

PLAN DE CONTINUIDAD DE TI



**Universidad Francisco
de Paula Santander**

Ocaña - Colombia
Vigilada Mineducación

www.ufpso.edu.co

PLAN DE CONTINUIDAD DE TI

División de Sistemas

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
2025



Vía Acolsure, Sede el Algodonal, Ocaña, Colombia - Código postal: 546552
atencionalciudadano@ufpso.edu.co - www.ufpso.edu.co
Línea de atención: 311 436 1717

CONTENIDO

GLOSARIO	5
INTRODUCCIÓN	6
OBJETIVO GENERAL	7
1. MARCO CONCEPTUAL	8
1.1 IMPORTANCIA E IMPACTO DEL PLAN DE CONTINUIDAD DE SERVICIOS DE TI	8
1.2 BENEFICIOS	8
1.3 FASES DEL PLAN DE CONTINUIDAD DE SERVICIOS DE TI	9
2. PLAN DE CONTINUIDAD DE SERVICIOS DE TI	11
2.1 ESTRUCTURA TECNOLÓGICA.....	11
2.1.1 Sistema de Información Académico - SIA	11
2.1.2 PP Sistema de Información Académico - SIAPP - (Android - IOS)	13
2.1.3 Sistema de Información de Admisiones, Registro y Control.....	13
2.1.4 Sistema de Gestión Académica	14
2.1.5 Sistema de Información de Bienestar Universitario - SIBU	15
2.1.6 Centro de Idiomas - SIA.....	16
2.1.7 Sistema de Información Académico de Bellas Artes - SIABE	17
2.1.8 Sistema de Información de Pasantías.....	18
2.1.9 Sistema de Información Académica Egresados.....	19
2.1.10 Sistema de Información de Bibliográfico - SIB	19
2.1.11 Repositorio Digital (DSPACE).....	20
2.1.12 Sistema de Información Financiero - SIF	21
2.1.13 Sistema de Facturación Electrónica	22
2.1.14 Sistema de Información Documental - SID	23
2.1.15 Sistema de Peticiones, Quejas, Reclamos, Sugerencias, Felicitaciones y Denuncias - PQRS.....	24
2.1.16 Sistema de Información de Revisión y Control - SICI	25
2.1.17 Sistema de Información de Autoevaluación y Acreditación - SIAC	26
2.1.18 Sistema de Información de Gestión Humana – SGH	27
2.1.19 Sistema de Información de Solicitudes y Requerimientos de División de Sistemas	28
2.1.20 Sistema de Información de Solicitudes y Requerimientos de Planeación ...	29
2.1.21 Sistema de Información de Solicitudes y Requerimientos de Bienestar	30
2.1.22 Sistema de Información de Solicitudes y Requerimientos de Multimedios ..	31
2.1.23 La UFM	32
2.1.24 Portal de Encuestas	33
2.1.25 Portal Estadísticas – Datos Abiertos	34
2.1.26 Sistema de Respaldo de Información ownCloud.....	35
2.1.27 Sistema de Notificaciones y Publicaciones	36
2.1.28 Unidad de Educación Virtual	37
3. TELECOMUNICACIONES	39
3.1 Red Inalámbrica.....	43
3.2 Telefonía.....	45



4.	TECNOLOGÍA.....	46
4.1	Equipos Tecnológicos.....	46
4.2	Salas de Cómputo	46
4.3	Infraestructura de video vigilancia por IP.....	48
4.4	Trabajo colaborativo	49
4.5	Chatbot.....	¡Error! Marcador no definido.
4.6	Chat Institucional	49
4.7	Correo Electrónico	49
4.8	Seguridad	50
5.	LÍMITE Y ALCANCE DEL PLAN DE CONTINUIDAD	51
6.	FASE I. ANÁLISIS DEL NEGOCIO Y EVALUACIÓN DE RIESGOS	52
7.	FASE II. ESTRATEGIAS DE RESPALDO	63
8.	FASE III. DESARROLLO DEL PLAN	67
9.	FASE IV. PRUEBAS Y MANTENIMIENTO	71



GLOSARIO

Análisis de impacto: (BIA - Business Impact Assessment) el propósito del BIA es crear un documento que ayude a entender el impacto que un desastre pueda tener sobre un negocio en particular.

Análisis de riesgos: (RA - Risk Assessment) metodología orientada a determinar la vulnerabilidad de la empresa. Con base en los diversos riesgos encontrados, se les asigna un valor específico, según la probabilidad de ocurrencia y de la cobertura del seguro contratado, con el fin de proponer alternativas para reducir el riesgo.

Backup: Aplicación de copia de seguridad de ficheros, carpetas o unidades completas que permite dividir la información y exportarla a una unidad externa, los backup se realizan bajo demanda del interesado.

Base de datos: Es un sistema de almacenamiento colectivo de las bibliotecas de datos que son requeridas y organizadas para cubrir sus requisitos de procesos y recuperación de información.

Firewall: Conjunto de programas de protección y dispositivos especiales que ponen barreras al acceso exterior a una determinada red privada. Es utilizado para proteger los recursos de una organización de consultas externas no autorizadas.



INTRODUCCIÓN

El proceso de Sistemas de Información, Telecomunicaciones y Tecnología de la UFPS Ocaña tiene dentro de sus funciones la Gestión de la Seguridad de la Información en la institución, reconociendo la información como su activo más importante, por esta razón es fundamental adoptar medidas y planes que mitiguen el impacto ante cualquier incidente o riesgo ya sea este provocado por un desastre natural como un terremoto o inundación, o también por aquellos riesgos que son generados por el hombre, ataques cibernéticos, bombas, interrupción del fluido eléctrico o un robo que han de considerarse amenazas reales que deben ser tratadas de forma preventiva para evitar, en caso de que éstas sucedan, que las pérdidas sean tan graves que afecten a la prestación del servicio.

Aparte de prevenir o minimizar las pérdidas para la institución que un desastre puede causar, el objetivo principal de cualquier programa orientado a gestionar la continuidad de TI de una organización es garantizar que ésta dispone de una respuesta planificada ante cualquier trastorno importante que puede poner en peligro su supervivencia. De este modo, es necesario establecer una serie de medidas técnicas, organizativas y procedimentales que garanticen la continuidad de las actividades o procesos de TI en caso de tener que afrontar una contingencia grave.



OBJETIVO GENERAL

Fortalecer la capacidad de respuesta de la Universidad Franciscos de Paula Santander Ocaña, ante eventos catastróficos, mediante la creación y mejora continua del Plan de Continuidad que garantice el restablecimiento de la operación y de los servicios críticos de la Institución.



1. MARCO CONCEPTUAL

1.1 IMPORTANCIA E IMPACTO DEL PLAN DE CONTINUIDAD DE SERVICIOS DE TI

Actualmente las TIC están contribuyendo, significativamente, a expandir los horizontes tanto de personas como de empresas e instituciones, así como, de tener alcance a nivel mundial con recursos relativamente bajos y velocidad elevada. Por esta razón, las tecnologías de la información están tomando auge día a día. En ese sentido, las organizaciones hacen sus procesos dependientes de las TIC, por ello ha surgido la necesidad de contar con políticas que garanticen el resguardo de estos sistemas para brindar, realmente, solución a los incidentes que puedan suceder de manera efectiva, rápida y segura. Lo anterior fundamenta la necesidad de contar con un plan de continuidad de servicios de TI en la institución.

El implementar un Plan de Continuidad de Servicios de TI en la Institución tiene un impacto positivo pues permite amortiguar y minimizar los efectos de la contingencia críticos, operativos y financieros, reduciendo el tiempo en la recuperación de la información, restaurando los procesos operacionales clave de sus recursos y servicios de TI, ocasionadas por fallas, desastres naturales, siniestros, entre otros.

1.2 BENEFICIOS

Los beneficios de implementar un plan de este tipo se describen a continuación de acuerdo a Gaspar Martínez, *El plan de continuidad de negocios*, 2006:

- Proteger la marca y la lealtad de los clientes proactivamente evitando o atenuando los desastres.
- Conlleva tener identificados los diversos eventos que podrían impactar sobre la continuidad de las operaciones y su impacto financiero, humano y de reputación sobre la organización.
- Disminuye o previene las pérdidas en cuanto a tiempo, recursos y credibilidad para el negocio en caso de desastre.
- Tener una recuperación oportuna y eficaz de interrupciones del negocio.
- Clasifica y categoriza los activos para priorizar su protección en caso de desastre.
- Mejorar la capacidad de sobrevivir y de prosperar en el actual clima de negocio competitivo.



- Fomenta e implica a los recursos humanos de la compañía en las actividades de continuidad, logrando un clima colaborativo y de cooperación.
- Mejorar la eficacia y productividad del personal automatizando y simplificando procesos de recuperación.

1.3 FASES DEL PLAN DE CONTINUIDAD DE SERVICIOS DE TI

Fase I. Análisis del negocio y evaluación de riesgos.

El objetivo de esta fase es adquirir información sobre los objetivos de la organización, del funcionamiento que permiten el cumplimiento de la misión institucional y de los procesos que se consideran críticos.

Con base en la información obtenida, se procede a realizar un análisis de los riesgos asociados a los procesos identificados y se determina cuáles son las causas potenciales que pueden llegar a interrumpir el funcionamiento de la empresa o institución.

Fase II. Estrategias de respaldo.

En esta fase se seleccionan las estrategias y se basa en dos aspectos fundamentales:

- La valoración de las diferentes alternativas y estrategias de respaldo existentes en función a los resultados obtenidos en la fase de análisis y evaluación de riesgos (fase I), con base en la información se determina y selecciona la estrategia más adecuada a las necesidades de la organización.
- Corregir las vulnerabilidades detectadas en la fase de análisis y evaluación de riesgos (fase I), de esta manera se logra disminuir la probabilidad que ocurran desastres.

Fase III. Desarrollo del plan.

En esta fase se desarrolla el plan, el cual involucra el tratamiento de los procedimientos y planes de actuación para las diferentes áreas y equipos creados, además, se organizan los equipos que intervendrán en cada una de las fases del plan.

Se deben establecer los siguientes parámetros para cada proceso crítico:

- **RTO (Recovery Time Objective):** Tiempo máximo tolerable para la interrupción.
- **RPO (Recovery Point Objective):** Cantidad máxima de datos que se pueden perder sin causar un daño significativo.



Estos objetivos guiarán la estrategia de recuperación y las inversiones en infraestructura.

•

Fase IV. Pruebas y mantenimiento.

En esta etapa del plan es importante ponerlo a prueba bajo diferentes contextos para verificar que realmente funciona y es efectivo para la organización.

Es recomendable llevar a cabo las pruebas lo más realista posible, es decir, trasladar el contenido del documento a procedimientos prácticos.

Debido a que con el tiempo las empresas e instituciones cambian de políticas de administración como de procedimientos, es de carácter obligatorio el contar con un plan de mantenimiento con el objetivo de mantener actualizado el plan de continuidad, para que este siempre responda a las necesidades de la institución.

El análisis del negocio y la evaluación de riesgos deben integrarse en la UFPSO, asegurando que:

- Los procesos críticos estén identificados y priorizados.
- Existan estrategias claras para la recuperación de cada proceso.
- Se cuente con recursos y capacidades adecuadas para implementar las estrategias de recuperación.
- Se realicen pruebas periódicas del plan para asegurar su efectividad.

Este enfoque garantizará que la UFPSO pueda mantener sus operaciones esenciales en caso de interrupciones y continuar brindando servicios educativos de calidad.



2. PLAN DE CONTINUIDAD DE SERVICIOS DE TI

2.1 ESTRUCTURA TECNOLÓGICA

La Universidad Francisco de Paula Santander Ocaña cuenta con varios Sistemas de Información los cuales permiten de una manera óptima manejar la información, logrando así, un mejor aprovechamiento del recurso humano y físico de la institución.

De esta manera la UFPSO está encaminada a brindar los mejores servicios a la comunidad universitaria, decide implementar una serie de proyectos que se iniciaron en el año 2001 y que inició con el Sistema de Información Académico SIA, para continuar con el Sistema de Información Bibliográfico SIB, luego el Sistema de Información Financiero SIF y así progresivamente a medida que surgían las necesidades se fueron desarrollando los sistemas de información con los que cuenta hasta el día de hoy la Universidad Francisco de Paula Santander Ocaña.

Los Sistemas de Información están desarrollados con el sistema manejador de base de datos relacional “RDBMS ORACLE 10G BAJO LINUX” el cual permitió diseñar un eficiente modelo relacional que garantiza la integridad y seguridad de la información, permitiendo la definición de diferentes políticas para su administración.

2.1.1 SISTEMA DE INFORMACIÓN ACADÉMICO - SIA

El Sistema de Información Académico (SIA) es una aplicación elaborada para facilitar la administración, de los diferentes procesos académicos que se llevan a cabo en la Universidad. El sistema cuenta con cuatro (4) módulos en cuales se cubren las funciones de consulta y gestión a través de las cuales el usuario puede llevar a cabo varias actividades sobre información personal, financiera y académica, según su rol: Estudiante, Docente, Jefe Plan de Estudios, Secretaria, Administrador.

Módulos del Sistema de Información Académico - SIA

- Datos personales
- Digitación de calificaciones
- Constancias y certificados
- Inclusiones y/o cancelación de asignaturas
- Solicitudes de becas trabajo y/o monitorias
- Solicitud de financiación de la matrícula
- Solicitud de vacacionales
- Trámites académicos
- Trámites para modalidades de graduación
- Matrícula actual
- Registro y control de hora cátedra
- Peticiones, quejas y reclamos
- Evaluación docente



- Inscripción en línea de aspirantes
- Cancelación de materia
- Derecho a grado
- Acceso a las bibliotecas digitales
- Consulta de notas
- Consulta liquidación
- Consulta de deudas
- Consulta de información académica
- Acceso a horarios
- Menú Alumno, Carrera, Materia, Profesor, Vacacional, Reportes
- Menú Consulta, Reportes, Grados, Alumno, Estado, Consulta de notas

<https://siaweb.ufpso.edu.co/>

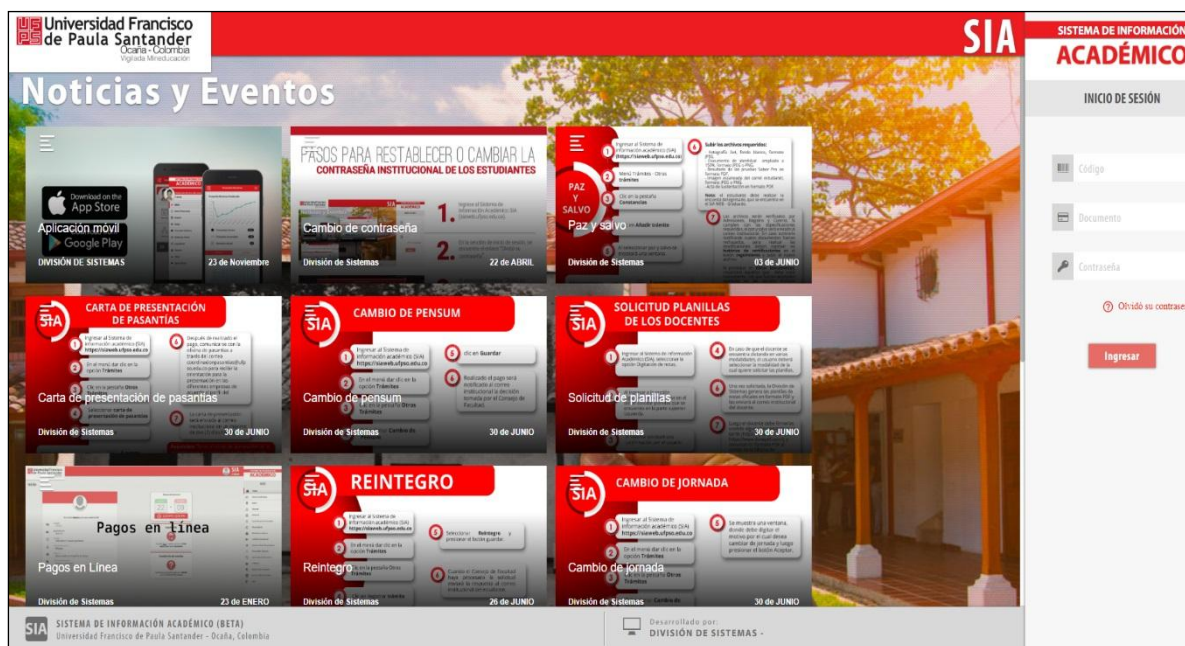


Figura 1: Sistema de información académica
Fuente: División de sistemas - UFPSO.

2.1.2 PP Sistema de Información Académico - SIAPP - (Android - IOS)

El sistema de información académico ofrece todos los datos correspondientes al estudiante de la Universidad, enfocado hacia los dispositivos móviles brindando una facilidad en el uso de la información académica.

Módulos de la APP Sistema de Información de Información Académico - SIAPP

- Consulta de los datos personales
- Consulta de horario (actual y por carrera)
- Consulta de notas (Actual y acumulada)
- Consulta de pensum
- Promedio (Histórico, actual y ponderado)
- Consulta matrícula
- Otros (YouTube, U tv, Noticias y Radio UFM)
- Consulta de liquidación

2.1.3 Sistema de Información de Admisiones, Registro y Control

Sistema de información para la admisión, el registro y control de la gestión académica de los aspirantes, estudiantes y egresados de la Universidad cuenta con los siguientes módulos:

Módulos del Sistema de Información de Admisiones, Registro y Control

- **Parametrización:** este módulo permite configurar las fechas de los procesos llevados a cabo por la oficina de admisiones y asignar la distribución de cupos para cada semestre académico.
- **Aspirantes:** este módulo permite realizar toda la gestión de los procesos de preinscripción, inscripción y admisión de los aspirantes.
- **Estudiantes:** este módulo lleva a cabo el proceso de generación de código, gestión de constancias, certificados, generación de paz y salvo y gestiona la información básica de los estudiantes.
- **Graduados:** este módulo gestiona la información de los egresados y lleva a cabo el proceso de graduar los estudiantes y generación de constancias y certificados.
- **Sistema:** este módulo permite gestionar el acceso y los permisos de los usuarios al sistema de información.

<https://admisiones.ufpso.edu.co/>



Vía Acolsure, Sede el Algodonal, Ocaña, Colombia - Código postal: 546552
atencionalciudadano@ufpso.edu.co - www.ufpso.edu.co
Línea de atención: 311 436 1717

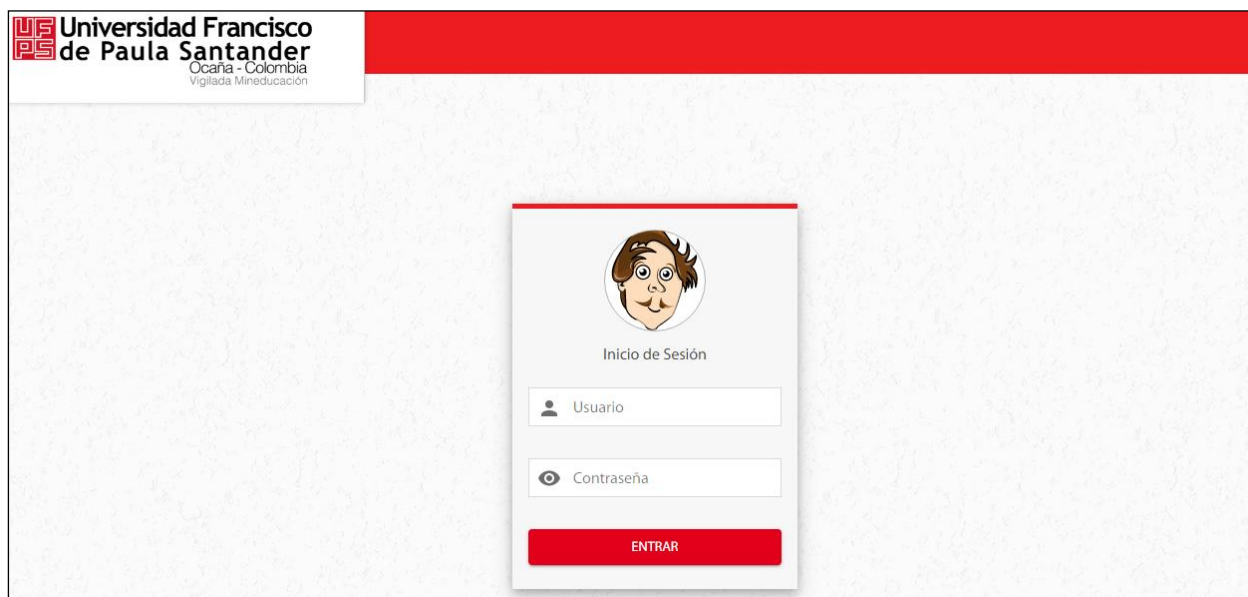


Figura 1: Sistema de información admisiones registro y control
Fuente: División de sistemas – UFPSO

2.1.4 Sistema de Gestión Académica

El sistema administra todo lo relacionada con la institución de carácter académico, como información de estudiantes, docentes, exalumnos, horarios, pensum, etc. Facilitando el acceso a la información y generación de reportes, haciendo distinción entre los usuarios del sistema como secretarias, jefes de plan de estudios, departamentos entre otros, para dar una búsqueda más rápida y eficaz de los procesos que les corresponden a los mismos.

<https://gestionacademica.ufpso.edu.co/>



Figura3: Sistema de información gestión académica

Fuente: División de sistemas – UFPSO

2.1.5 Sistema de Información de Bienestar Universitario - SIBU

El Sistema de Información de Bienestar Universitario (SIBU) es un sistema de información orientado a la web, con el fin de almacenar información de acuerdo a la actividad que se esté ejecutando por parte del profesional idóneo contratado. Corresponde al área de salud, cultura y deportes.

Módulos del Sistema de Información Bienestar Universitario - SIBU

- Módulo Administrador
- Módulo de Enfermería
- Módulo de Odontología
- Módulo de Psicología
- Módulo de Medicina General
- Módulo de Trabajo Social
- Módulo de Asesoría Espiritual
- Módulo de Deportes
- Módulo de Cultura
- Módulo de Egresados

<https://portalbienestar.ufpso.edu.co/index.php>



Vía Acolsure, Sede el Algodonal, Ocaña, Colombia - Código postal: 546552
atencionalciudadano@ufpso.edu.co - www.ufpso.edu.co
Línea de atención: 311 436 1717

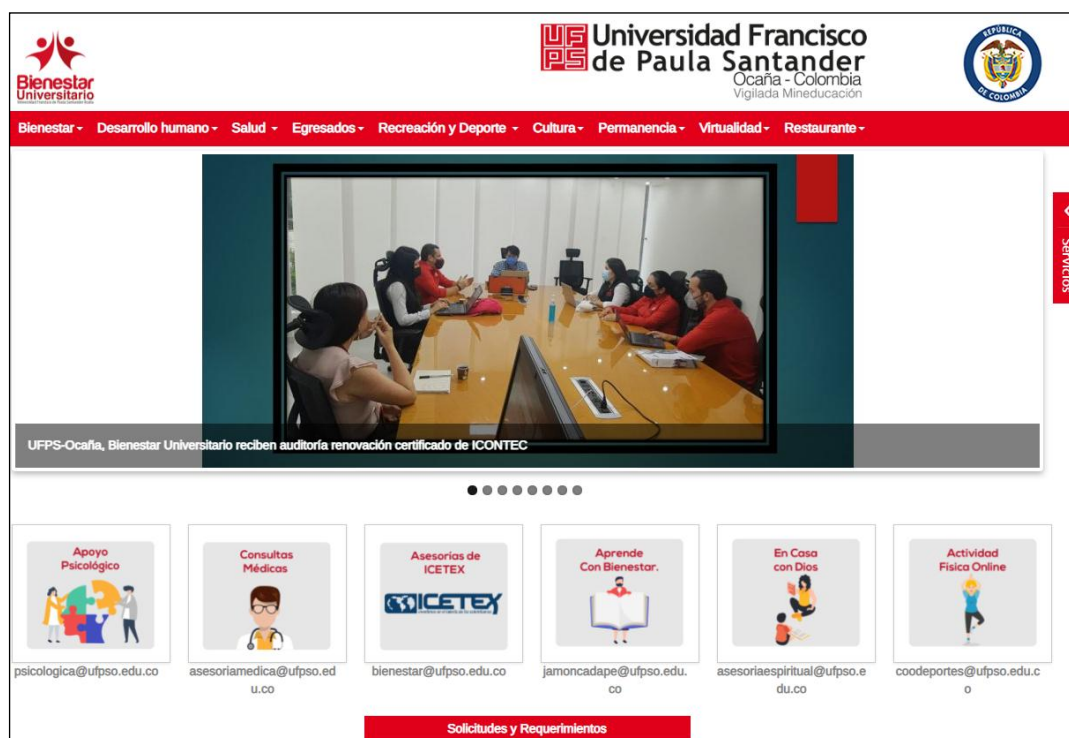


Figura 4: Sistema de información bienestar universitario
Fuente: División de sistemas – UFPSO

2.1.6 Centro de Idiomas - SIA

El Sistema de Información de Inglés (SIA Centro de idiomas) es una aplicación elaborada para facilitar la administración de la información académica de los usuarios que realizan cursos en el centro de idiomas de la Universidad.

Módulos del Centro de Idiomas - SIA

- Inscripción y Matricula
- Gestión de cursos (Fechas, Grupos, Horarios)
- Cátedra (Registro de horas, Listado de estudiantes, Ingreso de notas)
- Gestión de inscripciones y matricula (Cambios de grupos, de horarios)

<https://centrodeidiomas.ufpso.edu.co/>



Vía Acolsure, Sede el Algodonal, Ocaña, Colombia - Código postal: 546552
atencionalciudadano@ufpso.edu.co - www.ufpso.edu.co
Línea de atención: 311 436 1717



Figura 5: Sistema de información centro de idiomas

Fuente: División de sistemas – UFPSO

2.1.7 Sistema de Información Académico de Bellas Artes - SIABE

El Sistema de Información Académico de la Escuela de Bellas Artes (SIABE) de la Universidad Francisco de Paula Santander Ocaña, es una aplicación web que consta de cinco módulos y tiene como finalidad dar soporte a los procesos académicos de la Escuela de Bellas Artes beneficiando a toda la comunidad en especial a estudiantes, docentes y administradores, quienes podrán consultar toda su información académica en cualquier momento y desde cualquier lugar de forma rápida y segura.

Módulos del Sistema de Información Académico de Bellas Artes - SIABE

- Módulo Administrador - Matrícula por parte del administrador del portal
- Módulo Coordinador (Gestión de alumnos, matriculas, deudores)
- Módulo Usuario (Gestión de alumnos, matriculas, deudores)
- Módulo Docente (Registro de hora cátedra, digitación de notas)
- Módulo Estudiante (Datos personales, notas, evaluación docente, liquidación, financiación, horarios, deudas)

<https://artes.ufpso.edu.co/>



Vía Acolsure, Sede el Algodonal, Ocaña, Colombia - Código postal: 546552
atencionalciudadano@ufpso.edu.co - www.ufpso.edu.co
Línea de atención: 311 436 1717



UFPS Universidad Francisco
de Paula Santander
Ocaña - Colombia
Vigilada Mineducación

SIA
Escuela de Bellas Artes

Ayuda de Ingreso al Sistema

Usuario: Es el Código de usuario dado por el sistema de Información Financiero (SIF).

Contraseña: Es una cadena mínimo de 6 caracteres para los usuarios proporcionada por el Sistema de Información.

Inicio de Sesión

Código:

Contraseña:

Universidad Francisco de Paula Santander Ocaña - Colombia | Sede la granja - Vía al Algodonal
PBX: 5690088 Línea Gratuita: 01-8000-121022
E-mail: webmaster@ufpso.edu.co - info@ufpso.edu.co | © 2012 -2013
www.ufpso.edu.co

Figura 6: Sistema de información académico de bellas artes
Fuente: División de sistemas - UFPSO.

2.1.8 Sistema de Información de Pasantías

Este sistema controla el proceso de los estudiantes que van a realizar pasantías, desde la solicitud hasta la evaluación del coordinador de la pasantía, permitiendo hacer un seguimiento a las solicitudes, aprobaciones, documentos entregados, planes de trabajo y visitas, a su vez, permite generar reportes de los estudiantes y empresas involucrados en dicho proceso.

<https://sipa.ufpso.edu.co/>

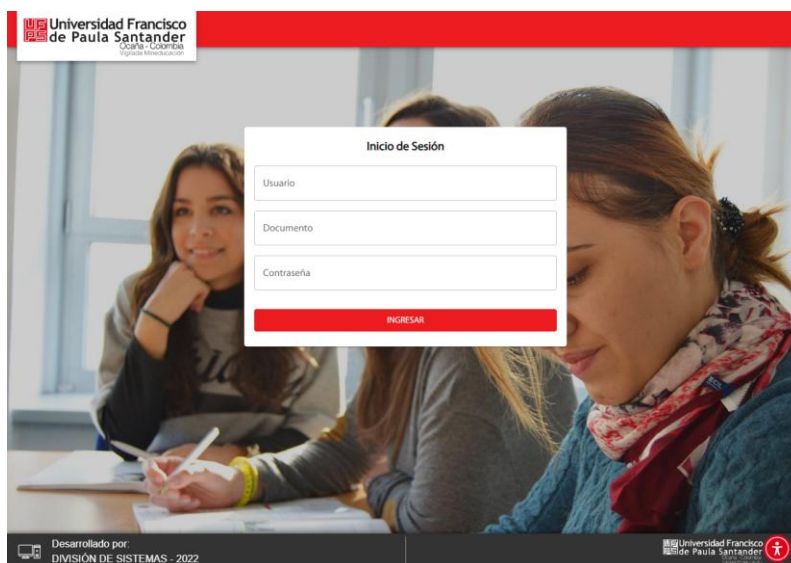


Figura7: Sistema de información de pasantías
Fuente: División de sistemas - UFPSO.

2.1.9 Sistema de Información Académica Egresados

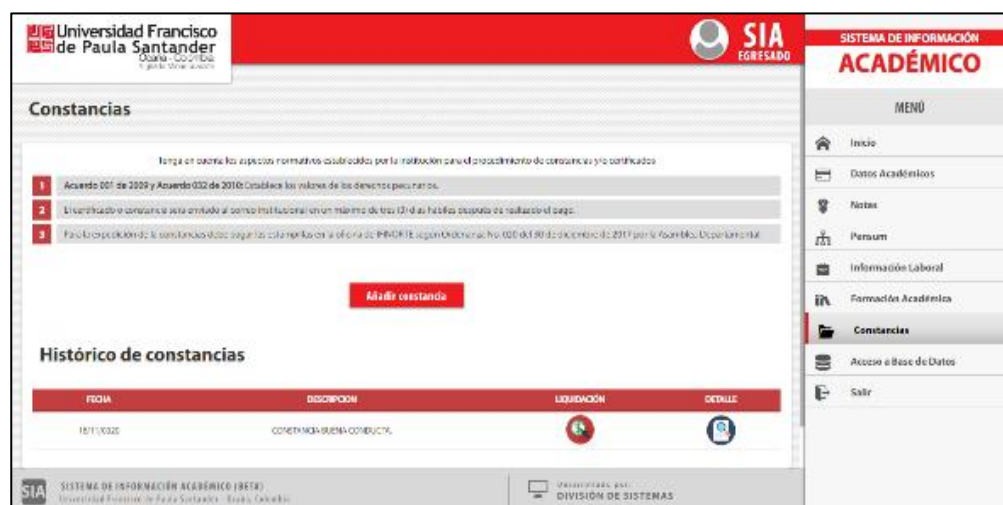


Figura 8: Sistema de información académica de egresados
Fuente: División de sistemas - UFPSO.

2.1.10 Sistema de Información de Bibliográfico - SIB

El Sistema de Información Bibliográfico (SIB) cuenta con una base de datos en el formato MARC para datos bibliográficos, que permiten manejar información de cualquier tipo de material bibliográfico y definir diferentes políticas propias de la Biblioteca Argemiro Bayona Portillo.



Este sistema permite registrar de todo el material bibliográfico que ingresa, como son Tesis, Libros, Documentos, Revistas, Publicaciones Seriadas, Audio Libros, Videos, entre otros; buscando que los tres estamentos universitarios puedan acceder a ellos en préstamos diarios con la finalidad de utilizarlos, y enriquecerse académicamente con el uso de la diversa bibliografía que es hallada en el espacio físico y Web de la universidad.

Módulos del Sistema de Información Bibliográfico - SIB

- Sistema vía web de Consulta de bibliografía
- Sistema de Catalogación, Circulación, Préstamo y Devoluciones
- Gestión de reportes y multas
- Biblioteca digital - Dspace (Consulta de trabajos de grado en línea)
- Bases de datos suscritas <https://ufpso.edu.co/Biblioteca>



Figura 9: Sistema de información biblioteca

Fuente: División de sistemas – UFPSO

2.1.11 Repositorio Digital (DSpace)

Es un sistema de información con arquitectura de repositorio digital; captura, almacena, ordena, preserva y distribuye material de investigación digital con el propósito de garantizar que se preserve y distribuya toda la producción intelectual generado al interior de las instituciones que hacen uso de este.

<https://repositorioinstitucional.ufpso.edu.co/>



Vía Acolsure, Sede el Algodonal, Ocaña, Colombia - Código postal: 546552
atencionalciudadano@ufpso.edu.co - www.ufpso.edu.co
Línea de atención: 311 436 1717



Figura 10: Repositorio institucional
Fuente: División de sistemas – UFPSO

2.1.12 Sistema de Información Financiero - SIF

El Sistema de Información Financiero de la Universidad Francisco de Paula Santander Ocaña reúne una serie de elementos con los cuales se coordina y controla las áreas contable y financiera de la institución, uno de estos elementos es el sistema informático que a su vez se compone de módulos por medio de los cuales se realizan actividades que permiten a la institución la adquisición de bienes y servicios facilitando la administración de los diferentes procesos contables y presupuestales.

Módulos del Sistema de Información Financiero - SIF

- Solicitudes de servicios y compras
- Presupuesto (CDP, Obligaciones, etc.)
- Contabilidad (Cuentas por pagar, Cuentas por Cobrar, Contabilidad)
- Subdirección administrativa (Órdenes, Autorización, Ingresos, etc.)
- Tesorería (Comprobantes de Egresos, Ingresos, etc.)



Vía Acolsure, Sede el Algodonal, Ocaña, Colombia - Código postal: 546552
atencionalciudadano@ufpso.edu.co - www.ufpso.edu.co
Línea de atención: 311 436 1717

- Recursos humanos (Nomina y Personal)
- Módulo de Almacén (Entradas, Salidas e Inventario)
- Modulo Granja (Órdenes de Compra y Servicio)



Figura11: Sistema de información financiero
Fuente: División de sistemas - UFPSO.

2.1.13 Sistema de Facturación Electrónica

Este sistema se enfoca en recolectar la información de todos los ingresos realizados a la Universidad Francisco de Paula Santander Ocaña, y generar las facturas correspondientes para el envío a la DIAN, además, se envía un correo al usuario notificando que el ingreso fue reportado, con una copia del documento XML y un enlace donde encontrará la factura en los sistemas de la DIAN.



Figura 12: Facturación electrónica

Fuente: <https://www.siigo.com/blog/empresario/factura-electronica-dian-objetivos-de-la-implementacion/>

2.1.14 Sistema de Información Documental - SID

El Sistema de Información Documental (SID) es una herramienta tecnológica desarrollada por la UFPSO bajo los más altos estándares de la Web, siguiendo los lineamientos de la oficina de Archivo y Correspondencia para el servicio de cada una de sus dependencias productoras de documentos.

El SID permite al usuario crear, actualizar e imprimir documentos como: Actas, Actas de Validación, Certificados, Circulares, Citaciones, Constancias, Memorandos, Resoluciones y Oficios. Además de soportar los tipos de documentos ya mencionados, cuenta con un módulo de radicación de ventanilla única para la recepción y control de documentos provenientes de instituciones o entidades externas a la Universidad.

Módulos del Sistema de Información Documental – SID

- Módulo de Administrador (gestión de usuarios, solicitudes, asignación de roles)
- Módulo de coordinador (asignación de usuarios a dependencias, responder solicitudes)
- Módulo de jefe (consulta y verificación de documentos)
- Módulo de secretaria (elaboración de documentos, radicación, envíos, registro de convenios, etc.)

<https://sid.ufpso.edu.co/>



Vía Acolsure, Sede el Algodonal, Ocaña, Colombia - Código postal: 546552
atencionalciudadano@ufpso.edu.co - www.ufpso.edu.co
Línea de atención: 311 436 1717



Figura 13: Sistema de información documental
Fuente: División de sistemas - UFPSO.

2.1.15 Sistema de Peticiones, Quejas, Reclamos, Sugerencias, Felicitaciones y Denuncias - PQRS

El Sistema de Peticiones, Quejas, Reclamos, Sugerencias, Felicitaciones y Denuncias de hechos de corrupción es un aplicativo Web que sirve de apoyo para el registro, clasificación, redirección y posterior trámite de las PQRS llegadas a través de los diferentes medios ofrecidos por la universidad, permitiendo así, agilizar los procedimientos de selección, distribución y respuesta de los distintos casos que se presentan ante la prestación de los servicios que brinda la Universidad.

Módulos del Sistema PQRS

- Módulo de Administrador (Gestión de usuarios)
- Módulo de coordinador (Asignación de usuarios, consulta y trámite de solicitudes)
- Módulo de funcionario responsable (Consulta y respuesta de solicitudes)
- Módulo de petionario (Registro y consulta de solicitudes)

<https://atencionalciudadano.ufpso.edu.co/pqrsdf>



Figura 14: Sistema de pqr
Fuente: División de sistemas - UFPSO.

2.1.16 Sistema de Información de Revisión y Control - SICI

El Sistema de Información de Revisión y Control (SICI) es un desarrollo establecido para llevar un registro de las revisiones eventuales iniciadas y ejecutadas por la oficina de control interno de la Universidad que permiten gestión de todas aquellas funcionalidades que son requeridas por los diferentes módulos para la gestión del sistema, en el cual se cubren las actividades de asignar usuario, registro de nuevas revisiones y responder las solicitudes, entre otros. La información contenida permite que el usuario tenga privilegios de gestionar el sistema como tal, en inserción, revisión y consulta en la base de datos.

Módulos del Sistema de Información de Revisión y Control - SICI

- Módulo Administrador
- Módulo Coordinador
- Módulo Usuario
- Asignación de revisiones eventuales
- Consulta de histórico de revisiones
- Ingreso de información



Vía Acolsure, Sede el Algodonal, Ocaña, Colombia - Código postal: 546552
atencionalciudadano@ufps.edu.co - www.ufps.edu.co
Línea de atención: 311 436 1717

<https://controlinterno.ufpso.edu.co/>

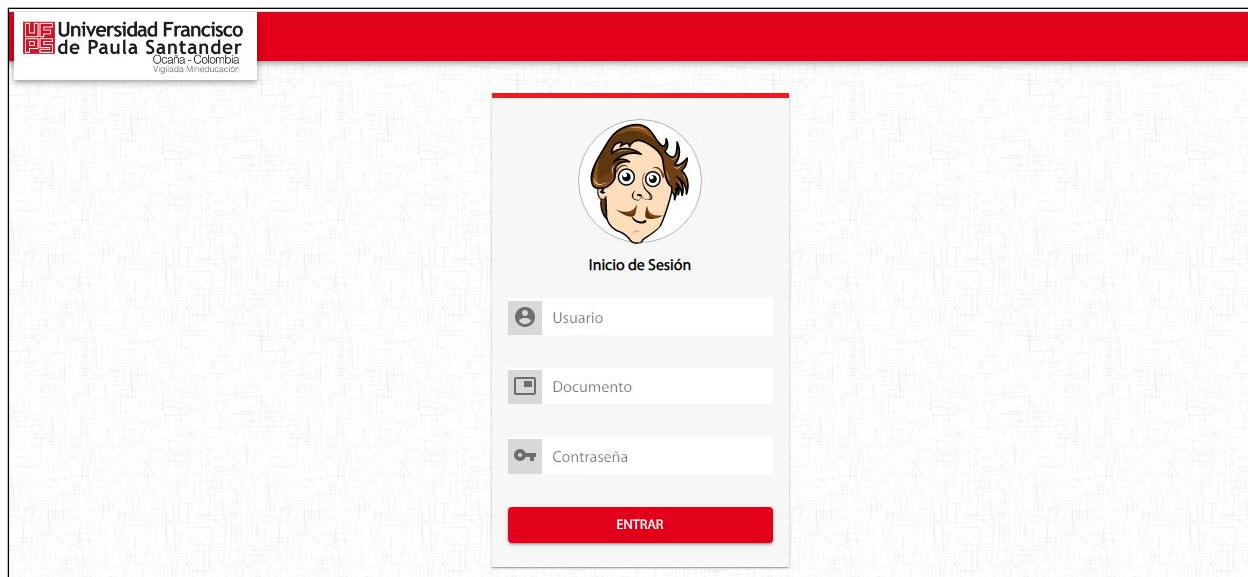


Figura 15: Sistema de información control interno
Fuente: División de sistemas - UFPSO.

2.1.17 Sistema de Información de Autoevaluación y Acreditación - SIAC

El Sistema de Información de Autoevaluación y Acreditación (SIAC) está diseñado principalmente para mejorar la calidad y lograr la acreditación, haciendo seguimiento con datos estadísticos de todas las áreas principales de los programas académicos de la Universidad.

Módulos del Sistema de Información de Autoevaluación y Acreditación - SIAC

- Registro de los datos del programa académico
- Realiza calificación, ponderación y análisis (Factores, Características y Aspectos)
- Seguimiento estadístico en tiempo real

<https://siac.ufpso.edu.co/>



Vía Acolsure, Sede el Algodonal, Ocaña, Colombia - Código postal: 546552
atencionalciudadano@ufpso.edu.co - www.ufpso.edu.co
Línea de atención: 311 436 1717

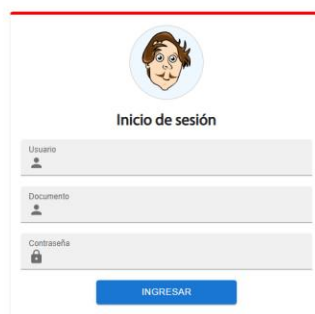


Figura 16: Sistema de información de autoevaluación y acreditación

Fuente: División de sistemas - UFPSO.

2.1.18 Sistema de Información de Gestión Humana – SGH

El Sistema de Información de Gestión Humana (SGH) está diseñado para facilitar a los docentes y administrativos el acceso a su información personal y visualizar el histórico de salarios, prestaciones sociales que le han sido pagados al empleado, consulta y descarga del certificado de ingresos y retenciones de la Dian, reserva de escenario, inventario.

Módulos del Sistema de Información de Gestión Humana - SGH

- Histórico de liquidaciones
- Consulta de datos personales
- Certificados de la DIAN
- Reserva de escenarios
- Asimilación categoría
- Inventario

<https://siadmon.ufpso.edu.co/>



Figura 17: Sistema de información de gestión humana
Fuente: División de sistemas - UFPSO.

2.1.19 Sistema de Información de Solicitudes y Requerimientos de División de Sistemas

El sistema de información de la división de sistemas está diseñado para administrar contenidos, recibir y dar respuesta a las solicitudes de los administrativos para el manejo y soporte de la infraestructura tecnológica de la Universidad y permite la gestión de todas aquellas funcionalidades que son requeridas por los diferentes módulos para la gestión del sistema, en el cual se cubren las actividades de gestionar usuario, preguntas de la encuesta de satisfacción, y gestionar las solicitudes entre otros. La información contenida permite que el usuario administrador o usuario tenga privilegios de gestionar el sistema como tal en inserción, actualización y consulta en la base de datos.

Como estrategia de seguimiento y evaluación de los servicios que presta la División de Sistemas, se aplica una encuesta de satisfacción a los usuarios (directivos, profesores, estudiantes y personal administrativo), una vez recibido el servicio solicitado, a través del portal <https://divisis.ufpso.edu.co>, se mide la oportunidad del servicio, atención del personal, calidad del servicio y eficacia de los sistemas de información.

Módulos del Sistema de Información de División de Sistemas

- Registro de solicitudes
- Recepción, asignación y ejecución de solicitudes
- Encuesta de satisfacción
- Gestión de contenido

<https://divisis.ufpso.edu.co/>





Figura18: Sistema de información de solicitudes y requerimientos división de sistemas

Fuente: División de sistemas - UFPSO.

2.1.20 Sistema de Información de Solicitudes y Requerimientos de Planeación

El sistema de infraestructura y mantenimiento está diseñado para recibir y dar respuesta a las solicitudes de los administrativos concernientes a la integridad de las instalaciones de la Universidad y permite la gestión de todas aquellas funcionalidades que son requeridas por los diferentes módulos para la gestión del sistema, en el cual se cubren las actividades de gestionar usuario, preguntas de la encuesta de satisfacción, y gestionar las solicitudes entre otros. La información contenida permite que el usuario administrador o coordinador tenga privilegios de gestionar el sistema como tal en inserción, actualización y consulta en la base de datos.

Módulos del Sistema de Información de Planeación

- Módulo Administrador
- Módulo Coordinador
- Módulo Funcionario
- Registro de solicitudes
- Recepción, asignación y ejecución de solicitudes
- Encuesta de satisfacción

<https://planeacion.ufpsedu.co/>



Vía Acolsure, Sede el Algodonal, Ocaña, Colombia - Código postal: 546552
atencionalciudadano@ufpsedu.co - www.ufpsedu.co
Línea de atención: 311 436 1717

Figura 19: Sistema de información de solicitudes y requerimientos de planeación

Fuente: División de sistemas - UFPSO.

2.1.21 Sistema de Información de Solicitudes y Requerimientos de Bienestar

El sistema de información de solicitudes y requerimientos está diseñado para recibir y dar respuesta a las solicitudes de los estudiantes y administrativos referentes al bienestar universitario y permite la gestión de todas aquellas funcionalidades que son requeridas por los diferentes módulos para la gestión del sistema, en el cual se cubren las actividades de gestionar usuario, preguntas de la encuesta de satisfacción, y gestionar las solicitudes entre otros. La información contenida permite que el usuario administrador o coordinador tenga privilegios de gestionar el sistema como tal en inserción, actualización y consulta en la base de datos.

Módulos del Sistema de Información de Planeación

- Módulo Administrador
- Módulo Coordinador
- Módulo Funcionario
- Registro de solicitudes
- Recepción, asignación y ejecución de solicitudes
- Encuesta de satisfacción

<https://gestionbienestar.ufpso.edu.co/>



Vía Acolsure, Sede el Algodonal, Ocaña, Colombia - Código postal: 546552
atencionalciudadano@ufpso.edu.co - www.ufpso.edu.co
Línea de atención: 311 436 1717

Figura 20: Sistema de información de solicitudes y requerimientos de bienestar universitario
Fuente: División de sistemas - UFPSO.

2.1.22 Sistema de Información de Solicitudes y Requerimientos de Multimedios

El sistema de información de multimedios está diseñado para recibir y dar respuesta a las solicitudes de los administrativos que requieran los servicios de la oficina de multimedios y permite la gestión de todas aquellas funcionalidades que son requeridas por los diferentes módulos para la gestión del sistema, en el cual se cubren las actividades de gestionar usuario, preguntas de la encuesta de satisfacción, y gestionar las solicitudes entre otros.

<https://multimedios.ufpso.edu.co/>



Vía Acolsure, Sede el Algodonal, Ocaña, Colombia - Código postal: 546552
atencionalciudadano@ufpso.edu.co - www.ufpso.edu.co
Línea de atención: 311 436 1717

Figura 21: Sistema de información de solicitudes y requerimientos de multimedia
Fuente: División de sistemas - UFPSO.

2.1.23 La UFM

Sistema de información para la gestión de contenido de la emisora institucional La UFM Stereo 95.2 cuenta con los siguientes módulos

Módulos del Sistema de Información de Admisiones, Registro y Control

- La UFM: este módulo permite gestionar el contenido de la identidad corporativa de la emisora, como alianzas, equipo de trabajo e información general.
- Noticias: este módulo permite gestionar el contenido de las secciones y sus noticias
- Programas: Este módulo permite gestionar la información de la parrilla de programación, los programas y los podcasts de la emisora.
- Estadísticas: este módulo lleva a cabo un seguimiento de los aspectos más importantes de la emisora a través de herramientas como gráficas para obtener un análisis rápido del comportamiento de la emisora.
- Sistema: este módulo permite gestionar el acceso y los permisos de los usuarios al sistema de información.



<https://laufm.ufpso.edu.co/>

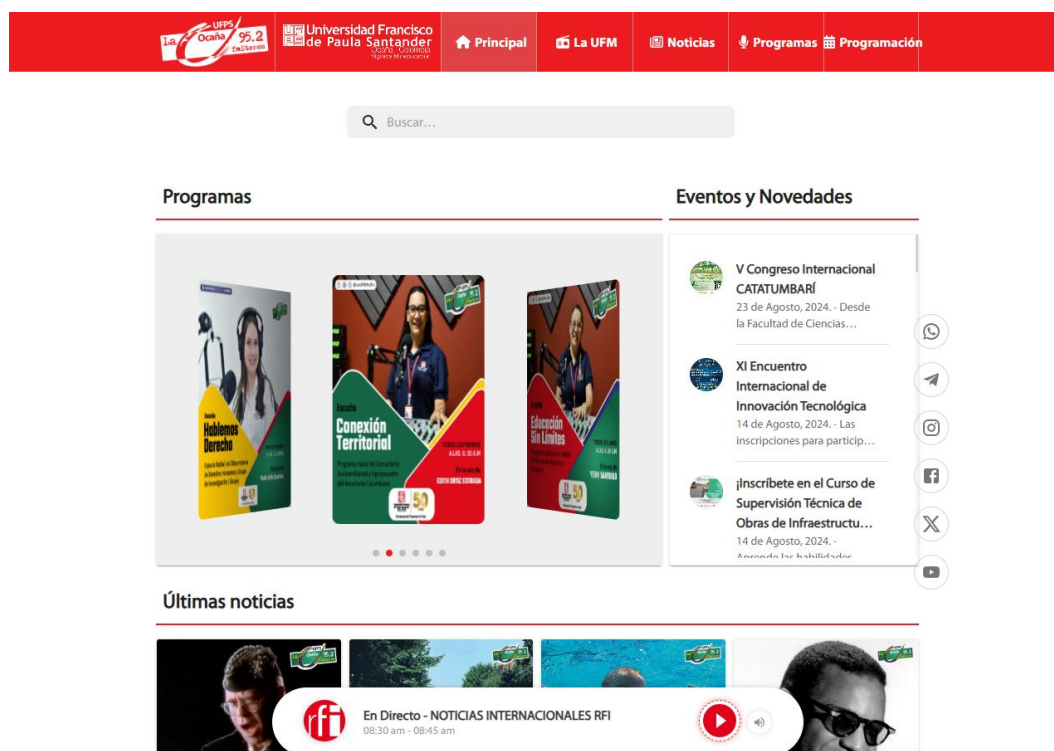


Figura 22: Portal web la ufm
Fuente: División de sistemas - UFPSO.

2.1.24 Portal de Encuestas

La Universidad cuenta con la herramienta de encuestas en línea LimeSurvey, óptima para organismos de investigación, universidades y otras instituciones de formación. LimeSurvey es una aplicación de software libre para la realización de encuestas en línea, escrita en PHP y que utiliza bases de datos MySQL, PostgreSQL o MSSQL. Esta utilidad brinda la posibilidad a usuarios sin conocimientos de programación el desarrollo, publicación y recolección de respuestas de sus encuestas.

<https://encuesta.ufpso.edu.co/admin>



Vía Acolsure, Sede el Algodonal, Ocaña, Colombia - Código postal: 546552
atencionalciudadano@ufpso.edu.co - www.ufpso.edu.co
Línea de atención: 311 436 1717

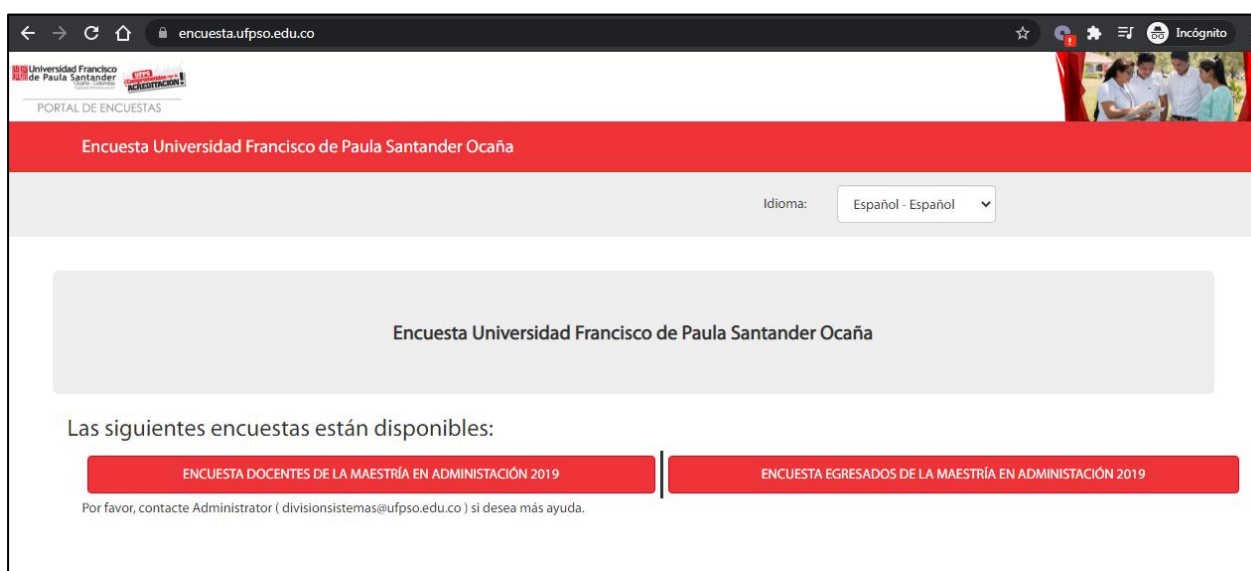
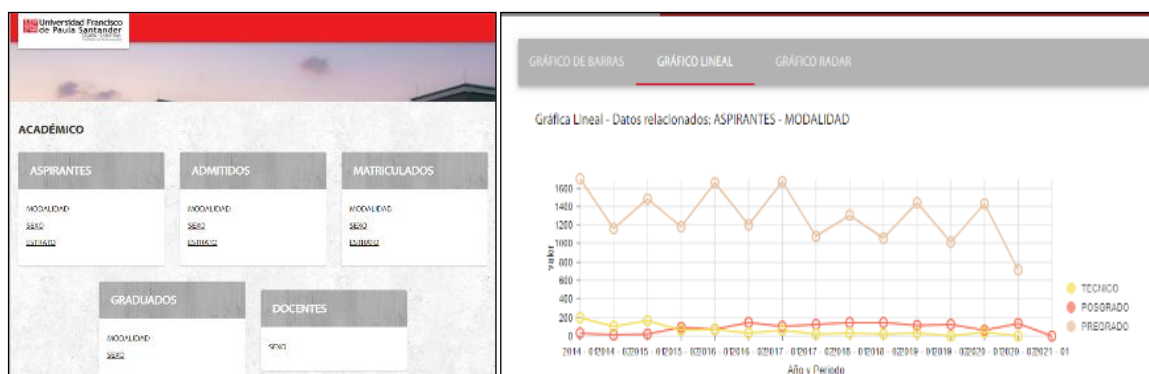


Figura 23: Portal de encuestas
Fuente: División de sistemas - UFPSO.

2.1.25 Portal Estadísticas – Datos Abiertos

En cumplimiento a la ley 1712 del 6 de marzo de 2014 "Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional.", la Universidad Francisco de Paula Santander seccional Ocaña dispone información de interés público, donde podrá encontrar los datos históricos y estadísticos institucionales, además, para mayor entendimiento del lenguaje que hace parte de las categorías de información institucional, puede consultar la sección de metadatos, asociados a la información cuantitativa que se pone a la disposición de los interesados.

<https://estadisticas.ufpso.edu.co/>



Vía Acolsure, Sede el Algodonal, Ocaña, Colombia - Código postal: 546552
atencionalciudadano@ufpso.edu.co - www.ufpso.edu.co
Línea de atención: 311 436 1717

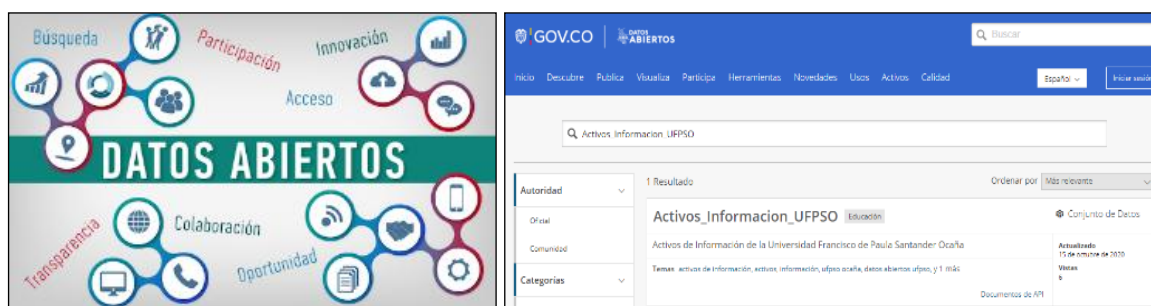


Figura 24: Portal de estadísticas
Fuente: División de sistemas - UFPSO.

2.1.26 Sistema de Respaldo de Información ownCloud

El sistema de respaldo ([cloud computing](#)) ownCloud es una plataforma para el intercambio seguro de archivos alojado en nuestro centro de datos. ownCloud ofrece transparencia, seguridad y control y se puede integrar de manera flexible en nuestro entorno existente. Al mismo tiempo, los usuarios pueden acceder rápida y fácilmente a los archivos de la universidad desde cualquier lugar y desde cualquier dispositivo aumentando la seguridad y la productividad por igual de acuerdo con las políticas y procedimientos de seguridad.

ownCloud ofrece a nuestro personal administrativo un modo fácil, flexible y seguro para compartir archivos y carpetas, colaborando desde cualquier sitio y dispositivo. Por tal motivo incrementa la eficiencia permitiendo que almacenen, compartan y trabajen en sus datos y documentos a través de un único punto de acceso, trabajando simultáneamente en documentos, creando presentaciones en colaboración a tiempo real, comentando archivos y mucho más, a la vez que ahorra tiempo en los procesos de coordinación y comentarios.

<https://respaldo.ufpso.edu.co>



Vía Acolsure, Sede el Algodonal, Ocaña, Colombia - Código postal: 546552
atencionalciudadano@ufpso.edu.co - www.ufpso.edu.co
Línea de atención: 311 436 1717

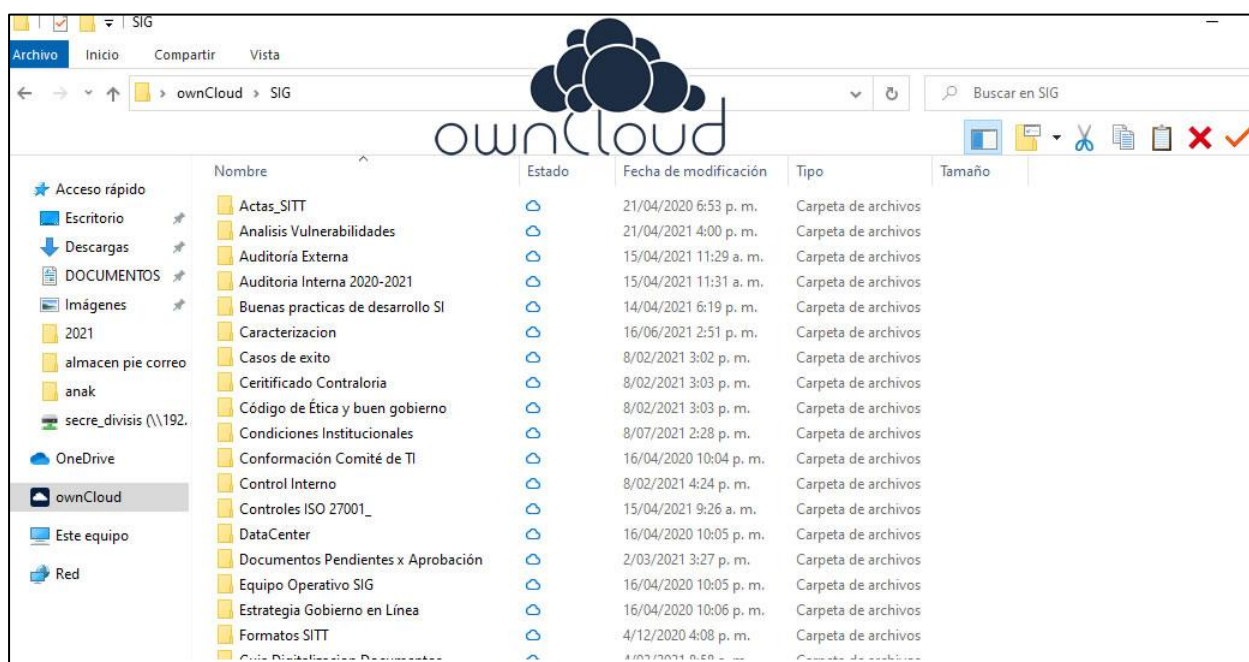


Figura 25: Sistema de respaldo owncloud

Fuente: División de sistemas – UFPSO

2.1.27 Sistema de Notificaciones y Publicaciones

El sistema de notificaciones y publicaciones es un sistema encargado de generar las publicaciones en el portal publicaciones.ufpso.edu.co, mediante herramientas que permiten la creación de texto con estilo, inserción de imágenes y video de forma que el usuario pueda darle elegancia a la notificación deseada, además, permite enviar dicha publicación a través de los correos institucionales, asociados a diferentes filtros como lo son Docentes, estudiantes, administrativos, etc. para que dicha información llegue a la población de interés y con un formato estandarizado por la universidad.

<https://ufpso.edu.co/Publicaciones-ufpso>



Vía Acolsure, Sede el Algodonal, Ocaña, Colombia - Código postal: 546552
atencionalciudadano@ufpso.edu.co - www.ufpso.edu.co
Línea de atención: 311 436 1717

The screenshot shows the official website of Universidad Francisco de Paula Santander (UFPS) Ocaña. The header includes the university logo, name, and location (Ocaña - Colombia, Vigilada Mineducación). A navigation bar lists various services: UFPSO, Admisiones, Programas, Internacionalización, SIG, Investigación, Extensión, Dependencias, Participa, Transparencia, Atención y Servicios a la Ciudadanía. Below the navigation bar, there's a section for 'Publicaciones' (Publications) with links to 'Noticias de Calidad 2025' and 'Píldora de Calidad N°2 2025'. The main content area displays two digital documents titled 'PÍLDORAS DE CALIDAD' (Quality Pills) for 2025. The first document is 'PÍLDORA DE CALIDAD N°1' and the second is 'PÍLDORA DE CALIDAD N°2'. Both documents feature a cartoon character and text related to quality management. The website also includes a search bar, a language selector, and a 'Servicios' (Services) button on the right side.

Figura 26: Sistema de notificaciones y publicaciones
Fuente: División de sistemas - UFPSO.

2.1.28 Unidad de Educación Virtual

Otro de los mecanismos para optimizar la comunicación entre profesores y estudiantes y apoyar el proceso de formación en los programas académicos, es la U virtual, plataforma de código abierto estructurado en Moodle, utilizada para la virtualización de actividades académicas como apoyo a la presencialidad, con acceso a estudiantes y docentes de la Universidad mediante el siguiente link: <http://uvirtual.ufpso.edu.co/>

Servicios:

- Capacitación a docentes manejo de plataforma Moodle.
- Servicios, noticias, videos.
- Uvirtual
- Cursos virtuales que son utilizados como apoyo a la presencialidad.
- Univirtual



Vía Acolsure, Sede el Algodonal, Ocaña, Colombia - Código postal: 546552
atencionalciudadano@ufpso.edu.co - www.ufpso.edu.co
Línea de atención: 311 436 1717

- Programas de postgrados virtuales (IE, SGI HSEQ).



Figura 27: Univirtual
Fuente: División de sistemas – UFPSO

3. TELECOMUNICACIONES

Además, en la Universidad Francisco de Paula Santander Ocaña en su Campus Universitario de la sede principal, se extiende un Backbone (Cableado principal de transporte de datos) en fibra óptica con topología estrella, que interconecta el centro de cableado principal ubicado en el edificio División de Sistemas con los demás edificios localmente dispersos mediante Switches.

Edificios interconectados:

- Edificio División de Sistemas (Nodo Principal)
- Edificio Casona (Conectado por medio de Fibra Óptica)
- Edificio Salas de Cómputo (Conectado por medio de Fibra Óptica)
- Edificio Anexos Académicos (Conectado por medio de Fibra Óptica)
- Edificio Granja (Conectado por vía Inalámbrica)
- Edificio de Aulas (Conectado por medio de Fibra Óptica)
- Edificio administrativo Admisiones y Dirección (conectado por fibra óptica)
- Edificio de Ingenierías (conectado por fibra óptica)

Igualmente existe red de datos en las siguientes sedes:

- Edificio Sede Primavera
- Edificio Escuela de Artes

En cada una de las sedes y edificios se encuentran conectadas todas las dependencias, las cuales cuentan con características técnicas que permiten una fácil conexión al medio de transmisión, como son los switch, access point, fibra óptica y cableado estructurado UTP en categorías 6 y 7A. Para la interconexión de las dependencias y puestos de trabajo la Universidad cuenta con 2850 puntos de red cableados y 206 teléfonos digitales IP.



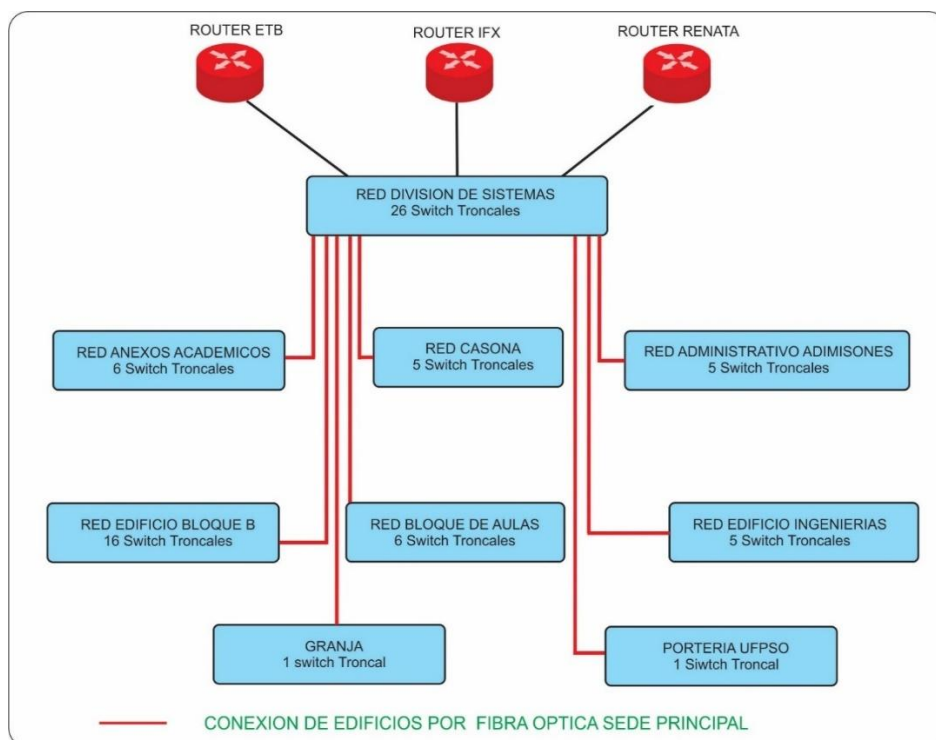


Figura28: Diagrama de conexión de Edificios en Sede Principal
Fuente: División de sistemas – UFPSO

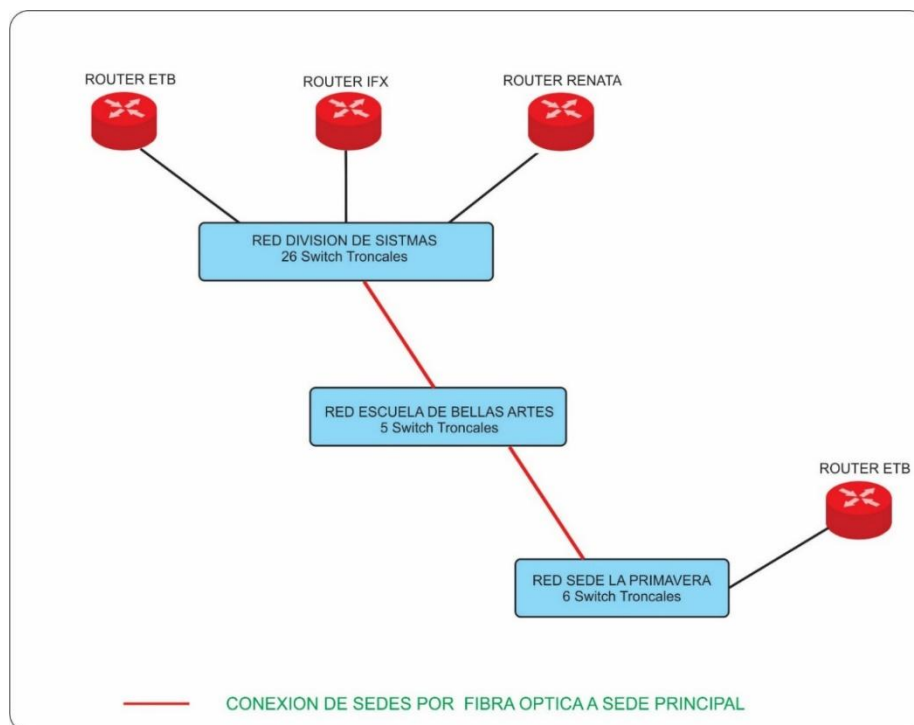


Figura 29: Diagrama de conexión sedes de la UFPSO
Fuente: División de sistemas – UFPSO.

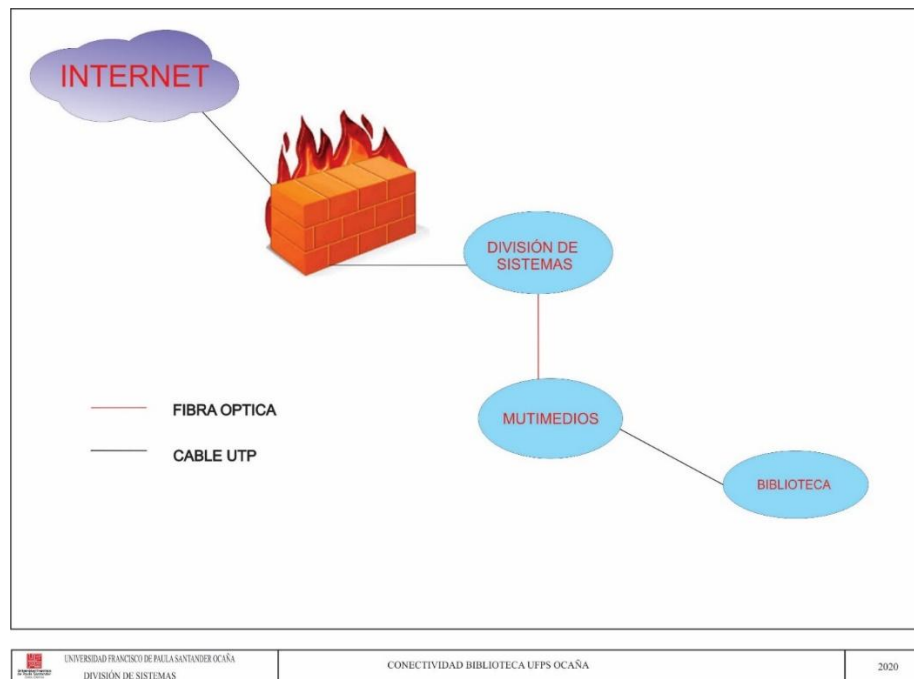


Figura 30: Diagrama de conexión Biblioteca UFPSO
Fuente: División de sistemas – UFPSO.

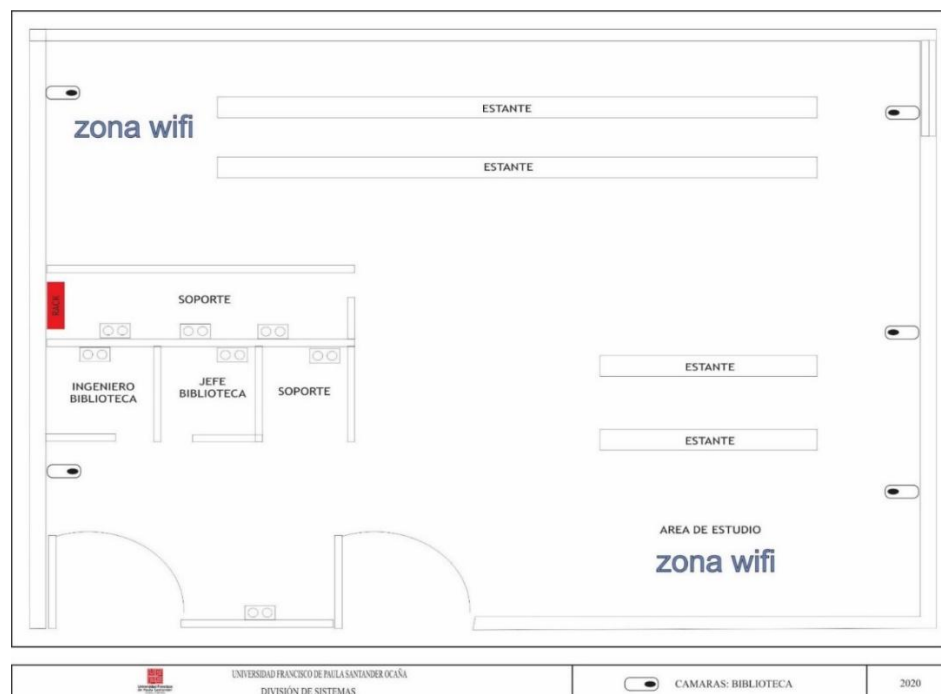


Figura 31: Infraestructura Física Biblioteca Zona 1
Fuente: División de sistemas – UFPSO

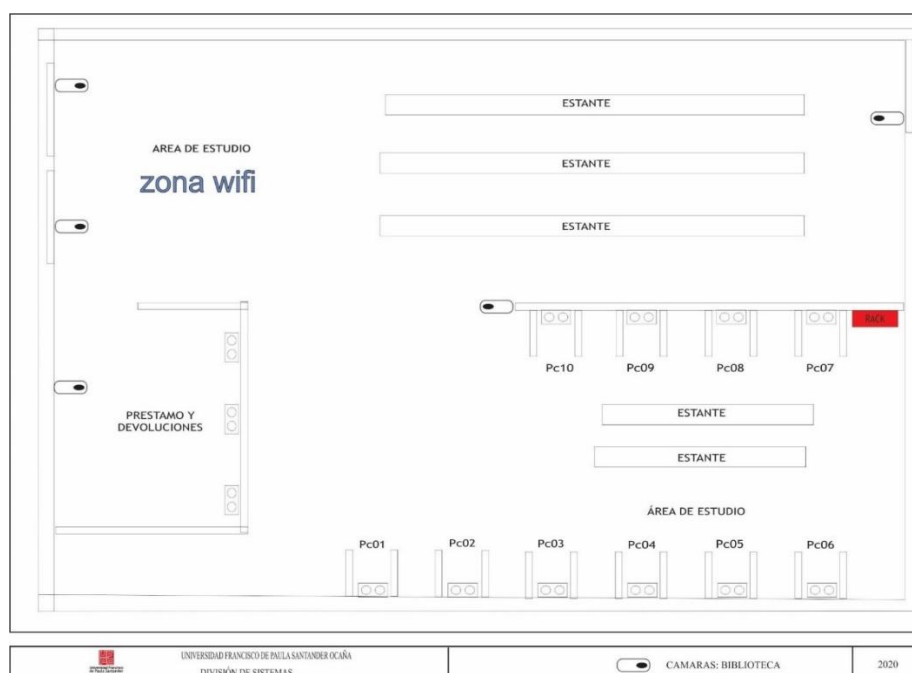


Figura 32: Infraestructura Física Biblioteca Zona 2

Fuente: División de sistemas – UFPSO

La figura 28, muestra la conexión de los edificios en la sede principal, todos conectados por medio de fibra óptica hacia el nodo central que es la División de sistemas. A cada uno de estos edificios por medio de enlaces con cable UTP categoría 6 de exteriores se realizan la conexión a las otras dependencias que están cerca de estos. La red de la UFPSO, está conformada por la conexión de las tres sedes como se muestra en la figura 29, todas estas con tecnologías de Switches HP de última generación con capacidad de trabajo y funcionalidades de capa 2; el Switch CORE, de la red es un Switch HP V1910 de 24 puertos que está ubicado en la División de Sistemas, la interconexión con las sedes se hace a través de Transceivers de fibra óptica de 1 Gbps. Se cuenta con un CORE de Switch de 71 en su totalidad, los cuales configurados por medio de Vlans se distribuye los diferentes tráficos que se generan por los servidores que se alojan en la división de sistemas. La figura 3, Describe como es la conexión de una de las dependencias como es la biblioteca. Las figuras 4 y 5 muestran la distribución física de cada uno de los puestos de trabajo en esta dependencia.

3.1 Red Inalámbrica

La Universidad Francisco de Paula Santander Ocaña cuenta con una red inalámbrica que cubre todo el campus universitario brindando respaldo a la red alámbrica permitiendo el acceso a internet desde cualquier punto de la universidad.

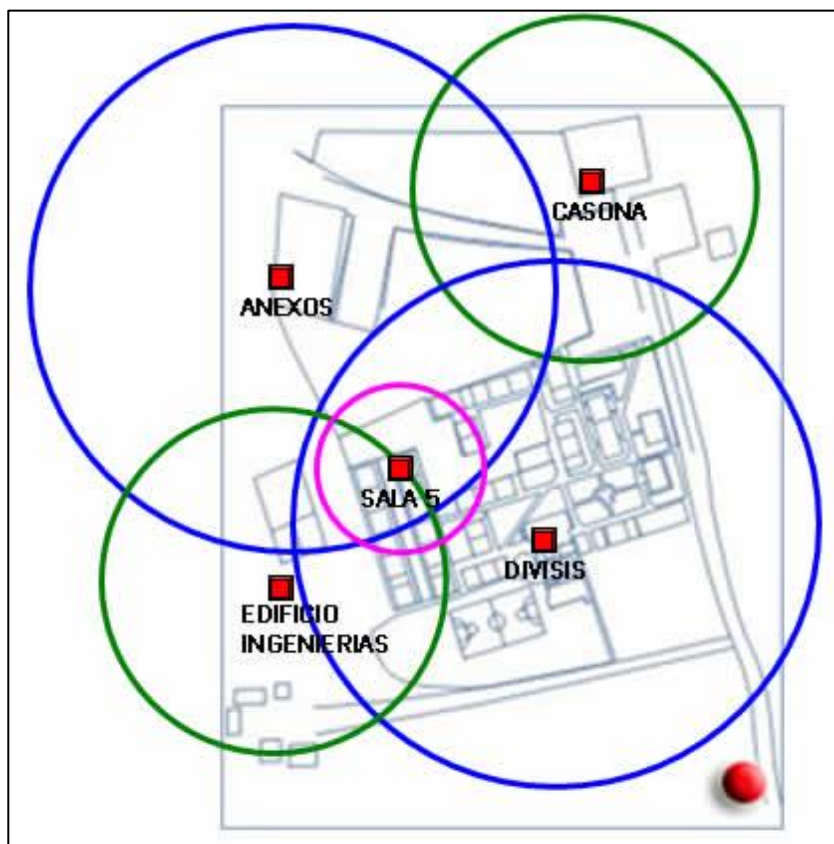


Figura 33: Conexión inalámbrica
Fuente: División de sistemas - UFPSO

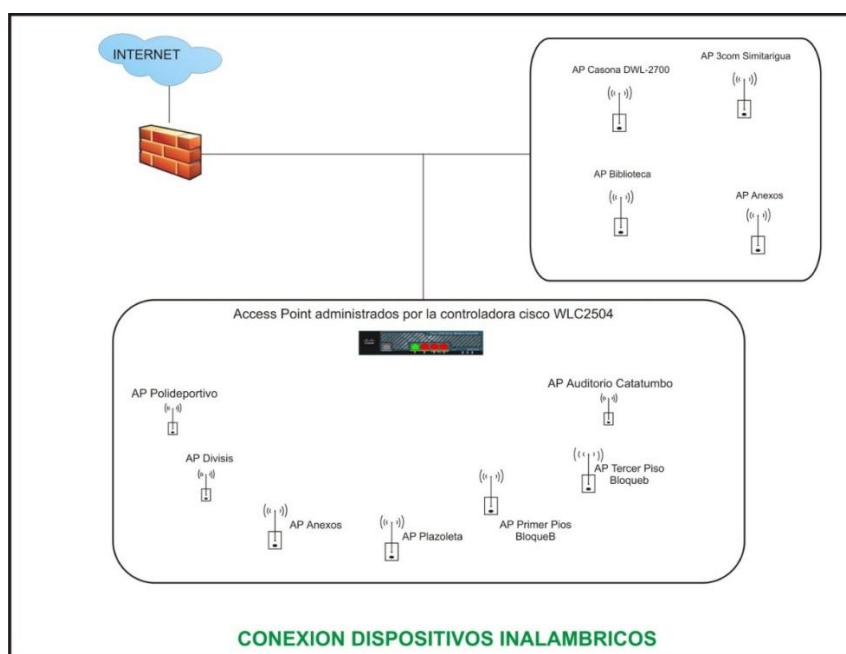


Figura34: Diagrama de conexión de dispositivos inalámbricos.

Fuente: División de sistemas – UFPSO

La red inalámbrica de la Universidad como se muestra en la figura 7, está soportada por nuevas tecnologías que permiten dar disponibilidad de conexión a los diferentes usuarios que la utilicen. Actualmente una parte de esta red está administrada por una controladora CISCO y los demás son puntos de acceso están independientes; a continuación, se muestra los dispositivos con que esta red cuenta.

Núm.	CARACTERÍSTICA	CANTIDAD	OBSERVACIÓN
1	Controladora cisco WLC2504	1	Dispositivo para la gestión de los Access Point AIR-CAP1702I-A-K9
2	Access Point AIR-CAP1702I-A-K9	7	Dispositivos administrados por la controladora WLC2504
3	Access Point TP-Link WR743DN	1	Dispositivo en el campus universitario
4	Access Point cisco WAP4410N	6	Dispositivo en el campus universitario
5	Access Point Dlink DWL-2700	1	Casona
6	Access Point Nano loco 2	1	Biblioteca
7	Access Point Cisco RV110W	1	Catedráticos

Tabla 1: Dispositivos inalámbricos

Fuente: División de sistemas - UFPSO.

3.2 Telefonía

Se puede hacer contacto telefónico con la Universidad Francisco de Paula Santander Ocaña a través del sistema de comunicaciones por medio de las líneas telefónicas con las que cuenta actualmente; 11 líneas análogas PSNT externas que llegan a la sede principal, una a la escuela de bellas artes y tres a la sede de la primavera que se interconectan a través del gateway 4108 y éste a su vez se comunica con nuestro servidor, que actualmente cuenta con el software Issabel PBX gestionando todo lo relacionado con la telefonía IP aprobando de esta manera que la Universidad administre las 206 extensiones IP que en este momento existen permitiendo la comunicación hacia todas las dependencias y oficinas de la institución.

(+57) (7) 569 00 88

<https://ufpso.edu.co/directorioufpso>

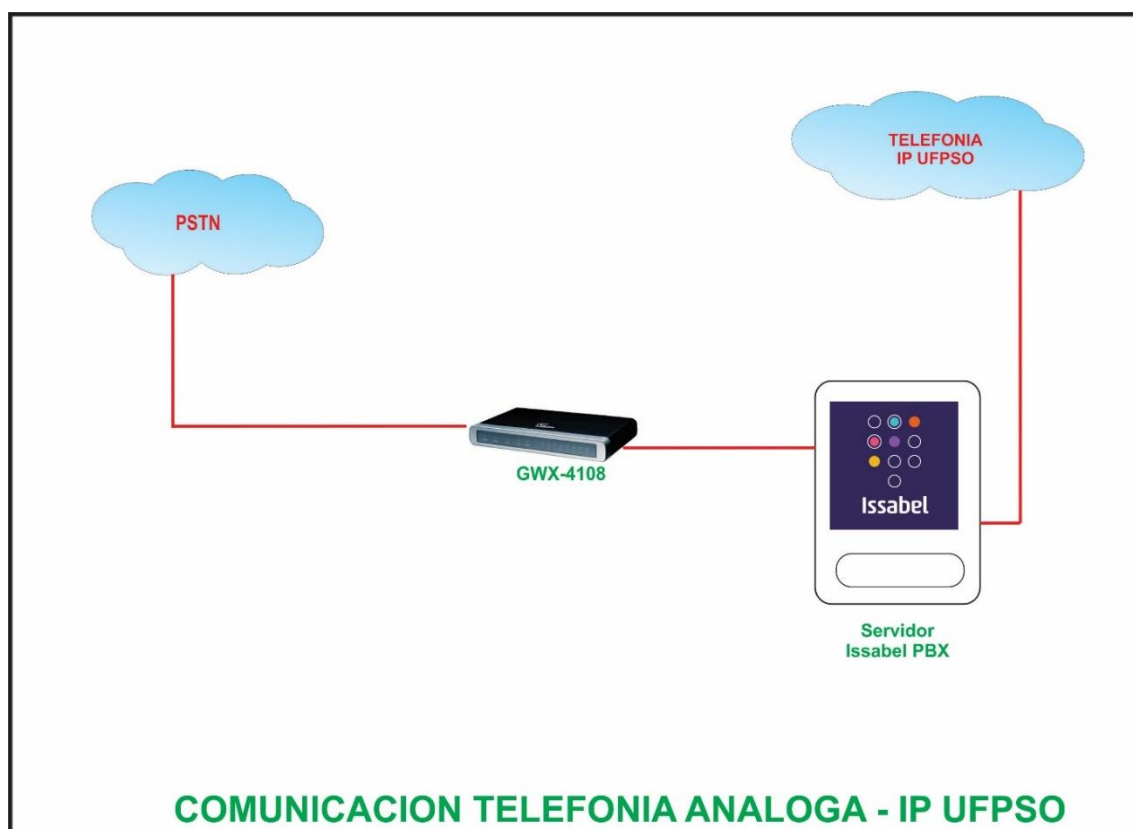


Figura 35: Comunicación telefonía analógica – IP
Fuente: División de sistemas – UFPso

4. TECNOLOGÍA

4.1 Equipos Tecnológicos

Los equipos o recursos tecnológicos permiten satisfacer las necesidades a los docentes y estudiantes para enriquecer el proceso educativo cumpliendo con las demandas de estos tiempos, así como a los funcionarios para brindar apoyo a todos los procesos logrando de esta manera alcanzar los objetivos institucionales trazados. Los equipos tecnológicos con que cuenta la Universidad Francisco de Paula Santander Ocaña son:

Equipos Tecnológicos	Cantidad
Access Point	55
Cámaras IP	106
Computadores	1236
Impresoras	179
Ipad-Tablet	41
Pizarras Digitales	17
Portátiles	185
Servidores	16
Televisores CCTV	55
Video Beam	103
Total	1993

Tabla 2: Equipos tecnológicos
Fuente: División de sistemas - UFPSO.

4.2 Salas de Cómputo

En aras de prestar un excelente servicio la División de Sistemas pone a disposición de toda la comunidad universitaria 21 salas de cómputo con sus respectivos sistemas operativos y programas instalados de acuerdo a las necesidades académicas. Cabe destacar que se deben respetar los horarios asignados para las clases, y, el servicio general de las salas que a bien tengan la necesidad educativa de utilizar dichos espacios o herramientas; deben hacer su reserva con suficiente anticipación.

21 Salas de cómputo equipadas con Pc's, acceso a internet, video beam, pizarras digitales y cámaras de seguridad.



SALA	DESCRIPCION
SCAE	ADMINISTRACION DE EMPRESAS - BLOQUE A
SCAE2	ADMINISTRACION DE EMPRESAS - BLOQUE DE AULAS SEGUNDO PISO
SCBA	BELLAS ARTES - SEDE ESCUELA DE ARTES
SCCS	COMUNICACION SOCIAL - BLOQUE DE AULAS TERCER PISO
SCCP	CONTADURIA PUBLICA - BLOQUE DE AULAS TERCER PISO
SCDE	DERECHO - BLOQUE DE AULAS SEGUNDO PISO
SCGR1	GENERAL UNO - BLOQUE DE AULAS TERCER PISO
SCGR2	GENERAL DOS - BLOQUE DE AULAS TERCER PISO
SCGR3	GENERAL TRES - BLOQUE DE AULAS SEGUNDO PISO
SCIA	INGENIERIA AMBIENTAL - BLOQUE A
SCIC	INGENIERIA CIVIL - BLOQUE DE AULAS TERCER PISO
SCIS2	INGENIERIA DE SISTEMAS - BLOQUE A
SCIS	INGENIERIA DE SISTEMAS - BLOQUE DE AULAS TERCER PISO
SCIM	INGENIERIA MECANICA - BLOQUE DE AULAS SEGUNDO PISO
SCTCS	TALLER DE DISEÑO DIGITAL DE COMUNICACIÓN SOCIAL - BLOQUE DE AULAS CUARTO PISO
SCTGC	TECNOLOGÍA EN GESTIÓN COMERCIAL Y FINANCIERA - BLOQUE A
SCZT	ZOOTECNIA - BLOQUE A
SCCAT	SALA DE CATEDRATICOS
SCCELEE	CENTRO DE IDIOMAS - CELEE
SCAUTI	LABORATORIO DE AUTOMATIZACION INGENIERIA MECANICA
CISCO	LABORATORIO DE REDES T TELECOMUNICACIONES

Tabla 3: Salas de cómputo

Fuente: División de sistemas - UFPSO.



Figura 36: Salas de cómputo

Fuente: División de sistemas – UFPSO

4.3 Infraestructura de video vigilancia por IP.

La Universidad Francisco de Paula Santander Ocaña a través de la división de sistemas en busca de salvaguardar la seguridad en las áreas principales ha implementado la video vigilancia por IP, utilizando dispositivos DNR 322L DLINK, distribuyendo las cámaras de la siguiente manera. 35 cámaras IP en las salas de cómputo (2 por cada sala y en las 3 salas nuevas 3 cámaras por cada sala), 1 en oficina de ventanilla única, 2 cámaras IP en el centro de idiomas, 6 cámaras IP en el consultorio jurídico, 4 cámaras IP en el gimnasio, 2 cámaras IP en la emisora UFM, 1 cámara IP en bienestar universitario, 8 cámaras IP en el restaurante universitario, 6 cámaras IP en la escuela de bellas artes, 1 cámara IP en bodega de almacén, 1 cámara IP en la sala de catedráticos, 1 cámara IP en la división de sistemas, 10 cámaras IP en la biblioteca, 4 cámaras IP en el laboratorio de física, 1 cámara IP de exteriores en la Universidad, 6 cámaras IP en auditorios (A16, A18, Simitarigua), 2 cámaras IP CAANC, 4 cámaras IP departamento de comunicación social, 2 cámaras IP en portería.

Cámara Termo gráfica con reconocimiento Biométrico



Figura37: Cámara termo gráfica
Fuente: División de sistemas - UFPSO.

4.4 Trabajo colaborativo

- Ampliación canal de internet, 1.204 Mbps
- Renovación con Renata
- Laboratorio: envío, VC espresso, VideoConferencia, Renata en vivo, Cómputo estadístico, Referencia, etc.
- Acceso a 11 salas Zoom

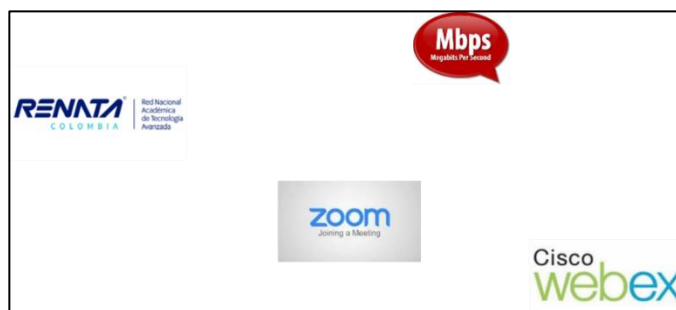


Figura 38: Trabajo colaborativo
Fuente: División de sistemas – UFPSO

4.6 Chat Institucional

Google Chat es una excelente herramienta tecnológica para comunicarnos, con la cual podemos dar inicio a un mensaje o conversación con uno o más contactos, crear una sala para tener conversaciones continuas con grupos de personas y usar bots para automatizar el trabajo. Chat funciona en el navegador de la computadora y en las apps para dispositivos móviles iOS y Android. Google chat se integra a la cuenta de correo institucional con el dominio **@ufpso.edu.co**

4.7 Correo Electrónico

El correo electrónico es un instrumento destinado para la recepción de solicitudes de información, para tratar temas, preguntas y los problemas de carácter técnico de los estamentos universitarios y a través del cual la División de Sistemas responde y suministra información y solución a los mismos. Todas las cuentas de correo electrónico institucional son del dominio **@ufpso.edu.co**



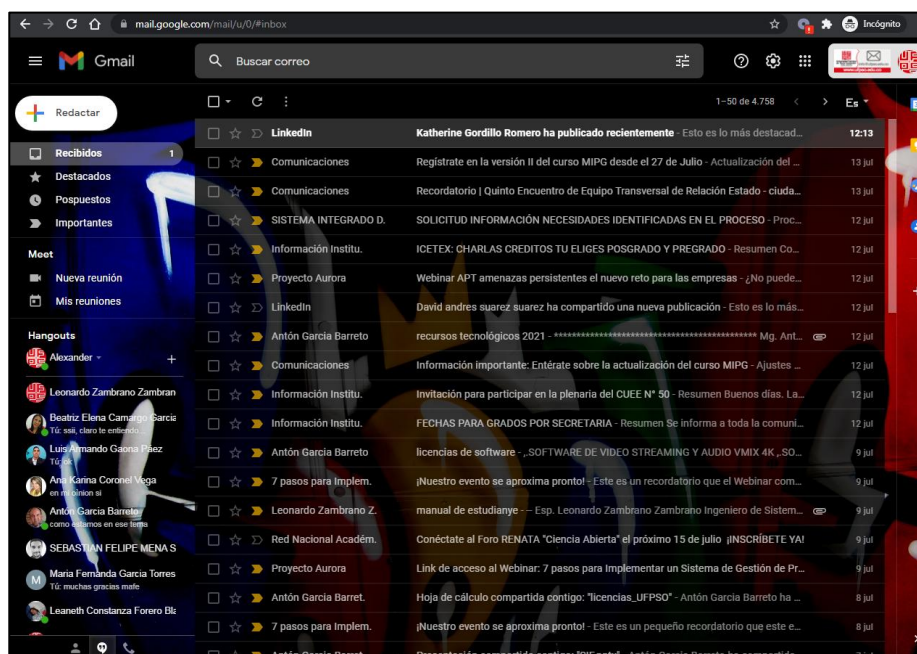


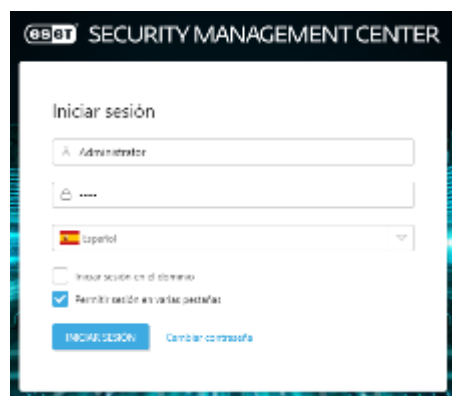
Figura 40: Correo institucional
Fuente: División de sistemas - UFPSO

4.8 Seguridad

En temas de seguridad la división de sistemas agrega una capa adicional de seguridad para detectar las amenazas en constante evolución, a través de la administración centralizada aprovechando los beneficios de una solución que se administra desde la consola ESET Endpoint Security + File Security, herramienta de gestión de seguridad unificada y basada en la nube, protegiendo los servidores de archivo en múltiples sistemas operativos y plataformas.

Se realizó el 100% de la migración de la consola de administración de antivirus.

Consola Antigua



Consola Nueva



Figura 41: Consola de antivirus eset
Fuente: División de sistemas - UFPSO.



5. LÍMITE Y ALCANCE DEL PLAN DE CONTINUIDAD

Límite: El trabajo se limita a la identificación y análisis de los servicios vulnerables de TI de la UFPS Ocaña, al diseño de las políticas y procedimientos que garanticen la continuidad de las operaciones analizadas previamente y a la elaboración del plan de pruebas y mantenimiento.

Alcance: El desarrollo del plan de continuidad de negocio prepara al proceso SITT de incidentes que impidan continuar con el proceso con el fin de identificar y analizar los elementos críticos y tomar acciones de mejora identificadas de la reacción ante la situación presentada mínimo una vez al año.

A.



6. FASE I. ANÁLISIS DEL NEGOCIO Y EVALUACIÓN DE RIESGOS

Análisis de riesgo (RA).

Una parte importante dentro del desarrollo del plan de continuidad es el análisis de riesgos el cual va a ayudar a identificar los procesos de TI, así como, priorizar cuáles de estos procesos son determinantes para seguir prestando el servicio y gestionarlos en forma adecuada.

Identificación de procesos de TI

El proceso de Sistemas de Información, Telecomunicaciones y Tecnología es un proceso de apoyo a la institución, encargado de la logística tecnológica de los procesos Académicos y/o Administrativos, suministrando soporte técnico, asistencia y asesoría en la adquisición y mantenimiento del software y hardware de la Universidad y entes externos, proponiendo y fijando pautas competitivas para el desarrollo e implementación de software, con el fin de fortalecer los sistemas tecnológicos institucionales y son sus funciones generales:

- Analizar las necesidades relacionadas con las tecnologías de la información en las áreas institucionales (docentes, investigación y servicios administrativos). Contribuyendo con los objetivos, procesos y procedimientos de la Universidad.
- Elaborar planes estratégicos que contemplen las necesidades básicas, para alcanzar objetivos comunes, en beneficio de la Institución.
- Asignar objetivos a las distintas divisiones, seguir el desarrollo de proyecto y actividades, controlar los resultados en materia informática y de telecomunicaciones.
- Gestionar y mantener aplicaciones orientadas a proporcionar información a la comunidad universitaria.
- Llevar a cabo la función gerencial para el desarrollo de los sistemas de información y telecomunicaciones en la Universidad.
- Adecuar los procedimientos en el uso de los sistemas informáticos y las normas de seguridad vigentes e implantar los medios y las medidas necesarias para ello.
- Asesorar, estudiar e implementar soluciones de equipamiento e infraestructura para la red de voz y la red de datos de la Universidad.
- Responder consultas técnicas, de seguridad y documentar la configuración del sistema.
- Prestar asesoramiento a la comunidad universitaria en la adquisición de equipos y programas informáticos de uso común.
- Velar porque las operaciones efectuadas se apliquen correctamente en los sistemas diseñados para cumplir con las necesidades de la Institución.
- Ofrecer soporte a la institución en la adquisición y uso de tecnologías de informática y de telecomunicaciones como apoyo a la administración, la docencia y la investigación.



- Analizar, evaluar, planear y ejecutar los proyectos que favorecen el desarrollo de la informática y las telecomunicaciones en la universidad de acuerdo con las políticas institucionales establecidas.
- Crear y mantener un sistema de información institucional integral y consistente de apoyo a la toma de decisiones de la dirección Universitaria.
- Asesorar en la utilización de sistemas de información a las diferentes dependencias de la Institución.
- Brindar soporte y contratar el mantenimiento de la infraestructura de redes y servidores, equipo de cómputo, servicios de Internet, sistemas de información y sistemas de comunicaciones.
- Fomentar y velar por el buen funcionamiento de los recursos de servicios de información.
- Velar por el cumplimiento de estándares, normas y leyes de uso de servidores de información.
- Efectuar ajustes sobre los sistemas que están operando de acuerdo a las nuevas necesidades.
- Responder ante el director por el cumplimiento de las actividades del personal de la División de Sistemas de la Universidad.
- Responder por el inventario de todos los equipos existentes en la División de Sistemas.
- Las demás que le asignen los reglamentos específicos y el director.

El proceso SITT está conformado de la siguiente manera:

1. Área de soporte y mantenimiento: teniendo entre sus funciones:

- Mantenimiento preventivo y correctivo de equipos
- Activación de puntos de red y/o teléfono
- Administración de cuentas de correo
- Controles de seguridad
- Capacitación al usuario
- Atención al Usuario

2. Área de sistemas de información y desarrollo: en la cual se llevan actividades de:

- Análisis y Desarrollo de aplicaciones de software que para solucionar necesidades detectadas
- Mantenimientos y Actualización en los sistemas de información existentes.
- Apoyar las funciones Académico - administrativas desarrollando soluciones integradas de Sistemas de información, que agilicen los procesos de toma de decisiones institucionales, facilitando los procesos internos y externos que aseguren la confiabilidad de la información en la Universidad.



Vía Acolsure, Sede el Algodonal, Ocaña, Colombia - Código postal: 546552
atencionalciudadano@ufpso.edu.co - www.ufpso.edu.co
Línea de atención: 311 436 1717

3. Área de redes y telecomunicaciones: realizando actividades tales como:

- Proveer la infraestructura tecnológica para el funcionamiento de Internet, redes alámbricas e inalámbricas.
- Administración de servidores.
- Administración de la infraestructura de red.
- Backup, protección y recuperación de la información.
- Administración de salas de cómputo.
- Administración de la base de datos.
- Administración de cámaras de vigilancia y monitoreo.

3.1 Evaluación de vulnerabilidades.

Análisis de impacto (BIA).

En esta etapa, el análisis de impacto del negocio, debe poder clarificar los siguientes requerimientos:

- Identificar las funciones y procesos importantes para la supervivencia de la entidad al momento de la interrupción, esto es tener en cuenta cuales de los procesos son claves para que entren en operación rápidamente asignándoles la mayor prioridad posible, frente a los de menor prioridad; debe quedar claro que para los procesos identificados como no tan prioritarios se deben preparar también planes de recuperación.
- Estimar los tiempos de recuperación, en razón a las posibles alteraciones de los procesos considerados de alta prioridad para el funcionamiento de las infraestructuras de TI.

3.1.2 Identificación de Funciones y Procesos.

Este punto tiene como resultado generar un listado de roles y procesos, que sirven de análisis para el cumplimiento de los siguientes pasos del BIA.

3.1.3 Evaluación de Impactos Operacionales.

El impacto operacional permite evaluar el nivel negativo de una interrupción en varios aspectos de las operaciones de TI; el impacto se puede medir utilizando un esquema de valoración, con los siguientes niveles: A, B o C.

- **Nivel A:** La operación es crítica del negocio. Una operación es crítica cuando al no contar con ésta, la función del negocio no puede realizarse.
- **Nivel B:** La operación es una parte integral del negocio, sin ésta el negocio no podría operar normalmente, pero la función no es crítica.



- **Nivel C:** La operación no es una parte integral del negocio.

La tabla siguiente muestra los niveles de criticidad en la Institución, contemplando un sistema de tolerancia a fallas por horas, cuya propiedad permite que un sistema pueda seguir operando normalmente a pesar de que una falla haya ocurrido en alguno de los componentes del sistema; por lo tanto, la tolerancia a fallas es muy importante en aquellos sistemas que deben funcionar todo el tiempo.

Categoría (Función del Negocio)	Proceso (Servicios)	Nivel	Tolerancia a Fallas (Horas)	Descripción
Sistema de Información de Admisiones, Registro y Control	Gestiona procesos de preinscripción, inscripción, admisión, matrícula y egresados.	A	4–8 horas	Crítico para la gestión académica. Su interrupción afecta directamente la operación administrativa y académica.
Sistema de Gestión Académica	Administra información de estudiantes, docentes, horarios, pensum y reportes.	B	4–8 horas	Fundamental para la programación académica y la gestión de actividades docentes. Su caída puede afectar la planificación de clases y la comunicación con estudiantes y docentes.
Redes y Telecomunicaciones	Infraestructura de redes alámbricas e inalámbricas, administración de servidores y backups.	A	30 minutos	Esencial para la conectividad y el funcionamiento de todos los sistemas. Su falla puede paralizar la operación de la universidad.

Tabla 4: Criticidad Institucional
Fuente: División de sistemas - UFPSO.

3.1.4 Identificación de Procesos Críticos

La identificación de los procesos críticos del negocio se da con base en la clasificación de los impactos operacionales de las organizaciones, según esta tabla:

Valor	Interpretación del proceso crítico
Matrículas estudiantiles	Procesos sensibles al calendario académico. Interrupción causa caos operativo.
Plataforma académica (clases virtuales)	Impacto directo en la enseñanza-aprendizaje.
Sistema financiero y pagos	Permite cierto retraso antes de afectar operaciones.
Sistema de correo institucional	Soporta comunicación crítica, pero puede tener respaldo alternativo.
Sistema de biblioteca virtual	Impacto menor si se interrumpe brevemente.
Página web institucional	Informativa, no transaccional.

Tabla 5: Procesos Críticos
Fuente: División de sistemas - UFPSO.

3.1.5 Establecimiento de Tiempos de Recuperación

Una vez identificados los procesos críticos del negocio, se deben establecer los tiempos de recuperación que son una serie de componentes correspondientes al tiempo disponible para recuperarse de una alteración o falla de los servicios; el entendimiento de estos componentes es fundamental para comprender el BIA. Los tiempos de recuperación se describen a continuación:

Tiempo de Recuperación	Descripción
3 días o más	Procesos NO Críticos
1 a 3 días	Procesos Moderados
8 horas a 1 día	Procesos Importantes
30min a 8 horas	Procesos Críticos

Tabla 6: Tiempo de Recuperación
Fuente: División de sistemas - UFPSO.

3.1.6 Gestión del Riesgo

La gestión del riesgo debe contemplar el cálculo del riesgo, la apreciación de su impacto en el negocio y la posibilidad de ocurrencia.

A pesar de la existencia de diversidad de métodos es recomendable iniciar con los más sencillos, que forman parte de lo que denominamos análisis previos.



3.1.7 Clasificación de escenarios de riesgo

A fin de conocer con precisión los riesgos potenciales de la prestación de servicios de tecnologías de la información en las Entidades, es recomendable clasificar los posibles escenarios de los riesgos potenciales y describir su nivel de impacto por cada función crítica del negocio. La siguiente tabla describe un ejemplo de esta clasificación.

Categorías	Escenarios	Descripción Impacto
Riesgos Tecnológicos	Fallas en el Fluido Eléctrico.	- Daño en equipos. - Pérdida de Información.
	Sabotaje Informático.	- Pérdida de elementos.
	Fallas en el Centro de Datos.	-Perdida o daño de información de salida, o conocimiento de información confidencial.
	Problemas Técnicos.	-Perdida de la veracidad de los datos.
	Fallas en equipos tanto de procesamiento, de telecomunicaciones como eléctricos.	-Pérdidas económicas. -Inestabilidad de los procesos.
	Servicios de Soporte a Sistemas de Producción y/o Servicios.	-Toma de decisiones errada.
Riesgos Humanos	Robos.	-Daño en equipos.
	Acto Hostil.	-Posibilidad de Incendio.
	Marchas, mítines.	-Perdida de información
	Artefactos explosivos.	-Toma de decisiones errada.
	Problemas organizacionales (huelgas, leyes aceptadas por el congreso, regulaciones gubernamentales, leyes internacionales)	-Desorden. -Pérdida de la confianza en el equipo humano de Ti.
	Problemas de terceros involucrados en la producción o soporte a un servicio.	-Condiciones no seguras de los proveedores. -Pérdidas económicas.
	Problemas con los proveedores de insumos o subproductos.	-Perdida de la comunicación interna y externa.
	Pandemias	-Inestabilidad de los procesos.
Desastres Naturales	Sismos	-Daño en equipos.
	Tormentas Eléctricas	-Posibilidad de Incendio.
	Incendios	-Perdida de información
	Inundaciones	-Pérdidas económicas

Tabla 7: Escenarios de riesgo
Fuente: División de sistemas - UFPSO.

3.1.8 Metodología del Riesgo

Es importante determinar los riesgos a los que están enfrentadas las infraestructuras de TI de las organizaciones con base en la identificación tanto de amenazas como de vulnerabilidades.

3.1.9 Identificación de amenazas

Norma NTC/ISO 22301

La Gestión de la Continuidad del Negocio (BCM) es un proceso de gestión que identifica amenazas potenciales y riesgos de tipo operacional a la institución y provee una estructura para construir confiabilidad y capacidades para una efectiva respuesta que proteja los intereses a nivel institucional, también involucra la gestión de la recuperación y continuidad después de un incidente y la gestión de todo el programa por medio de entrenamientos, pruebas, y revisiones para mantener el BCP al día.

El propósito principal de esta fase es conocer cuáles amenazas o riesgos específicos enfrenta la UFPSO en sus procesos y productos críticos del negocio, identificados como resultado del Análisis de Impacto al Negocio (BIA), con el fin de determinar la forma en que algunos riesgos serán controlados y mitigados a un nivel aceptable según criterios previamente definidos.

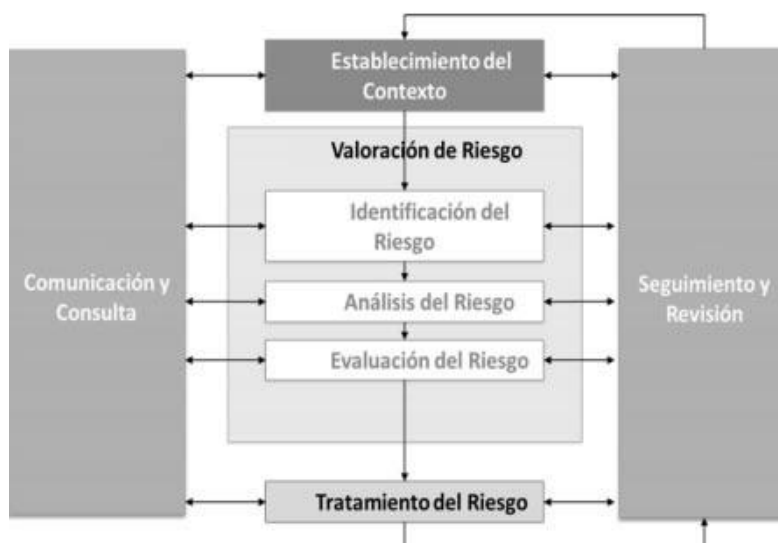


Figura 42: Evaluación/Identificación del Riesgo

Fuente: División de sistemas – UFPSO

Es conveniente mencionar que durante esta fase los riesgos (operativos) se analizarán desde la perspectiva de la continuidad del negocio considerando personas, servidores, edificios, tecnología, entre otros, sin dejar de lado su relación directa con los procesos

determinados como críticos. El tipo de vulnerabilidades y amenazas al que se ven expuestos estos activos varía dependiendo de la naturaleza de los mismos. Las amenazas y vulnerabilidades que se incluyen para el caso específico del proyecto, serán las relacionadas con la no disponibilidad (operación) de los activos asociados a los procesos críticos del negocio. Ahora bien, parte importante de contar con un BCP, es el hecho de realizar una efectiva gestión de riesgo y así evitar las recursivas activaciones del sitio alternativo, actividad que tiene sus propios riesgos, costos y dificultades.

En esta etapa, se analizaron las amenazas y vulnerabilidades identificadas previamente, analizando el escenario donde puede materializarse el riesgo de interrupción, así como su origen y las afectaciones potenciales a los activos, el análisis contempló 12 escenarios de riesgo que se describen a continuación:

1. Acceso a la edificación: Relaciona los controles, los procedimientos y las buenas prácticas que permiten mitigar el riesgo de que personal no autorizado ingrese a las instalaciones y pueda generar daños a los activos de la organización.
2. Administración y entorno tecnológico: Relaciona los hábitos y las buenas prácticas que permiten administrar, asegurar, disponer y controlar los sistemas tecnológicos, de tal forma que estén alineados con los estándares internacionales y regulaciones nacionales en temas de seguridad de la información.
3. Construcción del edificio y materiales: Relaciona los materiales de construcción, alternativas de mitigación y resistencia frente a riesgos naturales
4. Información y administración del edificio: Relaciona procedimientos de seguridad, responsabilidades del personal, cultura y capacitación para responder a incidentes en el edificio.
5. Oficina y estaciones de trabajo: Relaciona las políticas de seguridad de la información definidas por la compañía y las buenas prácticas del personal que aseguren, en el evento de una interrupción del negocio, la disponibilidad, confidencialidad, seguridad e integridad de la información.
6. Perímetro y estacionamiento: Relaciona los controles, las políticas y los procedimientos que permitan evitar y responder frente a incidentes de seguridad en el perímetro de la compañía.



7. Protección anti-incendios: Relaciona la capacitación del personal, los equipos de extinción y los sistemas de control que permitan responder rápida y eficientemente a un incendio en el edificio y/o en el centro de cómputo.
8. Riesgos entorno geográfico: Relaciona las fuentes latentes de riesgo aledañas a la organización.
9. Riesgos naturales: Relaciona los aspectos de ubicación geográfica, climática y del entorno natural que puedan afectar a la compañía.
10. Riesgos potencia eléctrica: Relaciona las políticas, los controles y los procedimientos que permitan asegurar el suministro de energía eléctrica al edificio y equipos críticos.
11. Riesgos telecomunicaciones: Relaciona las políticas, los controles y los procedimientos que permitan mantener la comunicación (voz y datos) de la organización.
- 12.. Centro de datos: Relaciona, los controles, infraestructura y procedimientos definidos para los centros de datos (principal y contingencia)



ESTRATEGIAS DE CONTINUIDAD

Una estrategia de continuidad es un mecanismo que permite la recuperación y continuidad de las funciones críticas de una organización frente a un desastre o una interrupción mayor. Son consideradas como estrategias no sólo los recursos y actividades requeridas frente a la interrupción, sino los requeridos para mitigar la probabilidad de ocurrencia y el impacto de la interrupción.

Para definir las estrategias de continuidades posibles o viables, de manera efectiva y eficiente, se debe contar con un entendimiento sobre los siguientes aspectos:

1. Resultados del Análisis de Impacto al Negocio (BIA).
2. Tiempos y puntos objetivo de recuperación (RTO y RPO) requeridos para los procesos críticos.
3. Procesos críticos a soportar.
4. Porcentaje aceptable de degradación de la operación del proceso.
5. Aspectos de carácter jurídico que se deben cumplir según la naturaleza del proceso al momento de implementar una estrategia de recuperación.
6. Resultados del análisis de riesgos y las alternativas de tratamiento de riesgo a implementar sobre los activos asociados a los procesos.
7. Amenazas posibles a los activos de los procesos.
8. Vulnerabilidades existentes en los activos de los procesos.

El propósito de esta fase consiste en seleccionar las estrategias de recuperación o continuidad, orientadas a brindarle confiabilidad a los servicios, considerando los resultados del BIA, la evaluación de riesgos y complementado lo anterior, con la realización de un análisis cuantitativo de los elementos requeridos para la recuperación. Parte del desarrollo involucró la definición de los escenarios de interrupción, las amenazas que los pudieran generar y las diferentes alternativas operativas para enfrentar una posible materialización. En la siguiente tabla se visualiza la información referente:



ESCENARIOS					
AMENAZAS	Infraestructura No Disponible	TI No Disponible	Recuso humano No disponible	Proveedor No Disponible	Información no disponible
	- Incendio. - Inundación. - Actos de violencia (Terremoto). - Cierre Parcial.	- Falla Eléctrica. - Incendio. - Inundación. - Terremoto. - Falla Tecnológica.	- Incendio. - Actos de violencia. - Terremoto. - Cierre Parcial. - Ausencia, retiro, muerte de un funcionario. - Pandemia.	- Falla eléctrica. - Incendio. - Inundación. - Terremoto. - Falla Tecnológica.	- Falla eléctrica. - Incendio. - Inundación. - Sismo. - Terremoto. - Fallas tecnológicas en comunicaciones, Hardware, Software, bases de datos. - Error Humano. - Hurto o Robo.

Tabla 8. Escenarios de Interrupción, amenazas y Alternativas Operativas
Fuente: División de sistemas - UFPSO.

La siguiente es la relación de alternativas operacionales que tiene la institución, para recuperar la funcionalidad de sus procesos críticos en términos de la ausencia de alguno(s) de sus recursos claves, estas estrategias pueden permitir la continuidad de sus operaciones más importantes en un nivel aceptable y buscan principalmente cumplir y satisfacer los requerimientos del producto solicitado por sus clientes, después de un evento de interrupción:

ESCENARIOS					
ALTERNATIVAS OPERATIVAS	Infraestructura No Disponible	TI No Disponible	Recurso Humano No Disponible	Proveedor No Disponible	Información No Disponible
	- Trabajo a Distancia. - Acuerdo con terceros. - Respaldo entre sedes. - Centro de trabajo alternativo.	Estrategia DRP.	- Definición de la estructura de recuperación en cascada (ERC). - Capacitación. - Rotación. - Documentación de procedimientos.	- Definir proveedores alternos. - Definir acuerdos de niveles de Servicio específicos para BCM.	- Respaldo de la información clave del proceso (Backup). - Proveedores y/o medios alternos para el servicio de comunicación.

Tabla 9. Escenarios de Interrupción, amenazas y Alternativas Operativas
Fuente: División de sistemas - UFPSO.



7. FASE II. ESTRATEGIAS DE RESPALDO

1. Identificación de sistemas y recursos críticos

Nombre del área o grupo	Dependencias	Accesos / Programas
Casona	DIE Secretaría general Subdirección administrativa Tesorería Subdirección académica Gestión Humana Presupuesto Contabilidad Control interno	SIA, SIB, SIF, SID, PQRS, SIABE, SIBU, SIIN, SICI, Portal Planeación, Portal Divisis, SGH, SIAA, SIAPP, Internet
Anexos	Planes de estudio	
Edificio de Ingenierías	Planes de estudio Ingeniería	
División de Sistemas	División de Sistemas	
Edificio Administrativo	Admisiones, Registro y Control Dirección	
Sede Bellas Artes	Escuela de Artes	
Sede Primavera - Invías	UFM Laboratorios	

Tabla 10: Sistemas y servicios sistematizados críticos para la UFPSO

Fuente: División de sistemas - UFPSO.

2. Estrategias de respaldo seleccionadas

Servidores
✓ Un Sistema de Alta Disponibilidad, Backup & Replicación de Servicios. ✓ Dos Sistemas SAN para la Virtualización, para ofrecer alta disponibilidad, Backup & Replicación en los servicios ✓ 12 servidores Físicos en la sede Algodonal. ✓ 48 Máquinas virtualizados en Sistema Operativo Linux. ✓ 1 Estación de trabajo para transmisión de la emisora UFM ✓ 1 Servidor para emisión de Streaming de la emisora UFM. ✓ 1 Servidor para emisión de video de alta performance.

Tabla 10: sistema de alta disponibilidad, backup & recopilación de los servidores

Fuente: División de sistemas - UFPSO.



Nota: La tabla anteriormente descrita se lleva diligenciada de manera interna en el proceso SITT, no se consignan los datos en este documento por la sensibilidad del nombre del servidor.

Es crucial para asegurar que una organización pueda continuar operando ante una interrupción inesperada. Las **estrategias de respaldo (o backup)** son una parte fundamental de este plan, ya que garantizan la recuperación de datos, sistemas y operaciones críticas.

2.1. Respaldo de datos

Objetivo: Asegurar que los datos importantes estén protegidos y disponibles tras una pérdida.

Estrategias:

- **3-2-1 Backup:** Mantener **3 copias** de los datos en **2 medios distintos**, con **1 copia fuera del sitio** (por ejemplo, en la nube).
- **Automatización de respaldos:** Programar respaldos diarios, semanales o mensuales según la criticidad de los datos.
- **Cifrado de respaldo:** Asegurar que los datos estén encriptados tanto en tránsito como en reposo.
- **Pruebas periódicas de restauración:** Para verificar que los respaldos funcionan correctamente.
- **Versionado de archivos:** Guardar múltiples versiones para recuperación ante errores humanos o ransomware.

2.2. Respaldo en la nube

Objetivo: Proteger los datos contra desastres físicos (incendios, robos, etc.).

Estrategias:

- Utilizar servicios de backup en la nube como **AWS Backup, Azure Backup, Google Cloud Storage, Veeam**, etc.
- Asegurar redundancia geográfica: elegir un proveedor que replique los datos en múltiples regiones.
- Monitorear el uso y la integridad del respaldo en la nube.

2.3. Respaldo de sistemas y aplicaciones

Objetivo: Recuperar servidores, sistemas operativos y aplicaciones críticas.



Estrategias:

- Imágenes completas de sistemas: crear copias exactas (snapshots) de máquinas físicas o virtuales.
- Respaldo de configuraciones (por ejemplo, firewalls, routers, servidores).
- Contenedores y automatización (ej. Docker + Kubernetes) para facilitar la reimplementación de sistemas.

2.4. Respaldo de la infraestructura física

Objetivo: Restaurar operaciones físicas mínimas en caso de pérdida total o parcial.

Estrategias:

- Contratos con centros de datos alternativos o espacios de trabajo temporales.
- Red de proveedores alternativos para suministros críticos.
- Equipos redundantes (generadores, servidores, estaciones de trabajo).

2.5. Respaldo del personal y operaciones

Objetivo: Asegurar que el personal pueda seguir trabajando.

Estrategias:

- Manuales de operaciones y procedimientos documentados.
- Capacitación cruzada de empleados clave.
- Acceso remoto seguro para trabajar desde casa (VPN, escritorios virtuales).
- Roles y contactos de emergencia definidos.

2.6. Documentación y pruebas

Objetivo: Garantizar la eficacia del plan de respaldo.

Estrategias:

- Documentar todas las estrategias de respaldo y recuperación.
- Simulacros regulares de recuperación ante desastres (DRP).
- Revisión y actualización del plan de respaldo cada 6-12 meses.

3. Estrategias de trabajo remoto o reubicación de personal

- Implementación de las políticas de **teletrabajo** con acceso seguro (VPN, autenticación multifactorial).



- Capacitación al personal en el uso de herramientas de colaboración remota.
- Contratación de espacios temporales de coworking o sedes alternas para personal esencial.
- Plan de comunicación interna para activación de protocolos de trabajo remoto.



8. FASE III. DESARROLLO DEL PLAN

En esta fase se documenta todo lo planificado: cómo actuar ante diferentes tipos de interrupciones y quién debe hacerlo.

1. Definición de roles y responsabilidades

Se asignan responsabilidades claras a personal clave:

ROL	CARGO
Responsable de la ejecución del Plan de Contingencia	Jefe de la División de Sistemas
Administrador de Servidores y Servicios a la web	Profesional Universitario División de Sistemas
Administrador de Telecomunicaciones	Profesional Universitario División de Sistemas
Técnico de Telecomunicaciones	
Técnicos de Mantenimiento de Hardware y Software	Auxiliar del centro de cómputo y sistemas
Administradores de SI y Desarrolladores de Software y Apps	Profesional Universitario División de Sistemas
Profesionales de apoyo a Calidad, Acreditación y Autoevaluación	Profesional Universitario División de Sistemas

Tabla 11: Roles y Responsabilidades del Equipo de Trabajo.

Fuente: División de sistemas - UFPSO.

2. Procedimientos paso a paso para respuesta a incidentes

Los procedimientos deben ser específicos para distintos escenarios:

Riesgo	Causa	Acciones
Fallas eléctricas. Electromagnetismo Sobrecarga eléctrica Falla de corriente (apagones)	Cableado eléctrico Sobrecargado de equipos. Condiciones no seguras del proveedor del servicio eléctrico. Condición física y ubicación geográfica del edificio	-Evitar el riesgo. -Monitorear y proponer si es el caso nuevos diseños de la red eléctrica y cambiar la actual con protectores tanto eléctricos como contra incendios. -Adquirir e instalar una planta eléctrica. Instalar más estabilizadores y ampliar los puntos eléctricos.
Desactualización del Software de verificación estado de la red	En la red de comunicaciones se presentan problemas tecnológicos y humanos que hacen que la comunicación de información se haga muy lentamente Mantenimientos mal hechos	-Evitar el riesgo. -Adquirir software a la medida de la red que tiene en la institución con el fin de poder solucionar los problemas con la debida anticipación. -Monitorear periódicamente los diagnósticos y estados de la red arrojados por el sistema Diligenciar bitácoras de control
Entrada física de personal no autorizado	No se tienen sistemas de seguridad ni protocolos de acceso	-Evitar el riesgo. -Adquirir sistemas de seguridad que permitan verificar identidad y permisos de acceso de quien ingresa a la división de

		sistemas y específicamente a los cuartos y salas de servidores o racks.
Pérdida de información por virus informáticos Utilización de programas no autorizados / software 'pirateado'	Falta de licencias y paquetes de programas actualizados y con soporte del proveedor Falta de controles en el acceso a páginas no autorizadas de Internet	-Evitar el riesgo. -Adquirir licencias de antivirus que detecten cualquier virus informático -Jornadas de capacitación al usuario sobre uso y manejo de la información -Administración y control de accesos -Implementación de políticas de comunicaciones -Control y monitoreo sobre uso e instalación de programas al usuario
Polvo / Falta de ventilación Falla de sistema / Daño disco duro	Falta de mantenimientos preventivos Desconocimiento del personal técnico sobre estándares informáticos Descuido y falta de organización en los insumos e inventario de partes	-Evitar el riesgo. -Planes de mantenimiento preventivo periódicos -Capacitación al usuario sobre uso de equipos -Monitoreo y supervisión de las condiciones físicas y lógicas -Información actualizada resguardada en un datacenter -Actualización y mantenimiento del stock de partes y dispositivos
Manejo inadecuado de datos críticos (codificar, borrar, etc.) Transmisión no cifrada de datos críticos Manejo inadecuado de contraseñas (inseguras, no cambiar, BD centralizada) Uso indebido de la información	Falta de políticas y estándares de desarrollo Falta de control de tareas, funciones y responsabilidades definidas Inadecuado uso de metodologías de desarrollo y control sobre requerimientos del cliente Falta de definición de perfil, privilegios y restricciones Ausencia de documentación Fraude interno Bajo nivel de seguridad para acceso	-Evitar el riesgo. -Actualización de registros de desarrollo -Uso de estándares de documentación de código fuente -Actualización del diccionario de datos -Aprobación y revisión de diseño preliminar de software -Protocolos de acceso y uso de base de datos y servidores -Administración de cuentas y roles de usuario -Capacitación al usuario -Encriptamiento -Protocolo de interfaces de usuario y acceso a los SI
Vulnerabilidad de los sistemas de información	Cortafuegos inadecuados Falta de definición de perfil, privilegios y restricciones Bajo nivel de seguridad para el acceso a la información	-Evitar el riesgo -Administración de cuentas y roles de usuario -Encriptamiento -Protocolo de interfaces de usuario y acceso a los SI -Monitoreo y control de accesos -Actualización permanente de programas y paquetes de seguridad
Ausencia y/o deficiencia de las redes de voz y datos	Equipos activos y pasivos de red obsoletos	-Evitar el riesgo -Planes de mantenimiento preventivo periódicos



		-Capacitación al usuario sobre uso de equipos -Monitoreo y supervisión de las condiciones físicas de los equipos y redes -Adecuado stock e inventario
Emergencia Sanitaria	Protocolos de bioseguridad establecidos por el Ministerio de Salud, Secretarías de Salud Departamental y Municipal y el SGSST de la Universidad (Aforo máximo en oficinas y otras disposiciones)	-Evitar el riesgo -Seguir los protocolos de bioseguridad establecidos por el gobierno y el equipo de - SGSST de la Universidad -Trabajo remoto desde casa a través de VPN -Aplicación de protocolos de autenticación (LDAP) -Préstamo de equipos tecnológicos para trabajo remoto -Trabajo colaborativo Suite de Google (Gmail, Docs, Forms, Calendar, Classroom, Jamboard, Drive) -Mensajería instantánea de Google Hangouts -Videoconferencias a través de Zoom, Meet -Renata, VC-Expreso

Tabla 12: Riesgos, Causas y Acciones paso a paso en respuesta de accidentes

Fuente: División de sistemas - UFPSO.

3. Planes de comunicación interna y externa

Comunicación interna:

- Canales oficiales: correo institucional, sistema de mensajería interna, llamadas.
- Plantillas de mensajes para situaciones específicas.
- Frecuencia y responsables de actualización del personal.

Comunicación externa:

- Protocolos para informar a usuarios, proveedores, autoridades y medios.
- Designación de voceros oficiales.
- Comunicación a través de página web, redes sociales, notas de prensa o llamadas directas.

4. Planes de evacuación, traslado de operaciones, activación del sitio alterno

- **Evacuación:**
 - Mapas de rutas de salida, puntos de encuentro.
 - Responsables de guiar evacuaciones por área.
 - Registros de asistencia y protocolos de emergencia médica.
- **Traslado de operaciones:**



- Identificación de procesos que pueden ser movidos a otra sede o realizarse de forma remota.
- Logística de transporte de equipos y documentos.
- **Activación del sitio alternativo:**
 - Procedimientos para cambiar operaciones al sitio de recuperación (caliente, tibio o frío).
 - Verificación de sistemas, personal y conectividad en el sitio alternativo.



9. FASE IV. PRUEBAS Y MANTENIMIENTO

En esta fase de pruebas y mantenimiento se verifica que el plan funciona correctamente y se mantiene actualizado con el tiempo, de la siguiente manera:

1. Pruebas regulares del plan

Realizar pruebas periódicas permite detectar fallos, evaluar tiempos de respuesta y garantizar que todos los involucrados conozcan sus responsabilidades.

a) Tipos de pruebas

- **Simulacros de evacuación:**
 - Ensayos prácticos con todo el personal para validar rutas de evacuación, puntos de reunión y tiempo de respuesta.
 - Evaluación posterior para corregir deficiencias detectadas.
- **Simulacros de recuperación de operaciones:**
 - Ejecución controlada del Plan de Continuidad (BCP) ante distintos escenarios (fallo de red, incendio, ciberataque, etc.).
- **Pruebas de restauración de sistemas desde respaldos:**
 - Recuperación real o simulada de bases de datos, servidores o archivos críticos para validar la integridad y tiempo de recuperación (RTO/RPO).
- **Pruebas de comunicación:**
 - Validación de los canales internos y externos, mensajes automáticos, líneas de emergencia y tiempo de respuesta de los equipos.

b) Frecuencia recomendada

- Simulacros generales: cada 6 o 12 meses.
- Pruebas de restauración de datos: cada 3 meses.
- Simulacros de evacuación: mínimo una vez al año o según normativa local.
- Pruebas de comunicación: trimestral.

2. Revisión posterior a cada prueba

Después de cada prueba, se debe realizar un **informe de evaluación** que incluya:

- Resultados obtenidos vs. objetivos previstos.
- Incidencias detectadas.
- Tiempos reales de respuesta y recuperación.
- Observaciones del personal participante.
- Recomendaciones de mejora.



Acciones correctivas deben ser implementadas y documentadas.

3. Actualización del plan

El plan debe actualizarse siempre que ocurra un cambio significativo en:

- **Estructura organizacional:** cambios de personal clave, creación/eliminación de áreas.
- **Tecnología:** actualización o reemplazo de sistemas críticos.
- **Procesos:** nuevas operaciones, eliminación de procesos antiguos o tercerización.
- **Infraestructura física:** mudanza, ampliación o cierre de oficinas.
- **Resultados de pruebas:** ajustes según fallos detectados en simulacros.

Responsables del plan deben revisar y validar versiones actualizadas, garantizando su distribución a todas las áreas afectadas.

4. Capacitación continua al personal

El personal debe estar permanentemente capacitado para responder de forma eficaz ante incidentes.

Estrategias de capacitación:

- Inducción obligatoria para nuevo personal.
- Talleres anuales por áreas sobre el BCP y DRP.
- Simulacros participativos y sesiones de retroalimentación.
- Materiales de apoyo: manuales, infografías, videos instructivos.

Objetivo de la capacitación:

- Asegurar que todos conozcan sus roles.
- Fomentar la cultura de prevención y respuesta.
- Reducir la improvisación durante una emergencia.



ELABORO:	REVISÓ:	APROBO:
	COORDINADOR SIG	LIDER DEL PROCESO

FECHA	CONTROL DE CAMBIOS	REVISIÓN

