTICAS

PÁGINAS:	PLANOS:	ILUSTRACIONES:	CD-ROM:

DISEÑO DE UN PLAN DE CONTINUIDAD PARA LA OFICINA DE ADMISIONES, REGISTRO Y CONTROL DE LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

CARLOS ANDRÉS GÓMEZ FLÓREZ

JOHAN SMITH RUEDA RUEDA

CARLOS ANDRÉS SÁNCHEZ BECERRA

NATALIA TORRADO PEÑARANDA

Trabajo de Grado presentado para optar al título de Especialista en Auditoría de Sistemas

DIRECTORA

Esp. Ing. YESICA PEREZ PEREZ

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

FACULTAD DE INGENIERÍAS

ESPECIALIZACIÓN EN AUDITORIA DE SISTEMAS

Ocaña, Colombia Octubre, 2016

Índice

Lista de tablas

Lista de figuras

Introducción

Como parte fundamental de la gestión segura de la información, las empresas deben contar con políticas que les orienten y les permitan mantener la integridad, disponibilidad y confiabilidad de la información, la cual es uno de los activos más importantes. Los riesgos, las amenazas están presentes diariamente en el desarrollo de las funciones y la materialización de los mismos se convierte en incidentes con diferentes tipos de impactos, por ello es fundamental que las empresas cuenten con herramientas que le permitan garantizar el desarrollo de los procesos normalmente o la recuperación de los mismos en un periodo de tiempo tolerable.

La oficina de Admisiones Registro y Control es la dependencia de la Subdirección Académica encargada de llevar, mantener actualizados y custodiar los registros académicos de los estudiantes, información primordial para la Universidad, la interrupción de sus funciones puede incidir de manera negativa en el no cumplimento de los objetivos misionales de la institución, por lo que es primordial que cuente con un Plan de Continuidad, El presente trabajo muestra la definición de dicho Plan basado en la norma ISO 22301: 2012 que permitirá garantizar la continuación de las operaciones ante una posible incidencia de seguridad.

Capítulo 1: Titulo

Diseño de un Plan de Continuidad para la oficina de Admisiones, Registro y Control de la Universidad Francisco de paula Santander Ocaña.

1.1. Planteamiento del problema

Las organizaciones desde que nacen tienen unos objetivos propuestos, una misión y una visión. Pero existen eventos que pueden poner en riesgo el cumplimiento de dichos objetivos organizacionales. Dichos eventos o incidentes pueden ser de origen natural, causado por un fallo o de forma intencionada.

Entre los eventos de origen natural, se encuentra los temblores, inundaciones, aludes, entre otros. En cuanto a los causados por fallos se pueden presentar los cortos circuitos, los fallos tecnológicos o humanos. Y en los incidentes provocados están aquellos cuya intención es destruir o sabotear, como los ciberataques, intrusiones físicas, conflagraciones, uso de explosivos, etcétera. Estos tipos de incidentes suelen comprometer los activos de la organización, impidiendo que esta continúe sus labores por un tiempo determinado.

La información es el activo más importante de una organización, el cual tiene tres características importantes: la confidencialidad, la integridad y la disponibilidad (Paredes , 2006) Dichas características pueden ser afectadas por cualquier incidente de los mencionados anteriormente y aplica tanto para la información almacenada en medios magnéticos como de forma física.

Así por ejemplo, en el caso de los ciberataques, un informe de *Enterprise Strategy Group* encargado por *Intel Security* afirma que los profesionales en seguridad enfrentaron un promedio de 78 casos por organización en el último año, y el 28 % de los cuales eran ataques dirigidos. El 79 % de los encuestados cree que tiene dificultades con la detección y respuesta a incidentes debido a la falta de integración y comunicaciones entre sus herramientas de seguridad (Everett, 2015)

La oficina de Admisiones, Registro y Control (ARC), según reza su misión, es la encargada de recopilar, articular, monitorear y salvaguardar la historia académica de la Universidad Francisco de Paula Santander Ocaña UFPSO al servicio de la comunidad en general, de acuerdo a la normatividad vigente, tecnologías de la información y comunicación, el sistema de gestión de calidad y un talento humano calificado, que contribuya al cumplimiento de los propósitos misionales (UFPSO, 2015).

Pero actualmente, esta oficina no cuenta con una política de prevención para salvaguardar de forma correcta la información que ellos manejan. La historia académica de los estudiantes de la universidad está soportada únicamente de forma física y reposan en el mismo espacio donde se desarrollan las actividades de esta dependencia.

Según una auditoría realizada por los autores de proyecto en el primer semestre del 2015, el cual se evalúo la seguridad física y lógica bajo la norma ISO/IEC 27001, se evidenció que no existe una política de digitalización de los documentos físicos. Siendo estos la única evidencia del historial académico con que cuenta esta institución.

Entre los documentos de los cuales la oficina de ARC es responsable está los registros oficiales de los procesos que adelanta la dependencia (inscripción, admisión, matrícula y desempeño académico de los estudiantes), la documentación de los estudiantes que están próximos a graduarse y el archivo de los estudiantes graduados, las planillas de notas de todas las carreras que oferta la universidad por semestre y las carpetas donde reside la vida académica de los estudiantes que ingresan al primer semestre, información necesaria para expedir las certificaciones académicas (constancias de estudios, certificados de notas, constancias de buena conducta, constancia terminación de materias y paz y salvo de grado). Documentos que, de ser comprometidos, traen grandes consecuencias para la entidad, afectando su funcionamiento y su nombre institucional, y de esta forma, afectando el cumplimiento de sus objetivos misionales, su misión y visión.

Cada día se presentan situaciones que pueden comprometer la continuidad de los procesos en la organización y causar grandes pérdidas tanto económicas como de la imagen corporativa. Por esta razón, es de vital importancia que las organizaciones creen un plan que les ayude en la gestión de la continuidad de su negocio y les permita tomar las mejores decisiones para mitigar los efectos causados por dichos incidentes.

1.2. Formulación del problema

¿El plan de gestión de la continuidad del negocio permitirá garantizar la continuación de las operaciones ante una posible incidencia de seguridad en la dependencia de Admisiones, Registro y Control de la UFPS Ocaña?

1.3. Objetivos

1.3.1. Objetivo general

Diseñar un plan de continuidad para la oficina de Admisiones, Registro y Control de la Universidad Francisco de Paula Santander Ocaña con la norma ISO/IEC 22301.

1.3.2. Objetivo específico

- Conocer el estado actual de la dependencia de Admisiones, Registro y Control, por medio de una auditoría pasiva.

- Definir estrategias que permitan la continuidad de los procesos de la dependencia de ARC.

- Elaborar el plan de gestión de la continuidad del negocio para la oficina de ARC.

A continuación se presenta a través de la tabla 1 cada las actividades realizadas con sus respectivos indicadores, para el cumplimiento de cada objetivo propuesto.

El desarrollo de las mismas se evidenciará más adelante en el capítulo 4.

Tabla 1

Seguimiento metodológico

Objetivo específico	Actividades	Indicadores
Conocer el estado actual de la dependencia de Admisiones, Registro y Control por medio de una auditoría pasiva.	-Reunión con jefe de la dependencia de Admisiones registro y control con propósito de solicitar la información inicial. -Estructurar los papeles de trabajo. Visitar la oficina de Admisiones Registro y Control para mediante la observación determinar de qué manera se llevan a cabo los procesos en esta dependencia y en que sitios se encuentra almacenada la información física. -Aplicar los instrumentos de recolección de la información. -Analizar la información recopilada y verificar la existencia de las políticas y demás documentos cuya existencia se afirme por jefe de la dependencia y demás funcionarios. -Proyectar en los papeles de auditoria los resultados obtenidos respecto al análisis de la seguridad de la información en base a la norma ISO 27002 del 2005.	• Resumen de la información general de la institución. • Resumen de la información general de la dependencia. • Instrumentos de recolección de la información (resultados) * Entrevista * Observación * Check List * Encuestas • Dictamen de la Auditoria.
Definir estrategias que permitan la continuidad de los procesos de la dependencia de ARC.	-Evaluación de procedimientos, determinar prioridades y establecer orden de recuperación. -Definición de recursos necesarios para el buen desarrollo de los procedimientos a nivel de tecnología, personal e infraestructura.	• Esquema de evaluación de procedimientos. • Matriz DOFA • Análisis de riesgos
Elaborar el plan de gestión de la continuidad del negocio para la oficina de ARC.	-Diseño de parámetros basado en la norma ISO 22301 -Establecer controles preventivos, detectivos y correctivos. -Planteamiento de estrategias para asegurar la continuidad del negocio	• Informe final del Plan de Gestión de la Continuidad del Negocio para la oficina de ARC.

Fuente. Autores

1.4. Justificación

Los riesgos de que ocurra un incidente no se pueden eliminar en un 100 %, pero sí gestionar qué hacer en caso de que ocurran, a través de la administración del plan de continuidad del negocio. En su manual de administración del plan de continuidad de negocio, el ICETEX (2013) define a esta administración del plan como "un sistema administrativo integrado, transversal a toda la organización, que permite mantener alineados y vigentes todas las iniciativas, estratégicas, planes de respuesta y demás componentes y actores de la continuidad del negocio. Busca mantener la viabilidad antes, durante y después de una interrupción de cualquier tipo. Abarca las personas, procesos de negocios, tecnología e infraestructura".

Los estándares son referencias que han sido avaladas y aceptadas a nivel internacional. La ISO 22301 "Gestión de la continuidad del negocio", especifica los requisitos para un sistema de gestión encargado de proteger a su empresa de incidentes que provoquen una interrupción en la actividad, reducir la probabilidad de que se produzcan y garantizar la recuperación de su empresa (BSI, 2015).

La ISO 22301 permite identificar las amenazas relevantes y las funciones críticas que podrían sufrir consecuencias. Dentro de las amenazas, incluye inclemencias meteorológicas extremas, incendio, inundación, desastres naturales, robo, interrupción de servicios de TI, enfermedad del personal o ataque terrorista (BSI, 2015).

La oficina de ARC realiza la función de proceso de apoyo en el cual, UFPS Ocaña se sustenta para cumplir con sus procesos misionales (UFPSO, 2015). La documentación operada por esta oficina es relevante para el proceso institucional. Aplicar un plan para la

gestión de la continuidad del negocio permitirá establecer políticas para el resguardo y salvaguarda de los documentos que maneja esta dependencia. Políticas como la gestión documental donde se establezca un protocolo para la digitalización de esta documentación del historial académico y demás documentos bajo la custodia de esta dependencia es debe ser de prioridad para esta oficina y la Universidad misma. A los incidentes que pueden afectar la confidencialidad, la integridad y la disponibilidad de la información no deben restar importancia, se deben asumir estos riesgos, gestionarlos y minimizarlos hasta un mínimo aceptable por la organización.

Por esta razón, y teniendo en cuenta la misión y los objetivos que tiene la oficina de Admisiones, Registro y Control se hace necesario diseñar un plan para la gestión de la continuidad del negocio, ya que esta dependencia es se suma importancia para el cumplimiento de los objetivos misionales de la UFPS Ocaña.

1.5. Delimitaciones

1.5.1. Operativas

Las posibles dificultades que se puede encontrar en este proyecto son:

- No encontrar la información completa acerca de la dependencia.

1.5.2. Conceptuales

La propuesta está enmarcada dentro de los conceptos y lineamientos establecidos en la norma ISO 22301 “Gestión de la continuidad del negocio”.

1.5.3. Geográficas

Este proyecto se desarrollará en la dependencia de Admisiones, Registro y Control (ARC) de la Universidad Francisco de Paula Santander seccional Ocaña (UFPS Ocaña).

1.5.4. Temporales

El tiempo necesario para el desarrollo de esta investigación, será de tres (3) semestres académicos, aproximadamente doce meses calendario.

Es importa resaltar que la auditoria pasiva realizada por los autores de este proyecto fue llevada a cabo durante el primer semestre del año 2015.

Capítulo 2: Marco referencial

2.1. Marco histórico

El concepto de continuidad del negocio y/o recuperación ante desastres se origina en Estados Unidos en la década de 1960, cuando las organizaciones comenzaron a depender de sistemas computarizados. En ese entonces, los sistemas eran procesos en lote que corrían en grandes computadoras centrales, los cuales podían estar caídos por varios días. Así, a medida que la recuperación ante desastres crecía, y al ser considerados los centros de cómputo como puntos únicos de falla se desarrolló un rubro de servicios que proveía centros de cómputo de respaldo, cuyo costo era menor que aquel de duplicar la infraestructura informática crítica. Esta estrategia se convirtió en el estándar para la recuperación de TI desde fines de los setentas, y hoy continúa siendo un importante rubro de servicios (Torres, Erik, & Velasco, 2014).

Con el rápido crecimiento del Internet en los noventas y la década del 2000, organizaciones de todos los tamaños se volvieron mucho más dependientes de la disponibilidad de sus sistemas informáticos —llegando algunas empresas a establecer niveles de disponibilidad de hasta 99.999%—. Este incremento de la dependencia con los sistemas de TI, así como la conciencia de posibles desastres a gran escala, como el del "11 de septiembre", contribuyeron al crecimiento de las diversas industrias relacionadas a la recuperación ante desastres y a la consolidación de la disciplina de continuidad de negocios (Torres, Erik, & Velasco, 2014)

Hoy en día, la gestión de la continuidad del negocio abarca a todas las funciones y recursos —procesos críticos del negocio, recursos humanos, mantenimiento y respaldo del suministro eléctrico, aspectos de transporte, alimentación, seguridad y salud—. Jerárquicamente, la continuidad del negocio está arriba; debajo está el plan de recuperación ante desastres; y debajo de este viene la tecnología —como el respaldo de datos, la recuperación y la restauración de TI—. El departamento de TI, con su plan de recuperación ante desastres, es un elemento (clave) dentro del gran escenario de la continuidad del negocio (el SGCN).

2.1.1. Antecedentes.

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

En Perú se realizó un Plan de Contingencia Informático 2012-2015 en el Instituto del Mar del Perú (IMARPE). La Implementación del Plan de Contingencia informático,

incluye los elementos referidos a los sistemas de información, equipos, infraestructura, personal, servicios y otros, direccionado a minimizar eventuales riesgos ante situaciones adversas que atentan contra el normal funcionamiento de los servicios de la institución (IMARPE, 2012).

Las empresas y los sistemas de información deben estar preparados para soportar las diversas amenazas que ponen en riesgo su funcionamiento.

Las empresas del sistema financiero, para el desarrollo de sus actividades dependen en gran medida de recursos críticos como: tecnología de la información, recurso humano, recurso económico, etc. La pérdida prolongada de tiempo en la disponibilidad de dichos recursos afectaría en alto grado la rentabilidad y viabilidad del negocio. Tomando en cuenta la importancia de estos antecedentes el Instituto Ecuatoriano de Crédito Educativo y

Becas cuenta con el presente documento de respaldo a la Continuidad de Negocio como resultado de la aplicación de una metodología de construcción aplicada y documentada con todos los responsables de los procesos críticos de la Institución (Instituto de Fomento al Talento Humano, 2012).

En Colombia se realizó una Propuesta de Mejoramiento y Contingencia de Sistemas Informáticos en la Empresa “T”, en la cual con el análisis de la información, el equipo consultor y el equipo de trabajo de Sistemas del negocio, detectan las problemáticas de Tecnologías de la Información y crean las estrategias para a promover la mejora del área y de los servicios informáticos para beneficio de la organización. El equipo consultor sugiere también una propuesta de mejoramiento, basada en guías de buenas prácticas de TI y en su

propia experiencia. Este documento presenta el desarrollo del mencionado proceso de consultoría y los resultados obtenidos representados en una propuesta de mejoramiento y un plan de contingencia de TI (Ramírez Robayo, Londoño Rúa, & Gómez Gómez, 2012).

El lugar donde se encuentra la Corporación Educativa Minuto De Dios (Vargas Daza, 2009), al estar ubicado en Bogotá se halla en una zona de Riesgo Sísmico Intermedio, habiéndose presentado anteriormente varios sismos de gran magnitud. Es por esto que al tener un plan de Emergencia, es un factor importante que permite una rápida y oportuna atención de una emergencia con los recursos internos disponibles, disminuyendo los efectos negativos de la misma.

En la ciudad de Ocaña, se han realizado diferentes planes de continuidad del negocio, uno de estos estudios, se realizó para la E.S.E Hospital Emiro Quintero Cañizares en el cual de determinó la necesidad de evaluar los riesgos tecnológicos y se desarrolló un plan de continuidad del negocio para mantener protegida la información del negocio (Sánchez Jaime, 2015). Otro caso en la ciudad de Ocaña es el de un plan de continuidad del negocio para el Centro de Desarrollo e Innovación Tecnológica de la UFPS Ocaña, donde se describe la realización del plan de continuidad que garantice la seguridad de la información 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 (Blanco, Martinez Vega, Quintero Prado, & Rincón Angarita, 2015).

2.2. Marco contextual

Este plan de continuidad del negocio se desarrollará en la dependencia Admisiones Registro y Control de la Universidad Francisco de Paula Santander Ocaña, dentro de este contexto se estudiará toda la información referente a la dependencia con cada una de las personas que hacen parte de ella donde se estudiará el modelo del negocio de los procesos del área, su estructura orgánica, sus recursos informáticos y de software, y se realizará la elaboración del Plan de Continuidad del Negocio según la Norma ISO/IEC 22301.

2.3. Marco conceptual

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

2.3.1. Direccionamiento Estratégico. Es un enfoque gerencial que permite a la alta dirección determinar un rumbo claro, y promover las actividades necesarias para que toda la organización trabaje en la misma dirección". Esto implica que la dirección estratégica va más allá de la simple y tradicional planeación, puesto que trata de dar elementos a los gerentes a fin de que estén preparados para enfrentar los cambios del entorno, y las situaciones complejas y no rutinarias que la actividad gerencial requiere (Aguilera Castro, 2010).

2.3.2. Plan de continuidad del negocio. Documento que refleja el conjunto de estrategias, acciones, procedimientos planificados y responsabilidades definidas para minimizar el impacto de una interrupción imprevista de las funciones críticas, de toda una

organización, y conseguir la restauración de las mimas, dentro de unos límites de tiempo establecidos. Se suele aplicar al plan que abarca las actividades de todos los departamentos funcionales de una organización (Gaspar Martínez, 2010).

2.3.3. Estructura organizacional. Cada actividad humana organizada da origen a dos requerimientos fundamentales y opuestos: la división del trabajo entre varias tareas a desempeñar y la coordinación de estas tareas para consumar la actividad. Así, la estructura de una organización puede ser definida como la suma total de las formas en que su trabajo es dividido entre diferentes tareas y luego es lograda la coordinación entre estas tareas (Mintzberg, 2003).

Vulnerabilidad. Susceptibilidad de un sistema, producto o instalación a sufrir daños ante sucesos accidentales o intencionados; potencialidad o posibilidad de ocurrencia de la materialización de una amenaza sobre un activo (Mintzberg, 2003).

Sistema de Información. Un Sistema de Información es un conjunto de elementos que interactúan entre sí con el fin de apoyar las actividades de una empresa o negocio. En un sentido amplio, un sistema de información no necesariamente incluye equipo electrónico. Sin embargo en la práctica se utiliza como sinónimo de sistema de información computarizado (Fernández Alarcón, 2006).

Los elementos que interactúan entre sí son: el equipo computacional, el recurso humano, los datos o información fuente, programas ejecutados por las computadoras, las telecomunicaciones y los procedimientos de políticas y reglas de operación.

Un Sistema de Información realiza cuatro actividades básicas:

Entrada de información: proceso en el cual el sistema toma los datos que requiere para procesar la información, por medio de estaciones de trabajo, teclado, diskettes, cintas magnéticas, código de barras, etc.

Almacenamiento de información: es una de las actividades más importantes que tiene una computadora, ya que a través de esta propiedad el sistema puede recordar la información guardad en la sesión o proceso anterior.

Procesamiento de la información: esta característica de los sistemas permite la transformación de los datos fuente en información que puede ser utilizada para la toma de decisiones, lo que hace posible, entre otras cosas, que un tomador de decisiones genere una proyección financiera a partir de los datos que contiene un estado de resultados o un balance general en un año base.

Salida de información: es la capacidad de un SI para sacar la información procesada o bien datos de entrada al exterior. Las unidades típicas de salida son las impresoras, graficadores, cintas magnéticas, diskettes, la voz, etc.

Seguridad de la información. La seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad y la integridad de la misma (Galindo, 2014).

La seguridad de la información se logra implementando un adecuado conjunto de controles; incluyendo políticas, procesos, procedimientos, estructuras organizacionales y

funciones de software y hardware. Se necesitan establecer, implementar, monitorear, revisar y mejorar estos controles cuando sea necesario para asegurar que se cumplan los objetivos de seguridad y comerciales específicos.

Planeación estratégica. Es el proceso mediante el cual quienes toman decisiones en una organización obtienen, procesan y analizan información pertinente, interna y externa, con el fin de evaluar la situación presente de la empresa, así como su nivel de competitividad con el propósito de anticipar y decidir sobre el direccionamiento de la institución hacia el futuro (Serna Gómez, 1997).

2.4. Marco teórico

La creación de un plan de continuidad del negocio contribuye a mantener segura la información de la dependencia, ya que a través de procedimientos apropiados que se adecúen a determinadas necesidades se logran optimizar los procesos.

Para la construcción del plan de continuidad del negocio, se requiere realizar un análisis profundo de todos los factores que intervienen en la ejecución de los procesos.

Según Jorge Burgos Salazar y Pedro G. Campos, para la correcta administración de del plan de continuidad se deben establecer y mantener acciones que busquen cumplir con los tres requerimientos de mayor importancia para la información, son los siguientes:

- Confidencialidad. Busca prevenir el acceso no autorizado ya sea en forma intencional o no intencional a la información. La pérdida de la confidencialidad puede ocurrir de muchas maneras, como por ejemplo con la publicación intencional de información confidencial de la organización (Burgos Salazar & Campos, 2008).

- Integridad. Busca asegurar que no se realicen modificaciones por personas no autorizadas a los datos o procesos y que los datos sean consistentes tanto interna como externamente.

- Disponibilidad. Busca asegurar acceso confiable y oportuno a los datos o recursos para el personal apropiado.

2.4.1. Normas Técnicas

***BS25999*.** Es la norma predecesora (remplazada por la actual ISO 22301) y es la primera norma británica para la gestión de continuidad y fue concebida con el fin de ayudar a minimizar el riesgo a las interrupciones, como un siniestro o una catástrofe. Consta de dos partes:

Parte 1: Código de Práctica. Establece el proceso por el cual una organización puede desarrollar e implementar la continuidad de negocio, incluyendo una completa lista de controles basada en las mejores prácticas de BCM (Business Continuity Management) (BSI, http://www.bsigroup.com/, 2006).

Parte 2: Especificación. Especifica los requisitos para establecer, implementar, operar, supervisar, revisar, probar, mantenery mejorar un sistema de gestión de continuidad de negocio en el contexto de la gestión global de riesgos de una organización (BSI, BSI, 2007).

ISO/IEC 22301:2012. La norma ISO/IEC 22301:2012 Seguridad de la sociedad (Sistemas de gestión de la continuidad del negocio). Requisitos, es el nuevo estándar internacional para la gestión de continuidad del negocio. Se ha creado en respuesta al gran interés internacional en el original norma británica BS 25999-2 y otras normas regionales. Proporciona el mejor marco de referencia y es el nuevo estándar global para gestionar la continuidad del negocio en una organización (Castro Marquina, 2013).

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

2.4.2. **Gestión de continuidad del negocio.**

El Sistema de Gestión de la Continuidad del Negocio (SGCN) se ha convertido en una exigencia para las empresas que

compiten el día de hoy en los mercados globalizados. La tendencia mundial es que ya las empresas no compitan entre sí: la competencia es entre cadenas de suministros. Una cadena de suministros, para mantenerse operando, no puede tener ningún eslabón débil; ninguno de sus componentes puede dejar de operar ya que si un elemento del todo dejara de funcionar se paraliza toda la serie, generando el caos. Cada miembro del sistema tiene que demostrar que es un proveedor confiable. Esto se logra teniendo en cada empresa un SGCN que proteja a los procesos esenciales que permiten originar los productos o servicios que desea el cliente.

El nuevo estándar ISO 22301:2012 tiene por nombre "Seguridad de la Sociedad: Sistemas de Continuidad del Negocio". Este modelo aparece como producto de una evolución de lineamientos, buenas prácticas y estándares en continuidad del negocio (Servat, 2012).

La ISO 22301 es la norma internacional para la ISO 22301: Gestión de la Continuidad de Negocio, que se basa en el éxito de la Norma Británica BS 25999 y otras normas regionales. Está diseñada para proteger su empresa frente a cualquier posible problema.

Esto incluye inclemencias meteorológicas extremas, incendio, inundación, desastres naturales, robo, interrupción de servicios de TI, enfermedad del personal o ataque terrorista. El sistema de gestión ISO 22301 le permite identificar las amenazas relevantes y las funciones empresariales críticas que podrían sufrir consecuencias. También le permite establecer planes con antelación para asegurarse de que su empresa no detiene su actividad.

2.4.3. <u>BCM (Business Continuity Management).</u> La Gestión de la Continuidad del Negocio es un proceso holístico que identifica amenazas potenciales a la organización e impactos a las operaciones del negocio que tales amenaza puedan causar en caso de materializarse; y proporciona la estructura para construir resilencia con capacidad para dar respuesta efectiva protegiendo los intereses de las partes interesadas, la reputación, el valor de la marca, la reputación y las actividades creadoras de valor (Castro Marquina, 2013).

Asignación de responsabilidades. Un programa de BCM exitoso depende de la identificación de roles y responsabilidades y autoridad claramente definidos para manejo del BCM y su proceso a través de la organización. El propósito de la asignación de roles y responsabilidades es garantizar que el personal comprenda sus funciones y responsabilidades y asegurar que las tareas requeridas para y mantener el BCM están asignadas a individuos competentes cuyo desempeño pueda monitorizarse.

Mantenimiento de BCM en la organización: El mantenimiento del BCM involucra la gestión de un número de proyectos relacionados y la coordinación de las actividades que lo equilibra:

- ***Sensibilización*.** Eventos que mantienen el entusiasmo para llevar a cabo el BCM.
- ***Planificación.*** Desarrollo de planes para responder a los incidentes que pudieran no ocurrir.

- ***Medidas de Mitigación.*** Implementación de medidas para mitigar el impacto de un incidente que pueda ocurrir mientras el programa está siendo desarrollado.

- ***Ejercicio.*** Ejercicios para practicar los planes de contingencia.

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

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

Gestión continua de la Continuidad del Negocio. El BCM necesita gestionarse en un ciclo continuo de mejora para su eficacia. Esto involucra la participación de varias áreas gerenciales, operativas, administrativas y técnicas que necesitan estar coordinadas.

Documentación del BCM. Una parte importante del BCM es la gestión de su documentación, la cual necesita llevarse a cabo de una manera que sea consistente y fácil de entender. El nivel y tipo de documentación debe ser apropiado al tipo y tamaño de la organización.

2.4.4. La organización. La Universidad Francisco de Paula Santander Ocaña, nace institucionalmente el 18 de julio de 1974, a través del acuerdo 003, como una opción de

Educación Superior, para los estudiantes de la provincia de Ocaña y su zona de influencia (UFPSO, www.ufpso.edu.co, 2015).

El 5 de marzo de 1975 se dio inicio a las labores académicas en el Antiguo Convento anexo al Templo de San Francisco, con un programa académico de corte tecnológico denominado "Tecnología en Matemáticas y Física". Posteriormente la Universidad empieza a ofertar la Tecnología en Producción Agropecuaria, Zootecnia, Tecnología en Administración Comercial y Financiera. En su constante preocupación el cuerpo docente y el personal Administrativo, logran más tarde su profesionalización con el programa de Administración de Empresas; así mismo empiezan las Ingenierías de Sistemas, Civil y Mecánica, igualmente se oferta un segundo ciclo de Profesionalización de Tecnología en Producción Agropecuaria, dirigido hacia la Ingeniería Ambiental. (UFPSO, 2015)

2.4.5. <u>Dependencia de la Organización</u>. La Oficina de admisiones, registro y control adscrita a la subdirección académica encargada de mantener actualizados y custodiar los registros académicos de los estudiantes y apoyar los procesos de inscripción, admisión y matrícula.

Misión: Prestar un buen servicio a los estudiantes y demás estamentos en cada uno de los requerimientos que se hagan ya que esta dependencia es un pilar fundamental por los documentos que allí reposan y hacer cumplir las normas del reglamento estudiantil en materia de desempeño.

Visión: La oficina de admisiones registro y control será la dependencia en donde los estudiantes encontrarán sistematizada toda la información académica y con sólo consultar a la página de la universidad y demás información que se requiera en la oficina.

Según Acuerdo N° 084 de septiembre 11 de 1995, el consejo superior universitario, con base en las atribuciones legales y estatutarias que le confieren la ley 30 de 1992 y el Acuerdo N° 029 del 12 de Abril de 1994, aprueba la estructura orgánica de la Universidad Francisco de Paula Santander Ocaña.

2.5. Marco legal

2.5.1. Constitución Política de 1991.

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

2.5.2. Leyes informáticas colombianas.

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

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

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

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

Ley estatutaria 1581 de 2012. Entró en vigencia la Ley 1581 del 17 de octubre 2012 de Protección De Datos Personales, sancionada siguiendo los lineamientos establecidos por el Congreso de la República y la Sentencia C-748 de 2011 de la Corte Constitucional (Alcaldía de Bogotá, 2012).

Como resultado de la sanción de la anunciada ley toda entidad pública o privada, cuenta con un plazo de seis meses para crear sus propias políticas internas de manejo de datos personales, establecer procedimientos adecuados para la atención de peticiones, quejas y reclamos, así como ajustar todos los procesos, contratos y autorizaciones a las disposiciones de la nueva norma

Aspectos claves de la normatividad:

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

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

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

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

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

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

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

Crea el Registro Nacional de Bases de Datos.

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

Capítulo 3: Diseño metodológico

3.1. Tipo de investigación

Para el desarrollo de este proyecto se utilizará la investigación descriptiva con enfoque cuantitativo.

3.1.1. Descriptivo. porque el objetivo principal es conseguir una perspectiva general de un problema o situación. En este caso, se identifican las posibles variables que intervienen y sus relaciones, así como las fuentes de información de problemas o situaciones similares y sus soluciones (Rodríguez Gómez & Valldeoriola Roquet, 2012).

3.1.2. Enfoque Cuantitativo. dado que se usa la recolección de datos para probar una hipótesis con base en la medición numérica y el análisis estadístico para establecer patrones de comportamiento y probar teorías (Dzul Escamilla, 2012).

3.2. Población y muestra

La población a estudiar está conformada directamente por los empleados de la dependencia de Admisiones, Registro y Control.

Debido a que la población objeto de investigación es limitada se trabajara con los 7 funcionarios de la dependencia de Admisiones, Registro y Control, correspondientes al 100% de la población.

3.3. Técnicas e instrumentos de recolección de la información

3.3.1. Fuentes Primarias. Entrevista al Jefe de la dependencia Admisiones Registro y Control.

Visita de observación y aplicación de instrumentos de recolección de la información en la dependencia Admisiones Registro y Control de la UFPS Ocaña.

Documentación institucional de la dependencia Admisiones Registro y Control de la UFPS Ocaña.

3.3.2. Fuentes secundarias. Libros relacionados con la auditoria y continuidad del negocio.

Artículos científicos relacionados con la continuidad del negocio y seguridad de la información.

Leyes, normas y estándares referentes al sistema de gestión de seguridad de la información SGSI.

Capítulo 4: Presentación de resultados

Diseño de un Plan de Continuidad para la Oficina de Admisiones, Registro y Control de la Universidad Francisco de Paula Santander Ocaña

El desarrollo de este trabajo se realizó tomando como referencia la ISO 22301:2012. En este sentido, se inicia contextualizando la institución Universidad Francisco de Paula Santander Ocaña y la dependencia de Admisiones, Registro y control para la cual se realiza el Plan de Gestión de Continuidad del negocio mediante la revisión documental y una auditoría externa, en la que se evaluó la seguridad física y lógica tomando como referencia la ISO 27001:2005.

- Conocer el estado actual de la dependencia de Admisiones, Registro y Control, por medio de una auditoría pasiva.
- Definir estrategias que permitan la continuidad de los procesos de la dependencia de ARC.
- Elaborar el plan de gestión de la continuidad del negocio para la oficina de ARC.

4.1. Conocer el estado actual de la dependencia de Admisiones, Registro y Control, por medio de una auditoría pasiva.

4.1.1 Resumen de la Información general de la Institución. Conocer a la organización implica la revisión de todos aquellos documentos que puedan bridar información sobre ella, como lo es su información organizacional (objetivos misionales, filosofía, misión y visión,

estructura organizacional), sus políticas establecidas ya sean las que rigen sus procesos administrativos, como también las del área de TI y de la seguridad de la información.

La Universidad Francisco de Paula Santander Ocaña (UFPSO), es una institución de educación superior con influencia en el nororiente colombiano. Como toda organización tiene una visión y misión y se ha establecido cinco objetivos misionales, esta información se condensa en la figura 1.

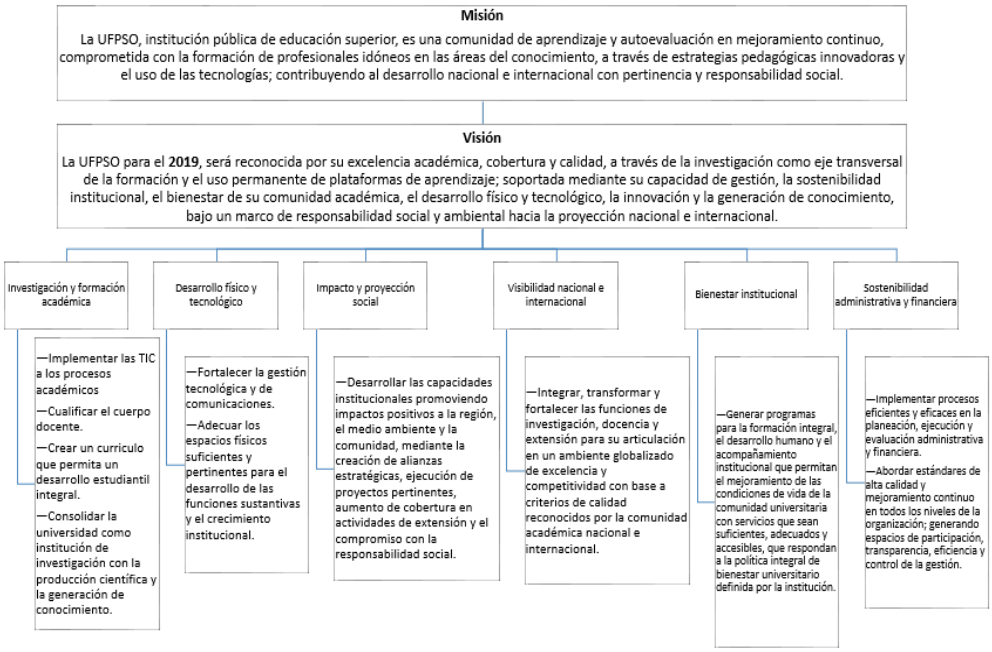


Figura 1. Misión, visión y objetivos misionales

La estructura orgánica fue aprobada por el Consejo Superior Universitario según Acuerdo No. 084 de septiembre 11 de 1995. En esta se puede detallar que la oficina de ARC es una dependencia de la subdirección académica como se muestra en la figura 2.

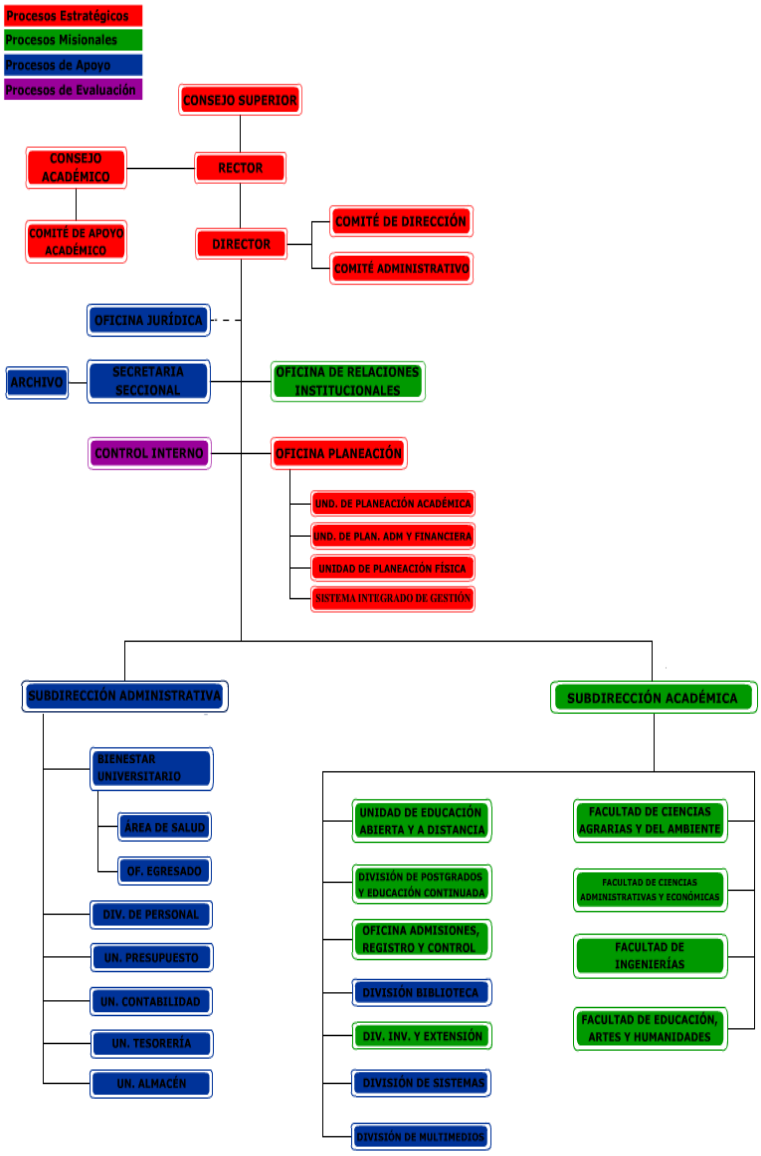


Figura 2. Estructura organizacional de la UFPSO.

4.1.2 Resumen de la Información general de la Dependencia. La oficina de ARC es una dependencia encargada de llevar, mantener actualizados y custodiar los registros académicos de los estudiantes y apoyar los procesos de inscripción, admisión y matrícula (UFPSO, 2016). Esta oficina ha establecido una misión y una visión propia, a saber:

Misión. La oficina de admisiones registro y control es la encargada de recopilar, articular, monitorear y salvaguardar la historia académica de la Universidad al servicio de la comunidad en general, de acuerdo a la normatividad vigente, tecnologías de la información y comunicación, el sistema de gestión de calidad y un talento humano calificado, que contribuya al cumplimiento de los propósitos misionales.

Visión. La oficina de admisiones registro y control académico para el 2019 reflejara criterios de integridad, disponibilidad y confidencialidad para la presentación de un servicio académico oportuno y veraz a la comunidad educativa, respaldado por los avances tecnológicos y de calidad, contribuyendo al desarrollo institucional.

Las funciones que desempeña esta oficina son:

- Coordinar todo lo relacionado con las inscripción, admisión, matrícula y desempeño académico de los estudiantes.
- Conceptuar y asesorar a los directores de planes de estudios aspectos relacionados con la aplicación de normas reglamentarias sobre registro y control del desempeño académico de los estudiantes.
- Expedir las certificaciones académicas entre ellas son: (constancias de estudios, certificados de notas, constancias de buena conducta, constancia terminación de materias y paz y salvo de grado).
- Conservar y custodiar los registros oficiales de los procesos que adelante la dependencia.
- Recibir la documentación de los estudiantes que solicitan graduarse.
- Actualizar los promedios por semestre de todos los estudiantes matriculados.

- Recibir las planillas de notas de todas las carreras de la Universidad por semestre.
- Organizar las carpetas y hacer las hojas de vida académica de los estudiantes que ingresan al primer semestre.
- Llevar el archivo de los graduados.

Por otra parte, también se revisó en el Sistema Integrado de Gestión de la UFPSO los procesos y procedimientos de la oficina de ARC para tener mayor claridad de las actividades realizadas por esta oficina. Entre los documentos que se revisaron se encuentran los siguientes:

- Admisiones, Registro y Control
  - Caracterización
    - Z-AR-ADM-001- Caracterización proceso Admisiones, Registro y Control_rev D
  - Procedimientos
    - R-AR-ADM-001 - Procedimiento Admisión de aspirantes_rev B
    - R-AR-ADM-002 - Procedimiento matricula estudiantes antiguos y control academico_rev B
    - R-AR-ADM-003 - Procedimiento matricula estudiantes nuevos_rev A
  - Instructivos
    - I-AR-ADM-001 - Instructivo tramite a solicitudes y servicios academicos_rev B
  - Manuales
    - M-AR-ADM-001 - Manual especifico de proceso Admisiones Registro y Control_rev D

Una vez se hizo la revisión documental de la dependencia, sus objetivos, misión y visión, funciones y los procesos y procedimientos de la ARC, se procedió a definir los procesos claves como se observa en la figura 3.

Se definieron dos procesos misionales (claves): Admisiones, Matrícula y Registro.

Figura 3. Procesos misionales y procesos de apoyo de ARC.

Los procesos misionales son la razón de ser de la oficina, son quienes definen sus funciones y responsabilidades dentro de la organización. Los procesos de apoyo son otras oficinas/dependencias de la UFPSO que dan soporte técnico o administrativo a los procesos de ARC.

Las figuras 4, 5 y 6 a continuación presentan respectivamente los procesos de Admisiones, Matrícula y Registro con sus respectivos subprocesos; la diagramación realizada se basa en el Método de modelado de negocios (BMM) el cual es orientado al desarrollo de sistemas de información empresarial.

Por otra parte las figuras 7, 8 y 9 presentan una descripción de los procesos principales evidenciado quien los regula, quien los supervisa, que se produce, quien apoya, ejecuta y regula.

El proceso de Admisiones incluye los procesos que va desde la planeación del proceso hasta la selección de los aspirantes como se muestra en la figura 4.

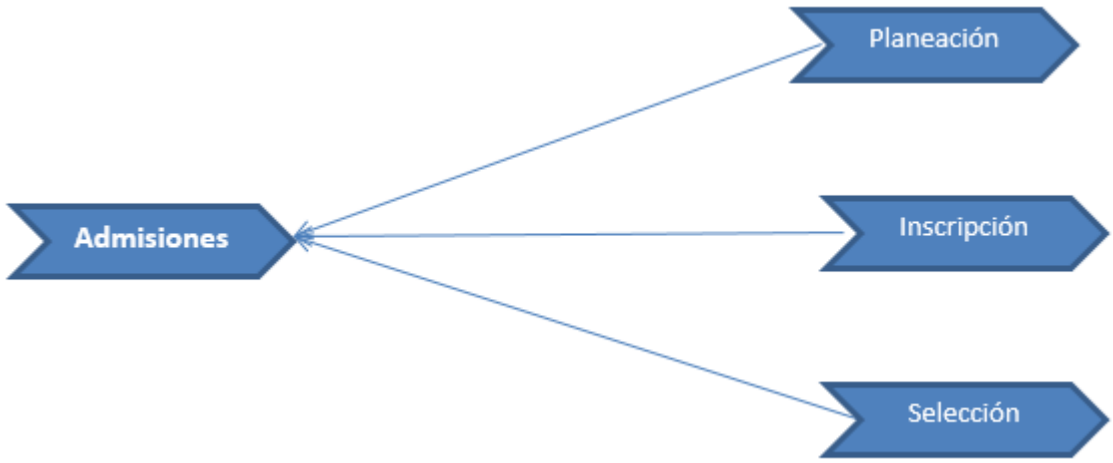


Figura 4. Proceso de Admisiones y sus subprocesos.

El proceso de Matrícula incluye los procesos de matrícula de los alumnos nuevos y matrícula de los alumnos antiguos como se muestra en la figura 5.

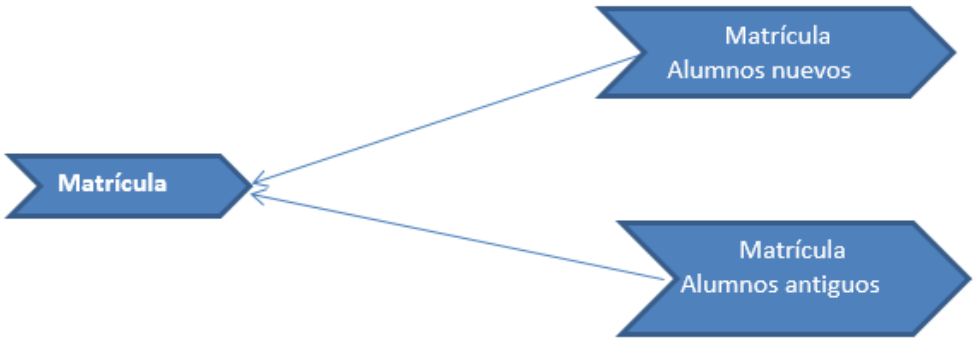


Figura 5 Proceso de matrícula y sus subprocesos.

En el proceso de Registro académico incluye los procesos que tienen que ver con la gestión de la hoja de vida estudiantil, archivo de planillas de notas oficiales, y trámites de grados como se observa en la figura 6.

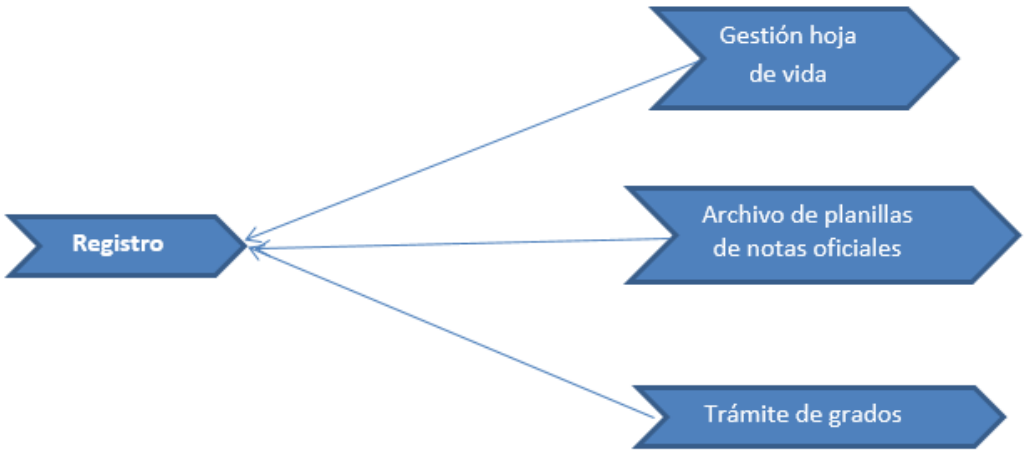


Figura 6 Proceso de Registro académico y sus subprocesos.

Se realizó de igual manera los diagramas de descripción de los procesos.

Para estas gráficas se tuvo en cuenta las siguientes consideraciones: quién supervisa ese proceso, qué requiere y qué genera (entradas y salidas), qué ejecuta ese proceso, por cuáles procesos es apoyado el proceso en cuestión.

En la figura 7 se observa la descripción del proceso de admisiones.

Figura 7 Descripción del Proceso de Admisiones.

En la figura 8 se observa la descripción del proceso de Matrícula.

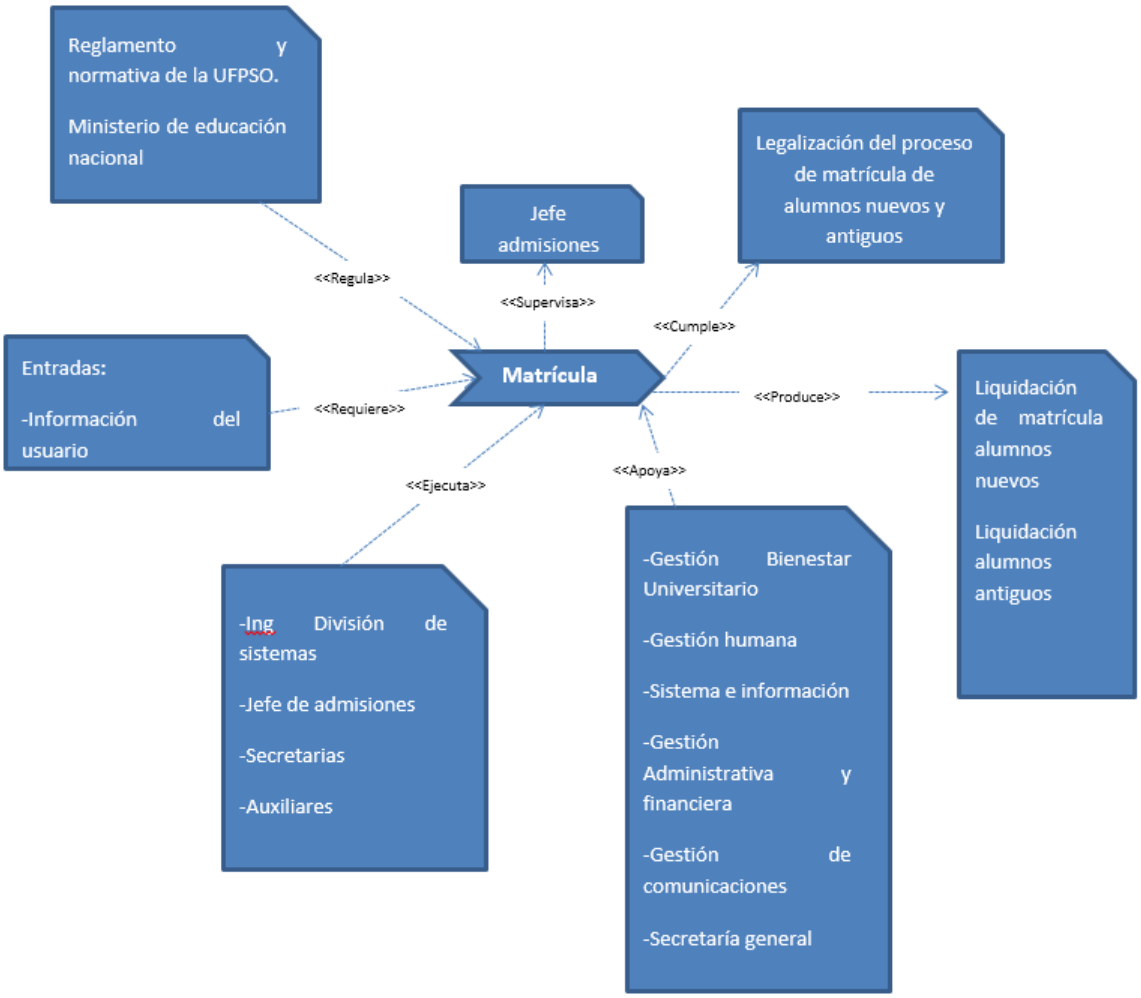


Figura 8 Descripción del Proceso de Matrícula.

En la figura 9 se observa la descripción del proceso de Registro.

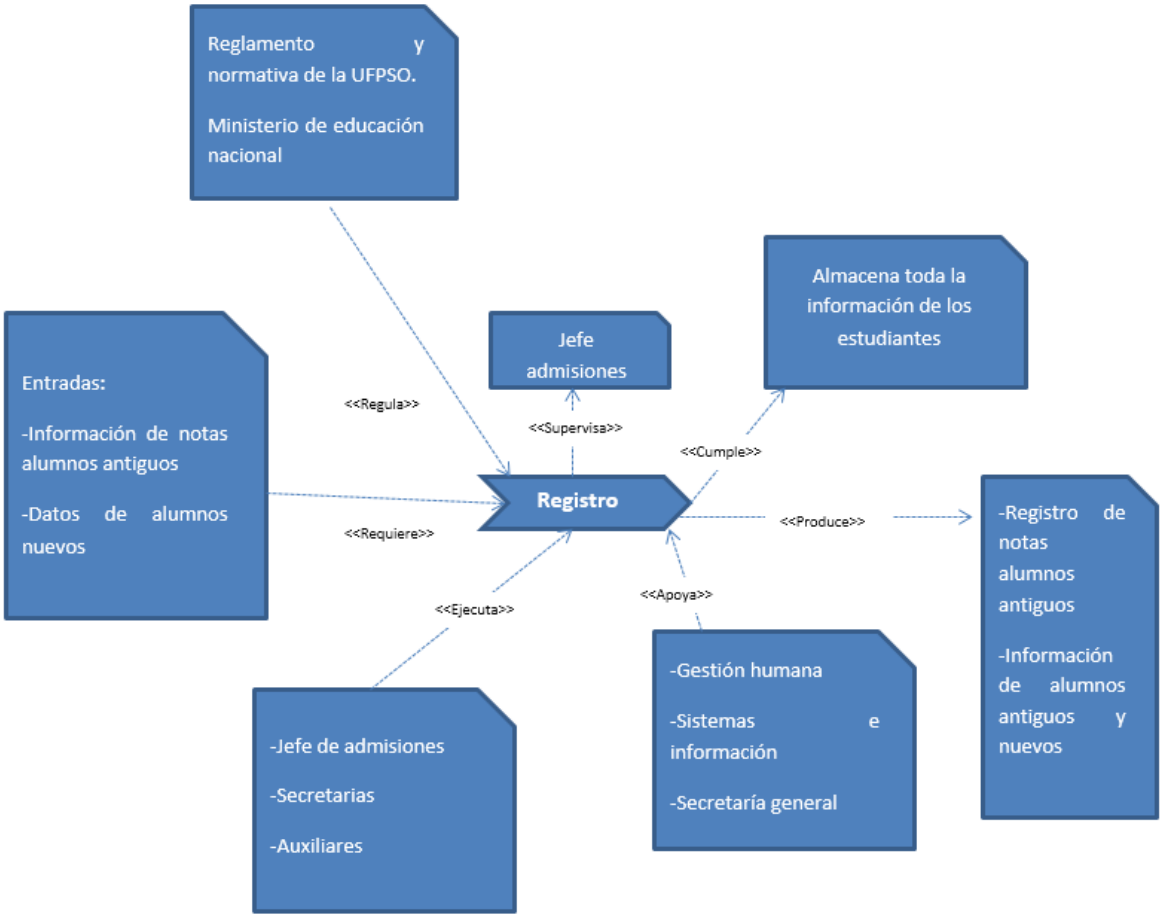


Figura 9 Descripción del Proceso de Registro.

4.1.3. Modelado de Actores

Tabla 2

Proceso 1: Admisiones

Subproceso: Planeación			
Actores	**Ejecuta**	**Supervisa**	**Apoya**
Jefe de Admisiones Registro y Control	**X**		
Subdirección académica		**X**	
Planeación académica		**X**	
División de sistemas			**X**
Subproceso: Inscripción			
Actores	**Ejecuta**	**Supervisa**	**Apoya**
División de sistemas (Ingeniero de apoyo SIA)	**X**		
Secretarias	**X**		
Auxiliares	**X**		
Jefe de Admisiones Registro y Control		**X**	
Tesorería			**X**
Subproceso: Selección			
Actores	**Ejecuta**	**Supervisa**	**Apoya**
Comité de admisiones	**X**		
Jefe de Admisiones Registro y Control		**X**	
División de sistemas (Ingeniero de apoyo SIA)			**X**

Fuente. Autores

Tabla 3

Proceso 2: Matrícula

Subproceso: Matrícula alumnos nuevos			
Actores	**Ejecuta**	**Supervisa**	**Apoya**
División de sistemas (Ingeniero de apoyo SIA)	**X**		**X**
Jefe de Admisiones Registro y Control		**X**	
Planes de estudio			**X**
Jefes de departamento			**X**
Secretarias			**X**
Auxiliares			**X**
Subproceso: Matrícula alumnos antiguos			

Actores	Ejecuta	Supervisa	Apoya
División de sistemas (Ingeniero de apoyo SIA)	**X**		**X**
Jefe de Admisiones Registro y Control		**X**	
Planes de estudio			**X**
Jefes de departamento			**X**
Secretarias			**X**
Auxiliares			**X**

Fuente. Autores

Tabla 4

Proceso 3: Registro

Subproceso: Gestión de hoja de vida académica			
Actores	**Ejecuta**	**Supervisa**	**Apoya**
Secretarias	**X**		
Auxiliares	**X**		
Jefe de Admisiones Registro y Control		**X**	
Subdirección Administrativa			**X**
División de Sistemas			**X**
Planes de estudio			**X**
Subproceso: Archivo de planillas de notas oficiales			
Actores	**Ejecuta**	**Supervisa**	**Apoya**
Secretarias	**X**		
Auxiliares	**X**		
Jefe de Admisiones Registro y Control		**X**	
Planes de estudio			**X**
Subproceso: Trámite de grados			
Actores	**Ejecuta**	**Supervisa**	**Apoya**
Secretarias	**X**		
Auxiliares	**X**		
Jefe de Admisiones Registro y Control		**X**	
Subdirección Administrativa			**X**
División de Sistemas			**X**
Planes de estudio			**X**
Bienestar Universitario			**X**
Secretaria General			**X**
Centro de idiomas			**X**

Fuente. Autores

4.1.4. <u>Instrumentos de recolección de la información.</u> Para dar cumplimiento a este objetivo, se llevó a cabo la creación de los instrumentos de recolección de la información: lista de chequeo, encuesta y entrevista, asimismo se realizó la observación correspondiente a las instalaciones de la dependencia Admisiones Registro y Control, posteriormente se analizó la información recolectada a través de estos instrumentos.

Entrevista. La entrevista estuvo dirigida a la Jefe de la dependencia Admisiones Registro y Control:

- Msc. Torcoroma Velásquez Pérez

Por medio de la entrevista se evidenció que el objetivo principal de la dependencia es llevar y mantener actualizados los registros académicos de los estudiantes, allí se maneja toda la información correspondiente a los estudiantes, desde su inscripción hasta su grado, también se ofrecen servicios referente a certificaciones y registro de procesos académicos.

Existe un manual de funciones en la oficina de personal en el cual se rigen las actividades que deben realizar los empleados, asimismo la dependencia ARC da soporte del proceso de gestión académica e interactúa con las demás dependencias como subdirección académica, administrativa, planeación, secretaría general, dirección y facultades.

Se evidencia que no está siendo implementada una política de seguridad, por lo tanto los funcionarios se rigen por el uso de controles ya establecidos, igualmente se encuentran inventariados los equipos y el software instalado de los cuales es responsable la división de sistemas.

En cuanto a la contratación, la división de personal es la encargada según la decisión de la dirección.

Los funcionarios de la dependencia no reciben capacitaciones con respecto a la gestión segura de la información.

Observación. Con el propósito de recolectar la información inicial para realizar la investigación acerca de la dependencia Admisiones, registro y control, se realizó una observación en la cual se evidenció lo siguiente:

- Las instalaciones físicas se encuentran dentro de la casona de la UFPS Ocaña, se pudo observar que existen ciertas divisiones dentro de la oficina con espacio pequeño para sus trabajadores, por lo tanto no es idóneo.

- Se observó que se mantiene un gran volumen de información física en carpetas y archivadores.

- En la recepción de la oficina se encuentran ubicadas dos secretarias encargadas de atender las solicitudes respecto a certificados, constancias y demás documentos que se gestiona desde la dependencia, de igual manera se pudo determinar que los el proceso realizado por la dependencia se relaciona con las de otras oficinas dado que el estudiante debe realizar varios procesos en otras dependencias para que se les pueda ser suministrado lo que solicitan.

- Por otra parte se observa que cada uno de los funcionarios cuenta con un equipo de cómputo, desde el cual realiza la gestión de información por lo que se evidencia la necesidad de garantizar la seguridad de los mismos, dado que contienen información relevante para el proceso.

- Tampoco se evidenció la existencia de detectores de humo, ni alarmas contra incendios ni otras medidas para prevenir incidentes de este tipo.

Lista de chequeo. Por medio de la lista de chequeo se evidenció que no está siendo implementada una política de seguridad de la información, sin embargo si se cuenta con una evaluación de riesgos. Con respecto a la seguridad física, no cuenta con dispositivos de seguridad para la extinción del fuego.

Tecnológicamente la oficina de ARC se encuentra soportada por otra dependencia de la UFPS Ocaña, llamada División de Sistemas, esta dependencia también es responsable de la gestión de las comunicaciones y operaciones, también se puede aclarar que en el momento no existe un plan de continuidad del negocio en la dependencia ARC.

Se evidencia de la misma manera que no se establecen responsabilidades ni existen procedimientos ante incidentes relacionados con la seguridad de la información, asimismo los equipos pertenecientes a la oficina no cuentan con el uso adecuado de contraseñas que permitan evitar cualquier acceso no autorizado.

Encuestas. La encuesta fue realizada a los empleados de la dependencia ARC, debido a motivos de ocupación de fuerza mayor sólo se obtuvo la información de cinco personas de las siete que se manifestaron en la muestra de este proyecto.

Tras analizar la información recolectada a través de la encuesta, se pudo apreciar la mayoría del personal encuestado afirma la existencia de la Política de Seguridad, pero dado a la entrevista realizada al jefe de la dependencia, se concluye que no está siendo implementada una política de seguridad de la información.

Los empleados expresaron que no firman acuerdos de confidencialidad y que desconocen los procesos disciplinarios en los cuales se pueden ver implicados en caso de divulgar información confidencial.

Se evidenció que se realizan copias de seguridad de la información tanto física, que se almacena en la misma dependencia, así como digital. Los empleados que diligenciaron la encuesta revelaron que desconocen la existencia de un plan de contingencia.

En la figura 10 se observa que el 60% de las personas encuestadas manifiesta que si existe una política de seguridad de la información, frente a un 40% que respondió que no existe tal política, estos resultados y los obtenidos en la entrevista nos permite concluir que a pesar de que no se pudo comprar la existencia de la política si se presume, sin embargo no se encuentra oficializada.

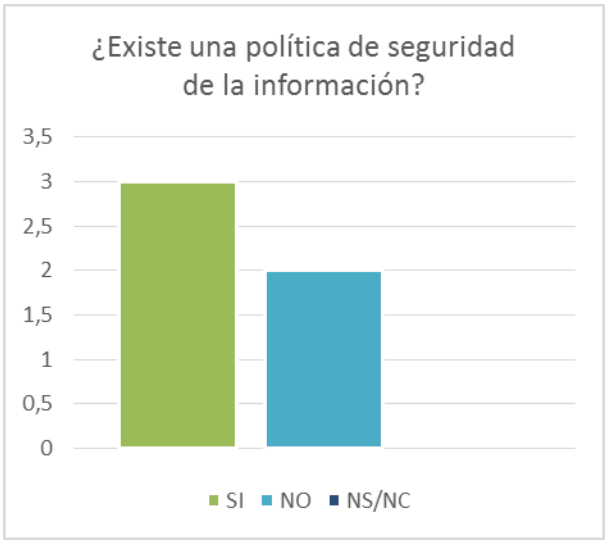


Figura 10. ¿Existen una política de seguridad de la información?

El 60% de los encuestados dice conocer y entender la política de seguridad, su propósito e implicaciones, como se muestra en la Figura 11. Se puede observar que la cantidad de personas que en la pregunta anterior afirman sobre la existencia de la política, son la misma que dicen conocerla, esto podría indicar que no se realizan las capacitaciones necesarias para el 100% de los funcionarios entiendan y conozcan sobre la política aunque no se halla oficializado.

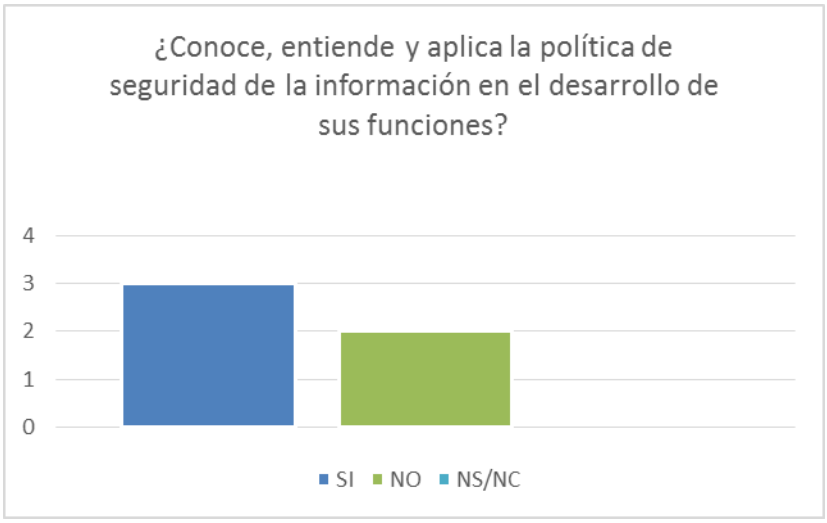


Figura 11. ¿Conoce, entiende y aplica la política de seguridad de la información en el desarrollo de sus funciones?

Con respecto a si reciben capacitaciones acerca de la gestión segura de la información, el 80% manifestó que casi nunca las reciben y el 20 % dijo que nunca recibían dichas capacitaciones, como lo muestra la figura 12, esto evidencia un grave riesgo de una posible mala gestión de la información por desconocimiento.

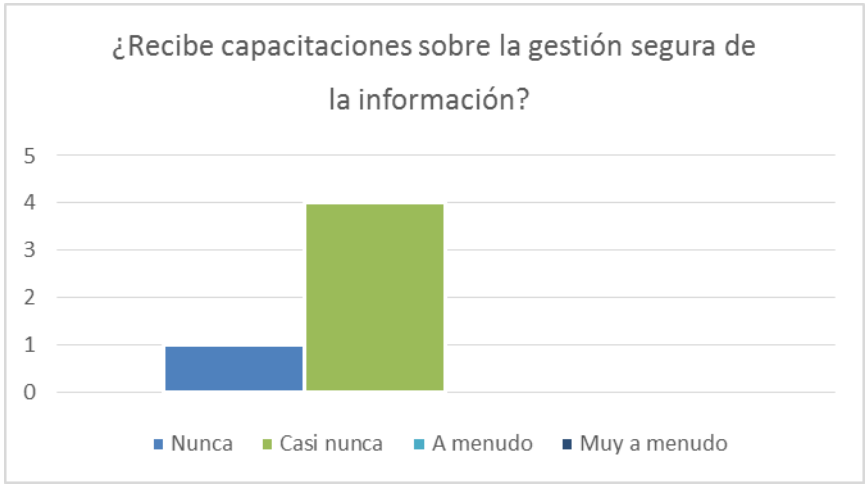


Figura 12. ¿Recibe capacitaciones sobre la gestión segura de la información?

Al preguntar si se entendía y tenía claro la importancia de conservar la integridad de la información que se maneja en la dependencia, el 100% de los encuestados manifestó que sin entienden con claridad la importancia de conservar la integridad de la información que se gestiona desde la dependencia, como se observa en la figura 13.

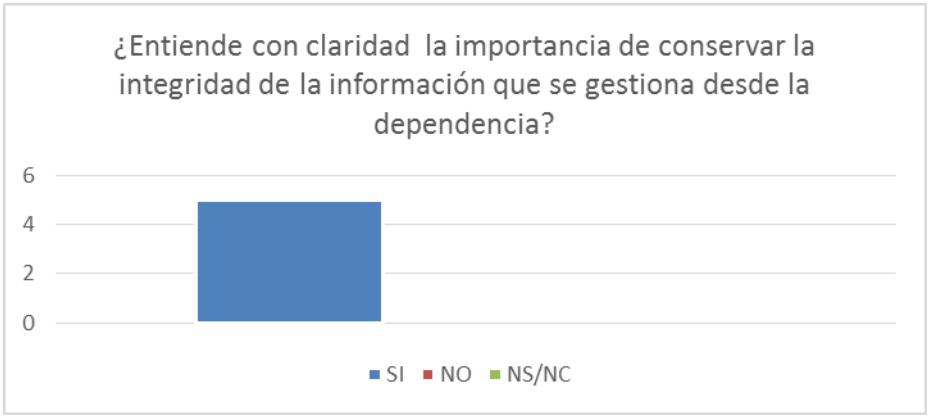


Figura 13. ¿Entiende con claridad la importancia de conservar la integridad de la información que se gestiona desde la dependencia?

El 80% de las personas encuestadas coincidieron en que existen restricciones de acceso a la información para el personal que labora en la dependencia Admisiones Registro y Control, frente a un 20% que manifiesta que no existen tales controles y que todos tienen acceso la misma, tal como se observa en la figura 14.

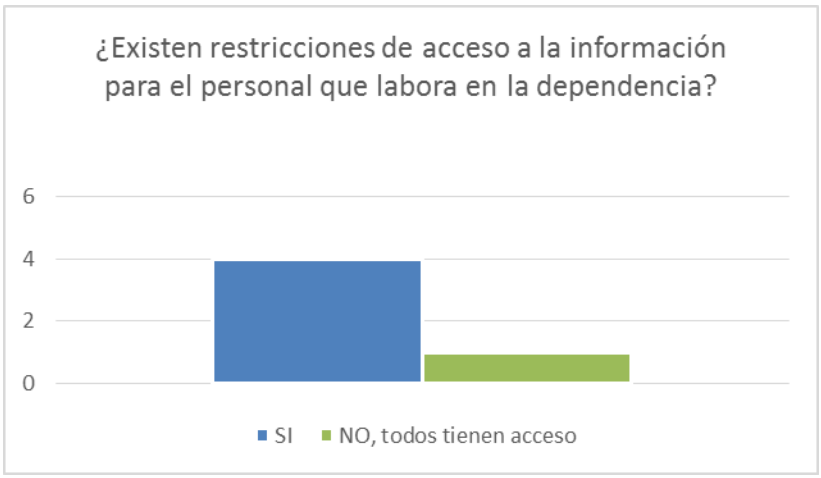


Figura 14. ¿Existen restricciones de acceso a la información para el personal que labora en la dependencia?

En cuanto a si se firmó un acuerdo de confidencialidad de no divulgación respecto al tratamiento de la información que se maneja en la dependencia, como se muestra en la figura 15, el 100% de los encuestados respondieron que no se firmó dicho acuerdo, esto evidencia que los funcionarios desconocen la cláusula de confidencialidad que existen en los contratos, por lo que se hace necesario establecer un mecanismos más específico para ellos comprendan a que comprometen en cuanto al manejo de la información y cuáles serían las recursiones que tendrían en caso de violar la confidencialidad.

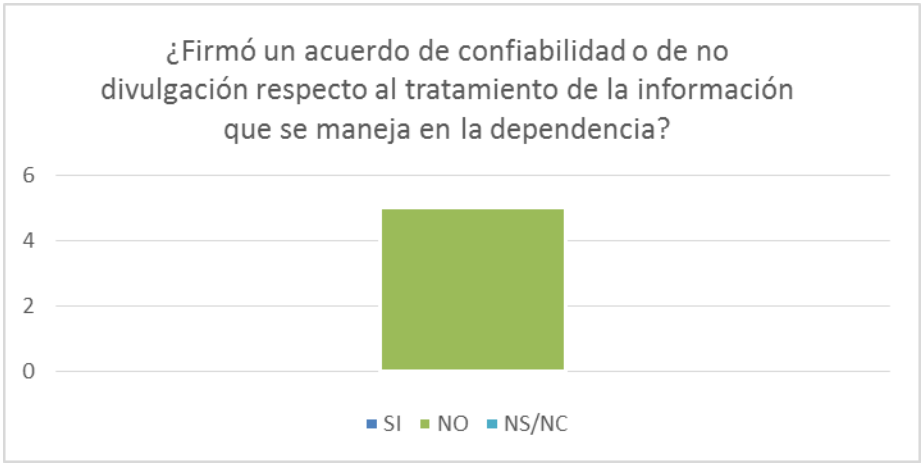


Figura 15. ¿Firmó un acuerdo de confiabilidad o de no divulgación respecto al tratamiento de la información que se maneja en la dependencia?

Al preguntar a los encuestados si conocen los procesos disciplinares en caso de divulgar información, el 60% contestó que no, frente a un 40% que respondió que si los conocen, como se observa en la figura 16.

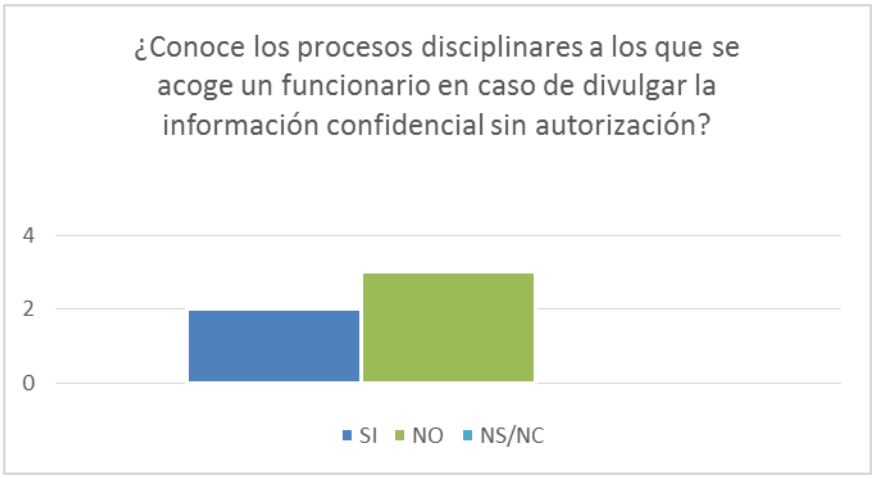


Figura 16. ¿Conoce los procesos disciplinares a los que se acoge un funcionario en caso de divulgar la información confidencial sin autorización?

El 60% de los encuestados manifestó que la información física que se almacena en la oficina está protegida frente a un 40% que respondió que no, como se muestra en la figura 17, estos resultados se contrastan con los obtenidos de otras fuentes y se asume que no existe respaldo de la información física y que la oficina no es la adecuada para mantener el volumen de información que se maneja.

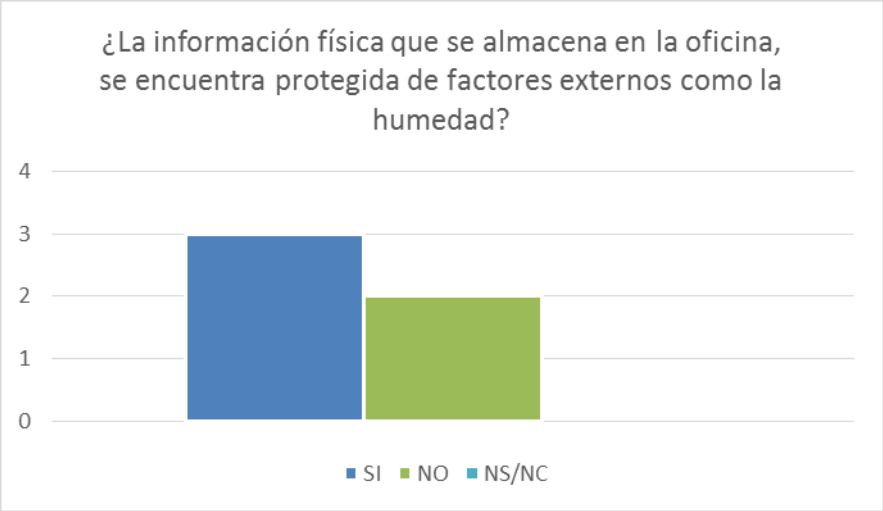


Figura 17. ¿La información física que se almacena en la oficina, se encuentra protegida de factores externos como la humedad?

La figura 18 muestra que el 100% de los encuestados manifiesta que existen copias de respaldo de la información física, sin embargo esta premisa no fue posible verificarla incluso los demás resultados obtenidos demuestran lo contrario.

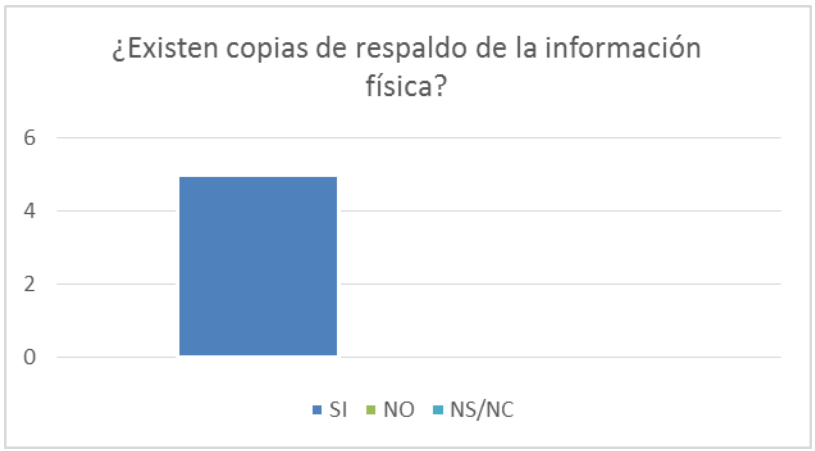


Figura 18. ¿Existen copias de respaldo de la información física?

La figura 19 muestra que así como el 100% de los encuestados manifestó que tenían copias de seguridad, estas se almacenan en la misma oficina, en caso de que esta premisa

sea verdadera el guardar dichas copias dentro de la misma oficina implica un alto porcentaje de riesgo de pérdida en las mismas condiciones que las originales.

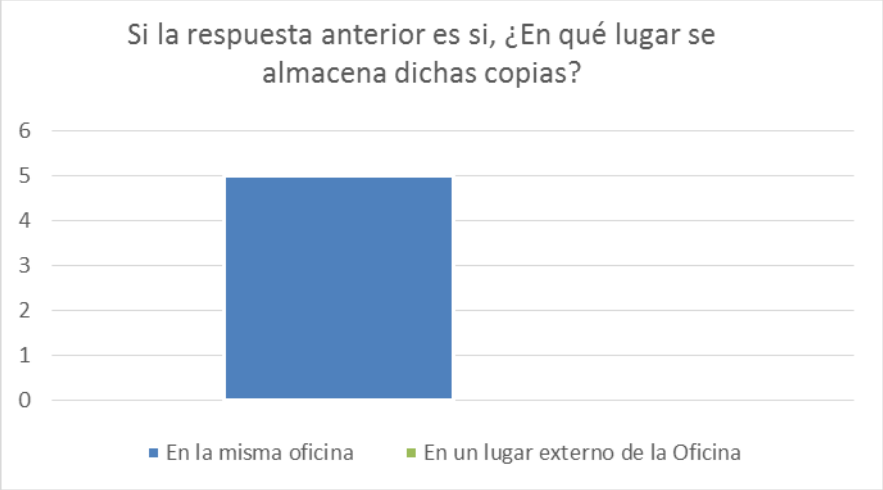


Figura 19. Si la respuesta anterior es si, ¿En qué lugar se almacena dichas copias?

De igual manera en la figura 20 se ve reflejado que el 100% de los encuestados respondió que existen copias de seguridad digitales de la información, este resultado contradice el obtenido a través de la entrevista al jefe de la dependencia y tampoco fue posible su comprobación.

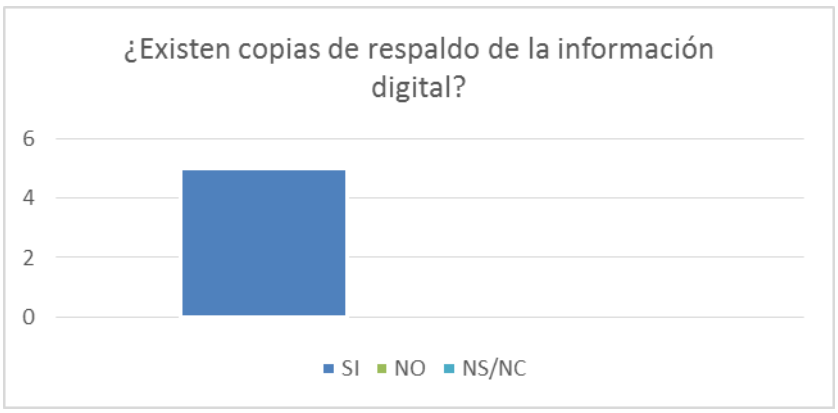


Figura 20. ¿Existen copias de respaldo de la información digital?

En la figura 21 el 80% se los encuestados manifiesta que existen restricciones para entregar información a terceros cuando la solicitan, por ejemplo cuando se solicita una constancia de terminación de materias o cualquier otro documento de los que se emitan desde la dependencia, frente a un 20% que no sabe la respuesta.

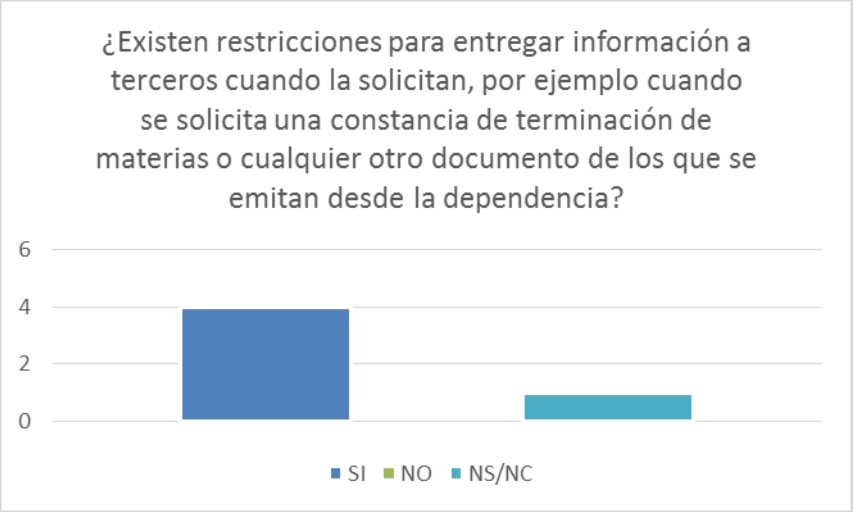


Figura 21 ¿Existen restricciones para entregar información a terceros cuando la solicitan, por ejemplo cuando se solicita una constancia de terminación de materias o cualquier otro documento de los que se emitan desde la dependencia?

Según las respuestas de los encuestados el 100% de ellos manifestó que no conocen la existencia de un plan de contingencia de riesgos, como lo muestra la figura 22.

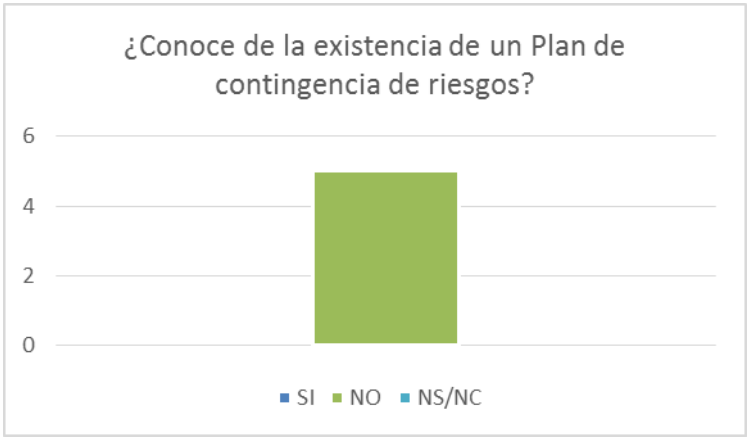


Figura 22 ¿Conoce de la existencia de un Plan de contingencia de riesgos?

Con respecto a la pregunta sobre si saben cómo actuar en caso de presentarse un incidente natural para proteger tanto su integridad personal, como la de la información almacenada en la dependencia el 100% de los encuestados respondió que no saben cómo actuar frente a estos casos, como lo muestra la figura 23.

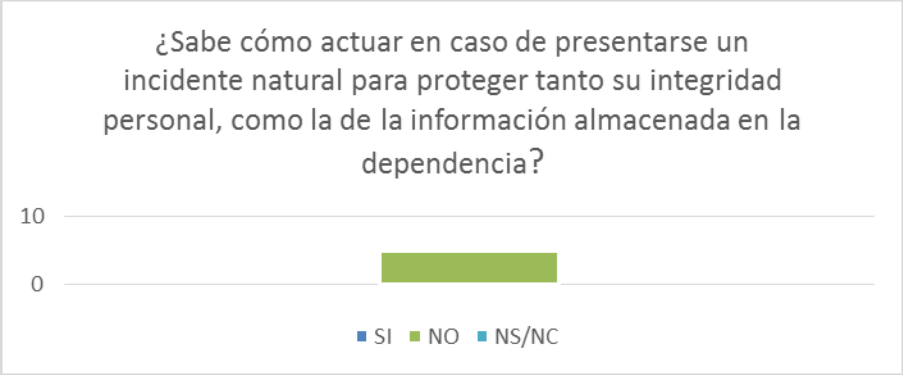


Figura 23 ¿Sabe cómo actuar en caso de presentarse un incidente natural para proteger tanto su integridad personal, como la de la información almacenada en la dependencia?

El 100% de los encuestados manifestó que no se tienen implementados controles de detección, prevención y recuperación contra el software malicioso, junto a procedimientos adecuados para la concienciación de los usuarios, como se muestra en la figura 24.

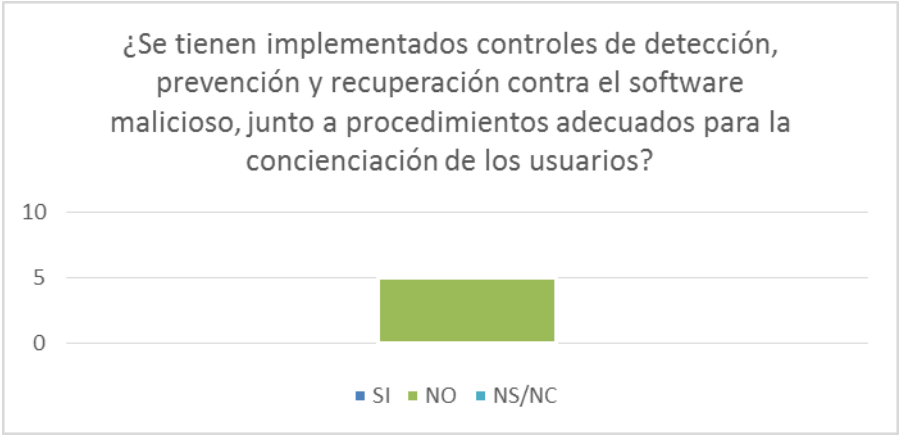


Figura 24 ¿Se tienen implementados controles de detección, prevención y recuperación contra el software malicioso, junto a procedimientos adecuados para la concienciación de los usuarios?

En la figura 25 el 80% de las personas encuestadas respondió que se implementan parámetros de contraseñas seguras, frente a un 20% que dijo que no se implementan dichos parámetros.

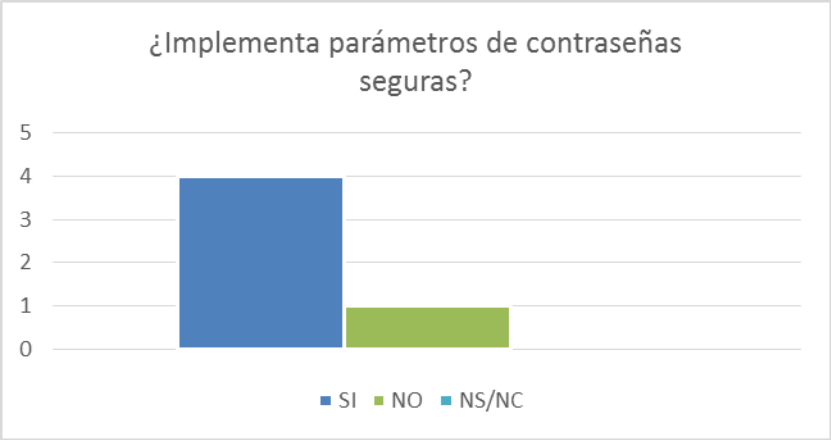


Figura 25 ¿Implementa parámetros de contraseñas seguras?

La figura 26 muestra que el 60% de las personas encuestadas manifiestan que se realiza mantenimiento preventivo y correctivo a los equipos de cómputo, frente a un 40% que respondió que no se hacen estas operaciones.

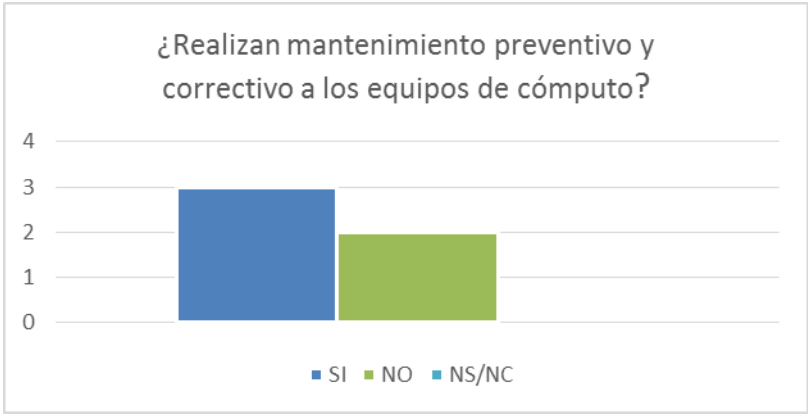


Figura 26 ¿Realizan mantenimiento preventivo y correctivo a los equipos de cómputo?

El mantenimiento preventivo y correctivo según el 60% de las personas encuestadas se realiza muy a menudo y el 40% restante manifiesta que se realizan a menudo, tal como se observa en la figura 27.

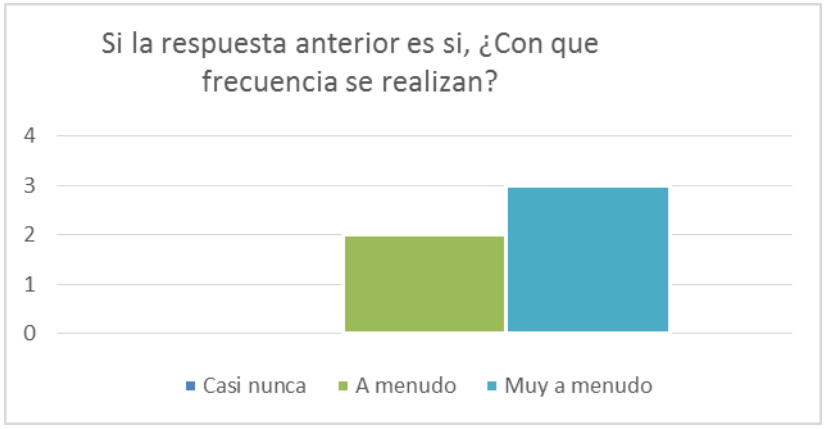


Figura 27 Si la respuesta anterior es si, ¿Con que frecuencia se realizan?

En lo referente a si se verifica la integridad de la información física que se almacena en la dependencia, el 20% manifiesta que casi nunca se verifica, frente al 80% restante que respondió que se verificaba a menudo y muy a menudo, como se observa en la figura 28.

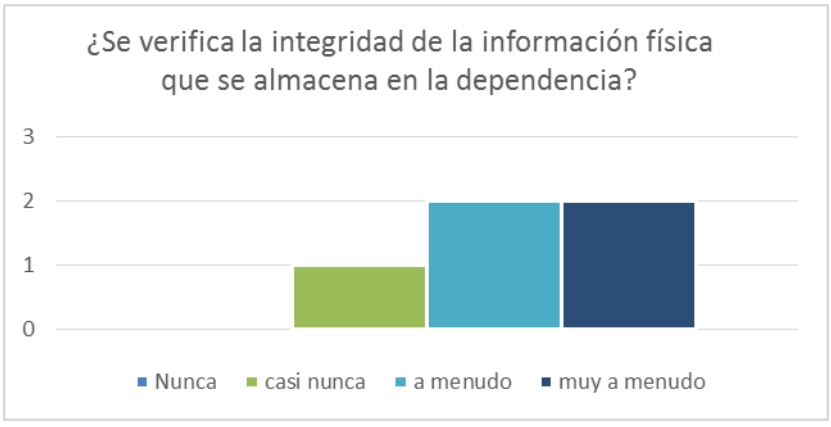


Figura 28 ¿Se verifica la integridad de la información física que se almacena en la dependencia?

A la pregunta sobre si se toman medidas preventivas para evitar que la información física se deteriore, el 60% manifestó que no, frente a un 40% que respondió afirmativamente, como se muestra en la figura 29.

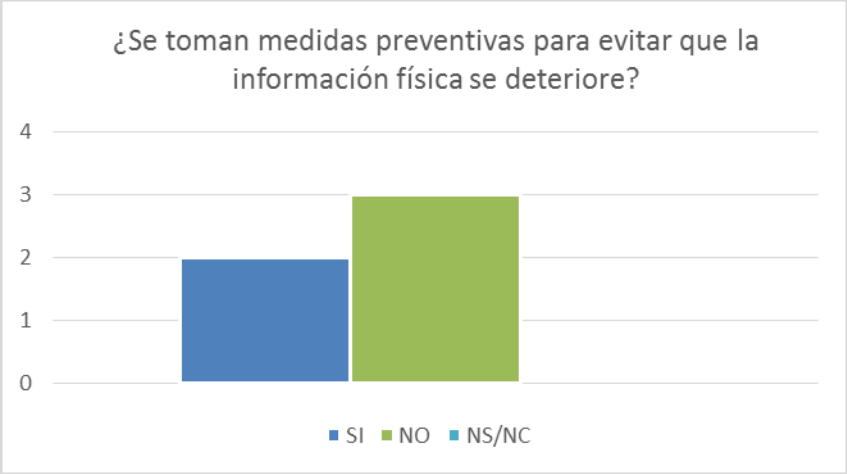


Figura 29¿Se toman medidas preventivas para evitar que la información física se deteriore?

La figura 30 muestra que el 60% de los encuestados manifestaron que si existen restricciones de acceso de personal no autorizado a l dependencia, mientras que el 40% restante respondió de forma negativa.

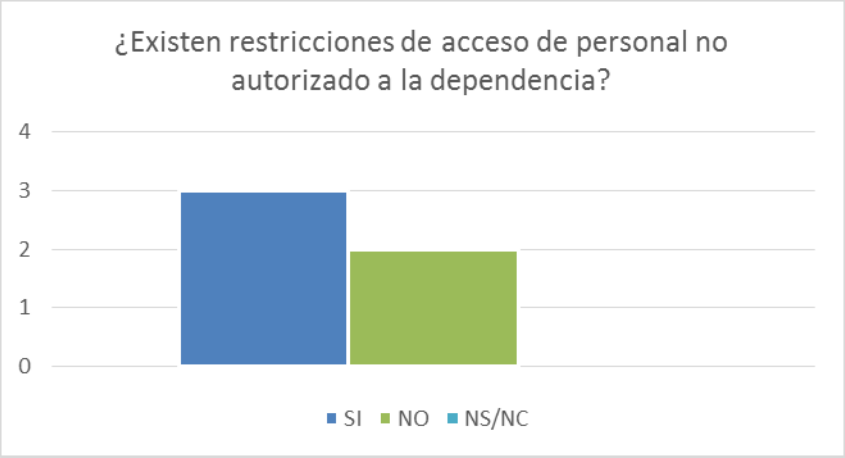


Figura 30 ¿Existen restricciones de acceso de personal no autorizado a la dependencia?

En cuanto a la pregunta sobre si considera que la ubicación de la dependencia dentro del campus es idónea, la figura 31 muestra que el 60% respondió que no, frente a un 40% que manifestó que si es una buena ubicación.

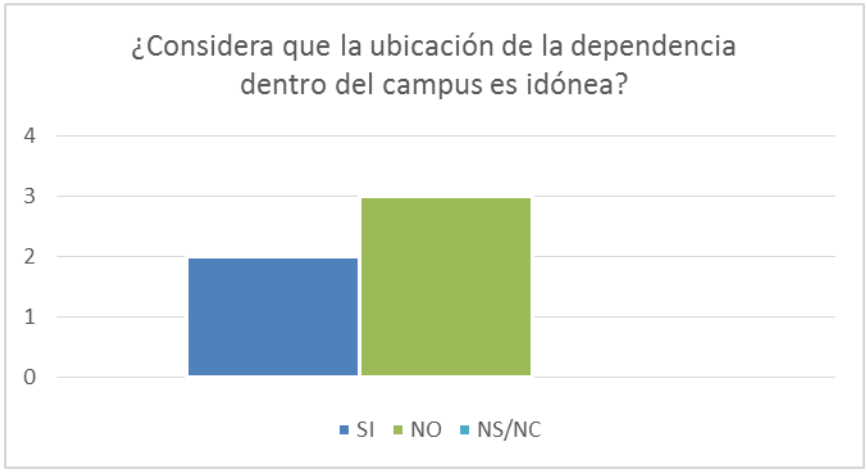


Figura 31 ¿Considera que la ubicación de la dependencia dentro del campus es idónea?

En la figura 32 se observa que el 100% de las personas encuestadas consideran que la amplitud física de la oficina no es adecuada para almacenar toda la información física.

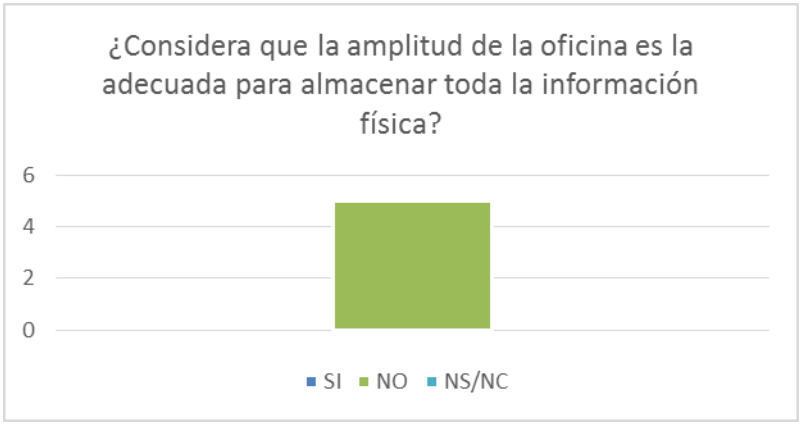


Figura 32 ¿Considera que la amplitud de la oficina es la adecuada para almacenar toda la información física?

4.1.5. Dictamen de la Auditoría. Para la realización de la auditoría externa de la dependencia ARC se siguió el Programa de Auditoría descrito en el anexo A.

Ocaña 01 de junio de 2015

Magister

TORCOROMA VELASQUEZ

JEFE DE ÁREA

E. S. D.

Reciba un cordial saludo de parte de nuestro equipo de auditores. Hacemos llegar a su despacho el dictamen de la auditoría practicada al área de Admisiones, Registro y Control orientada a la seguridad física y lógica de los equipos y la información, esta labor se realizó entre el 27 de marzo de 2015 y el 27 de mayo de 2015.

A continuación me permito informarle qué puntos fueron evaluados durante el proceso de auditoría:

Se efectuaron inspecciones sobre:

- Aspecto de seguridad general: lógica y física.
- Manuales: Procedimientos, planes de contingencia y uso de equipos.
- Recursos hardware y software
- Protección lógica

De acuerdo con lo antepuesto se jerarquizaron las situaciones presentes por su importancia, tomando como referencia los resultados que arrojó la investigación según las técnicas de recolección de datos aplicada como la observación directa, cuestionario al

personal administrativo, lista de chequeo y análisis de resultados, permitiendo presentar a continuación los siguientes hallazgos:

La dependencia no cuenta con respaldo digital de todos los archivos físicos que se maneja en el área, las copias digitales por tanto son realizadas por la División de Sistemas. Esto a causa de que no existe una política de digitalización de archivos según la normatividad establecida (Ley General de Archivo). No tener esta política en la oficina y teniendo en cuenta que la información manejada por la dependencia a su cargo es de vital importancia para la institución, la pérdida parcial o total de los documentos puede comprometer los registros históricos de la institución. Se recomienda establecer una política de digitalización de archivos.

No hay registro evidente de las licencias de software, eso a causa de la tercerización de la responsabilidad en los recursos tecnológicos a otra dependencia de la universidad. A la falta de legalidad de las licencias se incurre a una falta grave de sanción e inhabilidades por parte de los organismos de control. Se recomienda verificar que la dependencia de soporte tenga actualizada dicho registro, que los equipos cuenten con su respectiva licencia.

También se evidenció que no existen detectores de humo, ni alarmas contra incendios ni otras medidas para prevenir, detectar en el menor tiempo posible y mitigar este tipo de incidentes. La no implementación de estas medidas compromete la información almacenada en los archivos físicos, equipos de cómputo y demás activos de la dependencia. Recomendación: Aplicar las medidas de contingencia adecuadas a este tipo de situaciones.

Tampoco se cuenta con las medidas físicas apropiadas para evitar la entrada de personal no autorizado fuera del horario establecido, la oficina no cuenta con un sistema de protección ante robos; esto aumenta el robo, sabotaje, o pérdida intencional o involuntaria de la información y demás activos de la dependencia. Se recomienda establecer medidas de seguridad física a las instalaciones para evitar que se sustraigan equipos o información.

En cuanto a la seguridad lógica, los equipos de cómputo no cuentan con contraseñas para garantizar el ingreso de personas no autorizadas. Los accesos no autorizados a los sistemas de información tecnológica que puedan ser usados para comprometer la integridad, confidencialidad y disponibilidad de la información. Se recomienda establecer contraseñas a nivel de BIOS o sistema operativo o ambas para garantizar la confidencialidad de la información almacenada en dichos equipos.

Se recomienda en forma general implementar los elementos de seguridad tanto lógica como física para un buen funcionamiento de los equipos de cómputo y manejo de la información del área de Admisiones, Registro y Control.

4.2. Definir estrategias que permitan la continuidad de los procesos de la dependencia de ARC.

4.2.1. Esquema de evaluación de procedimientos

Procesos clave. Son aquellos que tienen un alto impacto sobre los clientes y su satisfacción y/o conducen a la organización a alcanzar sus objetivos. Producen resultados que son estratégicamente importantes para el éxito de la organización. (Koppell, 2011)

Procesos de Apoyo o secundarios. Son procesos, aunque no menos importantes, no tienen esos efectos tan inmediatos o, incluso, su fallo no se haría notar a corto o medio plazo sobre los productos y/o servicios de la organización. (Koppell, 2011)

A continuación se presentan la descripción de los procesos a través de la tabla 5 y 6. Como se podrá observar los procesos Claves o principales son:

- Admisiones
- Matrícula
- Registro

Y los procesos de apoyo son

- Conceptuar y asesorar a los directores de planes de estudios aspectos relacionados con la aplicación de normas reglamentarias sobre registro y control del desempeño académico de los estudiantes.

- Expedir las certificaciones académicas.

- Conservar y custodiar los registros oficiales de los procesos que adelante la dependencia.

- Recibir la documentación de los estudiantes que solicitan graduarse.

- Actualizar los promedios por semestre de todos los estudiantes matriculados.

- Recibir las planillas de notas de todas las carreras de la Universidad por semestre.
- Organizar las carpetas y hacer las hojas de vida académica de los estudiantes que ingresan al primer semestre.
- Llevar el archivo de los graduados.

Estos últimos se catalogaron como de apoyo dado que algunos de ellos se relacionan directamente con los procesos claves y otros no pero son también importantes y su posposición temporal (a corto plazo) no limita otras actividades de la dependencia o de la institución.

Como se puede observar todos los procesos realizados por las dependencia son importantes solo se podría aceptar interrupciones de procesos a corto plazo, buscando mecanismos que permitan restablecerlos rápidamente.

Este análisis se realiza con el propósito de determinar la prioridad de los mismos y así poder plantear estrategias de recuperación en ese orden, que permitan dar continuidad a la dependencia.

Se puede concluir a través de las descripciones de los procesos que ARC trabaja en conjunto con otras dependencia de la institución con el propósito de dar cumplimiento a los objetivos misionales.

Tabla 5

Evaluación de los procesos Claves o principales

Proceso		Descripción
Coordinar todo lo relacionado con las inscripción, admisión, matrícula y desempeño académico de los estudiantes.	Admisión	Gestionar las actividades necesarias para la inscripción de aspirantes, de tal manera que se pueda garantizar que el procedimiento se realice de manera oportuna y en los tiempos establecidos por calendario académico. Coordinar el procedimiento de selección mediante la generación de listados de inscritos, admitidos y no admitidos y la publicación en los medios de comunicación dispuestos para ello.
	Matrícula	*Establecer las actividades necesarias para realizar el procedimiento de matrícula de los estudiantes nuevos en los diferentes programas académicos que ofrece la institución. *Establecer las actividades necesarias para realizar el procedimiento de matrícula de los estudiantes antiguos y su control académico en los diferentes programas académicos que ofrece la institución.
	Registro	* Gestionar la hoja de vida académica de los estudiantes que estuvieron matriculados en el semestre que culminó y solicitar la expedición de carné de egresado de estudiantes próximos a graduarse. * Archivo de planillas oficiales de notas. * Revisión de documentos y expediente académico de estudiantes * Trámites de grado

Tabla 6

Evaluación de los procesos de apoyo

Proceso		Descripción
Conceptuar y asesorar a los directores de planes de estudios aspectos relacionados con la aplicación de normas reglamentarias sobre registro y control del desempeño académico de los estudiantes.		
Expedir las certificaciones académicas.	Certificados de notas.	* Para expedirlo se requiere un recibo de pago expedido por la oficina de Tesorería de la institución. * Para su validez requiere la firma del jefe de subdirección académica y del jefe de ARC.
	Constancias de estudio.	* Para expedirlo se requiere un recibo de pago expedido por la oficina de Tesorería de la institución. * Para su validez requiere la firma del jefe de ARC.
	Constancias de buena conducta.	* Para expedirlo se requiere un recibo de pago expedido por la oficina de Tesorería de la institución. * Para su validez requiere la firma del jefe de ARC.

	Constancia terminación de materias o paz y salvo académico.	* Para expedirlo se requiere un recibo de pago expedido por la oficina de Tesorería de la institución. * Para su validez requiere la firma del jefe de ARC.
	Paz y salvo de grado.	* Para expedirlo se requiere entrega de documentos para grado de parte del estudiante y el recibo de pago de tesorería de UFPS Ocaña.
	Hoja de vida académica.	* Para expedirlo se requiere Solicitud de fotocopia de hoja de vida académica por parte del estudiante con el recibo de pago expedido por la oficina de Tesorería de la institución. * Para su validez requiere la firma del jefe de subdirección académica y del jefe de Secretaria General.
	Cancelación de materias.	* Para expedirlo se requiere Solicitud de cancelación de materias por parte del estudiante con el formato F-ARADM-006 y el recibo de pago expedido por la oficina de Tesorería de la institución en caso de que el trámite se realice fuera del tiempo establecido para cancelaciones gratuitas.
	Cancelación de semestre (Matrícula).	Para expedirlo se requiere Recepción de oficio de aprobación de cancelación de semestre enviada por parte de la facultad donde se realizó la solicitud.
	Validaciones.	Para expedirlo se requiere la recepción de acta de validación debidamente diligenciada enviada por parte del plan de estudio donde se realizó la solicitud.
	Segundo y tercer calificador.	Para expedirlo se recepción de oficio del segundo y tercer calificador enviada por parte de los planes de estudio o de subdirección académica donde se realizó la solicitud.
	Homologaciones.	Para expedirlo se requiere recepción de la resolución de homologación debidamente diligenciada enviada por parte del plan de estudio donde se realizó la solicitud.
	Retiro de documentos.	Para expedirlo se requiere solicitud de retiro de documento por parte del aspirante inscrito.
	Transferencias.	Para expedirlo se requiere: * Recepción del listado de transferencias aprobadas por los planes de estudio y * Recepción del pago de liquidación de la matrícula por parte del aspirante * Recepción de la resolución de homologación F-AC-SAC-002 debidamente diligenciada enviada por parte del plan de estudio donde se realizó la solicitud.
	Reintegros.	Para expedirlo se requiere recepción de la aprobación de reintegro enviada por parte de los planes de estudio donde se realizó la solicitud.
	Traslados.	Para expedirlo se requiere: * Recepción del listado de traslados internos o traslados sede central aprobados por los planes de estudio. * Recepción del pago de liquidación de la matrícula por parte del aspirante.
Conservar y custodiar los registros oficiales de los procesos que adelante la		*Identificar los factores de riesgos asociados al proceso y establecer las acciones encaminadas a prevenirlos y mitigarlo.

dependencia.	
Recibir la documentación de los estudiantes que solicitan graduarse.	
Actualizar los promedios por semestre de todos los estudiantes matriculados.	
Recibir las planillas de notas de todas las carreras de la Universidad por semestre.	
Organizar las carpetas y hacer las hojas de vida académica de los estudiantes que ingresan al primer semestre.	
Llevar el archivo de los graduados.	

4.2.2. Matriz DOFA. Para esta investigación de implementó la matriz DOFA dado que es una herramienta analítica que le permitirá trabajar con toda la información que se recopila a través de las fuentes tanto primarias como secundarias, también en la figura 33 se detalla la estructura de una matriz DOFA, (UPIICSA).

Dejar siempre en blanco	Debilidades (D) Lista de Debilidades	Fortalezas (F) Lista de Fortalezas
Oportunidades (O) Lista de Oportunidades	Estrategias (DO) Vencer debilidades aprovechando oportunidades	Estrategias (FO) Uso de fortalezas para aprovechar oportunidades
Amenazas (O) Lista de Amenazas	Estrategias (DA) Reducir a un mínimo las debilidades y evitar las amenazas	Estrategias (FA) Usar fortalezas para evitar amenazas

Figura 33 Representación esquemática de la matriz DOFA. Fuente. *(UPIICSA)*

A continuación en la tabla 7 se observan las estrategias que a través de esta guía se definieron según las condiciones en las cuales se encuentra la dependencia ARC.

Tabla 7

Matriz DOFA

	DEBILIDADES	**FORTALEZAS**
	D1. No existe respaldo digital de la información física correspondiente a la historia académica de los estudiantes de la universidad que reposa en la dependencia de admisiones, registro y control. **D2.** No existe una política de digitalización de documentos. **D3.** El cableado estructurado y eléctrico no cumple con las normas establecidas. **D4**. No existen detectores de humo, ni alarmas contra incendios que permitan prevenir daños que pueda ocasionar el fuego.	**F1.** Existencia de un buzón de sugerencias (permite conocer los requerimientos de los clientes y su percepción del servicio prestado, lo que posibilita tomar acciones de mejora ante dichos resultados). **F2.** Los archivos se encuentran debidamente organizados y etiquetados (lo que permite una fácil ubicación sin importar su antigüedad). **F3**. Se han iniciado estrategias para incluir trámites en línea con el fin de cumplir con los requerimientos del buen gobierno en línea. **F4.** Existencia del plan de mejoramiento Institucional.

	D5. No existen mecanismos como UPS que permitan proteger la información digital y los equipos de cómputo en caso de ocurrir interrupciones de energía eléctrica.	**F5**. Existencia de inventario de equipos y software.
	D6. No se lleva un registro de las fallas detectadas, ni el proceso realizado para solucionarlas.	**F6**. La existencia del Plan de acción de la dependencia.
	D7. No todos los equipos de cómputo cuentan con las licencias de software requerido actualizado y vigente.	**F7**. Se establece la evaluación de riesgos dentro del plan de acción de la dependencia.
	D8. No se ha oficializado, ni puesto en marcha una política de seguridad de la información en la dependencia.	**F8**. Existen extintores ubicados adecuadamente y vigentes para su uso.
	D9. No existen controles para retirar de la oficina información o equipos.	**F9**. Existe aire acondicionado en la dependencia lo que sirve como mecanismo de refrigeración para los equipos de cómputo.
	D10. Las áreas de trabajo no se encuentran debidamente delineadas.	**F10.** Los activos de la oficina están claramente identificados e inventariados.
	D11. Según los resultados obtenidos con los diferentes instrumentos de recolección de la información se presume que se realizan copias de seguridad sin embargo las mismas se guardan en las mismas oficinas de la dependencia.	**F11**. Se realizan copias de seguridad desde la división de sistemas a la de la información que se maneja a través del software en la dependencia.
	D12. No se cuenta con plan de continuidad del negocio debidamente establecido.	
	D13. Los equipos de cómputo no cuentan con contraseña de seguridad.	
	D14. Los funcionarios aseguran no haber firmado un acuerdo de confidencialidad.	
	D15. Los funcionarios desconocen el plan de contingencia institucional.	
	D16. No existen los controles adecuados para evitar el acceso a personal no autorizado a las instalaciones de la dependencia.	
	D17. No se toman las medidas	

	necesarias para evitar que la información almacenada físicamente no se deteriore o dañe. **D18**. No existen roles y responsabilidades de seguridad asignados a los funcionarios de la dependencia. **D19**. Los funcionarios no reciben las capacitaciones de seguridad necesarias.	
OPORTUNIDADES	**ESTRATEGIAS DO**	**ESTRATEGIAS FO**
O1. Única institución de Educación Superior pública de la región. **O2**. Creciente demanda de aspirantes a ingresar a las carreras de la universidad. **O3.** Ágil y oportuno manejo la información de la historia académica de los estudiantes. **O4.** Manejo seguro de la información que se gestiona desde la oficina de admisiones, registro y control. **O5.** Apoyo y orientación oportuna a demás dependencias de la institución que permitan dar cumplimiento a propósitos misionales. **O6.** Fortalecimiento de la dependencia. **O7.** Que la dependencia pueda garantizar la disponibilidad, integridad y confiabilidad de la información a través de respaldo digital con las debidas copias de seguridad. **O8.** Equipo fuertemente capacitado para afrontar diferentes situaciones que atenten contra la seguridad de la información, el norma desempeño y el prestigio de la institución.	*Adquirir un software para digitalización de los archivos físicos. D1, D2, D8, D11, D17, O2, O3, O4, O6, O7. * Solicitar una reestructuración del cableado de la oficina, que permita separar la red de datos, de la corriente eléctrica y que no queden cables expuestos. D3, D6, O6. * Solicitar cambio de instalaciones y adecuarla con medidas de seguridad como detectores de humo, alargas contra incendios que sean hagan complemento a los Extintores que ya existen para evitar y contrarrestar el fuego. D4, D6, D10, D17, O2,O4,O7. * Invertir recursos en la adquisición de software y licencias que permitan el desarrollo legal y seguro de las actividades propias de la dependencia. D7, O1, O2, O3,O4. * Establecer una política de seguridad y aplicarla, además de capacitar al personal sobre la misma y todo lo relacionado a seguridad de la información. D2, D6, D8, D14, D18, O3, O4, O6, O7.	* Brindar oportunidades a los clientes para expresar insatisfacciones y así saber en qué se está fallando para poder mejorar. F1, F3, O1, O2, O5,O6 * A pesar de no estar digitalizados, la buena organización y etiquetado de los mismos permitirá una buena gestión y un buen servicio. F2, F3, O1, O3,O4. * Contar con lineamientos, orientación institucional y hacer buen uso de ellos permite tener herramientas para la buena gestión. F4, F7, O1, O6, O8. * Establecer un plan de continuidad en el que se determine la necesidad de afrontar de seguridad entre ellas la realización de copias de seguridad de la información y el resguardo seguro de las mismas. F11, O1, O3, O7.
AMENAZAS	**ESTRATEGIAS DA**	**ESTRATEGIAS FA**

A1. Los funcionarios afirman no saber cómo actuar en caso de presentarse una catástrofe natural. **A2.** Cese de actividades académicos y administrativas . **A3**. Daños a los equipos de cómputo debido a cortes imprevistos del servicio eléctrico. **A4.** Incendios debido a la presencia de materiales de rápida propagación del fuego en la dependencia y dependencias cercanas. **A5**. Perdida de información debido al ingreso de personal no autorizado a la dependencia. **A6.** Divulgación de la información confidencial por parte de funcionarios quienes según encuesta realizada afirman no haber firmado un acuerdo de confiabilidad, lo que indican que la cláusula establecida en el contrato con este fin pasa por desapercibida en muchas ocasiones. **A7**. Deterioro o daño de información física por falta de medidas efectivas de prevención. **A8**. Acceso no permitido a la información digital debido a la falta de contraseñas de seguridad en algunos equipos. **A9.** Cortos eléctricos o fallas en servicios de red dado que no se cumple con normas de cableado estructurado. **A10.** Atentado contra la seguridad de la información por parte de los funcionarios debido a desconocimiento de normatividad y sanciones por uso indebido. **A11.** Desprestigio de la institución.	* Asegurar la integridad de la información a través de un respaldo digital. D1, D2, A2, A5, A11. * Adecuar las instalaciones, redistribuir las estaciones de trabajo, realizar cambio a una oficina más amplia. D10, A2, A3, A7. * Capacitar a los empleados frecuentemente sobre la importancia de mantener segura la información y establecer acuerdos de confidencialidad. D9, D15, D18, A8, A10, A11.	* Establecer y reforzar según sea el caso los alineamientos para la dependencia, política de seguridad, plan de contingencia y ponerlos en práctica. F2, f4, F6, A2, A6, A7. * Dar un seguimiento oportuno a los riesgos, amenazas y fallas detectadas, priorizar procesos, establecer medidas de seguridad que garanticen la continuidad del negocio. F1, F2, F7, A1, A2, A6, A8. * Definir estrategias y mecanismos que permitan dar continuidad al negocio y así poder brindar un buen servicio y contribuir con el cumplimiento de los objetivos misionales de la institución. F1…F11, A1…A11.

Fuente. Autores

4.2.3 Análisis de riesgos. Este análisis se realizará siguiendo algunos parámetros establecidos en el documento K-DP-OPL-001C "Guía para la gestión del riesgo" de la Universidad Francisco de Paula Santander.

Para este proceso se realizaran los siguientes pasos:

1) Identificación de los riesgos.
2) Análisis del riesgo.
3) Calificación del riesgo.

Identificación de los riesgos. La identificación de los riesgos se realizará con base a la tabla 8.

Tabla 8

Factores internos y externos

FACTORES INTERNOS	FACTORES EXTERNOS
Económicos: disponibilidad de capital, emisión de deuda o no pago de la misma, liquidez, mercados financieros, desempleo,competencia.	Infraestructura: disponibilidad de activos, capacidad de los activos, acceso al capital.
Medioambientales: emisiones y residuos, energía, catástrofes natrales, desarrollo sostenible.	Personal: capacidad del personal, salud, seguridad.
Políticos: cambios de gobierno, lesgislación, políticas públicas, regulación.	Procesos: capacidad, diseño, ejecución, proveedores, entradas, salidas, conocimiento.
Socialesç: demografía, responsabilidad social, terrorismo.	Tecnología: integridad de datos, disponibilidad de datos y sistemas, desarrollo, producción, mantenimiento.
Tecnológicos: interrupciones, comercio electrónico, datos exte3rnos, tecnología emergente.	

Fuente. (Departamento Administrativo de la Función Pública (DAFP), 2011)

Tabla 9

Identificación de los riesgos

Num	Riesgo	Descripción de los riesgos
1	Perdida de información tanto física como digital, equipos, incluso vidas humanas debido a Catástrofes naturales o incendios.	Casi imposibles prever y su posibilidad de ocurrencia es mínima sin embargo no se deben descartar entre ellos la lluvia, terremotos, huracanes o el viento los cuales se convierten en desastre cuando superan un límite de normalidad y los posibles

		incendios, debido a la cantidad de documentos físicos que se almacenan en la dependencia la propagación del fuego podría ser muy rápido.
2	Interrupción de funciones por paros estudiantiles o cierre de vías.	Se prohíbe el paso a los estamentos de la institución debido a un paro estudiantil o bloqueos en la vía por manifestaciones de diferente índole.
3	Daño a equipos de cómputo por interrupciones de energía.	Dado que no se cuenta con mecanismos como UPS que permitan apagar debidamente los equipos.
4	Suspensión del servicio de red.	Dado que se encuentran algunos cables por fuera de las canaletas es posible que estos sufran deterioro y daños.
5	Acceso de personal no autorizado a la información manejada a través de los computadores.	No todos los equipos de cómputo no cuentan con contraseñas de acceso.
6	Repetición de fallas o mal manejo de las mismas.	No se lleva registro de las fallas detectadas
7	Acceso de terceros a información física.	Las instalaciones no cuentan con los debidos controles de seguridad de acceso, por ejemplo el material de la puerta principal es fácil de penetrar.
8	Divulgación de información confidencial.	No se firma un acuerdo de confidencialidad y la cláusula establecida en el contrato es pasada por desapercibida por algunos de los funcionarios.
9	Pérdida de información e imposibilidad de recuperación.	En caso de presentarse circunstancias que impliquen la perdida de la información será poco probable la recuperación de la misma dado que no se cuenta con respaldo digital de la información física y en cuento a la digital se almacena en la misma dependencia inclusive en los mismos equipos, lo cual hace muy probable su perdida al igual que la original.
10	Fallas en los sistemas operativos.	No se evidencian licencias del software y sistemas operativos actualizados en todos los equipos de cómputo.
11	Indebida gestión de la información que atentan contra la integridad, confidencialidad y disponibilidad de la información.	No se ha establecido oficialmente una política de seguridad, ni un plan de continuidad y no se realiza capacitación al personal acerca de la seguridad e importancia de la información.
12	Perdida de la oportunidad de proteger la información e incluso la vida humana frente a una emergencia.	El personal afirma desconocer el plan de contingencia, lo que evidencia la falta de capacitación al respecto.
13	Reducción de la demanda de aspirantes a ingresar a la institución.	Si por diversas causas se interrumpen los servicios y no existe un plan de continuidad para restaurar funciones críticas se corre el riesgo de perder clientes en este caso estudiantes.
14	Pérdida de prestigio.	
15	Deterioro de la información física.	Dado que las instalaciones son muy pequeñas no es ideal para almacenar la información que se maneja en la dependencia ni para albergar a todo el personal.

Fuente. Autores

Análisis del riesgo. El objetivo es medir el riesgo inherente. Es decir, determinar la probabilidad de materialización del riesgo y sus consecuencias o impacto, con el fin de establecer la zona de riesgo inicial (UFPSO, 2016).

-*Probabilidad del riesgo.* La selección del nivel de la probabilidad del riesgo la debe realizar el equipo de trabajo, para efectos de esta investigación se realizara por el equipo investigador en base a la información recopilada, sin embargo es importante resaltar que no se puede tomar como precisa, la medición de la probabilidad del riesgo se muestra en la tabla 10.

Tabla 10

Medición de la probabilidad del riesgo

DESCRIPTOR	DESCRIPCIÓN	FRECUENCIA	NIVEL
RARA VEZ	**EXCEPCIONAL** Ocurre en excepcionales	No se ha presentado en los último 5 años	1
IMPROBABLE	**IMPROBABLE** Puede ocurrir	Se presentó una vez en los últimos 5 años	2
POSIBLE	**POSIBLE** Es posible que suceda	Se presentó una vez en los últimos 2 años	3
PROBABLE	**ES PROBABLE** Ocurre en la mayoría de los casos	Se presentó una vez en el último año	4
CASI SEGURO	**ES MUY SEGURO** El evento ocurre en la mayoría de las circunstancias. Es muy seguro que se presente.	Se ha presentado más de una vez al año	5

Fuente. (UFPSO, 2016)

Clasificación del riesgo.

Tabla 11

Clasificación del riesgo de ARC según la probabilidad

Riego	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
Nivel	1	4	3	5	2	3	4	2	2	3	4	3	1	1	2

Fuente. Autores

Impacto del riesgo. Son las consecuencias o efectos que puede generar la materialización del riesgo de corrupción en la entidad (UFPSO, 2016).

Tabla 12

Medición del impacto del riesgo

Descriptor	Descripción	Nivel
Moderado	**AFECTACIÓN PARCIAL AL PROCESO Y A LA DEPENDENCIA** Genera a medianas consecuencias para la entidad.	5
Mayor	**IMPACTO NEGATIVO DE LA ENTIDAD** Genera altas consecuencias para la entidad	10
Catastrófico	**CONSECUENCIAS DESASTROSAS SOBRE EL SECTOR** Genera consecuencias desastrosas para la entidad.	20

Fuente. (UFPSO, 2016)

El impacto se mide según el efecto que puede causar el hecho de corrupción al cumplimiento de los fines de la entidad (UFPSO, 2016). Para facilitar la asignación del puntaje se resolverán las siguientes preguntas para cada uno de los riesgos:

Tabla 13

Formato para determinar impacto

N°	Pregunta
	Si el riesgo se materializa podría
1	¿Afectar al grupo de funcionarios del proceso?
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?
3	¿Afectar el cumplimiento de la misión de la dependencia?
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?
5	¿Generar pérdida de confianza de la entidad, afectando su reputación?
6	¿Generar pérdida de recursos económicos?
7	¿Afectar la generación de productos y la prestación de servicios?
8	¿Dar lugar al detrimento de la calidad de vida de la comunidad por la pérdida del bien o servicios o los recursos públicos?
9	¿Generar pérdida de información de la entidad?
10	¿Generar intervención de los órganos de control, de la fiscalía u otro ente?
11	¿Dar lugar a procesos sancionatorios?
12	¿Dar lugar a procesos disciplinarios?
13	¿Dar lugar a procesos fiscales?
14	¿Dar lugar a procesos penales?
15	¿Generar pérdida de calidad del sector?

16	¿Ocasionar lesiones físicas o pérdida de vida humana?
17	¿Afectar la imagen regional?
18	¿Afectar la imagen nacional?

Fuente. Adecuación del formato para determinar el impacto (UFPSO, 2016)

Para determinar el nivel de impacto se debe seleccionar SI o NO a las preguntas de la hoja "Riesgos de Corrupción" del formato Matriz de Identificación de riesgos.

Según el total de las respuestas el impacto se clasifica:

• Responder afirmativamente de UNO a CINCO preguntas genera un impacto *Moderado*.

• Responder afirmativamente de SEIS a ONCE preguntas genera un impacto *Mayor*.

• Responder afirmativamente de DOCE a DIECIOCHO preguntas genera un impacto *Catastrófico* (UFPSO, 2016)

Tabla 14

Valoración del impacto

Riesgo	**Pregunta**																	
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**
1	**Si**	Si	Si	Si	No	Si	Si	Si	No	No	No	No	No	No	No	Si	No	No
2	**Si**	**Si**	**Si**	**Si**	No	**Si**	**Si**	No	No	**Si**	**Si**	**Si**	**Si**	**Si**	**Si**	**Si**	**Si**	**Si**
3	No	**Si**	**Si**	**Si**	No	**Si**	**Si**	No	**Si**	No	No	No	No	No	No	No	No	No
4	No	**Si**	**Si**	**Si**	No	**Si**	**Si**	No	**Si**	No	No	No	No	No	No	No	No	No
5	**Si**	**Si**	**Si**	**Si**	**Si**	No	Si	No	**Si**	**Si**	**Si**	**Si**	No	Si	No	No	No	No
6	No	**Si**	**Si**	**Si**	**Si**	**Si**	**Si**	No	**Si**	**Si**	No	No	No	No	No	No	No	No
7	**Si**	**Si**	**Si**	**Si**	**Si**	No	Si	No	**Si**	**Si**	**Si**	**Si**	No	Si	No	No	No	No
8	No	Si	Si	Si	Si	Si	Si	No	Si	Si	Si	Si	Si	Si	No	No	No	No
9	No	Si	Si	Si	Si	Si	Si	No	Si	No	No	No	No	No	Si	No	No	No
10	No	Si	Si	Si	No	Si	Si	No	Si	No	No	No	No	No	No	No	No	No
11	Si	Si	Si	Si	Si	Si	Si	No	Si	No	Si	Si	No	No	No	No	No	No
12	Si	Si	Si	Si	No	Si	Si	Si	Si	No	No	No	No	No	No	Si	No	No
13	No	Si	Si	Si	Si	Si	No	No	No	No	No	No	No	No	No	No	Si	No
14	No	Si	Si	Si	Si	Si	No	No	No	No	No	No	No	No	No	No	Si	Si
15	No	Si	Si	Si	No	No	No	Si	Si	No	No	No	No	No	No	No	No	No

Fuente. Autores

Tabla 15

Resultado de la medición del impacto del riesgo

Pregunta	Cantidad de si	Cantidad de No	Impacto
1	8	10	Mayor
2	15	3	Catastrófico
3	6	12	Mayor
4	6	12	Mayor
5	11	7	Mayor
6	8	10	Mayor
7	11	7	Mayor
8	12	6	Catastrófico
9	8	10	Mayor
10	6	12	Mayor
11	10	8	Mayor
12	9	9	Mayor
13	5	13	Moderado
14	7	11	Mayor
15	5	12	Moderado

Fuente. Autores

Para determinar la zona de riesgo se tiene en cuenta la multiplicación del nivel de probabilidad con el nivel de impacto, como se muestra en la siguiente tabla:

Tabla 16

Resultado de la clasificación del riesgo

RESULTADO DE LA CALIFICACIÓN DEL RIESGO DE CORRUPCIÓN				
PROBABILIDAD	**PUNTAJE**	**ZONA DE RIESGO DE CORRUPCIÓN**		
CASI SEGURO	5	25 MODERADO	50 ALTA	100 EXTREMA
PROBABLE	4	20 MODERADO	40 ALTA	80 EXTREMA
POSIBLE	3	15 MODERADO	30 ALTA	60 EXTREMA
IMPROBABLE	2	10 BAJA	20 MODERADA	40 ALTA
RARA VEZ	1	5 BAJA	10 BAJA	20 MODERADA
IMPACTO		MODERADO	MAYOR	CATASTROFICA
PUNTAJE		5	10	20

Fuente. (UFPSO, 2016)

Tabla 17

Cálculo de la zona de riesgo

Pregunta	Probabilidad	Impacto	Total	Zona de riesgo
1	1	10	10	Baja
2	4	20	80	Extrema
3	3	10	30	Alta
4	5	10	50	Alta
5	2	10	20	Moderado
6	3	10	30	Alta
7	4	10	40	Alta
8	2	20	40	Alta
9	2	10	20	Moderado
10	3	10	30	Alta
11	4	10	40	Alta
12	3	10	30	Alta
13	1	5	5	Baja
14	1	10	10	Baja
15	2	5	10	Moderado

Fuente. Autores

ZONA DE RIESGO ALTA	
PUNTAJE DE 30-50 PUNTOS	
PROBABILIDAD	IMPROBABLE,POSIBLE, PROBALE Y CASI SEGURO
IMPACTO	MAYOR Y CATASTRIFICO
TRATAMIENTO	DEBEN TOMARSE LAS MEDIDAS NECESARIAS PARA LLEVAR EL RIESGO A LA ZONA DE RIESGO MODERADA,BAJA O ELIMINARLO
NOTA: EN TODO CASO SE REQUIERE QUE LAS ENTIDADES PROPENDEN POR ELIMINAR EL RIESGO DE CORRUPCIÓN O POR LO MENOS LLEVARLO A LA ZONA DE RIESGO BAJA.	

ZONA DE RIESGO EXTREMA	
PUNTAJE DE 60-100 PUNTOS	
PROBABILIDAD	POSIBLE, PROBALE Y CASI SEGURO
IMPACTO	CATASTRIFICO
TRATAMIENTO	LOS RIESGOS DE ESTA ZONA REQUIEREN DE UN **TRATAMIENTO PRIORITARIO.** SE DEBEN IMPLEMENTAR LOS CONTROLES ORIENTADOS A REDUCIR LA POSIBILIDAD DE OCURRENCIA DEL RIESGO O DISMINUIR EL IMPACTO DE SUS EFECTOS Y TOMAR LAS MEDIDAS DE PROTECCIÓN
NOTA: EN TODO CASO SE REQUIERE QUE LAS ENTIDADES PROPENDEN POR ELIMINAR EL RIESGO DE CORRUPCIÓN O POR LO MENOS LLEVARLO A LA ZONA DE RIESGO BAJA.	

ZONA DE RIESGO BAJA	
PUNTAJE DE 5 A 10	
PROBABILIDAD	RARA VEZ O IMPROBABLE
IMPACTO	MODERADO Y MAYOR
TRATAMIENTO	LOS RIESGOS DE CORRUPCIÓN LAS ZONAS BAJAS SE ENCUENTRA EN UN NIVEL QUE PUEDE **ELIMINARSE** O **REDUCIRSE** FÁCILMENTE CON LOS CONTROLES ESTABLECIDOS EN LA ENTIDAD.

ZONA DE RIESGO MODERADA	
PUNTAJE DE 15-25	
PROBABILIDAD	RARA VEZ, IMPROBABLE,POSIBLE Y CASI SEGURO
IMPACTO	MODERADO, MAYOR Y CATASTRIFICO
TRATAMIENTO	DEBEN TOMARSE LAS MEDIDAS NECESARIAS PARA LLEVAR EL RIESGO A LA ZONA DE RIESGO BAJA O ELIMINARLO
NOTA: EN TODO CASO SE REQUIERE QUE LAS ENTIDADES PROPENDEN POR ELIMINAR EL RIESGO DE CORRUPCIÓN O POR LO MENOS LLEVARLO A LA ZONA DE RIESGO BAJA.	

Figura 34 Criterios de la zona de riesgo *(UFPSO, 2016)*

4.3. Informe final Plan de Continuidad

4.3.1. Introducción. Ninguna empresa esta excepta de la posibilidad de ocurrencia de un incidente que afecte el normal desarrollo de las operaciones, por lo que es importante contar con herramientas, mecanismos o procedimientos que permitan la recuperación oportunidad y por ende la continuidad del negocio.

En el 2007 se publicaba la norma BS 25999, el primer estándar certificable que definía los requisitos y buenas prácticas que debería seguir una empresa, independiente de su tamaño, para implementar un sistema para la gestión de la continuidad del negocio. Después de una serie de revisiones, fue publicado el estándar ISO 22301:2012 que basado en el ciclo de mejora continua, plantea los pasos para planear, implementar, operar, revisar y mejorar la gestión de la continuidad del negocio. (Wilivesecurity, 2014)

ISO 22301:2012 en su inciso 8.4 plantea establecer e implementar procedimientos de continuidad del negocio, dentro de ellos estable el plan de continuidad

"La organización debe establecer procedimientos documentados para responder a un incidente perturbador y cómo va a continuar o recuperar sus actividades dentro de un marco de tiempo predeterminado". (ISO 22301:2012, s.f.)

4.3.2. Alcance. La Administración del Plan de Continuidad de Negocios permitirá a la dependencia de Admisiones, Registro y Control de la UFPSO contar con los mecanismos necesarios para recuperarse ante una crisis, incidente o emergencia, permitiendo la continuidad de los servicios clave para la normal operación.

4.3.3. Conceptos básicos.

***Riesgo*.** Es la probabilidad de materialización de una amenaza por la existencia de una o varias vulnerabilidades con impactos adversos resultantes para la Entidad. (ICETEX, 2013)

***Impacto*.** Es el efecto que causa la ocurrencia de un incidente o siniestro. La implicación del riesgo se mide en aspectos económicos, imagen reputacional, disminución de capacidad de respuesta y competitividad, interrupción de las operaciones, consecuencias legales y afectación física a personas. Mide el nivel de degradación de uno de los siguientes elementos de continuidad: Confiabilidad, disponibilidad y recuperabilidad. (ICETEX, 2013)

***Probabilidad*.** Posibilidad de ocurrencia de un evento.

Control. Es el proceso, política, dispositivo, práctica u otra acción existente que actúa para minimizar el riesgo o potenciar oportunidades positivas. (ICETEX, 2013)

***Acceso*.** Es la recuperación o grabación de datos que han sido almacenados en un sistema de computación. (UFPSO, PLAN DE CONTINGENCIA DE TI, 2015)

***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. (UFPSO, PLAN DE CONTINGENCIA DE TI, 2015)

***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. (UFPSO, PLAN DE CONTINGENCIA DE TI, 2015)

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. (UFPSO, PLAN DE CONTINGENCIA DE TI, 2015)

***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 e forma parcial o total. (UFPSO, PLAN DE CONTINGENCIA DE TI, 2015)

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. (UFPSO, PLAN DE CONTINGENCIA DE TI, 2015).

4.3.4. <u>Etapas para realizar un Plan de Continuidad.</u> En la tabla 18 se observan las etapas para realizar el plan de continuidad.

Tabla 18

Etapas ISO 22301

Etapa	Descripción
1	Objeto, ámbito de aplicación y usuarios
2	Documentos de referencia
3	Supuestos
4	Funciones y responsabilidades
5	Contactos clave
6	Plan de activación y desactivación
7	Comunicación
8	Respuesta a incidentes
9	Sitios físicos y transporte
10	Orden de recuperación para las actividades
11	Los planes de recuperación para las actividades
12	Plan de recuperación de desastres
13	Recursos necesarios
14	La restauración y la reanudación de las actividades de medidas temporales

Fuente: (Blanco Lindarte, Martínez Vega, Quintero Prado, & Rincón Angarita, 2012)

Etapa 1: Objeto, ámbito de aplicación y usuarios. El objetivo de este Plan de Continuidad está orientado a lograr que la dependencia de Admisiones Registro y Control de la UFPSO pueda recuperar sus procesos claves en caso de presentarse un incidente o emergencia y dar continuidad a la normal operación, además de garantizar la integridad, disponibilidad, confiabilidad de la información y la protección de las personas.

Etapa 2: Documentos de referencia. Para el desarrollo del Plan de Continuidad de la dependencia de Admisiones Registro y Control de la Universidad Francisco de Paula Santander (UFPSO), se tomará como referencia la siguiente documentación:

- Plan de Contingencia – División de sistemas – UFPS Ocaña.
- Informe de Auditoria Interna F-CI-CIN-018 (Anexo A)

- Auditoría realizada por el equipo investigador, autor de este proyecto.(Anexo B)
- Organigrama de la Universidad Francisco de Paula Santander Ocaña.
- Informe anual de la ejecución de los planes de acción de la UFPSO.
- Guía para la administración del riesgo.
- Guía para el análisis de causas y la formulación de acciones para el mejoramiento continuo UFPSO.
- Manual de indicadores.
- Organigrama de la dependencia de admisiones, registro y control (ARC).
- Visión y Misión de la dependencia (ARC).
- Manual específico de proceso, admisiones, registro y control.
- Plan de acción de la dependencia de admisiones registro y control.
- Caracterización de los procesos de admisiones registro y control.
- Instructivo trámites a solicitudes de servicios académicos.

Etapa 3: Supuestos. Los requisitos previos que deben existir para que el Plan de continuidad del Negocio para la dependencia de Admisiones Registro y Control de la UFPSO sea eficaz son:

- Inventariar los recursos hardware y software
- Existencia de documentos institucionales relacionados con la seguridad de la información:
    - Política de seguridad de la información.
    - Plan de contingencia
    - Guía para la administración del riesgo

Los mismos deben estar formalizados por escrito y contar con la aprobación y apoyo de los directivos de la institución.

- Contar con el personal necesario y capacitado.
- Contar con canales idóneos de comunicación tanto interna como externa.
- Contar con reservas financieras para la ejecución del plan.

Etapa 4: Funciones y responsabilidades. Para dar continuidad a los negocios es necesario establecer un comité de continuidad. En la institución a través del plan de contingencia de TI se establecieron roles con las respectivas funciones para poner en marcha dicho plan de contingencia, en la presente investigación se establecen roles complementarios, específicos para el Plan de Continuidad los cuales integrados con los ya definidos en el documento en mención permitan que la dependencia funcione correctamente, es decir que recupere rápidamente los procesos claves y posteriormente la totalidad de ellos en caso de presentarse algún tipo de incidente.

Los cinco primero roles establecidos en el plan de **contingencia** deben ser asumidos por el personal de la División de Sistemas dado que son profesionales capacitados para asumirlos, dicha dependencia da soporte a toda la institución en cuanto a las Tecnologías de la Información y la comunicación (TIC), no obstante los roles directamente relacionados a la **continuidad** se propone sean asumidos por personal de la dependencia dado que son quienes conocen los procesos que se llevan a cabo, deberán ser asignados teniendo en cuenta las capacidades de cada quien, estos constituirán el comité de continuidad y solicitaran la participación del personal de la división en caso de ser requeridos.

En la tabla 19 se muestra detalladamente el rol y se especifican las funciones y responsabilidades.

Tabla 19

Roles y funciones del Plan de Contingencia de TI, UFPSO

ROL	ROL FUNCIONES Y RESPONSABILIDADES
Responsable de la ejecución del Plan de Contingencia (Jefe de la División)	Es el responsable de aprobar la realización del Plan de Contingencia de TI, 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 de Contingencia, 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 el centro de cómputo alterno 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 de Contingencia, 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 del centro de cómputo alterno, la restauración de datos e instalación de BD. Una vez que se encuentre aprobado el Plan de Contingencia, será el Coordinador General quien lleve a cabo formalmente la declaración de una contingencia grave y de inicio formal de la aplicación del Plan de Contingencia, 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 de Contingencia, 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 de Contingencia. 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 en el datacenter. Coordinará las actividades correspondientes a los servicios de comunicaciones al declararse una contingencia, hasta su restablecimiento total.
	Es el responsable de llevar a cabo el inventario de equipo, software y equipos periféricos, como impresoras, escáners, faxes, 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.

Coordinador de Soporte Técnico	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 de Contingencia. 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 de Contingencia 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 de Contingencia 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 de Contingencia 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 UFPSO	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 de Contingencia, 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 de Contingencia Informático 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: (UFPSO, PLAN DE CONTINGENCIA DE TI, 2015)

Tabla 20

Roles y funciones del plan de continuidad

ROL	ROL FUNCIONES Y RESPONSABILIDADES
Director de Continuidad	• Actualizar, mantener y probar el Plan de continuidad. • Liderar comunicaciones internas y externas. • Advertir sobre nuevos riesgos y amenazas que afectan la continuidad de la operación normal de la dependencia. • Monitorear los reportes de fallas e incidentes. • Velar no solo por la seguridad de la información, sino también por la seguridad del personal. • Autorizar la activación del plan de continuidad.
Líder administrativo	• Coordinar los aspectos logísticos internos cuando la Entidad se encuentre operando bajo contingencia. • Coordinar el suministro de elementos esenciales como transporte, recursos de infraestructura y papelería. • Gestionar la consecución y adecuación de los centros alternos de operaciones según el plan de operaciones en contingencia. • Coordina el cumplimiento de las funciones de los empleados de la dependencia cuando se encuentren activos procesos para dar continuidad al negocio. • Apoya el proceso de comunicación.
Líder de recuperación tecnológica y coordinador de recuperación	• Junto con el Coordinador de Sistemas liderar la recuperación tecnológica, basados en las estrategias de continuidad implementadas. • Identificar los posibles riesgos de aspectos tecnológicos que afectan la continuidad de la operación normal de la Entidad y que ponen al descubierto debilidades del plan de continuidad. • Colaborar en la comunicación a los proveedores de los temas o servicios de su competencia, sobre el estado de contingencia en que se encuentra la Entidad, esto previa decisión y autorización del Director de Continuidad. • Entregar los reportes correspondientes sobre el estado de la recuperación del incidente. • Velar por la actualización de la Estrategia Tecnológica en los casos que se presenten situaciones como: cambios en los aplicativos, cambio en la infraestructura, roles y responsabilidades, disponibilidad de los recursos, entre otros. • Velar por la realización de las pruebas del plan de continuidad y revisar los resultados obtenidos en las mismas. • Mantener comunicación constante durante el estado de contingencia.

Responsables de tareas de apoyo, control y cumplimiento.	• Ejecutar los planes de contingencia ante el incidente presentado según las tareas que le hayan sido asignadas. • Advertir sobre riesgos que puedan afectar la continuidad en la prestación del servicio o la funcionalidad del plan.

Fuente. Adaptación del Manual de Administración del Plan de Continuidad del Negocio (ICETEX, 2013)

Etapa 5. Contactos clave. El líder administrativo es responsable del contacto con las personas que participaran en la activación de procedimientos propios del Plan de Continuidad, estos contactos claves se listan a continuación y para todos los casos debe existir un sucesor en caso de que el principal responsable no pueda llevar a cabo la labor encomendada, los contactos claves se especifican en la tabla 21.

Tabla 21

Contactos claves

Contacto	Teléfono
Rector de la Institución.	5690088 Ext 104
Subdirector Académico	5690088 Ext 121
Coordinador de la División de Sistemas.	5690088 Ext 156
Jefe de Admisiones, Registro y Control.	5690088 Ext 129
Coordinador de la oficina de Tesorería	5690088 Ext 139
Secretaria general	5690088 Ext 145
Demás dependencias de la institución.	https://ufpso.edu.co/directorioufpso
Grupos de interés especial	
Defensa Civil	144
Fiscalía	5613849-5611220
Policía Nacional	112
Cuerpo de Bomberos Voluntarios	119 – 5611002
Urgencias Hospital Emiro Quintero Cañizares	5611940
Cruz Roja	132
Otros	
Energía eléctrica – daños	115
Ambulancias	125-5611425-5611940

Fuente: Autores del proyecto

Será responsabilidad del líder administrativo recopilar de los contactos claves información adicional y actualizada como número de teléfonos móviles, correo electrónico, dirección de residencias entre otros que se consideren necesarios.

Etapa 6. Plan de activación y desactivación. La activación o desactivación del Plan de Continuidad de la oficina de ARC es responsabilidad del Director de continuidad, sin embargo para que esta se lleve a cabo se debe pasar las fases de alerta que se describen a continuación siempre y cuando no se trate de una emergencia que requiera de una repuesta inmediata en cuyo caso se dará por activado el plan inmediatamente.

a) Notificación
b) Evaluación
c) Activación y desactivación del Plan de Continuidad.

Notificación. Cualquier persona puede dar aviso, puede ser funcionarios de la UFPSO o simplemente una persona próxima al lugar donde se desarrolle el incidente, los funcionarios deben recibir capacitación sobre cómo actuar cuando detecte un incidente o cuando sean informados de alguno por parte de personal ajeno a la institución, la primera reacción es dar aviso inmediato con el máximo detalle al director de continuidad o al responsable encargado, por lo que todos deben contar con los datos de contacto de estas personas, de igual manera deben velar por preservar la vida humana y la integridad de la información.

Evaluación. Una vez el director de continuidad haya sido informado del incidente debe buscar los mecanismos necesarios para corroborar la veracidad del incidente comunicado, para ello puede delegar funciones al resto del equipo, siempre cuidando no tardar demasiado tiempo en la identificación del mismo.

Una vez confirmada se procederá a evaluar la situación con la recopilación de la mayor información posible, el director debe reunir al resto del equipo de continuidad y tomar la decisión de activarlo y cuando desactivarlo.

Activación y desactivación del Plan de Continuidad. El director de continuidad da la orden de activación del Plan de Continuidad, acción seguida cada una de los funcionarios debe actuar de acuerdo a las funciones que le hayan sido establecidas; de igual manera debe establecer las pautas para la desactivación del Plan una vez se hayan restablecidos las actividades según el orden de prioridad y la posterior evaluación.

Etapa 7. Comunicación. Los medios de comunicación que se pueden implementar en caso de existir un incidente son:

a) Comunicación directa

b) Telefonía celular

c) Telefonía fija

d) Correo electrónico

e) Chat

f) Correspondencia escrita

g) Portal web

h) Servicio de mensajería

Responsables. Si se requiere comunicación con proveedores de servicios de tecnológicos el responsable será el líder de recuperación tecnológica; para comunicaciones con los grupos de interés especial el encargado puede ser directamente el director de continuidad o el líder administrativo, en caso de emergencia cualquier funcionario deberá

dar aviso según las recomendaciones dadas a través de capacitaciones y las comunicaciones internas las podrá realizar el líder administrativo o un responsable delegado a través de los medios establecidos por el director de continuidad según sea el caso.

***Etapa 8. Respuesta a incidentes*.** Cuando se presente una situación de emergencia se debe tener en cuenta que hay que controlar el pánico, lo primero que hay que hacer es mantener seguras a las personas y comunicarse con las entidades encargadas de proceder antes este tipo de situaciones como bomberos, policía, defensa civil etc.

Cada vez que ocurra algún tipo de emergencia dentro de lo posible es necesario localizar el lugar y qué lo origina, de manera que pueda ser controlado sin que se corran riesgos de pérdidas de vidas.

Según la emergencia, existen elementos disponibles para controlar la situación, como el uso de extintores, desconexión del servicio de agua, de electricidad entre muchos otros; de ser controlada la situación se observará qué tanto daño ha realizado.

Los incidentes identificados en la oficina de Admisiones Registro y Control, se especifican de la siguiente manera: Catástrofes naturales o incendio, Interrupción de Energía, Suspensión del servicio de red, Fallas en los Sistemas Operativos, Acceso no autorizado a la información manejada a través del computador, Paros Estudiantiles o cierre de vías. Estas situaciones se describen a continuación:

Catástrofes naturales o incendio. Sin pérdida o daños menores del lugar, el siniestro puede afectar diferentes sitios de donde se encuentra ubicada la oficina, se pueden ver afectadas algunas zonas del lugar, en los cuales no se verían afectados los datos, pero, se debe tener en cuenta que ante este tipo de emergencias es importante evacuar las

instalaciones, trasladando a los empleados a un sitio seguro. Con pérdida del lugar, la pérdida de las instalaciones afectaría gravemente a las operaciones de la dependencia ARC 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; Si la emergencia es a causa de una inundación, podría causar grandes pérdidas tanto en los dispositivos electrónicos como en la información física que reposa dentro del lugar, esto conllevaría que se detuvieran las operaciones totalmente. Es importante tener en cuenta también las instalaciones de la división de sistemas, ya que allí reposan todas las copias de seguridad de la información y mantienen en funcionamiento todos los servidores, así como se podrían presentar cortos circuitos, también, teniendo en cuenta el datacenter, la recuperación de las copias sería rápida pero no necesariamente lo sería para los servidores.

en caso de presentarse un incendio; en la división de sistemas, existe un gran impacto en la información, debido a que las copias de seguridad y los servidores se encuentran en ese lugar, en caso de sufrir daños se necesitarán nuevos equipos, instalar nuevamente los sistemas con su respectiva configuración y utilizar las copias de seguridad mantenidas hasta el momento. En áreas distintas al sitio de cómputo; dependiendo de la magnitud del incendio, se pueden ver afectados los sitios de trabajo localizados en áreas administrativas, se tendría un impacto alto ya que en ese sitio reposa la información y se vería afectado la operación del servicio.

Interrupción de energía. Al presentarse una interrupción de energía las operaciones informáticas no podrían continuar, debido a que los dispositivos en los cuales se trabaja dependen de la corriente para su utilización. Si la situación se presenta durante un periodo de tiempo corto, no sería grave, ya que se pueden retomar las operaciones rápidamente,

mientras que si la interrupción de energía es prolongado, se pueden frenar las operaciones por un transcurso de tiempo largo, sin embargo, no afectaría la información.

En la oficina no se cuenta con una planta eléctrica por lo tanto no es posible restablecer la energía al momento del corte, sin embargo los equipos servidores alojados en la división de sistemas cuentan con una UPS para remediar inmediatamente la situación después del corte y evitar daños en los equipos.

Suspensión del servicio de red. Red; si se presenta una falla en la red fallarían todas las operaciones, ya que en la oficina se cuenta con gran utilización de equipos informáticos.

Aplicaciones; una falla en los sistemas utilizados en la dependencia, sería significativo en el desarrollo de las operaciones, sin embargo estos se pueden chequear inmediatamente para continuar con los procesos.

Fallas en los Sistemas Operativos. Las fallas que se puedan presentar en los sistemas operativos pueden ser solucionadas casi siempre, pero si la situación llega a prolongarse se pueden suspender las operaciones hasta por días.

Acceso no autorizado a la información manejada a través del computador. 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.

Paros estudiantiles o cierre de vías. Este tipo de situaciones bien sea mayor o no, podría afectar los equipos utilizados por los empleados, así como daño a las instalaciones así como a las comunicaciones. Si el daño es mayor afectaría gravemente la seguridad de

las instalaciones tanto de la división de sistemas como de la dependencia ARC, ya que tendrían daño los servidores y todos los dispositivos, afectando así el desarrollo de las operaciones.

Etapa 9. Sitios físicos y transporte. Los puntos físicos y transporte hacen referencia a los lugares de la dependencia, en este caso la dependencia ARC está ubicada en la Sede Principal. Vía Acolsure, Sede el Algodonal - Ocaña Norte de Santander, los alternos para complementar la realización de los procesos se tiene en cuenta a la División de sistemas ubicada en la misma sede.

En cuanto al transporte, es importante tener los recursos suficientes para el traslado de los equipos necesarios para mantener la realización de las actividades, asimismo se debe establecer una contratación para dicho transporte.

Etapa 10. Orden de recuperación para las actividades.

En el punto 4.2.1 se incluyó como estrategia de continuidad, la evaluación de los procedimientos que realiza la oficina de Admisiones, Registro y Control, a través de este fue posible identificar los procesos claves, entendiendo que los demás no son menos importantes si no que su pos poción temporal (a corto plazo) no limita otras actividades de la dependencia o de la institución.

Esto permite entender que en caso de presentarse un incidente, se debe velar por realizar una restauración de los procesos comenzando por los clave, a continuación de estiman en la tabla 22 el tiempo máximo en que se puede parar un proceso según su prioridad y de esta manera se podrá entender el orden de recuperación de los mismos.

Tabla 22

Orden de recuperación para las actividades

Proceso	Tiempo máximo de interrupción
Admisión	2-3 días
Matrícula	2-3 días
Registro	2-3 días
Conceptuar y asesorar a los directores de planes de estudios aspectos relacionados con la aplicación de normas reglamentarias sobre registro y control del desempeño académico de los estudiantes.	8-15 días
Expedir las certificaciones académicas.	
Certificados de notas	4-8 días
Constancias de estudio	4-8 días
Constancias de buena conducta	4-8 días
Constancia terminación de materias o paz y salvo académico	4-8 días
Paz y salvo de grado	4-8 días
Hoja de vida académica.	4-8 días
Cancelación de materias	4-8 días
Cancelación de semestre (Matrícula).	4-8 días
Validaciones	4-8 días
Segundo y tercer calificador.	4-8 días
Homologaciones	4-8 días
Retiro de documentos	4-8 días
Transferencias	4-8 días
Reintegros	4-8 días
Traslados	4-8 días
Conservar y custodiar los registros oficiales de los procesos que adelante la dependencia.	Menos de 24 horas
Recibir la documentación de los estudiantes que solicitan graduarse.	3-4 días
Actualizar los promedios por semestre de todos los estudiantes matriculados.	8-15 días
Recibir las planillas de notas de todas las carreras de la Universidad por semestre.	4-8 días
Organizar las carpetas y hacer las hojas de vida académica de los estudiantes que ingresan al primer semestre.	8-15 días
Llevar el archivo de los graduados.	8-15 días

Fuente. Autores

Nota: Los tiempos son estimaciones realizadas por los autores del proyecto en base a la investigación realizada, se recomienda a la dependencia revisar y ajustarlos de ser necesarios.

Tabla 23

Descripción de rangos de interrupción de procesos

Rango de tiempo	Descripción	Orden de recuperación
Menos de 24 horas	Es primordial que este proceso no se interrumpa en lo posible en ningún momento, ya que la falla del proceso pone en riesgo la materia prima para los procesos realizados por la dependencia que son los registros oficiales.	1
2-3 días	Si este proceso no se podrá gestionar lo relacionado al ingreso de estudiantes a cursar cualquiera de los programas ofrecidos por la institución.	2
4-8 días	La interrupción por tiempo prolongado de estos procesos, impide el cumplimiento de otros, es importante solucionarlos prontamente.	3
8-15 días	Estos procesos son importantes para la dependencia pero su puesta en marcha puede esperar un tiempo corto sin generar ningún tipo de caos en el desempeño normal de los procesos.	4

Fuente: Autores del proyecto

Etapa 11. Los planes de recuperación para las actividades. Los planes de recuperación para las actividades, describen el paso a paso de las acciones y responsabilidades de mano de obra, recuperación, instalaciones, infraestructura, software e información.

Los planes de recuperación para las actividades de la dependencia Admisiones Registro y Control se describen como:

- Estimación de las necesidades materiales y recursos económicos necesarios para efectuar el plan de recuperación.
- Organización de grupos de trabajo y operaciones de protección de la información.
- Realización de un documento en donde se describa los casos que ocurrieron, sus costos y requerimientos.
- Anexar evidencias de los informes e instalaciones afectadas.

- Acondicionamiento de sitios para almacenar la documentación 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 12. Plan de recuperación de desastres. El plan de recuperación de desastres, se centra en la recuperación de la infraestructura de tecnología de la información y la comunicación. Para este plan es necesario aspectos como seguridad física y lógica, como se describen a continuación.

*Seguridad física, m*antener la seguridad física es garantizar la integridad de los activos materiales de un sistema de información así como de su infraestructura. Desde el lugar donde se encuentran ubicados, lo importante es cubrir las amenazas ocasionadas tanto por el hombre como por la naturaleza del medio físico del entorno.

El grado de seguridad física, es una serie de acciones empleadas para evitar fallos o para hacer que las consecuencias que puedan ocurrir de él sean menores.

Es importante tener en cuenta la ubicación de la oficina Admisiones Registro y Control y la división de sistemas, la potencia eléctrica, el sistema contra incendios, la selección del personal, el control de accesos y medidas de protección; las principales amenazas en la seguridad física son:

- Desastres naturales
- Incendios accidentales e inundaciones.
- Amenazas ocasionadas por el hombre

- Disturbios, y sabotajes

A continuación se analizan los peligros más importantes que se corren en las dependencias mencionadas anteriormente, con el objetivo de mantener una serie de acciones para mantener una prevención, reducción y recuperación y corrección de los diferentes tipos de riesgos.

Incendios. Los incendios pueden ser causa de mal uso de combustibles y fallas en las instalaciones eléctricas que estén en mal estado, este tipo de situaciones relacionadas con los incendios son altamente peligrosos para los equipos de cómputo ya que puede destruir los programas y el activo más importante de la organización como lo es la información (Galindo, 2014).

Estos son algunos factores importantes para reducir el riesgo de incendio:

- Se debe prohibir fumar en el lugar de trabajo
- Utilizar elementos metálicos para que no se afecten ante un eventual incendio.
- El piso y el techo tanto de la oficina como del centro de cómputo deben ser impermeables.
- Mantener un control de acceso y evitar el ingreso a personal no autorizado.
- Es indispensable que todas las áreas tengan ventilación y detección de incendios.

Para proteger los equipos y las instalaciones se debe tener en cuenta que la temperatura no debe sobrepasar los 18ºC y el límite de la humedad no debe superar el 65% para evitar deterioro; asimismo es necesario tener en cuenta que el centro de cómputo debe estar provisto de equipo para la extinción de incendios y se deben instalar extintores. Algunas recomendaciones son:

- El personal designado para usar extinguidores debe estar capacitado en su uso.
- Mantener aseguradas las áreas cercanas a los servidores para proteger contra el incendio.
- Proteger el sistema contra daños causados por el humo, ya que puede contener materiales y es espeso, por lo tanto sería más costosa la reparación de los equipos.
- Establecer correctamente cómo se mantendrán y almacenarán los 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 (Castillo, 2013).

Instalaciones Eléctricas. Las instalaciones eléctricas son un aspecto delicado el cual se debe tratar y darle la importancia que requiere, se pueden tener subidas y caídas de tensión, así como interrupciones en el funcionamiento de los dispositivos electrónicos.

En las instalaciones de la oficina se debe tener en cuenta los cables utilizados y la forma cómo están conectados para evitar daños futuros, de esta manera se puede reducir el daño y riesgo de corte. El cableado puede tener problemas de interferencia, que puede modificar o interrumpir el proceso de comunicación; cortes en los cables que impide la conexión y daños en el cable, los cuales afectarían el normal funcionamiento de la organización.

Aire acondicionado. La temperatura en la que se realizan los procesos es importante, el aire acondicionado debe estar presente en donde existan equipos de cómputo y en el cuarto de servidores.

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 extintores, cámaras de vigilancia y alarmas efectivas.

*Amenazas ocasionadas por el hombre***.** La infraestructura tecnológica de la Universidad Francisco de Paula Santander Ocaña es muy valiosa y siempre puede estar expuesta, por lo tanto es probable que los empleados utilicen los equipos de cómputo para realizar laboras ajenas a su trabajo, por ello se está utilizando tiempo de ese quipo en cosas para lo cual no está dispuesto; a esto se le suma que la información confidencial puede ser copiada fácilmente.

Otras de las amenazas ocasionadas por el hombre es que se sustraiga fácilmente el software utilizado en la organización y puedan ser llevados fuera del recinto.

Algunas recomendaciones son: 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. Los funcionarios de la institución deben dar buen uso al equipo que se les asigna, por lo tanto debe estar registrado y mantener asegurados los programas y componentes, asimismo se deben tener unas políticas del buen uso de estos elementos.

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, por otra parte 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 software e información, dependiendo del tipo de usuario.
- Asegurar que los usuarios no puedan modificar programas ni archivos y que se estén utilizando correctamente los sistemas.
- 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, es decir velar por la integridad de la información que se transmite.

Controles de Acceso. Implementar estos controles en el Sistema Operativo, sobre los sistemas y bases de datos, estos constituye 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 resguardar la información confidencial de accesos no autorizados. Para asegurar los sistemas se recomiendan los siguientes requisitos: identificación en el sistema, roles, transacciones, restringir servicios según el rol de la persona, registros, y control de acceso interno y externo.

Las actividades para la creación de roles, privilegios y administración de usuarios, se encuentran definidas en los procedimientos de la división de sistemas, como lo es el SIA (Sistema de Información Académico) que es una aplicación elaborada para facilitar la administración de los diferentes procesos académicos que se llevan a cabo en la Universidad Francisco de Paula Santander Ocaña, dicho sistema tiene la opción de 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; también existe el SIB (Sistema de Información de Biblioteca), que cuenta con una Base de Datos, 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.

Etapa 13. 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 20. 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 Apéndice A.

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 14. 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 la dependencia Admisiones Registro y Control se deben interrumpir por un lapso de tiempo considerable, solo se podría admitir las planteadas en la tabla tiempo máximo de interrupción.

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

- Adecuación de los espacios físicos.
- Reinstalación y adaptación de los servicios de acueducto, alcantarillado, energía eléctrica, internet, y telefonía fija.

4.3.5. <u>Prevención de riesgos.</u> En la tabla 24 se observan los riesgos asociados a la dependencia Admisiones Registro y Control, especificando su respectiva prevención de incidentes.

Tabla 24

Prevención de riesgos

No.	Riesgo	Prevención de Incidentes
1	Perdida de información tanto física como digital, equipos, incluso vidas humanas debido a Catástrofes naturales o incendios.	Para prevenir la pérdida de información física y digital debido a catástrofes o incendios se recomienda mantener extintores en la oficina, no utilizar elementos combustibles, realizar simulacros para que al presentarse el siniestro saber cómo actuar, revisar que la infraestructura es la más adecuada para soportar movimientos telúricos, mantener siempre en la oficina botiquín y capacitar a los empleados en cuanto a primeros auxilios.
2	Interrupción de funciones por paros estudiantiles o cierre de vías.	Para prevenir este tipo de situaciones o que no se vean afectados los procesos es necesario mantener los sistemas más importantes de la dependencia en la web, de manera que muchas transacciones se puedan realizar de forma virtual; asimismo retomar las actividades inmediatamente en cuanto se resuelva la situación.
3	Daño a equipos de cómputo por interrupciones de energía.	Para prevenir daño en los equipos debido a interrupciones de energía es necesario que la oficina mantenga una UPS para controlar la situación lo más pronto posible y evitar el daño den los equipos
4	Suspensión del servicio de red.	La suspensión en el servicio de red puede ser prevenido utilizando tanto red cableada, como Wifi, asimismo, tener una atención rápida y oportuna por la persona encargada de la administración de dichas redes.
5	Acceso de personal no autorizado a la información manejada a través de los computadores.	La prohibición a personal no autorizado logra prevenir alteraciones en la información manejada a través de los equipo de la oficina, es necesario también utilizar contraseñas en todos los equipos para evitar el ingreso a la información por parte de personas no autorizadas, y cuando el empleado no esté en el espacio de trabajo debe bloquearse el equipo inmediatamente.
6	Repetición de fallas o mal manejo de las mismas.	Para evitar este tipo de reincidencias se recomienda establecer mecanismos de control para conocer el por qué se repiten las fallas, igualmente se debe mantener una bitácora de los fallos ocurridos.
7	Acceso de terceros a información física.	El acceso a terceros a la dependencia en la cual se pueda ver afectada la información física debe ser totalmente restringido, sólo se debe permitir acceso a personal autorizado tanto a las instalaciones como a los sistemas alojados en la web.
8	Divulgación de información confidencial.	Es importante que los empleados que están a cargo de la información de la dependencia firmen un acuerdo de confidencialidad y así prevenir la divulgación de información confidencial, como datos personales de estudiantes, notas, certificados, etc.
9	Pérdida de información e imposibilidad de recuperación.	Para prevenir la pérdida de información es necesario realizar frecuentemente copias de seguridad de toda la información de la dependencia, de esta manera se podrá recuperar restaurando dichas copias en caso de pérdida.
10	Fallas en los sistemas operativos.	Los sistemas operativos utilizados por la dependencia deben ser auténticos y actualizados, para prevenir fallas en los mismos, igualmente se deben tener todos

		los programas utilizados licenciados e incluir un antivirus que proteja ante cualquier intrusión.
11	Indebida gestión de la información que atentan contra la integridad, confidencialidad y disponibilidad de la información.	Para esto se deben tener asignados los roles de los empleados que manejan la información, determinando así a qué tipo de información tiene acceso cada uno, esto con el fin de evitar una indebida gestión a la integridad, confidencialidad y disponibilidad de la misma.
12	Pérdida de la oportunidad de proteger la información e incluso la vida humana frente a una emergencia.	
13	Reducción de la demanda de aspirantes a ingresar a la institución.	Para prevenir reducción de aspirantes y pérdida de prestigio se hace necesario mantener actualizada la información y los sistemas, así como la excelente atención al cliente por parte de los empleados.
14	Pérdida de prestigio.	
15	Deterioro de la información física.	Para prevenir el deterioro de la información física se recomienda que se tengan en un lugar seguro la información física que se tenga en la dependencia, libre de incendios inundaciones y humedad

Fuente. Autores

Capítulo 5: Conclusiones

El Plan de Continuidad desarrollado para la oficina de Admisiones Registro y Control de la Universidad Francisco de Paula Santander Ocaña está basado en la norma ISO 22301:2012 la cual plantea los pasos para planear, implementar, operar, revisar y mejorar la gestión de la continuidad del negocio; el plan contempla las acciones que la dependencia debe seguir para recuperar y restaurar las actividades de manera progresiva regresar a la normalidad; garantizando en todo momento la integridad, confidencialidad y disponibilidad de la información.

Se desarrolló una auditoria pasiva basada en la norma ISO 27002 del 2005 con el propósito de conocer el estado actual de la dependencia de Admisiones, Registro y Control, tras el análisis de la información recolectada fue posible la identificación de 15 posibles riesgos, su análisis y evaluación y determinar acciones para su prevención y mitigación.

Se elaboró un documento formal donde se incorporan las etapas para llevar a cabo el Plan de Continuidad de la Oficina Admisiones Registro y Control que pretende suministrar a la dependencia de las herramientas necesarias que le permitan recuperarse de incidentes en un tiempo prudente sin causar traumatismo en normal desarrollo de las funciones manteniendo el prestigio de la Universidad y contribuyendo al cumplimiento de objetivos misionales.

Capítulo 6: Recomendaciones

Después de diseñado el Plan de continuidad es necesario realizar pruebas antes de ser aprobado y oficializado, dichas pruebas permitirán evaluar la capacidad de respuesta ante un incidente que afecte la seguridad de la información y al mismo tiempo identificar aspectos de mejorar.

Una vez aprobado el Plan de Continuidad es indispensable la formalización del mismo y la posterior socialización con todo el personal de la dependencia quienes a su vez deben recibir la capacitación necesaria para una correcta activación del mismo.

Conjuntamente se recomienda capacitar al personal sobre la seguridad de la información: Norma ISO 27001: 2005, ISO 27001: 2013 y demás normativa establecida por la institución, entre ella el Plan de contingencia de TI.

Después de aplicado los procedimientos establecidos en el Plan de Continuidad y recuperada la normalidad después de un incidente es importante realizar un seguimiento del mismo y verificar los impactos causados, para ello se deben realizar informes de las acciones llevadas a cabo y sobre el cumplimiento de los objetivos del Plan de Continuidad, los tiempos empleados, dificultades con las que se encontraron, toda esta información servirá para valorar si el Plan ha funcionado según lo planeado, así como conocer los posibles fallos, y en su caso, tenerlos en cuenta para la adecuación del mismo.

Referencias

Aguilera Castro, A. (2010). Direccionamiento estratégico y crecimiento empresarial: algunas reflexiones en torno a su relación. *SCIELO*, 85-106.

Alcaldía de Bogotá. (2012). *Alcaldía de Bogotá.* Obtenido de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

Blanco Lindarte, J., Martínez Vega, L., Quintero Prado, C., & Rincón Angarita, J. (2012). *PLAN DE CONTINUIDAD PARA EL CENTRO DE DESARROLLO.*

Blanco, J. A., Martinez Vega, L. F., Quintero Prado, C. d., & Rincón Angarita, J. F. (2015). *Univeridad Francisco de Paula Santander Ocaña.* Recuperado el 20 de Mayo de 2016, de http://repositorio.ufpso.edu.co:8080/dspaceufpso/handle/123456789/596

BSI. (2006). *http://www.bsigroup.com/.* Obtenido de http://www.bsigroup.com/es-MX/continuidad-delnegocio-ISO-22301/

BSI. (2007). *BSI.* Obtenido de http://www.bsigroup.com/es-ES/ISO-22301-continuidad-de-negocio/Requisitos-de-la-norma-ISO-22301/

Burgos Salazar, J., & Campos, P. (2008). Modelo Para Seguridad de la Información en TIC. *CEUR Workshop Proceedings*, 234-253.

Castillo, M. (2013). *Conceptos Básicos de la Seguridad Informática.* Obtenido de http://ccns.jimdo.com/presentaci%C3%B3n/presentaci%C3%B3n-marco-castillo/desastres/

Castro Marquina, L. (2013). *PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ.* Obtenido de http://tesis.pucp.edu.pe/repositorio/bitstream/handle/123456789/5110/CASTRO_LAURA_DISE%C3%91O_SISTEMA_GESTION_CONTINUIDAD_NEGOCIOS_RENIEC_NORMA_ISO_IEC_22301.pdf?sequence=1&isAllowed=y

Departamento Administrativo de la Función Pública (DAFP). (2011). *Guía Para la Administración del Riesgo.* Obtenido de http://portal.dafp.gov.co/portal/pls/portal/formularios.retrive_publicaciones?no=1592

Dzul Escamilla, M. (2012). *Univeridad Autónoma del Estado de Hidalgo.* Obtenido de http://www.uaeh.edu.mx/docencia/VI_Presentaciones/licenciatura_en_mercadotecnia/fundamentos_de_metodologia_investigacion/PRES39.pdf

Everett, C. (2015). Cyberwar and protecting critical national infrastructure. *Computer Fraud & Security, 2015*.

Fernández Alarcón, V. (2006). Desarrollo de sistemas de información : una metodología basada en el modelado. En V. Fernández Alarcón, *Desarrollo de sistemas de información : una metodología basada en el modelado.* Edicions UPC.

Galindo, C. (2014). Seguridad de la Información: Revista de la Segunda Cohorte del Doctorado en Seguridad Estratégica. En C. Galindo, *Seguridad de la Información: Revista de la Segunda Cohorte del Doctorado en Seguridad Estratégica.*

García Fort, J. (2010). *http://www.iit.comillas.edu/.* Recuperado el 17 de junio de 2016, de UNIVERSIDAD PONTIFICIA COMILLAS: http://www.iit.comillas.edu/pfc/resumenes/4c2474cf9a017.pdf

Gaspar Martínez, J. (2010). El plan de continuidad de negocio: Una guia práctica para su elaboracción. En J. Gaspar Martínez, *El plan de continuidad de negocio: Una guia práctica para su elaboracción* (págs. 204-205). Díaz de Santos.

ICETEX. (30 de Mayo de 2013). *MANUAL DE ADMINISTRACION DEL PLAN DE.* Recuperado el Julio de 2016, de https://www.icetex.gov.co/dnnpro5/Portals/0/Documentos/La%20Institucion/manuales/Manual_continuidad_negocio.pdf

IMARPE. (2012). *http://www.imarpe.pe/.* Recuperado el 17 de junio de 2016, de INSTITUTO DEL MAR DEL PERÚ: http://www.imarpe.pe/imarpe/archivos/informes/imarpe_resol_de_158_2012_contin g.pdf

Instituto de Fomento al Talento Humano. (2012). *Instituto de Fomento al Talento Humano*. Recuperado el 3 de junio de 2016, de http://www.fomentoacademico.gob.ec/: http://www.fomentoacademico.gob.ec/docs/lotaip/planes_programas_en_ejecucion/2012/plan_de_continuidad_de_negocios.pdf

Internatitional organization for estandardization. (2013). *Sistemas de gestión de calidad segun la ISO 9001*. Obtenido de http://iso9001calidad.com/clasificacion-de-procesos-49.html

ISO 22301:2012. (s.f.). *Societal security -- Business continuity management systems --- Requirements*. Recuperado el Julio de 2016, de http://www.iso.org/iso/catalogue_detail?csnumber=50038

Koppell, J. (2011). International organization for standardization. 289.

MinTIC. (2009). Obtenido de http://www.mintic.gov.co/portal/604/articles-3707_documento.pdf

MinTIC. (2009). *El Ministerio de Tecnologías de la Información y las Comunicaciones.* Obtenido de http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

Mintzberg, H. (2003). Diseño de organizaciones eficientes. En H. Mintzberg, *Diseño de organizaciones eficientes* (págs. 189-190). Buenos Aires: Ateneo.

Paredes , G. (2006). Introducción a la Criptografía. *Revista Digital Universitaria*, 7(7).

Pérez Escobar, J. (1991). *http://www.procuraduria.gov.co/.* Obtenido de http://www.procuraduria.gov.co/guiamp/media/file/Macroproceso%20Disciplinario/Constitucion_Politica_de_Colombia.htm

Ramírez Robayo, M., Londoño Rúa, E., & Gómez Gómez, J. (2012). *http://www.universidadean.edu.co/.* Recuperado el 3 de junio de 2016, de http://repository.ean.edu.co/bitstream/handle/10882/2603/RamirezMaritza2012.pdf;jsessionid=7BBBC08D2214AB682450F7AC128C601E?sequence=1

Rodríguez Gómez, D., & Valldeoriola Roquet, J. (2012). Obtenido de http://zanadoria.com/syllabi/m1019/mat_cast-nodef/PID_00148556-1.pdf

Sánchez Jaime, K. (2015). *Universidad Francisco de Paula Santander Ocaña.* Recuperado el 16 de mayo de 2016, de http://repositorio.ufpso.edu.co:8080/dspaceufpso/handle/123456789/576

Serna Gómez, H. (1997). Gerencia estratégica : planeación y gestión - teoría y metodología. En H. Serna Gómez, *Gerencia estratégica : planeación y gestión - teoría y metodología.* Santafé de Bogotá.

Servat, A. (2012). NUEVO ESTÁNDAR INTERNACIONAL EN CONTINUIDAD DEL NEGOCIO ISO 22301:2012. *Gestión*.

Torres, Á., Erik, J., & Velasco, H. (2014). *Diseño y propuesta de implementación de un plan de continuidad del negocio aplicable a los hospitales en la ciudad de Bogotá.*

UFPSO. (2015). Obtenido de https://ufpso.edu.co/admisiones/Presentacion

UFPSO. (2015). *PLAN DE CONTINGENCIA DE TI.*

UFPSO. (2015). *www.ufpso.edu.co.* Recuperado el 2016, de https://ufpso.edu.co/Historia

UFPSO. (2016). Obtenido de https://ufpso.edu.co/sig/procedimientos_arg#arbol_procesos

UFPSO. (2016). *Universidad Francisco de Paula Santander Ocaña.* Obtenido de https://ufpso.edu.co/ftp/pdf/guias/dp/K-DP-OPL-001C.pdf

UPIICSA. (s.f.). *Unidad Profesional Interdisciplinaria de Ingeniería y Ciencias sociales y Administrativas.* Obtenido de http://www.sites.upiicsa.ipn.mx/polilibros/portal/polilibros/p_terminados/Planeacion_Estrategica_ultima_actualizacion/polilibro/Unidad%20IV/Tema4_5.htm

Vargas Daza, F. (2009). *Plan de Emergencias Corporación Educativa Minuto De Dios.* Recuperado el 10 de mayo de 2016, de http://colegios.minutodedios.org/saludocupacionalcemid/imagenes/plan.pdf

Wilivesecurity. (6 de Enero de 2014). *ISO 22301:2012 el estándar de la continuidad del negocio*. Recuperado el 20 de julio de 2016, de http://www.welivesecurity.com/la-es/2014/01/06/iso-22301-2012-estandar-continuidad-negocio/

Apéndices

Apéndice A: Auditoria

Número de la auditoria: 001
Oficio de orden de auditoria: A-001/2015
Fecha de inicio : 27 de Marzo 2015
Fecha de término: 27 de Mayo de 2015

Empresa a Auditar: Universidad Francisco De Paula Santander Ocaña
Dependencia: Admisiones, Registro y Control

	NOMBRE	INICIALES
Auditores Responsables	Carlos Andrés Sánchez,	**CS**
	Natalia Torrado,	**NT**
	Johan Smith Rueda,	**JR**
	Carlos Andrés Gómez	**CG**
Numero de Folios	43	

Documento preparado por:
Carlos Andrés Sánchez, Natalia Torrado, Johan Smith Rueda, Carlos Andrés Gómez.

Fecha: Del 27 de Marzo de 2015 **Fecha:** Al 27 de Mayo de 2015

Archivos permanentes

Secciones	Nomenclatura
Organigrama de la Universidad Francisco de Paula Santander Ocaña.	**AP1**
Informe anual de la ejecución de los planes de acción de la UFPSO.	**AP2**
Guía para la administración del riesgo.	**AP3**
Guía para el análisis de causas y la formulación de acciones para el mejoramiento continuo UFPSO.	**AP4**
Manual de indicadores.	**AP5**
Organigrama de la dependencia de admisiones, registro y control (ARC).	**AP6**
Visión y Misión de la dependencia (ARC).	**AP7**
Manual específico de proceso, admisiones, registro y control.	**AP8**
Plan de acción de la dependencia de admisiones registro y control.	**AP9**
Caracterización de los procesos de admisiones registro y control.	**AP10**
Instructivo trámites a solicitudes de servicios académicos.	**AP11**

Archivos corrientes

Secciones	Nomenclatura
Programa de auditoria	**AC1**
Desviaciones detectadas	**AC2**
Inventario de software	**AC3**
Inventario de hardware	**AC4**
Entrevista	**AC5**
Lista de chequeo	**AC6**
Encuesta	**AC7**
Hallazgos	**AC8**
Pruebas	**AC9**

Programa de auditoria

OBJETIVO	Realizar una auditoría a la dependencia de Admisiones, Registro y Control de la Universidad Francisco de Paula Santander Ocaña, bajo los lineamientos de la norma ISO 27001:2005.
ALCANCE	Esta auditoria tendrá lugar en la dependencia de Admisiones, Registro y Control de la UFPS Ocaña con una duración de dos meses iniciando el 27 de marzo del 2015 y concluyendo el 27 de mayo de 2015.

AUDITORES	CG: Carlos Andrés Gómez Flórez JR: Johan Smith Rueda Rueda NT: Natalia Torrado Peñaranda CS: Carlos Andrés Sánchez Becerra

FASE	DESCRIPCIÓN	**ACTIVIDAD**	**NUM. DEL PERSONAL PARTICIPANTE**	**PERIODO ESTIMADO**	
				INICIO	**TERMINO**
1	Conocer los aspectos generales de la UFPSO y de la dependencia de Admisiones, Registro y Control (ARC), y recopilar la información respectiva.	Revisar documentación organizacional de la UFPSO Conocer el funcionamiento interno de la dependencia, sus procesos y subprocesos. Diseñar y aplicar instrumentos de recolección de la información (entrevista, lista de chequeo, encuesta).	CS JR NT CG	27/03/2015	17/04/2015
2	Revisión de la infraestructura tecnológica institucional y de la dependencia ARC	Solicitar información de la infraestructura tecnológica de la organización y la dependencia. Solicitar información sobre los recursos hardware y software de la dependencia y realizar las respectivas pruebas.	CS JR NT	09/04/2015	17/04/2015
3	Reunión con la jefe de ARC para establecer los objetivos y alcances de la auditoría.	Solicitar reunión con el jefe de ARC. Reunión con el jefe de ARC.	CS JR	21/04/2015	28/04/2015
4	Solicitar los reglamentos internos e institucionales pertinentes a la ARC	Solicitar los documentos que contienen la reglamentación de la organización y la dependencia.	NT CG	23/04/2015	29/04/2015
5	Evaluar la gestión de los activos de la dependencia	Comprobar la existencia de los inventarios de los activos de la dependencia y que estos fueron asignados correctamente a dicha oficina. Probar que los inventarios estén actualizados.	CS JR NT	30/04/2015	11/05/2015
6	Evaluar la seguridad física y ambiental de la dependencia	Evaluar la existencia y cumplimiento de los controles para la protección contra amenazas externas y ambientales. Evaluar los controles aplicados a los equipos, su ubicación, protección, mantenimiento.	CS JR NT	12/05/2015	14/05/2015

7	Valorar la gestión de las comunicaciones y las operaciones	Verificar y probar las políticas de respaldo de la información.	CS JR NT	14/05/2015	15/05/2015
8	Evaluar la gestión de incidentes en la seguridad de la información	Verificar la existencia de documentos para el reporte de los eventos en la seguridad de la información y aplicación de los mismos.	CS JR	15/05/2015	18/05/2015
9	Evaluar la gestión de la continuidad comercial	Verificar la existencia de plan de continuidad del negocio.	NT CG	19/05/2015	19/05/2015
10	Elaboración del dictamen y recomendaciones por parte del equipo auditor.	Análisis de los instrumentos de recopilación aplicados: listas de chequeo, encuestas y visitas a la oficina de admisiones, registro y control.	CS JR NT CG	20/05/2015	27/05/2015

Desviaciones detectadas

AC2_01

SITUACIONES ENCONTRADAS

EMPRESA:	**ÁREA AUDITADA:**	**DÍA**	**MES**	**AÑO**
Universidad Francisco de Paula Santander Ocaña	Admisiones, Registro y Control	14	05	2015

REF:	**SITUACIONES**	**CAUSAS**	**SOLUCIÓN**
Lc_02_01	No se delimitan las áreas de trabajo	Ausencia de límites estructurales en las áreas de trabajo	Establecer delimitaciones en las áreas de trabajo
Lc_02_02	El acceso a los equipos no es muy severo.	La puerta de ingreso es muy débil y brinda muy poca seguridad.	Mejorar la vía de acceso de personal autorizado a las instalaciones de la dependencia.
Lc_02_04	El cableado eléctrico y estructurado se encuentra en la misma canaleta.	Se le dio un mal manejo a las redes del cableado.	Instaurar canaletas independientes para cada tipo de cableado.
Lc_02_05	El cableado estructurado no cumple con las normas establecidas.	Se encuentran por fuera de la canaleta y en el suelo enredado.	Que todo el cableado se encuentre en su respectivo compartimiento.
Lc_02_06	No hay señalizaciones del tipo de cableado.	No se tuvo en cuenta las normas de instalaciones eléctricas ni de seguridad.	Señalizar el tipo de cableado.

ELABORÓ: Carlos A. Sánchez, Natalia Torrado, Johan S. Rueda, Carlos Gómez

AC2_02

SITUACIONES ENCONTRADAS

EMPRESA:	AREA AUDITADA:	DIA	MES	AÑO
Universidad Francisco de Paula Santander Ocaña	Admisiones, Registro y Control	14	05	2015

REF:	SITUACIONES	CAUSAS	SOLUCIÓN
Lc_02_07	No existen detectores de humo, ni alarmas contra incendios.	No existen medidas de prevención contra incendios.	Aplicar las medidas de contingencia.
Lc_02_08	No cuentan con UPC	No se han tomado medidas preventivas ante las posibles fallas de energía eléctrica.	Adquirir una UPC para la dependencia.
Lc_02_12	El sistema de refrigeración para los equipos no es suficiente.	El aire acondicionado es muy pequeño para la oficina y la cantidad de equipos. Igualmente la puerta se encuentra abierta lo cual no permite que el aire se manga en el lugar y refrigere los equipos.	Adquirir un aire acondicionado más grande y permanecer con la puerta cerrada.

ELABORÓ: Carlos A. Sánchez, Natalia Torrado, Johan S. Rueda, Carlos Gómez

C2_03

SITUACIONES ENCONTRADAS

EMPRESA:	ÁREA AUDITADA:	DÍA	MES	AÑO
Universidad Francisco de Paula Santander Ocaña	Admisiones, Registro y Control	15	05	2015

REF:	SITUACIONES	CAUSAS	SOLUCIÓN
Lc_02_21	No existe señalización para salidas de emergencia ni rutas de evacuación.	La dependencia no ha tomado medidas de evacuación en caso de emergencias.	Implementar señalización que indique las vías de evacuación de la dependencia.
Lc_02_27	No se cuenta con las medidas físicas apropiadas para evitar la entrada de personal no autorizado fuera del horario establecido.	La oficina no cuenta con un sistema de protección ante robos.	Establecer medidas de seguridad física a las instalaciones para evitar que se sustraigan equipos o información.

ELABORÓ
Carlos A. Sánchez, Natalia Torrado, Johan S. Rueda, Carlos Gómez

SITUACIONES ENCONTRADAS

SITUACIONES ENCONTRADAS

EMPRESA:	ÁREA AUDITADA:	DÍA	MES	AÑO
Universidad Francisco de Paula Santander Ocaña	Admisiones, Registro y Control	15	05	2015

REF:	SITUACIONES	CAUSAS	SOLUCIÓN
Lc_02_21	No existe señalización para salidas de emergencia ni rutas de evacuación.	La dependencia no ha tomado medidas de evacuación en caso de emergencias.	Implementar señalización que indique las vías de evacuación de la dependencia.
Lc_02_27	No se cuenta con las medidas físicas apropiadas para evitar la entrada de personal no autorizado fuera del horario establecido.	La oficina no cuenta con un sistema de protección ante robos.	Establecer medidas de seguridad física a las instalaciones para evitar que se sustraigan equipos o información.

ELABORÓ
Carlos A. Sánchez, Natalia Torrado, Johan S. Rueda, Carlos Gómez

EMPRESA:	AREA AUDITADA:	DIA	MES	AÑO
Universidad Francisco de Paula Santander Ocaña	Admisiones, Registro y Control	15	05	2015

REF:	SITUACIONES	CAUSAS	SOLUCIÓN
Lc_01_01	La dependencias no lleva el registro de las fallas detectadas en los equipos	Tercerización de las responsabilidades en los recursos tecnológica de la dependencia.	La dependencia debe llevar un registro propio de qué equipos presentan fallas, cuales salen a reparación para controlar qué tipo de información contienen esos equipos y establecer las medidas adecuadas para su resguardo.
Lc_01_02 Lc_01_03	Las copias de seguridad, de archivos tanto físicos como digitales se almacenan dentro de la misma dependencia.	No se tiene previsto dentro de la institución otro espacio para archivar los archivos físicos y en cuanto a los digital no se han hecho conocer para los funcionarios medidas de seguridad.	La dependencia debe establecer si las políticas establecidas por la dependencia de soporte son suficientes para garantizar el cumplimiento de sus objetivos y la continuidad del negocio.
Lc_01_04	Los sistemas operativos no están actualizados, y en algunos equipos.	Como la parte tecnológica depende de la división de sistemas, dicha dependencia no está actualizando periódicamente el software utilizado y los empleados de ARC no exigen dichas actualizaciones dejando toda la responsabilidad en dicha dependencia.	Adquirir la licencia de las versiones de Windows con soporte, e instalar dicho sistema operativo en los equipos con Windows XP. Mínimo la versión de Windows 7, pero sí es una versión más reciente garantiza que Microsoft le brinde soporte por más tiempo.
Lc_01_05	El software instalado no se encuentra actualizado		Establecer actualizaciones generales de software, que sea de conocimiento por los empleados de ARC para que así, si división de sistemas no brinda el soporte estos puedan exigirlo a dicha dependencia.
Lc_01_06	No hay registro evidente de las licencias de software	Tercerización de la responsabilidad en los recursos tecnólogos.	Verificar que la dependencia de soporte tenga actualizada dicho registro, que los equipos cuenten con su respectiva licencia.
Lc_01_07	Los equipos de cómputo no cuentan con contraseñas para garantizar el ingreso de personas no autorizadas	Tercerización de la responsabilidad en los recursos tecnólogos.	Establecer contraseñas a nivel de bios o sistema operativo o ambas para garantizar la confidencialidad de la información almacenada en dichos equipos.

ELABORÓ Carlos A. Sánchez, Natalia Torrado, Johan S. Rueda, Carlos Gómez

Empresa	Universidad Francisco de Paula Santander Ocaña
Área o Proceso	Admisiones, Registro y Control
Fecha	Mayo 19 del 2015
Responsables	Carlos A. Sánchez, Natalia Torrado, Johan S. Rueda, Carlos Gómez

REF	Software	Versión
Equipo 1	Windows 7	Ultimate SP1
	Adobe Reader XI	10.0.11
	Avast Free	2015.10.2.2218
	McAffe Security Scan plus	3.8.150.1
	Microsoft Office Professional plus 2013	15.0.4569.1506
	Oracle Interprise	6

REF	Software	Versión
Equipo 2	Windows 7	Professional SP1
	Adobe Reader	8.1.1
	Microsoft Office Professional plus 2013	15.0.4569.1506
	Oracle Interprise	6
	Eset EndPonit Security	5.0.2126.6

REF	Software	Versión
Equipo 3	Windows 7	Professional SP1
	Adobe Reader	11.0.1
	Microsoft Office Professional plus 2013	15.0.4420.1017
	Oracle Interprise	6
	Eset EndPonit Security	5.0.2126.6

REF	Software	Versión
Equipo 4	Windows XP	Professional 2002 SP2
	Adobe Reader	8.1.1
	Microsoft Office Professional	2003
	Oracle Interprise	6
	Open office	1.1.4

REF	Software	Versión
	Windows XP	Professional 2002 SP3
	Adobe Reader	8.1.1

Equipo 5	Eset EndPonit Security	5.0.2126.6
	Microsoft Office Professional	2003
	Oracle Interprise	6

REF	**Software**	**Versión**
Equipo 6	Windows XP	Professional 2002 SP2

REF	**Software**	**Versión**
Equipo 7	Windows 7	Professional SP1
	Adobe Reader	11.0.1
	Microsoft Office Professional plus 2013	15.0.4420.1017
	Oracle Interprise	6
	Eset EndPonit Security	5.0.2126.6

Inventario de hardware **AC4**

Equipo 1

Elemento / Dispositivo	Serial	Marca	Modelo
,.COMPUTADOR COMPLETO (TODO EN UNO)	MXL22405X4	HP	AOX72LT#ABM
CPU-PROCESADOR (ALL IN ONE 3420, INTEL CORE I3-2120)			
MEMORIA RAM 4GB			
TARJETA DE SONIDO INTERNA			
TARJETA DE VIDEO INTERNA			
TARJETA DE RED INTERNA			
DISCO DURO 500 GB		SATA 6G SMART	
MONITOR DE 20"		HP	
TECLADO		HP	
MOUSE		HP	
BOARD			

Equipo 2

Elemento / Dispositivo	Serial	Marca	Modelo
,.COMPUTADOR COMPLETO,REF 6200 PRO	MXL1311YMZ	HP	
CPU-PROCESADOR (INTEL CORE I5-2400(6M CACHE 3.1 GHZ)			
MEMORIA RAM 4GB PC3-10600			
TARJETA DE SONIDO INTERNA			
TARJETA DE VIDEO INTERNA			
TARJETA DE RED (CONEXION DE RED INTEL 82579M GBE)			
DISCO DURO 500 GB		SATA NCQ HDD	
MONITOR DE 18.5"	CNC111PDQ0	HP	
TECLADO	BAUDU0KVB0N6SO	HP	
MOUSE		HP	
BOARD			

Equipo 3

Elemento / Dispositivo	Serial	Marca	Modelo
,.COMPUTADOR DE ESCRITORIO TODO EN UNO 600 G1	MXL4280N44	HP	PRO ONE 600
CPU-PROCESADOR INTEL CORE I7 4770S QC 3.1GHZ			
MEMORIA RAM DE 8 GB 1600			
TARJETA DE SONIDO			
TARJETA DE VIDEO			
TARJETA DE RED			
DISCO DURO 1TB 7200			
PANTALLA 21,5" HD LED AG		HP	
TECLADO USB	BDMHE0CCP6O4MZ	HP	
MOUSE USB	9W603I7	HP	
MAINBOARD			
DVD/CD-RW			
SISTEMA OPERATIVO WIN 7 PRO64 CON LIC WIN 8 PRO64			

Equipo 4

Elemento / Dispositivo	Serial	Marca	Modelo
,.COMPUTADOR DE ESCRITORIO (TORRE ATX)	EQ1623037030	CLON	
CPU-PROCESADOR (PENTIUN IV 3.2 GHZ)		INTEL	
MEMORIA RAM (512 MB DDR1)		KINGSTON	
TARJETA DE SONIDO (INTERNA)			
TARJETA DE VIDEO (INTERNA)			
TARJETA DE RED (1 INTERNA)			
DISCO DURO (80 GB)		SAMSUNG	
MONITOR		HP	
TECLADO		GENIUS	
MOUSE		GENIUS	
BOARD (775i65G)		ASROCK	
DVD/CD-RW			

Equipo 5

Elemento / Dispositivo	Serial	Marca	Modelo
,.COMPUTADOR DE ESCRITORIO	MXJ94308FX	HP	WB992LA#ABM
CPU-PROCESADOR INTEL CORE 2 DUO DE 2.93 GHZ		INTEL	
MEMORIA RAM 2GB			
TARJETA DE SONIDO			
TARJETA DE VIDEO			
TARJETA DE RED			
DISCO DURO DE 250 GB			
MONITOR DE 17"	3CQ93914KV	HP	
TECLADO	BAUDU0HVBY0812	HP	
MOUSE			
MAINBOARD			

Equipo 6

Elemento / Dispositivo	Serial	Marca	Modelo
,.COMPUTADOR PENTIUM DUAL CORE 2140 (1.6 GHZ)	SQ2432200002ZF	GENERICO	ATX TLA776
CPU-PROCESADOR (PENTIUM DUAL CORE 2140 (1.6 GHZ))			
MEMORIA RAM (1 GB DDR2)			
TARJETA DE SONIDO INTERNA			
TARJETA DE VIDEO INTERNA			
TARJETA DE RED INTERNA			
DISCO DURO 160 GB		SATA	
MONITOR 732N DE 17"	PE17H9NP804235	SAMSUNG	
TECLADO		GENIUS	
MOUSE		GENIUS	
PARLANTES			
BOARD 945 GCNL		INTEL	
DVD/CD-RW			

Equipo 7

Elemento / Dispositivo	Serial	Marca	Modelo
,.COMPUTADOR DE ESCRITORIO TODO EN UNO 600 G1	MXL4280N3B	HP	PRO ONE 600
CPU-PROCESADOR INTEL CORE I7 4770S QC 3.1GHZ			
MEMORIA RAM DE 8 GB 1600			
TARJETA DE SONIDO			
TARJETA DE VIDEO			
TARJETA DE RED			
DISCO DURO 1TB 7200			
PANTALLA 21,5" HD LED AG		HP	
TECLADO USB	BDMHE0CCP6O4LB	HP	
MOUSE USB	9W66O3H9	HP	
MAINBOARD			
DVD/CD-RW			
SISTEMA OPERATIVO WIN 7 PRO64 CON LIC WIN 8 PRO64			

Entrevista **AC5**

Entrevista dirigida al jefe de la oficina de Admisiones Registro y Control
Universidad Francisco de Paula Santander
Facultad de Ingenierías
Especialización en Auditoría de Sistemas

Buenos días, como parte de nuestra tesis para la especialización en Auditoria de Sistemas de la Universidad Francisco de Paula Santander Ocaña (UFPSO), nos encontramos adelantando una investigación acerca de la oficina de Admisiones Registro y Control de la UFPSO. La información recolectada a través de este medio es de carácter confidencial, solo será utilizada con los propósitos que acoge la investigación. Agradecemos su colaboración.

NOMBRE Y APELLIDOS **Torcoroma Velásquez Pérez**
NUMERO DE CÉDULA _____ TELEFONO_____
E-MAIL _____ FECHA: _____ _____ _____

CONTEXTO CON LA ORGANIZACIÓN
¿Cuál es el objetivo principal de la dependencia?
¿Qué información maneja la dependencia?
¿Qué servicios brinda la dependencia a la comunidad Universitaria?
¿Se encuentran documentadas las funciones del personal de la dependencia? ¿Dónde?
¿Existen otras dependencias que dependan del trabajo realizado por la dependencia de Admisiones Registro y Control (ARC)?
¿La oficina de ARC depende del trabajo realizado por otras dependencias?
¿Existe alguna normativa legal por la que debe regirse la dependencia para el desempeño de sus funciones?
¿Existen objetivos claramente determinados para el cumplimiento de la Visión de la dependencia trazada para el año 2019? ¿Cuáles?
Dominio 5: Política de Seguridad
¿Existe una política de seguridad de la información por la cual se rija la dependencia? ¿Cuál es?
¿Los funcionarios de la dependencia conocen y ponen en práctica la política de seguridad de la información?
¿Cada cuánto se actualiza la política de seguridad de la información?
Dominio 6: Organización de la seguridad de la información
¿Cómo se distribuye la responsabilidad en el manejo de la información tanto física como digital a los funcionarios de la dependencia?
Dominio 7: Gestión de activos
¿Existe un inventario de los equipos de cómputo?
¿Existe un inventario del software instalado en los equipos de cómputo?
¿Se actualizan periódicamente los inventarios anteriormente descritos?
¿Existen responsabilidades asignadas respecto a la manipulación de activos de soporte físico en tránsito (ej: Discos duros externos)?
Dominio 8: Seguridad de los recursos humanos
¿Qué criterios establece para saber que el personal que se va a contratar es el idóneo?
¿Existe un acuerdo de confiablidad de la información debidamente establecido entre la Universidad y los funcionarios de la oficina de ARC? ¿Cuál?
¿Se encuentran documentadas las funciones que le corresponden a cada una de los funcionarios de la oficina de ARC?
¿Con que regularidad se capacita al personal en cuanto a la gestión segura de la información?
¿Existe algún proceso disciplinario en caso de que uno de los funcionarios atente contra la integridad de la información? ¿Cuál?
¿La dependencia se rige por alguna política de Gestión de riesgos laborales? ¿Cuál es?
Dominio 9: Seguridad física y ambiental
¿Considera que la ubicación física de la oficina dentro del campus universitario es la idónea?
¿Existen controles para asegurar que personal no autorizado acceda a la dependencia? ¿Cuáles?
¿Existe un plan de contingencia en caso de presentarse una catástrofe natural tanto para el personal, como

para el recuperado de la información? ¿Cuál?
¿La información física se encuentra en un lugar seguro y protegido de agentes externos como humedad?
¿Existen diferentes niveles de privilegios de usuario que acceden a los equipos de cómputo desde los cuales se gestiona información?
¿Las contraseñas implementadas por los funcionarios de la oficina de ARC se rigen por algún parámetro de contraseñas seguras? ¿Cuáles?
Dominio 10: Gestión de las comunicaciones y operaciones.
¿Existe un proceso debidamente establecido en que se oficialice la planificación y la organización del trabajo desarrollado por la dependencia?
¿Se realiza monitoreo del desarrollo de las laborares desarrolladas por los funcionarios de la dependencia? ¿Con que frecuencia?
¿Qué tipo de mantenimiento se realiza a los equipos? ¿Con que frecuencia?
¿Qué controles se llevan a cabo en cuanto al código malicioso?
¿Con que frecuencia se realizan las copias de seguridad de la información digital? ¿Con que frecuencia?
¿Existen copias de respaldo de la información física? ¿Dónde se almacenan?
¿Existe restricción para instalar programas diferentes a los relacionados con el oficio?
¿Qué restricciones de acceso a internet existen?
¿Existen restricciones para dar acceso a información a terceros que la soliciten? Por ejemplo constancia de terminación de materias
Dominio 11: Control de acceso
¿Existen controles de acceso a la información física? ¿Cuáles?
¿Existen y se aplican normas para los equipos desatendidos? Es decir cuando el funcionario se retira del equipo por un tiempo ya sea corto o largo y el mismo continúa encendido, existen normas para prevenir que terceros puedan acceder a la información.
Dominio 12: Adquisición, desarrollo y mantenimiento de los sistemas de información
¿Se realiza control, verificación y actualización del software que se utiliza en la dependencia para la gestión de la información?
¿Cuándo se realiza actualización de sistemas operativos se prevé que las aplicaciones, programas empleados por la dependencia sean compatibles?
Dominio 13: Gestión de incidentes en la seguridad de la información
¿En caso de presentarse alguna falla en los sistemas, se posee un plan de contingencia para salvaguardar la seguridad de la información digital?
En caso de presentarse un incidente de tipo natural que atente contra seguridad tanto física como digital ¿Existe un plan de contingencia qué permita contrarrestar o mitigar los riesgos?
¿En caso de verificarse el uso indebido de la información por parte de un funcionario existe un proceso disciplinario debidamente establecido?
Dominio 14: Gestión de la continuidad comercial
¿Conoce usted y los demás funcionarios de la dependencia conocen la importancia de la Gestión de la continuidad del negocio?
¿Existe una política para la Gestión de la continuidad del negocio, en la dependencia?
¿En caso de contar con dicha política esta es conocida por los funcionarios de acuerdo a su función?
¿Se actualiza periódicamente?
Dominio 15: Cumplimiento
¿Se verifica que la gestión de la información tanto física como digital cumpla con las políticas, normas, y procedimientos de seguridad establecidas? ¿De qué manera?

Lista de chequeo **AC6**

Admisiones Registro y Control			**R/PT: 001**	
CheckList			**C01**	
Dominio			**A5. Políticas de seguridad**	
Cuestionario				
Pregunta	**SI**	**NO**	**NA**	**Comentarios**
Al ser la información el activo más importante para la organización ¿están definidos los recursos de información que deben ser protegidos dentro de la dependencia ARC?				
¿Incluye un esquema de clasificación que preserve los criterios de confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información contenida en la dependencia ARC?				
¿La Política de Seguridad de la Información implementada incluye normas y/o procedimientos para garantizar la continuidad del negocio, minimizando los riesgos de daño y asegurando el eficiente cumplimiento de los objetivos?				
¿Está sustentada la Política por una evaluación de riesgos?				
¿Contempla la Política las disposiciones legales vigentes?				
¿Establece el resguardo adecuado de la información documentada?				

Admisiones Registro y Control			**R/PT: 002**	
CheckList			**C02**	
Dominio			**A6. Organización de la seguridad de la información**	
Cuestionario				
Pregunta	**SI**	**NO**	**NA**	**Comentarios**
¿Existe un Responsable de Seguridad Informática designado por la máxima autoridad de la organización?				
¿Se encuentran definidos correctamente los procesos de seguridad de la información?				
¿Se ha realizado y documentado una evaluación de riesgo de la información de la dependencia ARC?				

Admisiones Registro y Control			**R/PT: 003**	
CheckList			**C03**	
Dominio			**A7. Gestión de activos**	
Cuestionario				
Pregunta	**SI**	**NO**	**NA**	**Comentarios**
¿Se encuentran completamente identificados y clasificados los activos importantes asociados a cada sistema de información en función de la administración de riesgos potenciales?				
¿Se elaboró un inventario con la información recabada sobre activos importantes? ¿Está actualizado?				
En la clasificación de los activos de información ¿se evalúan las tres (3) características sobre las que se basa la seguridad: confidencialidad, integridad y disponibilidad?				
¿Se realiza periódicamente un mantenimiento preventivo y prueba de los dispositivos de seguridad				

para la prevención, detección y extinción del fuego?				

Admisiones Registro y Control			**R/PT: 004**	
CheckList			**C04**	
Dominio			**A8. Seguridad de los recursos humanos**	
Cuestionario				
Pregunta	**SI**	**NO**	**NA**	**Comentarios**
¿Se llevan a cabo controles de verificación (investigación de antecedentes) del personal en el momento en que se solicita el puesto?				
Quienes se incorporan a la organización ¿firman un acuerdo de confidencialidad o de no divulgación, respecto del tratamiento de la información?				
¿Es retenida por el Área de Recursos Humanos otra área competente, en forma segura la copia del acuerdo de confidencialidad suscripto por el personal, cualquiera sea su situación de revista?				
¿Se comunican en forma detallada al empleado las actividades que van a ser monitoreadas por el acuerdo?				
¿Se planifica la revisión del contenido del acuerdo de confidencialidad o de no divulgación a un plazo inferior a un año?				
¿Se determina la responsabilidad del empleado en materia de seguridad de la información, en los términos y condiciones del empleo?				
¿Se encuentran aclarados en los términos y condiciones de empleo, los derechos y obligaciones del empleado relativos a la seguridad de la información?				
¿Reciben los empleados de la dependencia ARC una adecuada capacitación y actualización periódica en materia de la política, normas y procedimientos?				
¿Se tiene una política de inducción al personal antes de otorgar privilegios de acceso a los sistemas e información que corresponden?				
¿Se tiene un proceso formalizado para la terminación del contrato donde se incluya la devolución de contraseñas e información así como el equipo entregado previamente?				
¿Existe un canal de comunicación formalmente establecido para informar y dar respuesta a incidentes indicando la acción que ha de emprenderse?				

Admisiones Registro y Control			**R/PT: 005**	
CheckList			**C05**	
Dominio			**A9. Seguridad Física y Ambiental**	
Cuestionario				
Pregunta	**SI**	**NO**	**NA**	**Comentarios**
¿Establece la Política, en forma clara y sencilla, sus objetivos y alcances generales?				
¿Incluye mínimamente los tópicos de organización de la seguridad, clasificación y control de activos, seguridad del personal, seguridad física y ambiental, gestión de comunicaciones y las operaciones, control de acceso, desarrollo y mantenimiento de los sistemas, administración de la continuidad de las actividades				

cumplimiento, entre otros?				
Al ser la información un activo para la organización ¿están definidos los recursos de información que deben ser protegidos?				
¿Incluye un esquema de clasificación que preserve los criterios de confidencialidad, integridad, disponibilidad, legalidad y confiabilidad?				
¿La Política de Seguridad de la Información implementada incluye normas y/o procedimientos para garantizar la continuidad de los sistemas de información, minimizando los riesgos de daño y asegurando el eficiente cumplimiento de los objetivos de la dependencia?				
¿Está sustentada la Política por una evaluación de riesgos?				
¿Es la Política concordante con los objetivos de la dependencia ARC?				
¿Contempla la Política las disposiciones legales vigentes?				
¿Define las responsabilidades de las personas, departamentos y organizaciones para los que aplica la política de seguridad?				
¿Define los roles objetivos para cada nivel de responsabilidad?				
¿Existe una adecuada segregación de funciones dentro del área de sistemas?				
¿Define las sanciones en caso de incumplimiento?				
¿Establece el resguardo adecuado de la información documentada?				
¿Establece la existencia de controles de acceso a la información?				
¿Establece la existencia de procedimientos de copias de seguridad de la información?				
¿Se lleva a cabo la asignación de responsabilidades de la seguridad informática?				
¿Resguarda todos los procesos vinculados a la dependencia?				
¿Define la Política sanciones ante casos de incumplimientos?				
¿Cuenta el centro de cómputos con sistemas de control de acceso físico a sus instalaciones?				
¿Cumple el personal del Área de Sistemas con el perfil adecuado para el cargo que desempeña?				

Admisiones Registro y Control			**R/PT: 006**	
CheckList			**C06**	
Dominio			**A10. Gestión de las comunicaciones y operaciones**	
Cuestionario				
Pregunta	**SI**	**NO**	**NA**	**Comentarios**
¿Se controlan los cambios en los sistemas y en los recursos de tratamiento de la información?				
Se gestionan los cambios en la provisión del servicio, procedimientos, controles y se tiene en cuenta la importancia de los sistemas y procesos de la dependencia ARC?				

¿Los cambios propuestos tienen la autorización de los usuarios y/o del propietario de la información?				
¿Pueden los cambios comprometer la integridad de los controles y procedimientos?				
¿Están definidos los procedimientos para el manejo de incidentes de seguridad y para la administración de los medios de almacenamiento?				
¿Se documenta la gestión de incidentes de seguridad en el ambiente de procesamiento y comunicaciones?				
¿Se han desarrollado procedimientos vinculados a la concienciación de los usuarios en materia de seguridad, controles de acceso al sistema y administración de cambios?				
¿Es conocida la política de seguridad de la información para suministradores?				
¿Se cuenta con un tratamiento del riesgo dentro de acuerdos de suministradores?				
¿Se tiene en cuenta una cadena de suministro en tecnologías de la información y Comunicaciones?				
¿Se realiza una supervisión y revisión de los servicios prestados por terceros?				
¿Se realiza una gestión de cambios en los servicios prestados por terceros?				
¿Se documenta y se mantienen los procedimientos de operación y se ponen a disposición de todos los usuarios que lo necesiten?				
¿Se tiene separadas las tareas y las áreas de responsabilidad con el fin de reducir las oportunidades de una modificación no autorizada o no intencionada, o el de un mal uso de los activos de la dependencia ARC?				
¿La organización verifica la implementación de acuerdos con terceros?				
¿Los servicios, informes y registros suministrados por terceros son monitoreados y revisados regularmente?				
¿Se realiza proyecciones de los requisitos de capacidad a futuro para reducir el riesgo de sobrecarga de los sistemas?				
¿Se documenta y se prueba, antes de su aceptación, los requisitos operacionales de los nuevos sistemas?				
¿Se desarrollan las pruebas adecuadas del sistema durante el desarrollo y antes de su aceptación?				
¿Se tiene implementado controles de detección, prevención y recuperación contra el software malicioso, junto a procedimientos adecuados para la concienciación de los usuarios?				
¿Se cuenta con ciertas precauciones para prevenir y detectar la introducción de código malicioso no autorizado?				
¿Los administradores introducen controles y medidas especiales para detectar o evitar la introducción de software malicioso o no autorizado?				
¿Se tiene establecido procedimientos de respaldo para realizar copias de seguridad y probar su puntual recuperación?				
¿Se realiza regularmente copias de seguridad de toda la información almacenada en la dependencia ARC?				
¿Tiene establecido el tipo de almacenamiento, frecuencia de copia y prueba de soportes y lugar de				

respaldo?				
¿Se controla adecuadamente las redes para protegerlas de amenazas?				
¿Se mantiene la seguridad en los sistemas y aplicaciones que utilizan las redes?				
¿Tiene implantado estándares, directrices y procedimientos de seguridad técnicos para redes y herramientas de seguridad de red?				
¿Tiene establecido procedimientos para la gestión de los medios informáticos removibles?				
¿Se protege la documentación de los sistemas contra accesos no autorizados?				
¿Tiene establecido los procedimientos operativos adecuados para proteger los documentos, medios informáticos (discos, cintas, etc.), datos de entrada o salida y documentación del sistema contra la divulgación, modificación, retirada o destrucción?				
¿Se protegen los medios que contienen información contra acceso no autorizado, mal uso o corrupción durante el transporte fuera de los límites físicos de la dependencia?				
¿Tiene establecido los procedimientos y normas para proteger la información y los medios físicos que contienen información en tránsito?				

Admisiones Registro y Control			**R/PT: 007**	
CheckList			**C07**	
Dominio			**A11. Control de acceso**	
Cuestionario				
Pregunta	**SI**	**NO**	**NA**	**Comentarios**
¿Existen políticas, normas y procedimientos para Control de Acceso a los sistemas empleados en la dependencia ARC?				
¿Existen reglas de control de acceso obligatorias? Indicar en comentarios cuál es el criterio.				
¿Se promueve el desarrollo y uso de rutinas del sistema para evitar la necesidad de otorgar privilegios a los usuarios?				
¿Los usuarios dan acuse de recibo de la recepción de la contraseña de carácter provisorio?				
¿Las contraseñas provisorias asignadas cuando los usuarios olvidan su contraseña se suministran sólo una vez identificado el usuario?				
¿Se suspende o bloquea permanentemente al usuario luego de tres (3) intentos de ingresar una contraseña incorrecta, siendo responsabilidad del usuario solicitar su rehabilitación?				
¿Se solicita a los usuarios el cambio de la contraseña cada 30 días?				
¿Se toman los recaudos necesarios a fin de garantizar que los usuarios cambien en su primer ingreso al sistema las contraseñas iniciales que les son asignadas?				
¿Se revisan las autorizaciones de privilegios especiales de derechos de acceso a intervalos no mayores de tres (3) meses?				
A fin de garantizar que no se obtengan privilegios no autorizados ¿se revisan las asignaciones de privilegios de todos los usuarios a intervalos no mayores de seis				

(6) meses?				
¿Garantizan los usuarios que los equipos desatendidos sean protegidos adecuadamente contra accesos no autorizados?				
¿Concluyen los usuarios las sesiones activas al finalizar las tareas o bien se protegen mediante un mecanismo de bloqueo adecuado?				
¿Existen procedimientos para la activación y desactivación del derecho de acceso a redes?				
¿Existen gateways/firewalls en la dependencia ARC, que direccionen los puertos específicos a su correspondiente aplicación y a la vez descarten los paquetes con puertos de destino que no estén específicamente direccionados?				
¿Existen procedimientos que los usuarios deben seguir para solicitar el acceso a Internet en el caso de existir políticas de restricción para su utilización?				
¿Existen dispositivos de hardware o software utilizados para el monitoreo del uso de Internet?				
¿Existe en la dependencia ARC, documentación en la que figuren las pautas de propiedades de seguridad de los servicios de red?				
¿Se limitan los horarios de conexión al horario normal de oficina?				
Sobre las sesiones de usuario ¿se establecieron controles de caducidad, tiempos de espera, etc.?				
¿Se han contemplado los sistemas críticos en las políticas de seguridad?				
¿Se monitorean accesos no autorizados?				
¿Se monitorean todas las operaciones que requieren privilegios especiales?				
¿Se monitorea el inicio y cierre del sistema?				
¿Se monitorea el cambio de fecha/hora?				
¿Se monitorean violaciones de la Política de Accesos y notificaciones para Gateway de red y firewalls?				

Admisiones Registro y Control			**R/PT: 008**	
CheckList			**C08**	
Dominio			**A12. Adquisición, desarrollo y mantenimiento de los sistemas de información**	
Cuestionario				
Pregunta	**SI**	**NO**	**NA**	**Comentarios**
¿Se han planificado, documentado y ejecutado los requerimientos de seguridad de las etapas de Desarrollo, Implementación y Mantenimiento del sistema?				
¿Existen registros de auditoría que controlen la validación de los datos de entrada, salida y procesamiento interno?				
¿Se ha implementado un formulario de solicitud de modificación de programas una hoja de seguimiento de los casos de la modificación?				
¿Se garantiza que la implementación se llevará a cabo minimizando la discontinuidad de las actividades?				

Admisiones Registro y Control			R/PT: 009	
CheckList			**C09**	
Dominio			**A13. Gestión de incidentes en la seguridad de la información**	
Cuestionario				
Pregunta	**SI**	**NO**	**NA**	**Comentarios**
¿Se establecen responsabilidades y procedimientos de manejo de incidentes?				
¿Existen procedimientos para los planes de contingencia normales ante eventuales incidentes?				
¿Se documentan en forma detallada todas las acciones de emergencia adoptadas?				
¿Se notificó de la medida adoptada ante la contingencia a la autoridad y/o organismos pertinentes?				
¿Se contemplan los incidentes relativos a la seguridad ocasionados por fallas operativas?				
¿Se contemplan los incidentes relativos a la seguridad ocasionados por código malicioso?				
¿Se contemplan los incidentes relativos a la seguridad ocasionados por intrusiones?				
¿Se contemplan los incidentes relativos a la seguridad ocasionados por fraude informático?				
¿Se contemplan los incidentes relativos a la seguridad ocasionados por error humano?				
¿Se contemplan los incidentes relativos a la seguridad ocasionados por catástrofes naturales?				
¿Se analizó el incidente y se identificó su causa?				
¿Se planificaron e implementaron las soluciones a efectos de evitar la repetición del incidente?				
¿Se comunican las acciones de emergencia al jefe inmediato? ¿Se revisa su cumplimiento?				

Admisiones Registro y Control			R/PT: 010	
CheckList			**C10**	
Dominio			**A14. Gestión de la continuidad comercial**	
Cuestionario				
Pregunta	**SI**	**NO**	**NA**	**Comentarios**
Existe un Comité de Seguridad de la Información el responsable de la coordinación del desarrollo de los procesos que garanticen la continuidad de la actividad de la dependencia ARC?				
¿Se han definido objetivos organizacionales de las herramientas de procesamiento de información?				
¿Comprenden los integrantes del negocio los riesgos que el mismo enfrenta, en términos de probabilidades de ocurrencia e impacto de las posibles amenazas, así como los efectos que una interrupción puede tener en la actividad del organismo?				
¿Se ha elaborado y documentado una estrategia de				

continuidad de las actividades de la dependencia consecuente con los objetivos y prioridades acordadas?				
¿Se han aprobado planes de continuidad de las actividades de la dependencia de conformidad con la estrategia de continuidad acordada?				
¿Se han coordinado pruebas y actualizaciones periódicas de los planes y procesos implementados?				
¿Se ha considerado la contratación de seguros que podrían formar parte del proceso de continuidad de las actividades de la dependencia ARC?				
¿Se han identificado los eventos (amenazas) que puedan ocasionar interrupciones en los procesos de las actividades como por ejemplo, fallas en el equipamiento, comisión de ilícitos, interrupción del suministro de energía eléctrica, inundación e incendio?				
¿Se han evaluado los riesgos para determinar el impacto de dichas interrupciones, tanto en términos de magnitud de daño como del período de recuperación?				
¿Se identificaron los recursos críticos, los impactos producidos por una interrupción, los tiempos de interrupción aceptables o permitidos, y se especificaron las prioridades de recuperación?				
¿Se han identificado los controles preventivos (sistemas de supresión de fuego, detectores de humo y fuego, contenedores resistentes al calor y a prueba de agua para los medios de backup, los registros no electrónicos vitales, etc)?				
¿Han participado los propietarios de los procesos y recursos de información y el Responsable de Seguridad Informática en el proceso de identificación y evaluación de riesgos?				
¿Se consideraron todos los procesos de las actividades de la dependencia ARC sin Imitarse a las instalaciones de procesamiento de la información?				
Como resultado de la evaluación de riesgos ¿se ha desarrollado un plan estratégico para determinar el enfoque global con el que se abordará la continuidad de las actividades de la dependencia ARC?				
¿El plan estratégico ha sido aprobado por el Comité de Seguridad de la Información?				
Dicho Comité ¿ha elevado el Plan Estratégico a la máxima autoridad de la organización para su aprobación?				
¿Se documentaron los procedimientos y procesos de emergencia acordados?				
¿Se llevó a cabo la capacitación adecuada del personal en materia de procedimientos procesos de emergencia incluyendo el maneo de crisis?				
¿Se desarrolló el proceso de capacitación del personal involucrado en los procedimientos de reanudación y recuperación?				
¿Se trataron mecanismos de coordinación y comunicación entre equipos (personal involucrado)?				
¿Se incluyeron procedimientos de divulgación en el plan de contingencia?				
¿Se contemplaron requisitos en materia de seguridad?				
¿Se adecuaron procesos específicos para el personal involucrado?				
¿Cuenta el personal involucrado con documentación				

específica que indique cuál es su participación en el proceso de contingencia?				
¿Se designó a los responsables de ejecutar cada componente del mismo?				
¿Se encuentran definidos los procedimientos de emergencia que describan las acciones a emprender una vez ocurrido un incidente que ponga en peligro las operaciones de la dependencia ARC y/o la vida humana?				
¿Existen procedimientos de emergencia que describan las acciones a emprender para el traslado de actividades esenciales de la dependencia o de servicios de soporte a ubicaciones transitorias alternativas?				
¿Se redactaron los procedimientos de recuperación que describan las acciones a emprender para restablecer las operaciones normales de la dependencia?				
¿Se definió un cronograma de mantenimiento que especifique cómo y cuándo se probará el plan, y el proceso para el mantenimiento del mismo?				
¿Se realizaron actividades de concientización y capacitación diseñadas para propiciar la comprensión de los procesos de continuidad del negocio y garantizar que los procesos sigan siendo eficaces?				
¿Se realizaron simulaciones (especialmente para entrenar al personal en el desempeño de sus roles de gestión luego de incidentes o crisis)?				
¿Se revisan y actualizan periódicamente los planes de continuidad de las actividades de la dependencia para garantizar su eficacia permanente?				
¿Existe un programa de administración de cambios de la dependencia ARC que incluya procedimientos para garantizar que se aborden adecuadamente los tópicos de continuidad de las actividades?				

Admisiones Registro y Control			**R/PT: 011**	
CheckList			**C11**	
Dominio			**A15. Cumplimiento**	
Cuestionario				
Pregunta	**SI**	**NO**	**NA**	**Comentarios**
¿Incluyen estas normas de procedimiento controles específicos y responsabilidades individuales que garanticen el cumplimiento de los recursos de tecnología informática?				
¿Se verifica que los sistemas de información cumplan con las políticas, normas, y procedimientos de seguridad establecidas?				
¿Se solícita, en caso de ser necesario, la participación de especialistas externos?				
El funcionario a cargo del Área Legal con la asistencia del Responsable de la Seguridad Informática ¿redactaron un Acuerdo de Confidencialidad para ser suscripto por todos los integrantes de la organización?				
¿Existe una figura sobre la cual recae la responsabilidad de hacer cumplir las normas y procedimientos de seguridad?				
¿Se han implementado procedimientos adecuados para garantizar el cumplimiento de las restricciones legales				

al uso del material protegido por las normas de propiedad intelectual?				
¿Utilizan los empleados únicamente material autorizado por la dependencia ARC?				
¿Se respetan las normas que fijan los derechos de propiedad intelectual de los sistemas de información, procedimientos, documenta?				

Encuesta **AC7**

Encuesta dirigida al personal de la Oficina de Admisiones Registro y control (ARC) de la Universidad Francisco de Paula Santander Ocaña (UFPSO)

Objetivo: Esta encuesta tiene como objetivo recopilar información que nos permita realizar un análisis sobre la gestión de la información tanto física como digital que se realiza desde la oficina de ARC de la UFPSO. La información que usted nos suministre será muy importante para la investigación y será utilizada con toda reserva por los investigadores.

Esta encuesta está compuesta en su mayoría por preguntas cerradas con varias opciones de respuesta, por favor marque con una X la respuesta que considere apropiada según su criterio.

1. ¿Existen una política de seguridad de la información?

   SI____ NO _____ NS/NC_____

2. ¿Conoce, entiende y aplica la política de seguridad de la información en el desarrollo de sus funciones?

   SI____NO _____ NS/NC_____

3. ¿Recibe capacitaciones sobre la gestión segura de la información?

   Nunca____ casi nunca_____ a menudo_____ muy a menudo_____

4. ¿Entiende con claridad la importancia de conservar la integridad de la información que se gestiona desde la dependencia?

   SI____NO _____ NS/NC_____

5. ¿Existen restricciones de acceso a la información para el personal que labora en la dependencia?

   SI _____ NO, todos tienen acceso a toda la información_____

6. ¿Firmó un acuerdo de confiabilidad o de no divulgación respecto al tratamiento de la información que se maneja en la dependencia?

SI____NO _____ NS/NC_____

7. ¿Conoce los procesos discipulares a los que se acoge un funcionario en caso de divulgar la información confidencial sin autorización?

   SI____NO _____ NS/NC_____

8. ¿La información física que se almacena en la oficina, se encuentra protegida de factores externos como la humedad?

   SI____NO _____ NS/NC_____

9. ¿Existen copias de respaldo de la información física?

   SI____NO _____ NS/NC_____

10. Si la respuesta anterior es si, ¿En qué lugar se almacena dichas copias?

    En la misma oficina _____ En un lugar externo de la Oficina _____

11. ¿Existen copias de respaldo de la información digital?

    SI____NO _____ NS/NC_____

12. ¿Existen restricciones para entregar información a terceros cuando la solicitan, por ejemplo cuando se solicita una constancia de terminación de materias o cualquier otro documento de los que se emitan desde la dependencia?

    SI____NO _____ NS/NC_____

13. ¿Conoce de la existencia de un Plan de contingencia de riesgos?

    SI____NO _____ Sé que existe pero no lo conozco _____

14. ¿Sabe cómo actuar en caso de presentarse un incidente natural para proteger tanto su integridad personal, como la de la información almacenada en la dependencia?

    SI____NO _____ NS/NC_____

15. ¿Se tienen implementados controles de detección, prevención y recuperación contra el software malicioso, junto a procedimientos adecuados para la concienciación de los usuarios?

    SI____ NO_____ NS/NC_____

16. ¿Implementa parámetros de contraseñas seguras?

    SI____ NO_____ No utilizo un equipo de cómputo en el desempeño

de mis funciones _____

17. ¿Realizan mantenimiento preventivo y correctivo a los equipos de cómputo?

    SI____ NO_____ NS/NC_____

18. Si la respuesta anterior es si, ¿Con que frecuencia se realizan?

    Casi nunca_____ a menudo_____ muy a menudo_____

19. ¿Se verifica la integridad de la información física que se almacena en la dependencia?

    Nunca____ casi nunca_____ a menudo_____ muy a menudo_____

20. ¿Se toman medidas preventivas para evitar que la información física se deteriore?

    SI____ NO_____ NS/NC_____

21. ¿Existen restricciones de acceso de personal no autorizado a la dependencia?

    SI____ NO_____ NS/NC_____

22. ¿Considera que la ubicación de la dependencia dentro del campus es idónea?

    SI____NO_____ NS/NC_____

23. ¿Considera que la amplitud de la oficina es la adecuada para almacenar toda la información física?

    SI____NO_____ NS/NC_____

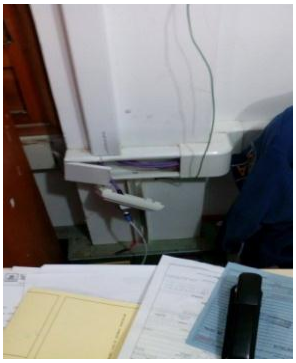
Hallazgos AC8

AC8_01

NOMBRE EMPRESA AUDITADA: Universidad Francisco de Paula Santander Ocaña
ÁREA AUDITADA: Dependencia Admisiones, Registro y Control

FECHA INICIO: 27 de Marzo de 2015
FECHA FINALIZACIÓN: 29 de Mayo de 2015

Cédula N° 1 Elaborado por: CS y NT
HALLAZGO:
El cableado eléctrico y el cableado estructurado se encuentran en la misma canaleta.



Recomendaciones:
Separar el cableado eléctrico del cableado estructural usando canaletas independientes.

AC8_02

NOMBRE EMPRESA AUDITADA: Universidad Francisco de Paula Santander Ocaña
ÁREA AUDITADA: Dependencia Admisiones, Registro y Control

FECHA INICIO: 27 de Marzo de 2015
FECHA FINALIZACIÓN: 29 de Mayo de 2015

Cédula N° 2 Elaborado por: CS y NT
HALLAZGO:
Se evidencia que en ciertos lugares de la oficina de ARC el cableado se encuentra por fuera de la canaleta.

Recomendaciones:
Procurar que todo el cableado este dentro de la canaleta respectiva, disminuyendo así el riesgo de accidente.

AC8_03

NOMBRE EMPRESA AUDITADA: Universidad Francisco de Paula Santander Ocaña
ÁREA AUDITADA: Dependencia Admisiones, Registro y Control

FECHA INICIO: 27 de Marzo de 2015
FECHA FINALIZACIÓN: 29 de Mayo de 2015

Cédula N° 3 Elaborado por CS y NT
HALLAZGO:
El acceso a las áreas de trabajo no proporciona seguridad ni reserva de los equipos y la información.

Recomendaciones:
Instalación de elementos de delimitación de áreas físicas que garanticen un acceso controlado y confiable ante el personal no autorizado.

AC8_04

NOMBRE EMPRESA AUDITADA: Universidad Francisco de Paula Santander Ocaña
ÁREA AUDITADA: Dependencia Admisiones, Registro y Control

FECHA INICIO: 27 de Marzo de 2015
FECHA FINALIZACIÓN: 29 de Mayo de 2015

Cédula N° 4 Elaborado por JR y CG

HALLAZGO:
La puerta de acceso a la oficina de ARC permanece abierta la mayoría del tiempo, evitando así que la refrigeración de los equipos se cumpla adecuadamente; de igual forma es una puerta que no brinda seguridad a la información y equipos que se encuentran en la dependencia, pues es fácil de violenta.

Recomendaciones:
Procurar que se cumpla con la política de mantener un espacio cerrado para que los equipos se mantengan ventilados y funcionen adecuadamente. Por otra parte se sugiere instalar una puerta que proporcione mayor seguridad.

Pruebas **AC9**

AC9_01

PRUEBA N° 1

Empresa auditada: Universidad Francisco de Paula Santander Ocaña
Área auditada: Dependencia Admisiones, Registro y Control.
Fecha de inicio: 19 de mayo de 2015
Fecha finalización: 21 de mayo de 2015
Cedula : N° 5
Elaborado por: CS y NT

Objetivo:	Verificar si el software instalado en los equipos de cómputo tiene instaladas las actualizaciones y contaban con las últimas versiones de dicho software.
Procedimiento:	1. Se ingresó a los equipos de cómputo, se revisó las actualizaciones del sistema operativo, suit de seguridad, y programas usados.
Hallazgos:	En cuanto a los sistemas operativos usados, se encontró que hay versiones de Windows obsoletas. Usan versiones Windows XP, sistema que ya no cuenta con soporte de seguridad por parte de Microsoft. Además, la última actualización instalada en los equipos con Windows 7 es de varios meses atrás. En cuanto a las suit de seguridad, están usando una versión mínima, la versión 'free' de una suit. Lo navegadores usados no son la última versión.
Situación de riesgo:	El usar una versión de sistema operativo que no está soportado por la empresa que lo crea, genera un alto riesgo, ya que no se están creando soluciones a las fallas de seguridad que se van generando. Lo anterior, sumado con las versiones con soporte por parte de Microsoft como Windows 7 pero a los cuales no se les han instalado las últimas actualizaciones de seguridad emitas por dicha empresa están creando serios problemas de seguridad. Dichas fallas no solucionadas pueden ser usadas por

	los ciberdelincuentes para que, con ataques dirigidos o a través de malware que se puede distribuir a través de internet, o por medios físicos puedan robar información o causar daños que comprometan las características de la información como la integridad, confidencialidad y la disponibilidad, y también, causar problemas para la continuidad del negocio. La usar una suit de seguridad no tan robusta, genera que no se establezcan los niveles más óptimos de seguridad, haciendo que dichas medidas no sean las más adecuadas para contrarrestar los posibles incidentes de seguridad.
Recomendaciones:	• Se recomienda adquirir las versiones recientes de los sistemas operativos de Microsoft, Windows 7 o posteriores. • Adquirir una suit de seguridad más robusta, que permita contrarrestar la mayor variedad de amenazas. • Establecer periodos para instalar las actualizaciones del sistema operativo, paquete de ofimática, navegadores y demás software utilizado en los equipos de cómputo.
Nomenclatura:	CS: Carlos Sánchez NT: Natalia Torrado

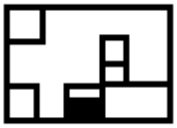
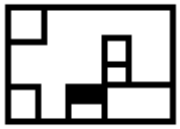
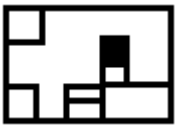
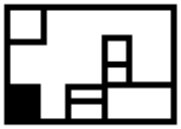
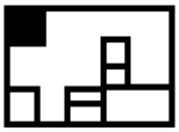
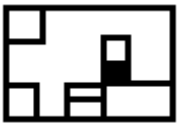
AC9_02

PRUEBA N° 2

Empresa auditada: Universidad Francisco de Paula Santander Ocaña
Área auditada: Dependencia Admisiones, Registro y Control.
Fecha de inicio: 19 de mayo de 2015
Fecha finalización: 21 de mayo de 2015
Cedula N°: 5
Elaborado por: CC y NT

Objetivo:	Verificar que los equipos de cómputo para verificar si cuentan con protección por contraseña para evitar el ingreso y uso por personas no autorizadas de dichos equipos. Y verificar todos los equipos usan una contraseñas son diferentes para el ingreso al mismo.
Procedimiento:	1. Se apagaron los equipos de cómputo. 2. Al reiniciar se observó si se habían establecido contraseña en la Bios, o en el sistema operativo. 3. Se revisa las contraseñas establecidas en los equipos.
Hallazgos:	Se observó que los equipos no están protegidos por ningún tipo de contraseña, ni en la bios ni en el sistema operativo.
Situación de riesgo:	Al no establecer protección para el ingreso a los equipos de cómputo no se está cumpliendo con la confidencialidad de la información. Cualquier persona ajena a la dependencia, o no autorizada para el ingreso puede acceder al computador y a la información almacenada en él; pudiéndola robar, manipular o destruir.
Recomendaciones:	• Se recomienda establecer contraseña en uno o ambos niveles de seguridad (Bios, sistema operativo) para el ingreso a los equipos de cómputo. • Cada equipo debe tener una contraseña con nivel de seguridad alta y diferente para cada equipo.
Nomenclatura:	JR: Johan Rueda CG: Carlos Gómez

Resumen de la prueba realizada

Equipo	SO	Office	Última actualización	Antivirus	Contraseña
 **E1**	OK	2013 OK	17-02-15	AVAST FREE	NO
 **E2**	OK	2013 OK	9-08-15 g.Chrome 27-8-13 Mozzilla 26-02-12	ESET	NO
 **E3**	WXP SP2	2003 10-12-10	Google 16-10-12 Mozzilla 21-05-15	NO	NO
 **E4**	WXP SP3	2003 11-9-13	Google 11-09-13 Mozzilla 14-05-15	Eset	NO
 **E5**	W7 sp1	2013 ok	9-07-2014 Google 23-10-14 Adobe 21-05-15	Eset	NO
 **E6**	W7 SP1	2013 OK	9-07-2014 Google 23-10-14 Adobe 21-05-15	ESET	NO
 **E7**	WXP SP2	2003 10-02-2010	Google 21-05-15 Adobe 21-05-15	NO	NO