UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES E INFORMÁTICOS

Tema:

ANÁLISIS DE RIESGO Y DISEÑO DE PLAN DE CONTINGENCIA PARA RECUPERACIÓN ANTE DESASTRES EN FLORIDA EDUCATION INSTITUTE (FL-USA) SEGÚN LA NORMA ISO 24762-2008.

Trabajo de Titulación Modalidad: Proyecto de Investigación, presentado previo a la obtención del título de Ingeniero en Sistemas Computacionales e Informáticos

ÁREA: Administrativas Informáticas

LÍNEA DE INVESTIGACIÓN: Normas y Estándares

AUTOR: Benjamín Paúl Montesdeoca López

TUTOR: Ing. Julio Enrique Balarezo, PhD.

Ambato - Ecuador

septiembre - 2022

APROBACIÓN DEL TUTOR

En calidad de tutor del Trabajo de Titulación sobre el tema: ANÁLISIS DE RIESGO Y DISEÑO DE PLAN DE CONTINGENCIA PARA RECUPERACIÓN ANTE DESASTRES EN FLORIDA EDUCATION INSTITUTE (FL-USA) SEGÚN LA NORMA ISO 24762-2008, desarrollado bajo la modalidad de Proyecto de Investigación por el señor Benjamín Paúl Montesdeoca López, estudiante de la Carrera de Ingeniería en Sistemas Computacionales e Informáticos, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, me permito indicar que el estudiante ha sido tutorado durante todo el desarrollo del trabajo hasta su conclusión, de acuerdo a lo dispuesto en el Artículo 15 del Reglamento para obtener el Título de Tercer Nivel, de Grado de la Universidad Técnica de Ambato, y el numeral 7.4 del respectivo instructivo.

Ambato, septiembre 2022

Firmado electrónicamente por:
JULIO ENRIQUE BALAREZO LOPEZ

. . . . . .

Ing. Julio Enrique Balarezo, PhD.

EL TUTOR

AUTORÍA

El presente Proyecto de Investigación titulado: ANÁLISIS DE RIESGO Y DISEÑO DE PLAN DE CONTINGENCIA PARA RECUPERACIÓN ANTE DESASTRES EN FLORIDA EDUCATION INST1TUTE (FL-USA) SEGÚN LA NORMA ISO 24762-2008 es absolutamente original, auténtico y personal. En tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato, septiembre 2022

Benjamín Paúl Montesdeoca López

CC: 1804181400

AUTOR

APROBACIÓN TRIBUNAL DE GRADO

En calidad de par calificador del Informe Final del Trabajo de Titulación presentado por el señor Benjamín Paúl Montesdeoca López, estudiante de la Carrera de Ingeniería en Sistemas Computacionales e Informáticos, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial , bajo la Modalidad Proyecto de Investigación , titulado ANÁLISIS DE RIESGO Y DISEÑO DE PLAN DE CONTINGENCIA PARA RECUPERACIÓN ANTE DESASTRES EN FLORIDA EDUCATION INSTITUTE (FL-USA) SEGÚN LA NORMA ISO 24762-2008, nos permitimos informar que el trabajo ha sido revisado y calificado de acuerdo al Artículo 17 del Reglamento para obtener el Título de Tercer Nivel, de Grado de la Universidad Técnica de Ambato, y al numeral 7.6 del respectivo instructivo. Para cuya constancia suscribimos, conjuntamente con la señora Presidente del Tribunal.

Ambato, septiembre 2022.

Firmado electrónicamente por:
ELSA PILAR URRUTIA

Ing. Pilar Urrutia, Mg.
PRESIDENTE DEL TRIBUNAL

Firmado electrónicamente por:
FELIX OSCAR FERNANDEZ PENA

Ing. PhD. Felix Fernandez
PROFESOR CALIFICADOR

Firmado electrónicamente por:
LEONARDO DAVID TORRES VALVERDE

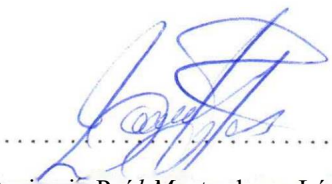
Ing. Leonardo Torres, Mg.
PROFESOR CALIFICADOR

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que haga uso de este Trabajo de Titulación como un documento disponible para la lectura, consulta y procesos de investigación.

Cedo los derechos de mi Trabajo de Titulación en favor de la Universidad Técnica de Ambato, con fines de difusión pública. Además, autorizo su reproducción total o parcial dentro de las regulaciones de la institución.

Ambato, septiembre 2022



Benjamin Paúl Montesdeoca López

CC: 1804181400
AUTOR

Dedicatoria

Dedico este proyecto a mi familia, quienes son pilar fundamental en mi vida y gracias a su apoyo incondicional me han permitido llegar a cumplir una de mis metas en el ambito academico.

A las personas que han sido parte de mi vida estudiantil, que me ha visto caer y levantarme y sin embargo estuvieron a mi lado para brindarme un aliento de ánimo.

A las personas que laboralmente me han apoyado con un consejo para poder llegar al fin de mi carrera universitaria.

Benjamín Paúl Montesdeoca López

Agradecimiento

Agradezco a mi familia por el gran apoyo que me ha brindado, por ser la fuente de mi fuerza y el coraje para no decaer ante este gran reto que Dios ha puesto en mi vida y que gracias a ellos lo he logrado.

A Alexandra Campaña y Ramon Valenti directivos de Florida education institute, quienes me han dado su confianza para la administracion de su area tecnologica y han permitido que pueda desarrollar este proyecto de investigacion.

A mi tutor Ing. PhD Julio Balarezo, quien me ha guiado correctamente en el desarrollo de mi proyecto de investigacion, brindandome sabios consejos para el avance eficiente y finalización del mismo.

A mi distingida FISEI a través de sus docentes y personal administrativo, quienes han contribuido en mi superación académica y el logro de mi titulo profesional.

Benjamín Paúl Montesdeoca López

Índice

Índice de figuras

Índice de cuadros

RESUMEN EJECUTIVO

En el mundo empresarial como en el de cualquier organización o entidad, que manejan información vital de sus clientes se enfrentan a varios problemas referentes al área tecnológica, especialmente al tratarse de almacenar, asegurar y recuperar todos los datos después de varios escenarios, así como, un ataque o mal uso de los equipos informáticos, obsolescencia en los servidores y hasta catástrofes naturales que pueden perjudicar y dañar toda la infraestructura establecida en la institución lo que conlleva a la pérdida de información, por lo cual perjudica a la cadena de negocio haciendo que las actividades diarias vuelvan un suplicio para los usuarios.

Para enfrentar estos problemas es de vital importancia tener un plan de contingencia que permita estar preparado ante cualquier eventualidad que pueda causar un gran daño dentro de cualquier organización y ser consiente de todo lo que puede ocurrir a nivel de desastres naturales o ataques directos a la información de las empresas.

Es por eso que Florida Education Institute (FEI) ha permitido crear un plan de contingencia para su área de tecnologías de la información, donde se procedió a evaluar los riesgos y falencias dentro de este departamento y tomar los correctivos necesarios para evitar cualquier tipo de problema en el futuro.

Se utilizó la norma ISO 24762-2008, debido a que toma en cuenta aspectos como el uso de servicios de otras empresas que proveen de soluciones informáticas a FEI con lo cual se evaluó si todo funciona correctamente y si se tiene las garantías correspondientes para operar con estas herramientas externas.

Al concluir el proyecto se obtuvo un plan de contigencia a la medida de los requerimientos y observaciones obtenidas de FEI con lo cual la institución puede estar preparada para la mayoría de riesgos que pueda existir y tener el conocimiento de que hacer ante estos problemas y solucionarlos de manera rápida y eficiente.

Palabras clave: norma, ISO, plan, contingencia, riesgos

ABSTRACT

In the business world as in that of any organization or entity, which handle vital information of their clients face several problems related to the technological area, especially when it comes to storing, securing and recovering all the data after various scenarios such as an attack or misuse of computer equipment, obsolescence in servers and even natural catastrophes that can harm and damage the entire infrastructure established in the institution, which leads to the loss of information, which harms the business chain, making daily activities an ordeal for users.

To deal with these problems, it is vitally important to have a contingency plan that allows you to be prepared for any eventuality that can cause great damage within any organization and to be aware of everything that can happen at the level of natural disasters or direct attacks on information of the companies.

That is why the Florida Education Institute (FEI) has allowed the creation of a contingency plan for its information technology area, where the risks and shortcomings within this department were evaluated and the necessary corrective measures were taken to avoid any type of problem in the future.

The ISO 24762-2008 standard was used, because it takes into account aspects such as the use of services from other companies that provide computer solutions to FEI, with which it was evaluated if everything works correctly and if there are the corresponding guarantees to operate with these external tools.

At the end of the project, a contingency plan was obtained tailored to the requirements and observations obtained from FEI, with which the institution can be prepared for most risks that may exist and have the knowledge of what to do in the face of these problems and solve them in a timely manner fast and efficient way.

Keywords: standard, ISO, plan, contingency, risks

INTRODUCCIÓN

Florida Education Institute (FEI) es una institución de educación técnica que maneja una gran cantidad de procesos y datos que pueden ser propensos ataques informáticos, o que por cualquier otra circunstancia se pueden perder, por lo tanto se ha propuesto crear un plan de contigencia ante estos riesgos mediante la utilización de normativas internacionales como es la norma ISO 24762-2008, la cual se adapta perfectamente a las necesidades que FEI requiere.

Debido a que FEI utiliza los servicios de terceros, esta norma ISO no solo contempla problemas internos sino también externos y como se puede solucionar en caso de existir problemas con esos servicios. El uso de esta norma no es muy conocida pero es conveniente e innovador en el campo de la seguridad informática.

Para recoger los datos se han utilizado encuentas, se ha recopilado información directamente de la personas encargadas en los puntos claves de la institución y se ha ordenado todo de acuerdo a un criterio propio para ofrecer un mejor entendimiento de la situación actual de FEI.

Finalmente se propone un plan de contigencia de acuerdo a las necesidades y falencias en el área informática de FEI, beneficiando a todos los miembros de la organización y procurando que todos los servicios estén asegurados en caso de existir algún desastre y que su recuperación sea fácil, ordenada y bien documentada.

Capítulo 1

Marco Teórico

1.1 Tema de investigación

Análisis de Riesgo y Diseño de plan de contingencia para recuperación ante desastres en Florida Education Institute (FL-USA) según la norma ISO 24762-2008

1.2 Antecedentes investigativos

Al realizar una búsqueda de otros proyectos similares enfocados en la recuperación de datos vale la pena mencionar el proyecto de titulación de Byron Vicente Nieto Muñoz de la Universidad Politécnica Salesiana Sede Guayaquil, donde propone utilizar la NORMA ISO/IEC 24762:2008 en los departamentos de TI de los gobiernos autónomos descentralizados del Ecuador para descubrir los posibles riesgos y amenazas que pueda sufrir la información en estos lugares y cuáles son las mejores prácticas que deben implementar para evitar la pérdida de datos [1].

A su vez en el proyecto de maestría de Ing. David Paúl Vinueza Ludeña de la Universidad de Las Américas plantea un escenario similar pero en una institución privada como lo es la empresas PRONACA en el Ecuador la cual también requiere de un plan de contingencia para la protección y recuperación de sus datos adicionalmente se realizó un análisis donde se identificó los activos, vulnerabilidades, amenazas y controles existentes para dar una estimación y evaluación de los riesgos, a su vez plantea "la estrategia de continuidad de los servicios de TI la cual consiste en definir las medidas de respuesta a riesgos y las opciones de recuperación ante un desastre [2]

1.2.1 Contextualización del problema

En el mundo empresarial como en el de cualquier organización o entidad, que manejan información vital de sus clientes se enfrentan a varios problemas referentes al área tecnológica, especialmente al tratarse de almacenar, asegurar y recuperar todos los datos después de varios escenarios, así como, un ataque o mal uso de los equipos informáticos, obsolescencia en los servidores y hasta catástrofes naturales que pueden perjudicar y dañar toda la infraestructura establecida en la institución lo que conlleva a la pérdida de información, por lo cual perjudica a la cadena de negocio haciendo que las actividades diarias se vuelvan un suplicio para los usuarios.

Países como Estados Unidos han sufrido una serie de ataques informáticos que comprometieron su información y han dejado al descubierto las vulnerabilidades de varios sistemas y la falta de conocimiento técnico de las empresas de servicio de TI (Tecnologías de la Información) o personal interno al administrar estos recursos críticos dentro de las empresas como lo sucedido con la empresa Kaseya en el estado de la Florida [3].

Pero no solo los riesgos provienen de ataques informáticos sino también de desastres naturales como el terremoto y posterior tsunami ocurrido en Japón de 2011 donde los data centers fueron puestos a prueba en una serie de inconvenientes, como cortes de electricidad frecuentes, peligro de colapsos de infraestructuras e inundaciones que provocaría daños en los equipos electrónicos [4].

Pero no solo los países del primer mundo sufre estos tipos de inconvenientes, países en vías de desarrollo como Perú también ha tenido un repunte en los ataques de ransomware entre 2020 y 2021 al igual que en otros territorios de Latinoamérica que sufren ataquen informáticos todos los días, especialmente ataques de phishing, cuentas falsas de redes sociales y apps de dudosa procedencia. [5]

Los ciberdelincuentes se han especializado mucho más lo que ha permitido que exista ataques mucho más elaborados como el ataque ocurrido a Aeronáutica Civil de Colombia que causó varios problemas en los servicios de correos electrónicos y página web. [6].

En Ecuador también se ha producido este tipo de ataques informáticos siendo un ejemplo el suscitado a una empresa pública conocida como Corporación Nacional Telecomunicaciones (CNT) la que por falta personal capacitado y al no cumplir los protocolos correspondientes en el ámbito de seguridad fue susceptible a un ataque de Ransomware, por consecuencia parte de su información, tanto de clientes como propia, fue secuestrada solicitando una rescate económico para a cambio devolver los datos sustraído y evitar su publicación [7].

Así mismo la Agencia Nacional de Tránsito (ANT) sufrió un ataque a su sistema AXIS lo cual retardó la entrega de licencias y matrículas vehiculares de forma regular por lo cual muchos usuarios se vieron afectados. Esto indica lo importante que es tener un plan de contingencia para todo tipo de problema, especialmente en el ámbito informático [8].

Es así como la empresa establecida en Estados Unidos en el estado de la Florida - Miami Dade conocida como Florida Education Institute (FEI) por sus siglas en inglés ha tomado la decisión de establecer protocolos para proteger sus datos y toda su infraestructura tecnológica [9].

FEI es una empresa que ofrece servicios educativos con carreras ocupacionales que almacena gran información sensible de sus estudiantes, departamentos como financiero, administrativos y educativo en los servidores propios, dentro de la infraestructura física del campus principal.

FEI ha iniciado la creación del puesto de TI dentro de la empresa para la administración de la infraestructura tecnológica, al ser un nuevo departamento, los planes de contingencia, prevención de desastres y capacitación a los usuarios no ha sido una prioridad ya que no se ha realizado un análisis a profundidad en relación con los posibles problemas tecnológicos que se puedan presentar [9].

1.2.2 Delimitación

Área Académica: Seguridad

Línea de investigación: Normas y estándares

Sublíneas de investigación: Seguridad de unidades informática

Delimitación especial: La investigación se realizará en el Departamento de Tecnologías de la Información (TI) de Florida Education Institute (FEI) que se encuentra ubicada en el ciudad de Miami, Estado de la Florida, Estados Unidos **Delimitación temporal:** La presente investigación se desarrollará durante los 6 meses posteriores a la aprobación del proyecto por parte del Consejo Directivo de la Facultad.

1.2.3 Justificación

Los riesgos informáticos tanto humanos, técnicos como naturales deberían tomarse muy en serio especialmente en empresas que manejan gran cantidad de datos sensibles y prevenir la pérdida de información; la cual debería ser la prioridad principal para que la continuidad del negocio no se vea afectada por estos fenómenos.

FEI brinda servicios educativos a personas migrantes y nativos que desean obtener una certificación en corto tiempo para poder trabajar en el estado de la Florida en trabajos ocupacionales. Siendo así, FEI almacena información sensible y trayectoria educativa de sus estudiantes, por tal motivo, se realizó el análisis y creación de un plan de riesgos que facilite la rápida resolución de problemas ante la pérdida o destrucción de la información.

FEI se beneficiará de este proyecto que contiene las mejores técnicas para la protección, recuperación y disponibilidad de la información, creando un ambiente de fácil administración con procedimientos documentados basados en estándares internacionales para un correcto funcionamiento de toda la infraestructura.

Con la ISO 24762:2008 se tomará en cuenta también los servicios contratados por FEI, lo que otras normas ISO no consideran en su normativa lo cual permite observar un espectro más amplio y tomar decisiones más acertadas de acuerdo a los requermientos del personal de la institución.

1.3 Fundamentación teórica

Inicialmente se debe conocer la ISO 24762:2008, que proporciona: "pautas para los servicios ICT DR (Information and Communications Technology Disaster Recovery), que incluyen tanto los que se brindan internamente como los subcontratados. Cubre la capacidad de las instalaciones y los servicios y proporciona respaldo y soporte de recuperación a los sistemas de TIC de una organización. Incluye los aspectos de implementación, prueba y ejecución de la recuperación ante desastres. No incluye otros aspectos de la gestión de la continuidad del negocio." [10].

Entre los términos más utilizados y de los cuales se basa la presente investigación son:

Plan de contingencia: "... Apuntan a las actividades que se deben realizar para evitar o minimizar el impacto de una contingencia y a recuperar el mayor porcentaje posible de nuestra plataforma informática dañada por alguna razón." [11]

Norma ISO: "Las normas ISO son documentos que especifican requerimientos que pueden ser empleados en organizaciones para garantizar que los productos y/o servicios ofrecidos por dichas organizaciones cumplen con su objetivo." [12]

Seguridad informática: "... se refiere a la protección de la información y, especialmente, al procesamiento que se hace de la misma, con el objetivo de evitar la manipulación de datos y procesos por personas no autorizadas. Su principal finalidad es que tanto personas como equipos tecnológicos y datos estén protegidos contra daños y amenazas hechas por terceros." [13]

Tecnologías de la información y comunicación: también llamada informática, es la ciencia que estudia las técnicas y procedimientos automatizados que actúan sobre los datos y la información. La "informática" proviene de la fusión de los términos información y automática. Y las tecnologías de la comunicación estudian el envío y recepción de información a distancia. [14]

1.4 Objetivos

1.4.1 General

- Implementar un plan de contingencia basado en la Norma ISO 24762:2008 para el departamento de TI de Florida Education Institute.

1.4.2 Específicos

- Realizar el análisis de la administración actual del departamento de TI.
- Realizar el análisis de riesgos naturales, informáticos y humanos que se pueden presentar en FEI.

- Implantar un plan de contingencia basado en la normativa ISO 24762:2008 para la recuperación de información en casos de desastres.

Capítulo 2

Metodología

2.1 Métodos

2.1.1 Modalidad de la investigación

- **Investigación Descriptiva**

  La investigación descriptiva se aplicará con el objetivo de establecer las opiniones y conocimientos del personal acerca del plan de respaldo y recuperación ante desastres, así detallar puntos críticos y específicos de las dimensiones de las variables, que ayuden a la comprensión de la realidad y detallar aspectos administrativos, de gestión de talento humano y tecnología dentro de la institución de análisis.

- **Investigación Explicativa**

  La investigación tiene como finalidad elaborar una explicación especifica e integral de las variables, con un análisis de sus componentes y sus dimensiones, con la finalidad de comprender aspectos puntuales y los posibles riegos para la aplicación del plan de respaldo y recuperación ante desastres.

2.1.2 Población y muestra

La Población de estudio son 32 personas en Florida Education Institute las cuales tienen contacto directo con los sistemas o subsistemas de la institución quienes pueden estar presentes en percances relacionados con estas tecnologías.

Área	**Número**	**Porcentaje**
Presidencia	1	3%
Business Office	1	3%
Register	1	3%
Student Services	1	3%
Admissions	4	13%
Marketing	3	9%
IT	2	6%
Maintenance	1	3%

Faculty	11	34%
Financial Aid	2	6%
Executive Officer	1	3%
Call center	4	13%
	32	100%

Cuadro 2.1: Población
Elaborado por: Paúl Montesdeoca

2.1.3 Procesamiento y análisis de datos

Los primeros datos obtenidos se realizan mediante una observación de campo con el fin de tener una idea clara de como está la infraestructura física y lógica de los sistemas informáticos que se manejan, con su respectiva documentación, además, se apoya este estudio con una entrevista al encargado del Área de Tecnologías de la información para conocer el estado actual de la institución educativa Florida Education Institute (FEI).

Mientras se desglosa toda la información recopilada se realiza algunas notas u observaciones que muestren las falencias de las políticas, normas o estándares de la institución, de este modo, poder crear un plan de riesgos acorde a las necesidades de la institución.

Después de recopilar toda la información se procede a realizar un análisis de riesgo a partir de una matriz de riesgo. Esta matriz se basa en los datos recogidos y en la prioridad que se da a cada potencial riesgo para luego calificarlos según su importancia.

Finalmente se utiliza un marco de referencia para poder crear el plan de contigencia que mejor beneficie a la institución y permita el correcto uso de los recursos de la organización además de terminar el proyecto

Análisis y clasificación de riesgos

La calificación de riesgo se logra a través de la estimación de la probabilidad de su ocurrencia y el impacto que puede causar la materialización del riesgo. La probabilidad representa el número de veces que el riesgo se ha presentado o se presentará en un determinado tiempo y el impacto se refiere a la magnitud de sus efectos.

Cuadro de probabilidad

Probabilidad	**Descripción**	**Frecuencia**	**Valor**

Casi seguro	El evento ocurrirá en la mayoría de los casos	Mas de una vez al año	5
Probable	El evento probablemente ocurrirá en la mayoría de los casos	Al menos una vez en el último año	4
Posible	El evento podría ocurrir en algún momento	Al menos una vez en los últimos dos años	3
Improbable	El evento casi nunca podría ocurrir en algún momento	Al menos una vez en los últimos cinco años	2
Raro	El podría ocurrir solo en circunstancias excepcionales	No se ha presentado en los últimos 5 años	1

Cuadro 2.2: Cuadro de probabilidad
Elaborado por: Paúl Montesdeoca

Cuadro de impacto

Impacto	**Consecuencias**	**Valor**
Catastrófico	Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la institución • Pérdida de recursos • Disminución del rendimiento de los procesos de negocio • Pérdida de información en general • Suspensión de los sistemas críticos • Deterioro de la imagen institucional	5
Mayor	Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la institución	4

Moderado	Si el hecho llegara a presentarse, tendría medianas consecuencias o efectos sobre la institución	3
Menor	Si el hecho llegara a presentarse, tendría bajas consecuencias o efectos sobre la institución	2
Insignificante	Si el hecho llegara a presentarse, tendría consecuencias o efectos pero mínimos sobre la institución	1

Cuadro 2.3: Cuadro de impacto
Elaborado por: Paúl Montesdeoca

Matriz de riesgo

Una matriz de riesgos, conocida también como "Matriz de Probabilidad de Impacto", es una herramienta, útil para toda empresa, que le permite identificar los riesgos a los que está expuesta. De esa forma, las compañías pueden determinar los niveles aceptables de exposición a aquellos, así como establecer el control apropiado frente a los mismos y monitorear la efectividad del método de control elegido [15].

Físicamente, es una guía visual que permite, mediante su diseño, una rápida identificación de las prioridades que deben ser atendidas. De esa forma también acelera la toma de decisiones [15].

Una matriz de riesgo debe presentar ciertas características para que pueda cumplir su función, estas son:

- Debe ser sencilla tanto en la forma cómo se elabore, como en la que se consulte. Y es que, como se ha dicho antes, se hace con el objetivo de facilitar la toma de decisiones y ordenar prioridades [15].
- Debe ser flexible en la que se puedan documentar los diferentes procesos de la empresa, así como evaluar de forma global los riesgos de aquella [15].
- Debe permitir hacer comparaciones entre diferentes proyectos, áreas, actividades, etc [15].
- Debe permitir realizar un diagnóstico objetivo de todos los factores de riesgo del negocio [15].

ISO 24762:2008

La ISO 24762 se introdujo en 2008 para describir un marco general para la recuperación ante desastres de tecnología de la información y las comunicaciones (RD TIC). Este estándar

PROBABILIDAD	IMPACTO				
	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
Casi seguro (5)	A	A	E	E	E
Probable (4)	M	A	A	E	E
Posible (3)	B	M	A	E	E
Improbable (2)	B	B	M	A	E
Raro (1)	B	B	M	A	A

B: Zona de riesgo baja: Asumir el riesgo

M: Zona de riesgo moderada: Asumir el riesgo, reducir el riesgo

A: Zona de riesgo Alta: Reducir el riesgo, evitar, compartir o transferir

E: Zona de riesgos extrema: Reducir el riesgo, evitar, compartir o transferir

Figura 2.1: Matriz de riesgo
Elaborado por: Paúl Montesdeoca

proporciona una descripción detallada de todos los requisitos del proveedor de recuperación ante desastres. Este estándar se introdujo en 2008 específicamente para abordar los servicios de recuperación ante desastres de TI proporcionados por empresas de terceros. También se puede aplicar a soluciones internas [16].

Este es un estándar multicapa:

1. Capa fundamental:
    - Políticas
    - Medición del desempeño
    - Procesos
    - Personas
2. Infraestructura de apoyo
3. Capacidad de servicios
4. Mejora Continua

La ISO 24762 es un marco de RD de TIC exhaustivo con las siguientes cláusulas principales.

1. **Recuperación de desastres de TIC**
    - **Estabilidad ambiental:** huelgas, manifestaciones, disturbios, crímenes, desastres naturales, pandemias y factores similares afectan la estabilidad ambiental de un sitio.
    - **Gestión de activos:** esto incluye la protección de activos a través de la lista y el almacenamiento del inventario, y la documentación pertinente.

- **Proximidad del sitio:** se emplean estrategias de selección del sitio para elegir una ubicación para la unidad comercial que esté bien aislada de varios peligros.
- **Gestión de proveedores:** el personal, los servicios, los suministros y las soluciones proporcionados por los proveedores de una empresa pueden verse afectados durante una emergencia. Esto, a su vez, afecta los plazos, los objetivos y los plazos de entrega de los procesos comerciales.
- **Acuerdos de subcontratación:** el grado limitado de control que una organización puede ejercer mientras subcontrata tareas y procesos se contrarresta mediante controles estrictos, acuerdos contractuales, revisiones periódicas y medidas para aumentar la conciencia.
- **Seguridad de la información:** los sistemas de TIC se agrupan en diferentes ubicaciones físicas en función de sus diferentes requisitos de protección durante situaciones de crisis. Asimismo, se evalúan periódicamente los distintos componentes de todos los incidentes relacionados con la seguridad informática (Detección, Notificación, Respuesta y Análisis de Eficacia).
- **Activación y desactivación del plan de recuperación ante desastres:** se establecen planes y procedimientos para identificar cuándo se debe activar un plan de recuperación ante desastres y cuándo se pueden detener las medidas de recuperación.
- **Capacitación y educación:** la transferencia de conocimientos juega un papel importante en la sensibilización entre el personal y el personal. Esto también implica revisiones periódicas para evaluar la pertinencia de los módulos de formación.
- **Pruebas en los sistemas de TIC:** las capacidades de continuidad comercial de los sistemas de TIC se prueban rigurosamente durante los cambios en los requisitos de la organización o la expansión de las operaciones comerciales.
- **Planificación de la continuidad del negocio para los proveedores de servicios de RD de TIC:** las prioridades, los plazos, los requisitos mínimos y la logística se elaboran estratégicamente y se prueba su eficacia para minimizar el impacto en los proveedores de servicios.
- **Documentación y revisión periódica:** todas las medidas de RD se archivan y consultan constantemente. Esto permite actualizaciones y mejoras periódicas.

2. **Instalaciones de recuperación de desastres de TIC**

- **Ubicación de los sitios de recuperación:** las ubicaciones de los sitios de recuperación se deciden en función de factores como la vulnerabilidad a los peligros naturales, incidentes climáticos extremos, disponibilidad de infraestructura,

proximidad de varios, como transporte público, instituciones médicas, servicios como agua, gas, electricidad, etc.

- **Controles de acceso físico:** se establecen categorías de seguridad, normas de entrada y salida, protocolos de conducta y otras restricciones para varios departamentos mientras se encuentran en los sitios de recuperación.
- **Seguridad de las instalaciones físicas:** los sitios de recuperación están protegidos contra el acceso no autorizado y otras infracciones de seguridad mediante inspecciones periódicas, vigilancia constante, sistemas de detección y alarma, control del personal mediante identificación visible, como insignias/tarjetas de identificación, y administración desde una ubicación central.
- **Áreas dedicadas:** se prevén áreas dedicadas para la ejecución de medidas de recuperación, como montaje, mantenimiento, puesta en escena y otras actividades.
- **Controles ambientales:** se abordan la temperatura, la ventilación, la humedad, la vibración, el ruido y otros factores ambientales en el sitio de recuperación. controles, acuerdos contractuales, revisiones periódicas y medidas de sensibilización.
- **Telecomunicaciones:** las capacidades de intercambio de información se establecen al garantizar la conectividad, la seguridad de los datos, la diversidad de la red, la confiabilidad y los estándares de calidad.
- **Suministro de energía:** un suministro continuo y estable de electricidad es vital para que las operaciones continúen sin interrupciones. Esto se logra mediante la identificación de proveedores de servicios confiables, el establecimiento de fuentes alternativas de suministro de energía, como generadores, instalaciones de suministro de energía ininterrumpida (UPS), etc.
- **Gestión de cables:** la fuente de alimentación y los cables relacionados con la electrónica cuentan con la protección y el blindaje adecuados para evitar interrupciones y pérdidas de información. Las bandejas y los conductos se revisan periódicamente para detectar daños, manipulaciones y otras vulnerabilidades.
- **Protección contra incendios:** esto incluye adherirse a las normas de cumplimiento normativo, establecer planes de escape en caso de incendio e instalar equipos como extintores, rutas de escape, etc.
- **Centro de operaciones de emergencia (COE):** el mantenimiento de la comunicación entre las unidades comerciales y las entidades externas se logra mediante el suministro adecuado de equipos, infraestructura relacionada con las telecomunicaciones, material de oficina, instalaciones físicas como áreas de reunión, etc.

- **Instalaciones restringidas:** el acceso a varias áreas en el sitio de recuperación está restringido según la designación y el propósito.
- **Servicios que no son de recuperación:** se toman medidas para atender el bienestar y la seguridad del personal presente en las instalaciones durante las emergencias.
- **Ciclo de vida de las instalaciones físicas y el equipo de soporte:** las instalaciones físicas y el equipo de soporte se administran mediante el cumplimiento de los requisitos de cumplimiento y las mejores prácticas durante todo el período de vida útil del activo para garantizar el acceso ininterrumpido para la actividad comercial.
- **Pruebas:** las instalaciones físicas y el equipo se mantienen actualizados mediante mantenimiento y pruebas regulares para garantizar una calidad óptima.

3. **Capacidad del proveedor de servicios subcontratados**

- **Requisitos de las instalaciones:** los proveedores de servicios se aseguran de que todos los requisitos enumerados según la cláusula de recuperación de desastres de TIC se cumplan adecuadamente.
- **Experiencia:** la capacidad del proveedor de servicios se destaca a través de la experiencia y la experiencia del personal para brindar soluciones de calidad.
- **Control de acceso lógico:** los proveedores de servicios subcontratados que brindan soporte operativo necesitan establecer sus credenciales para manejar los sistemas informáticos del sitio de recuperación.
- **Equipo de TIC y preparación operativa:** el equipo de cómputo y la infraestructura relacionada están instalados, operativos y bien mantenidos para un rendimiento óptimo.
- **Soporte de recuperación simultánea:** los proveedores de servicios deben asegurarse de que pueden cumplir con sus obligaciones contractuales a pesar de que muchos clientes activan sus servicios RD simultáneamente.
- **Niveles de servicio:** las organizaciones pueden decidir sobre el alcance de los servicios solicitados en función de la criticidad de sus necesidades.
- **Tipos de servicio:** las organizaciones pueden decidir sobre el rango de los servicios solicitados en función de la complejidad de las medidas de recuperación.
- **Proximidad de los servicios:** los proveedores de servicios se aseguran de tener las capacidades para abordar las necesidades de recuperación de múltiples clientes que enfrentan la misma interrupción del negocio.

- **Tasa de suscripción para servicios compartidos:** los proveedores de servicios deben mantener la cantidad de organizaciones que se suscriben a sus servicios en un número óptimo para garantizar que siempre se brinde un servicio de alta calidad.
- **Activación de servicios suscritos:** los términos y condiciones para activar y desactivar el servicio suscrito están claramente definidos.
- **Pruebas de la organización:** esto permite a las organizaciones probar periódicamente los servicios de recuperación ante desastres a los que se han suscrito.
- **Cambios en la capacidad:** los proveedores de servicios deben asegurarse de que las mejoras en sus capacidades debido a inversiones, avances tecnológicos, etc.
- **Plan de respuesta a emergencias:** los propios proveedores de servicios deben protegerse contra emergencias no planificadas que pueden obstaculizar las soluciones que brindan a sus clientes.
- **Autoevaluación:** las áreas de evaluación identificadas están sujetas a extensas auditorías internas y pruebas integrales para garantizar que las soluciones se mantengan actualizadas.

4. **Selección de sitios de recuperación:** Se establecen normas para la selección de una buena infraestructura donde se disponga fácilmente de mano de obra calificada. Esto incluye condiciones socioeconómicas favorables en la ubicación del sitio de recuperación. Esto está determinado por la disponibilidad de infraestructura, mano de obra calificada y apoyo, masa crítica de vendedores y proveedores, historial de proveedores de servicios locales y apoyo proactivo de la comunidad local.

5. **Mejora continua:** Los procesos existentes se actualizan constantemente con la última tecnología y tendencias según las demandas y los factores impulsores de la industria.
    - Tendencias TIC RD
    - Medición del desempeño
    - Escalabilidad
    - Mitigación de riesgos

Capítulo 3

Resultados y Discusión

3.1 Análisis y discusión de resultados

3.1.1 Analisis de la situación actual de Florida Education Institute y de su departamento de Tecnologías de la Información (TI)

Se empieza realizando una entrevista al encargado del área de sistemas con el objetivo de obtener datos y saber de mejor manera como se está manejando la infraestructura tecnológica de la institución.

Entrevista al encargado de TI de Florida Education Institute

La entrevista en cuestión se la realizó al presidente de FEI Ramón Valenti, encargado del departamento de TI, el cual contestó las preguntas de manera seria y técnica lo cual permitió conocer mucho mejor la realidad de la institución, obteniendo las siguientes respuestas.

Entrevistado / Preguntas	**Encargado del departamento de TI**
1. Para gestionar la información. ¿Se aplica algún tipo de política de seguridad? Si (), Enúncielas NO ()	Si existen políticas de seguridad pero están creadas de manera empírica, es decir se fueron creando de acuerdo a las necesidades que iban apareciendo. Así tenemos: • Manejo personalizado de File System • Manejo de Active Directory
2. ¿Se realiza un control de la seguridad de la información?	Si, a través de Active Directory se entrega control de varios recursos lógicos a las personas que lo necesiten.

3. ¿El personal tiene definidas sus responsabilidades en cuanto al uso adecuado de los recursos de la institución?	No, las personas no tienen capacitación ni documentación sobre el manejo responsable de los equipos responsables.
4. ¿Dependiendo del personal, existe restricciones para el acceso de ciertos sistemas o equipos en la institución?	Para sistemas lógicos existen restricciones pero en el área de servidores no existen restricciones.
5. ¿Se realiza un mantenimiento preventivo y correctivo periódico de los equipos de la institución?	Si se han realizado mantenimientos correctivos a los equipos de la institución.
6. ¿Se han realizado simulacros de caídas o fallos en los sistemas claves de la institución?	Se han realizado simulacros pero no se realizado documentación de dichas pruebas.
7. ¿Que mecanismos de seguridad se aplican a los sistemas informáticos claves de la institución?	A nivel lógico se utilizan firewalls y proxys y a nivel físico se utilizan U.P.S.
8. ¿Se han realizado tareas de monitoreo a los sistemas informáticos de la institución?	Se han realizado monitoreos pero no documentados.
9. ¿Existe un inventario sobre los activos informáticos de la institución?	Si existe inventario de los equipos informáticos.

10. ¿Se está aplicando alguna metodología o plan de gestión de riesgos para la infraestructura tecnológica de la institución?	En algunas áreas se utiliza la metodología BASC pero no en toda la organización.

Cuadro 3.1: Encuesta al encargado del área de TI

Elaborado por: Paúl Montesdeoca

Evaluación de la entrevista aplicada

Después de realizar la entrevista al presidente de FEI se puede sacar las siguientes conclusiones:

- Las políticas que se aplican son creadas de acuerdo a las necesidades que aparecen, por lo tanto se las puede considerar como reglas básicas que tienen una alta probabilidad de fallar si no se toma en cuenta todos los riesgos posibles si no se hace un estudio adecuado de la situación actual de la institución.
- No existe documentación formal donde se estipula las responsabilidades del personal respecto a los equipos informáticos de la institución, tampoco se ha realizado una socialización con los empleados del correcto uso de las instalaciones.
- Aunque se lleva control de acceso de los usuarios a nivel lógico, no lo hace a nivel físico por lo tanto no se sabe que personas tienen acceso a los servidores ni un registro de entrada o salida de esa área en específico.
- Existe un mantenimiento anual de los equipos lo cual se considera un punto positivo para la institución.
- Aunque se ha realizado simulacros en caso de caídas o fallos en sistemas claves de la institución, no se tiene documentación formal de los ensayos por lo tanto no se sabe con certeza como puede afectar realmente estos inconvenientes en escenario real.
- Muchas operaciones dentro del área informática no tienen la suficiente documentación por lo tanto sería un inconveniente en caso de que algún sistema falle y no se sepa los procedimientos correctos a seguir.
- Aunque se tiene algunos métodos para proteger los equipos informáticos y los datos de la institución, no existe un plan de contingencia real el cual seguir en caso de algún desastre, caída o fallo en los sistemas de la institución.

3.1.2 Ubicación de Florida Education Institute

Se encuentra ubicado en 5818 SW 8th Street Miami 33144, Florida

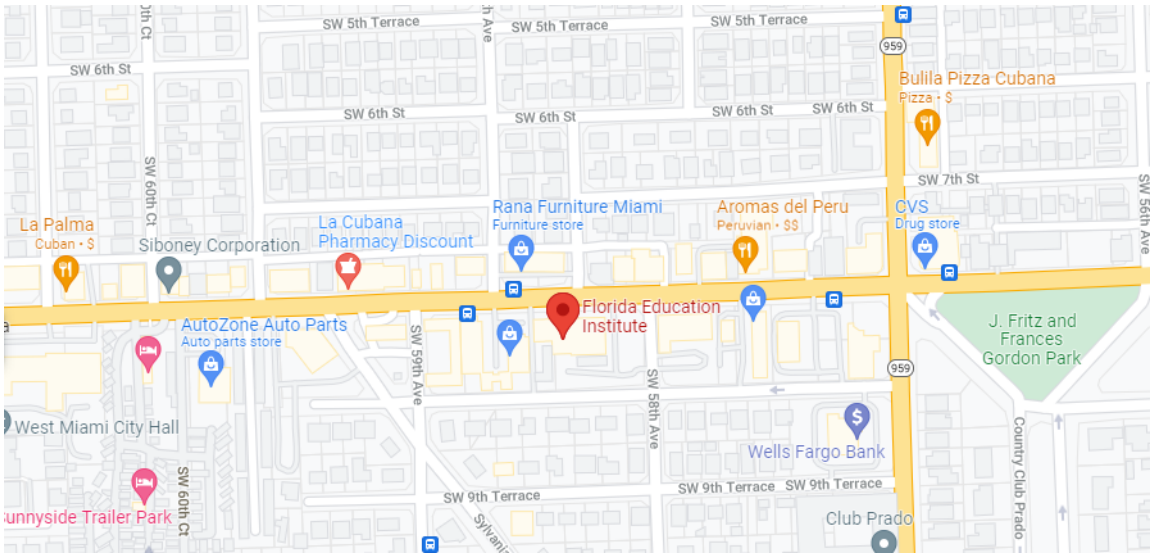


Figura 3.1: Localización de FEI en Google Maps
Elaborado por: Paúl Montesdeoca

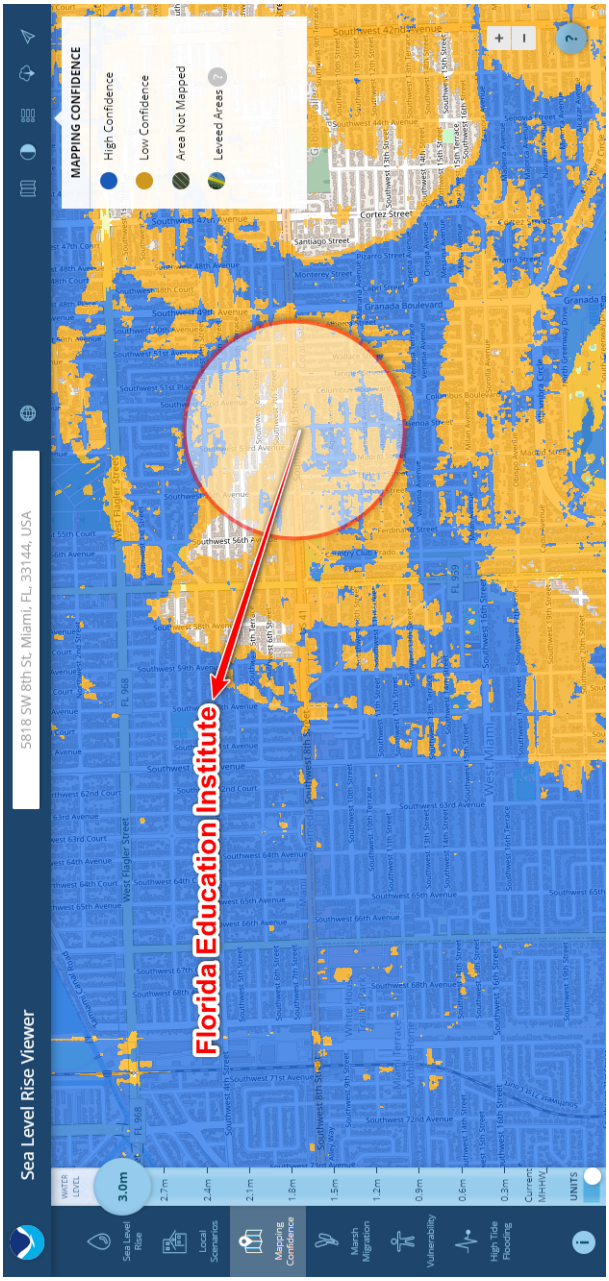


Figura 3.2: Mapa de marea alta en el área de FEI
Elaborado por: Paúl Montesdeoca

Observación: En la figura 3.2 se detalla que en caso de que exista probabilidades de marea alta la cual puede llegar a los tres metros sobre el nivel del mar, que es el promedio es lo que suele suceder en casos extremos dentro del área de Miami, existe poco impacto de un desastre a gran escala dentro de las instalaciones de FEI.

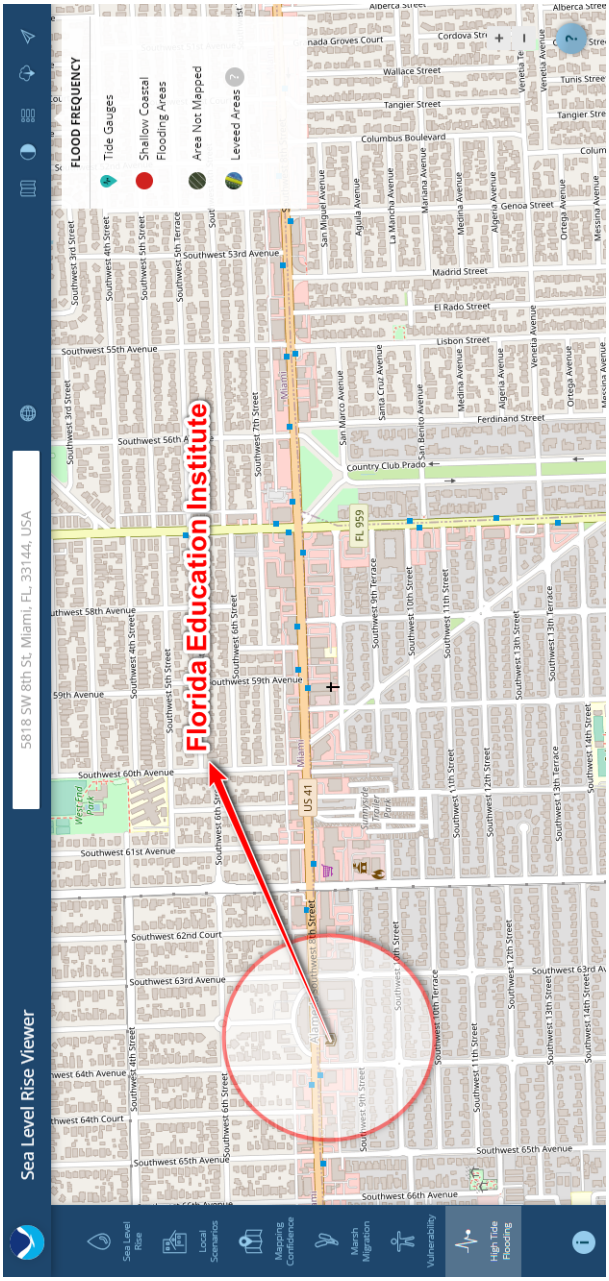


Figura 3.3: Mapa de posibles inundaciones en el área de FEI
Elaborado por: Paúl Montesdeoca

Observación: En la figura 3.3 se puede observar que las posibilidades de inundaciones en FEI son mínimas pero no cero, lo que indica que puede haber afectaciones bajas por este desastre dentro de las instalaciones de FEI, pero haría muy difícil el transportarse a los empleados hacia la institución.

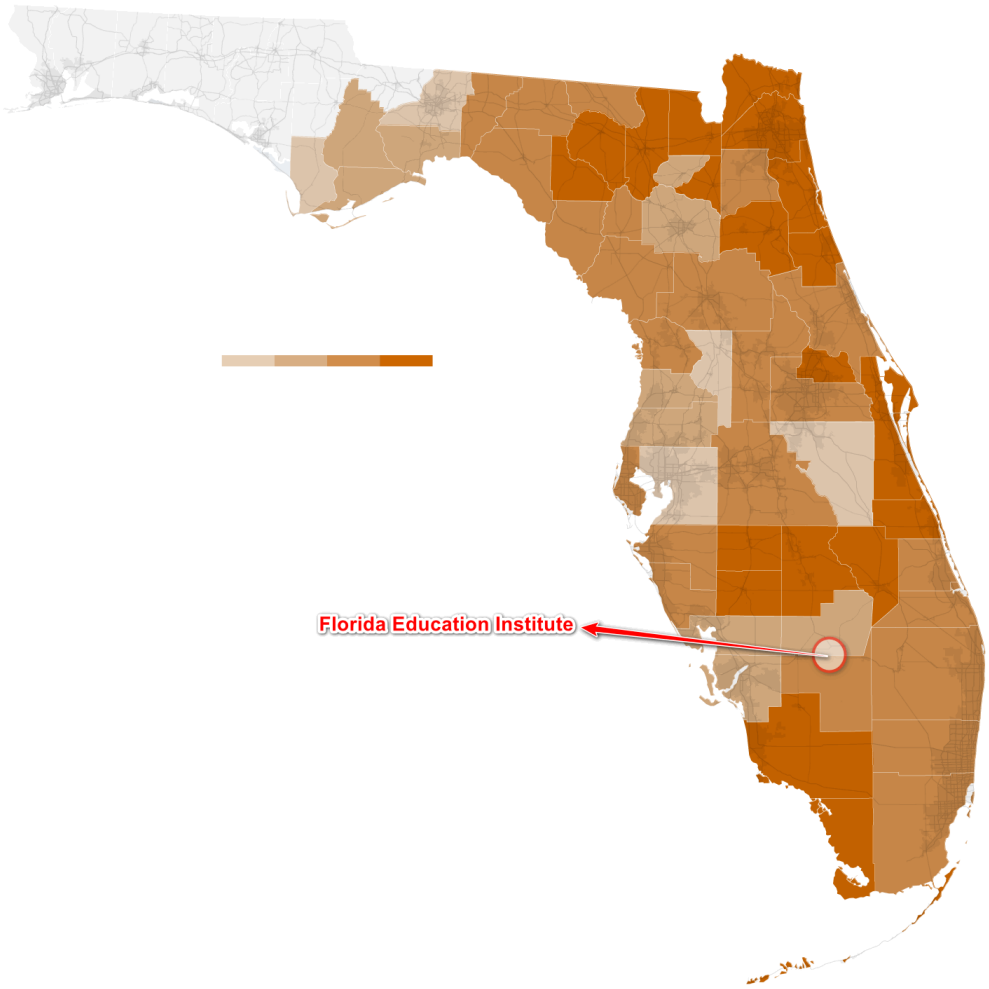


Figura 3.4: Mapa de posibles cortes de luz por huracanes en el área de FEI
Elaborado por: Paúl Montesdeoca

Observación: En la figura 3.4 existe la posibilidad de corte de energía eléctrica por múltiples factores externos e internos, FEI se encuentra en la mitad del promedio, por lo tanto no es muy común que suela suceder cortes de luz sorpresivos en el área de FEI.

Observaciones

- Debido a que Miami se encuentra muy cerca al mar, especificamente al océano Atlántico, tanto la institución como el departamento informático están expuestos a huracanes, que son las catástrofes más comunes dentro de la región oeste de los Estados Unidos.
- Los posibles problemas que podría causar un huracán son inundaciones, pérdida de energía, daños estructurales a los edificios, incendios, etc. Lo que provocaría una caída total del servicio por un largo tiempo hasta recuperarse.

3.1.3 Ubicación del departamento de TI

El área de TI se encuentra ubicado dentro de las instalaciones de FEI en el centro izquierdo de las instalaciones, al lado del aula 103 y el departamento de diplomas, en el departamento de Servicios Estudiantiles, donde también se encuentra el cuarto de servidores. El edificio es de un solo piso.

Observaciones:

- El departamento de TI se encuentra dentro del cuarto donde se ubica otro departamento, lo cual puede significar un riesgo de seguridad, ya que cualquier persona tendría acceso a ese lugar e incluso a los servidores donde podrían causar un gran daño a la institución.
- Debido a que el edificio de FEI consta de un solo piso, esto puede ser un problema en caso de inundación o terremoto, ya que se comprometería el buen estado de los servidores.

3.1.4 Ubicación de los servidores

Los servidores se encuentran al lado de del departamento de Servicios a los Estudiantes. Para ingresar al cuarto de servidores se debe ingresar al departamento de Servicios Estudiantiles.

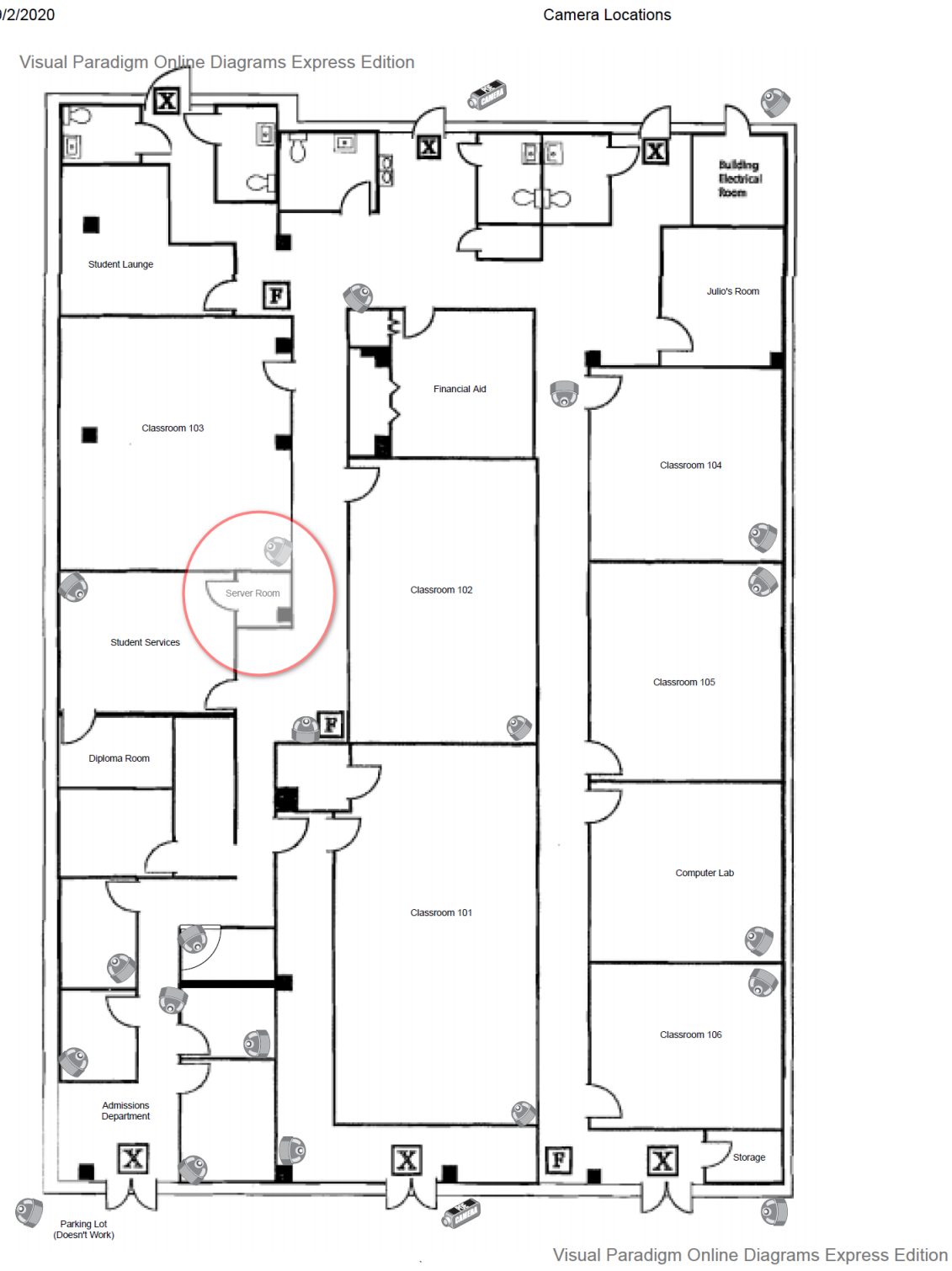


Figura 3.5: Localización del departamento de TI y servidores
Elaborado por: Paúl Montesdeoca

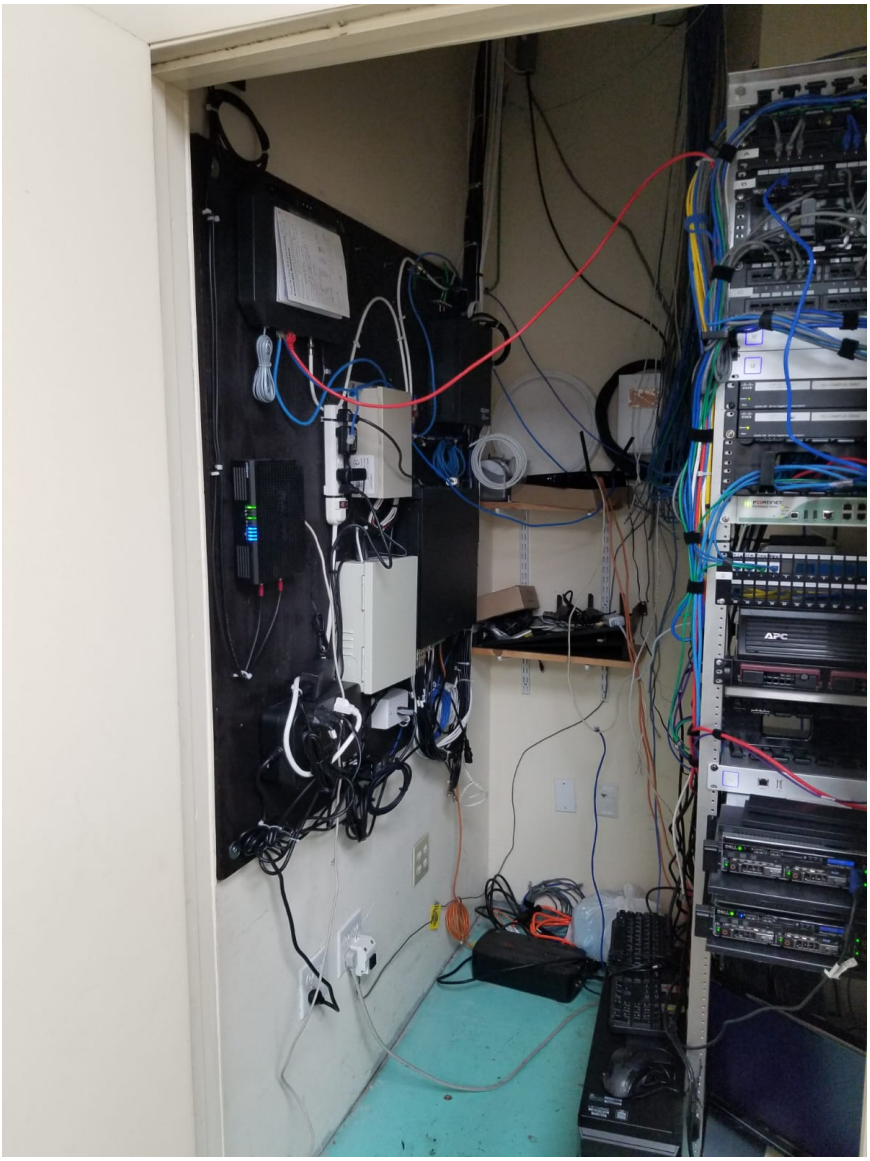


Figura 3.6: Entrada al cuarto de servidores
Elaborado por: Paúl Montesdeoca

Observación: Como se observa en la figura 3.6 el servidor no cuenta con una puerta de seguridad o algún acceso biométrico que registre la entrada y salida del área de servidores creando una brecha de seguridad en esta área incrementando la posibilidad de robo o daño de equipos sumamente importantes dentro de la institución.

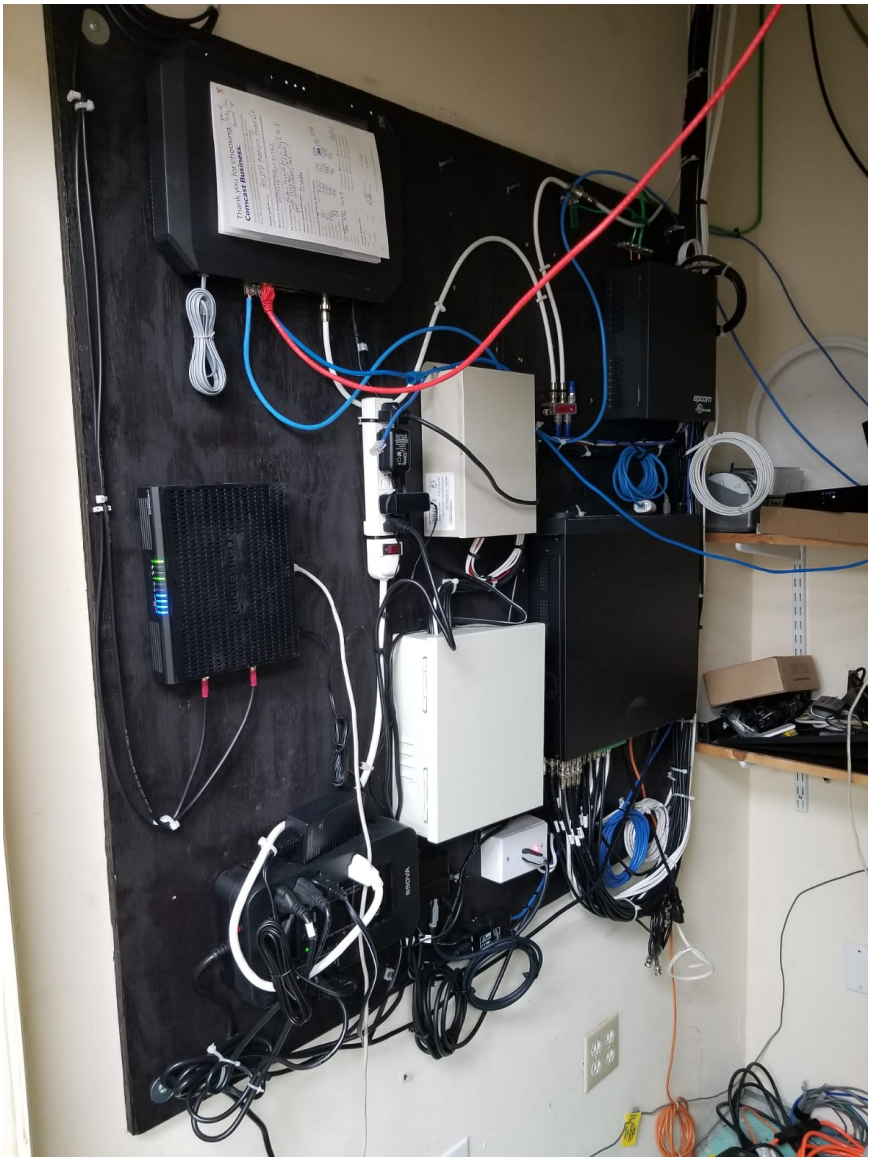


Figura 3.7: Panel de control del cuarto de servidores
Elaborado por: Paúl Montesdeoca

Observación: En la figura 3.7 el panel de control consta del Comcast, el breaker de luz y el control de cámaras de seguridad todos ubicados de manera aleatoria sin seguridad y con cables entrecruzándose lo que indica un riesgo a daños y pérdida de algunos servicios.

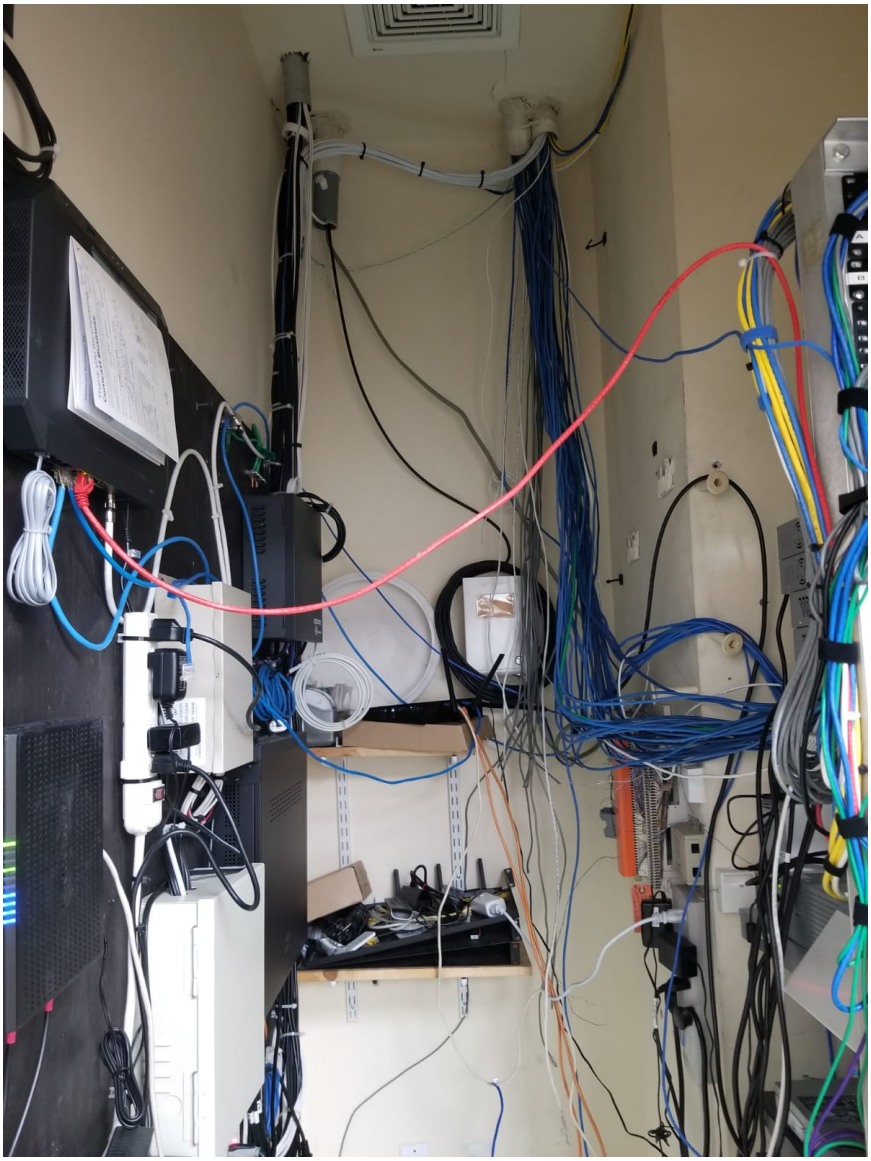


Figura 3.8: Cableado del cuarto de servidores
Elaborado por: Paúl Montesdeoca

Observación: En la figura 3.8 el cableado muestra un total desorden, lo que puede provocar confusión en caso de necesitar cambiar algún cable, además se nota que existe adaptaciones en la estructura física para que los cables lleguen hasta el lugar que le corresponde.

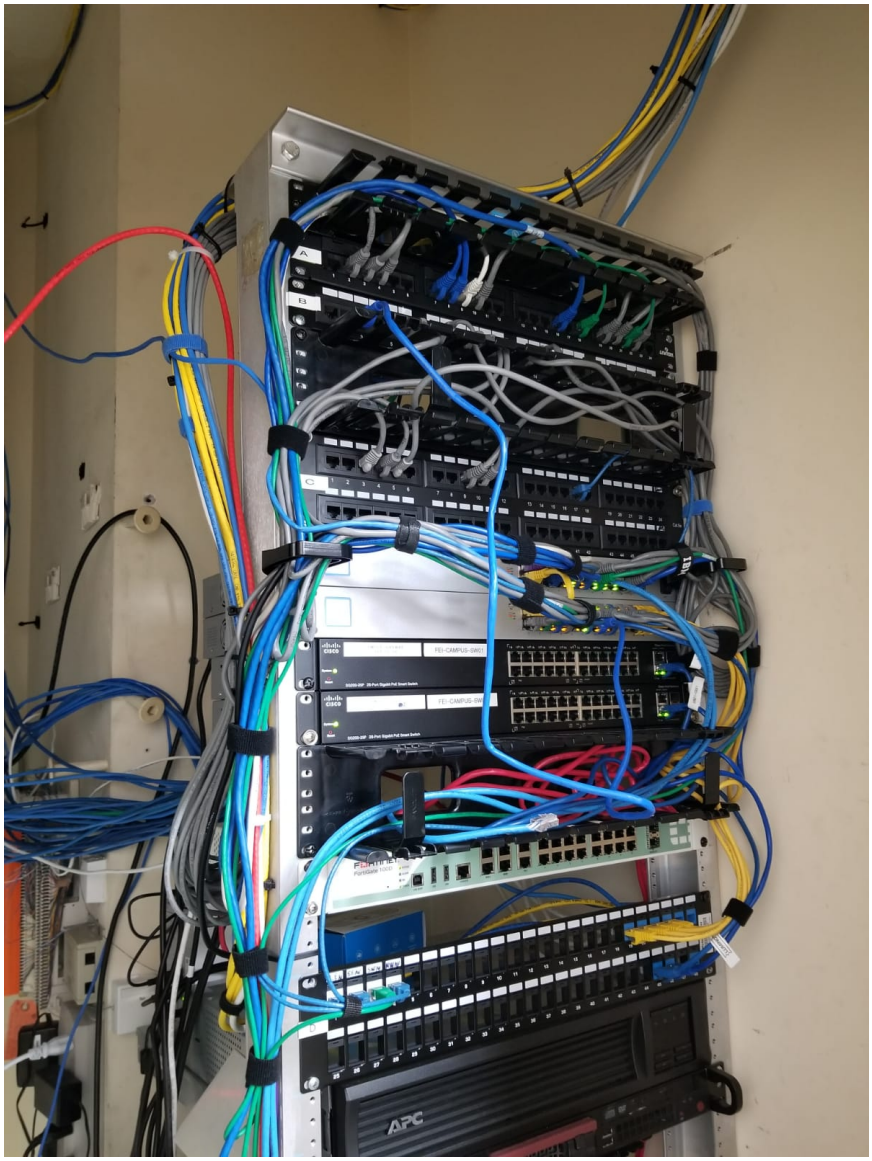


Figura 3.9: Servidores y switches
Elaborado por: Paúl Montesdeoca

Observación: En la figura 3.9 se muestra el cableado, dos servidores y cuatro switch que se utiliza en la institución. Se aprecia que los cables están desordenados y que dos switch no están en uso por lo tanto hay desperdicio de recursos.

Observaciones

- El cuarto de servidores fue adaptado para satisfacer las necesidades de los sistemas, contiene todas las seguridades en contra de incendios, caídas de energía y otros inconvenientes, pero tiene un fallo de seguridad ya que cualquier persona tiene acceso a los servidores.

- Otro problema con el cuarto de servidores es que no consta con una puerta para proteger los equipos que allí se encuentran por lo tanto es propenso a robo de activos. También se puede ver que esta área es utilizada como bodega de otros componentes informáticos que no deberían estar ahí.

- Existe un problema con los cables de red ya que se encuentran colgados y no pasan por canaletas o están cubiertos por algún aislante. Así mismo los cables de luz no tienen la seguridad correspondiente por que podría existir un incendio y se perdería todo.

3.1.5 Cuadro organizacional de FEI

En este cuadro se muestra la organización interna de FEI a nivel administrativo jerárquico.

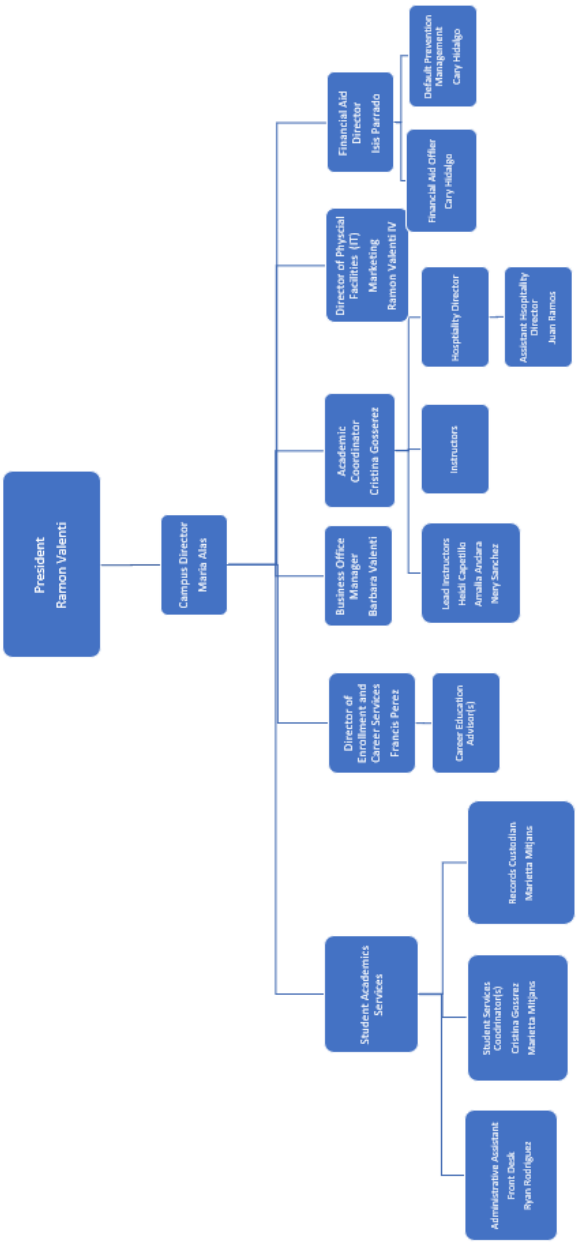


Figura 3.10: Cuadro organizacional de FEI
Elaborado por: Paúl Montesdeoca

3.1.6 Administración del departamento de TI

El departamento de TI es dirigido por Orlando Goza, quien se encarga de solucionar todos los problemas informáticos que se presente dentro de la institución, es decir, vela por el buen funcionamiento de los equipos tecnológicos o da soporte si algún sistema no funciona correctamente.

3.1.7 Problemas con los equipos informáticos de la institución

La institución tiene una normativa para manejar los equipos informáticos donde se estipula los siguientes pasos a realizar:

- Cualquier miembro de la facultad o del personal que necesite o identifique una mejora, reparación o problema con la infraestructura o el equipo de TI deberá enviar dicha solicitud a la mesa de ayuda de FEI. El encargado TI debe recibir estos tickets de inmediato y en orden de llegada. Cualquier necesidad de TI de emergencia o solicitud inusual se comunicará al encargado de TI.

- En caso de necesitar el reemplazo de un equipo o la adquisición de algún componente necesario para el buen funcionamiento de los recursos tecnológicos de la institución el encargado de TI deberá utilizar la lista de proveedores aprobados par realizar dichos cambios. Puede existir excepciones a la lista pero son casos muy particulares.

Observación: En esta normativa no se contempla la reparación de equipos como tal, es decir no está por escrito que hacer en caso de que un equipo solo necesite un mantenimiento correctivo, solo se intuye que se debe comunicar el problema al departamento de TI, y el encargado deberá resolverlo de acuerdo a su criterio.

3.1.8 Problemas con los servicios informáticos de la institución

Observación: Dentro de la documentación obtenida no se encuentra ninguna normativa que especifique que se debe hacer en casos de que algún servicio falle, tan solo se le comunica al encargado de TI y esa persona deberá resolver el problema de acuerdo a su criterio y sus conocimientos sobre el servicio que necesita revisión.

3.1.9 Inventario de activos físicos de la institución

FEI tiene un inventario de sus recursos informáticos físicos existentes, donde se indica a que departamento pertenece, el empleado a cargo, el tipo de dispositivo, la marca, el modelo, el sistema operativo (dependiendo el tipo de dispositivo), el estado (que depende de como se encuentra utilizado el activo) y un comentario en caso de necesitarlo. Los equipos con los que cuenta FEI son los siguientes:

Equipo	Características
Laptops	**Marca:** Lenovo, Dell **Cantidad:** 21
Tablets	**Marca:** Microsoft **Cantidad:** 1
Adaptador de energía	**Marca:** N/A **Cantidad:** 22
PC's de escritorio	**Marca:** HP Compaq, Dell, Acer, Lenovo **Cantidad:** 31
Impresoras	**Marca:** Lexmark, HP, Brother, Canon **Cantidad:** 10
Baterías de respaldo	**Marca:** APC **Cantidad:** 1
Router	**Marca:** Desconocida **Cantidad:** 1
Switch	**Marca:** Desconocida **Cantidad:** 2
Access Point	**Marca:** Desconocida **Cantidad:** 4

Cuadro 3.2: Inventario de recursos físicos

Elaborado por: Paúl Montesdeoca

Observación: El inventario de los recursos físicos es bueno pero carece de un código único que le permitiría ser encontrado o reemplazado de manera fácil y rápida, además solo hay un archivo de Excel donde consta una parte de los dispositivos, así que no está todo unificado y no existe un historial de como fue utilizado cada dispositivo a lo largo de un tiempo para verificar su buen estado.

3.1.10 Inventario de sistemas o software de la institución

El inventario de software describe el programa o sistema que se utiliza en FEI, este guarda el nombre del recurso informático y los servicios que presta; el orden de los programas está divido por departamento para una fácil identificación y asignación al personal de la institución. La lista consta de lo siguiente:

Departamento	Programa

Todos los empleados	Diamond • Diamond ADM • Diamond Student Portal • Diamond DCWS • Diamond SIS
Todos los empleados	Oooma: Service VOIP • Ooma Desktop • Ooma IP Phone
Todos los empleados	Office365 - Business Plan • Outlook (Desktop App, web) • Word (Desktop App, web) • Excel (Desktop App, web) • Power Point (Desktop App, web) • Kaizala (Movil App, web) • Teams (Desktop App, web) • OneDrive (Desktop App, web)
Todos los empleados	Zoom • Free Accounts • Business Accounts

Todos los empleados	Terminal Server • Se trabaja por protolo de servicio remoto de escritorio – Local: campus-rds01 – Externo: ts.fei.edu
Administración	Quick Books
Recursos Humanos	ADP
Admisiones, Ayuda Financiera y Recursos Humanos	DocuSign
Ayuda Financiera	TCF: streamline payment plan management
Marketing	• Redes Sociales (Youtube, FB, Instagram, Twitter, Pinterest, Tik Tok, LinkedIn) • SEMrush • Google (Analytics, Ads and Search Console) • Yelp • Zappier • WordPress • Mailchimp • SendHub • Google Drive

TI	• Round Cube • plesk • Windows Server (2012 R2 - 2016) • MySQL Server • FTP Server • Any Desk • Hyper V • Virtual Box • Linux (Centos 7) • Tawk to
Educación	• Moodle • Evolve

Cuadro 3.3: Inventario de sistemas o software

Elaborado por: Paúl Montesdeoca

Observación: El inventario de programas está organizado pero no lleva una descripción de que realiza cada sistema, ni un código especial para fácil identificación.

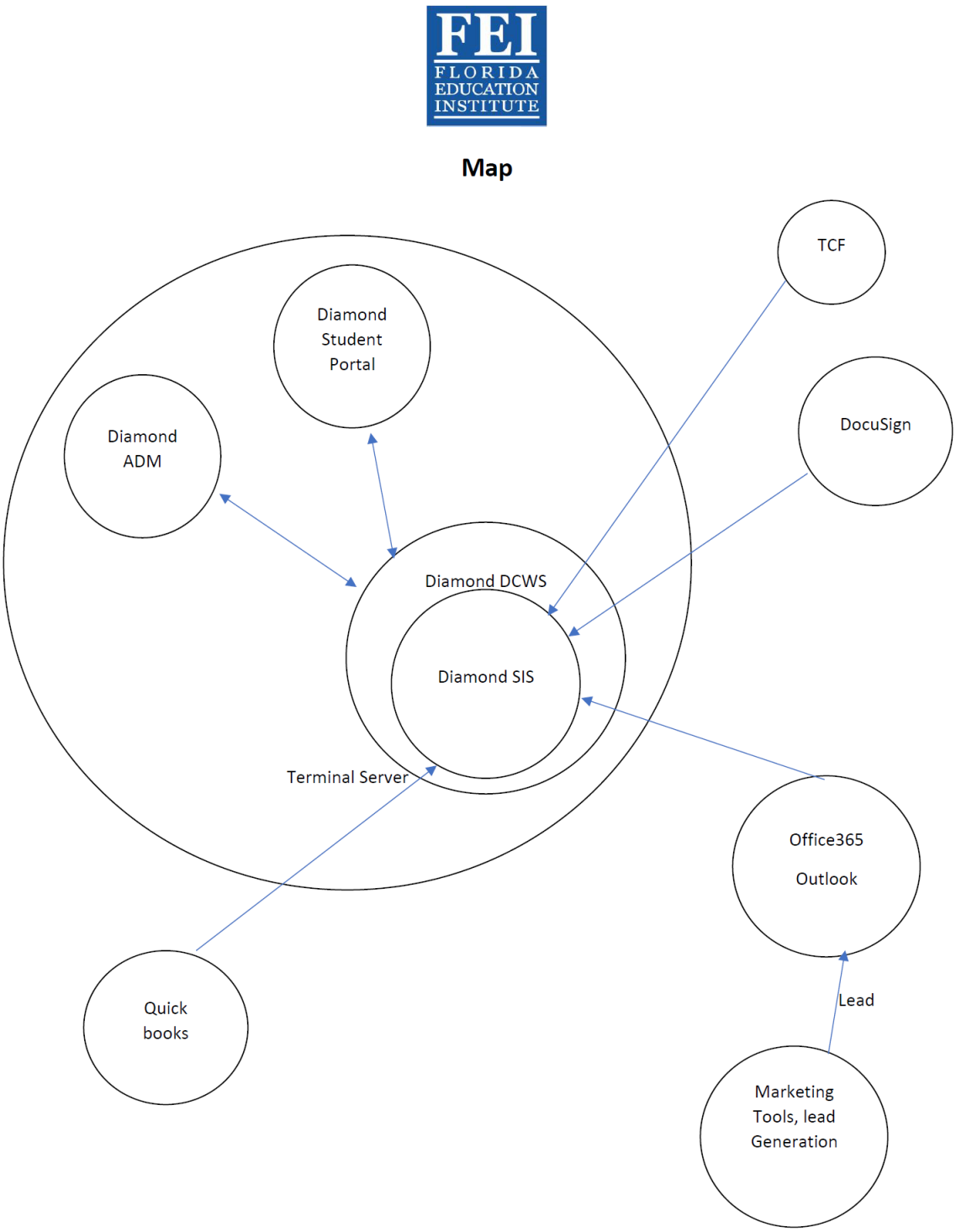


Figura 3.11: Mapa jerárquico de programas de FEI
Elaborado por: Paúl Montesdeoca

3.1.11 Servicios tecnológicos más utilizados por FEI

De acuerdo a la figura 3.11 los servicios que son más indispensables para FEI son el Diamond SIS, la cual es una herramienta contratada a la empresa Diamond SIS que se encuentra ubicada en California.

Este servicio controla todas las operaciones que se debe realizar durante todo el día en la institución es decir, esta herramienta maneja toda la información desde la presidencia, pasando por el control de contenidos educativos, supervisión de los profesores hasta llegar a la observación del estado de los estudiantes dentro de FEI.

Otro servicio muy importante es el Terminal Server, el cual permite conectarse al Diamond SIS, en cualquier parte del mundo mientras se tenga conexión a internet y las credenciales correspondientes que el departamente de TI provee a sus usuarios.

- Existen otros servicios y herramientas que son muy importantes para FEI como es el Office 365 y el portal para estudiantes, sin embargo, estas herramientas estan muy relacionadas entre si con Diamond SIS, por lo tanto si Diamond SIS cae o presenta fallas toda la organización queda fuera de servicio.
- Otro servicio que no tiene nada que ver con los programas especificados son el servicio de internet, el cual en caso de fallar, tanto profesores como estudiantes pueden acceder a las herramientas de FEI mediante sus propios medios, desde lugares donde exista señal de internet para continuar con el trabajo normal.
- En caso de que sea totalmente indispensable usar las herramientas dentro de las instalaciones de la institución existe un sistema de red celular que también provee internet en caso de que la red tradicional este fallando.

3.1.12 Software utilizado por el departamento de TI

Window Server

Window Server 2016 es el sistema operativo que FEI utiliza para almacenar archivos y aplicaciones multiusuario para ponerlos a disposición de toda la institución a través de Internet, además de monitorear la salud de todos los servidores que están bajo el dominio.

Con ayuda de este sistema operativo se crea terminales para los empleados para que puedan trabajar dentro de la red segura de la organización donde además se crean reglas de acceso y restricciones en la navegación web.

Este SO es operado unicamente por el encargado de TI, el cual puede realizar diferente cambios como añadir, modificar, buscar y eliminar usuarios, crear nuevas reglas a los usuarios, dar

permisos a otros usuarios para lectura y escritura de archivos y directorios dependiendo de su nivel dentro de la organización e instalar nuevos programas para mejorar la productividad de FEI.

La única persona que puede decidir estos cambios es el presidente de FEI, el cual notificará al encargado de TI y este proporcionará respuestas sobre si es correcto o válido realizar los cambios pedidos por presidencia.

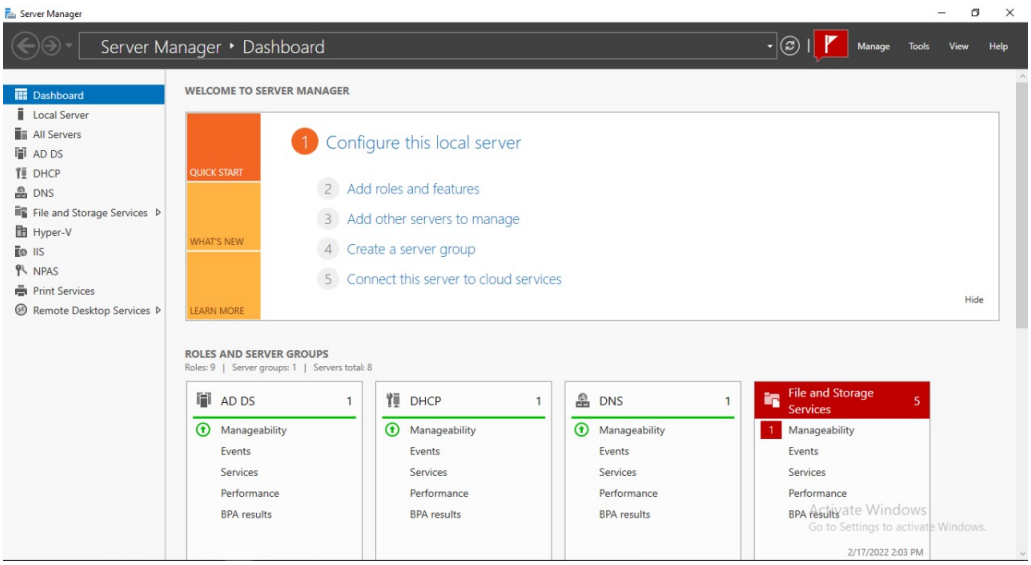


Figura 3.12: Window Server
Elaborado por: Paúl Montesdeoca

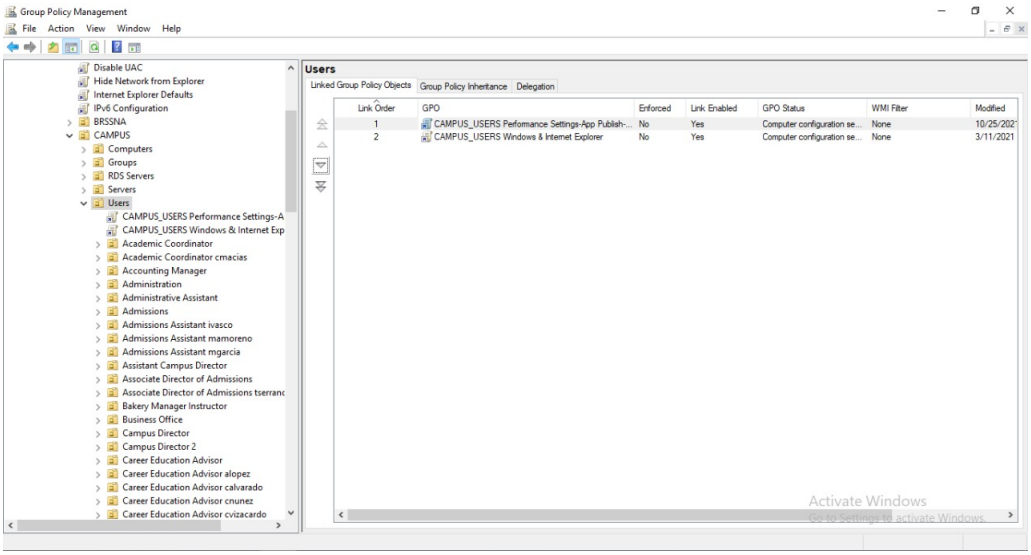


Figura 3.13: Reglas de Window Server
Elaborado por: Paúl Montesdeoca

3.1.13 Software utilizado por todo los departamentos de FEI

Diamond SIS

Diamond SIS es un software CRM para el manejo estudiantil, en este sofware se guarda toda la información de cada estudiante conjuntamente con su recorrido académico. Este programa además realiza el trabajo de captura de leads que permite el rastreo de posibles personas que podrían convertirse en estudiantes.

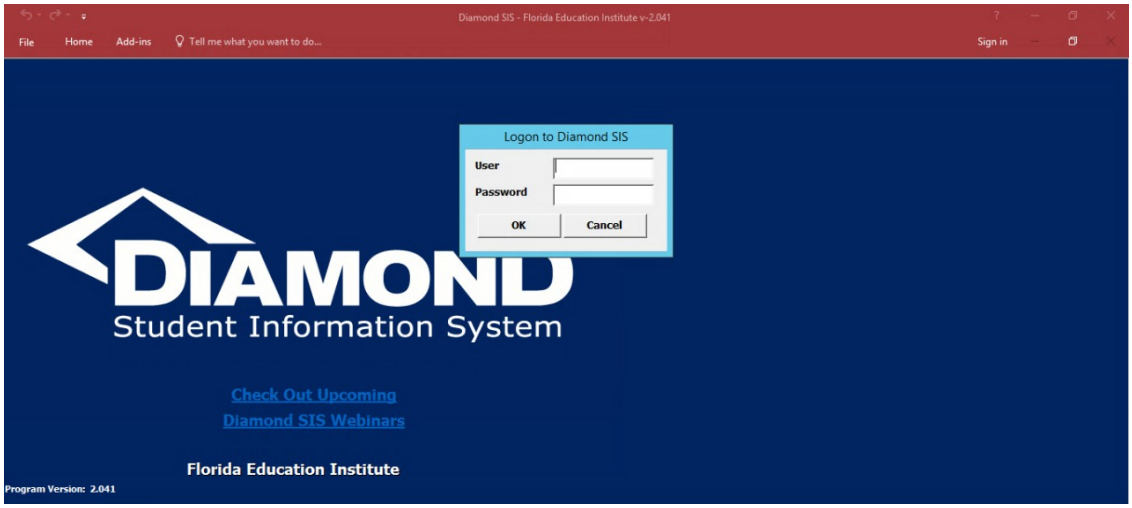


Figura 3.14: Diamond SIS
Elaborado por: Paúl Montesdeoca

Ooma

Ooma es un software que ofrece servicios de comunicaciones que incluyen llamadas de voz sobre IP (VoIP) para FEI, este programa controla todas las llamadas que ingresan y salen de FEI, además de grabar conversaciones que se guarda en una base de datos que el mismo proveedor de servicio proporciona.

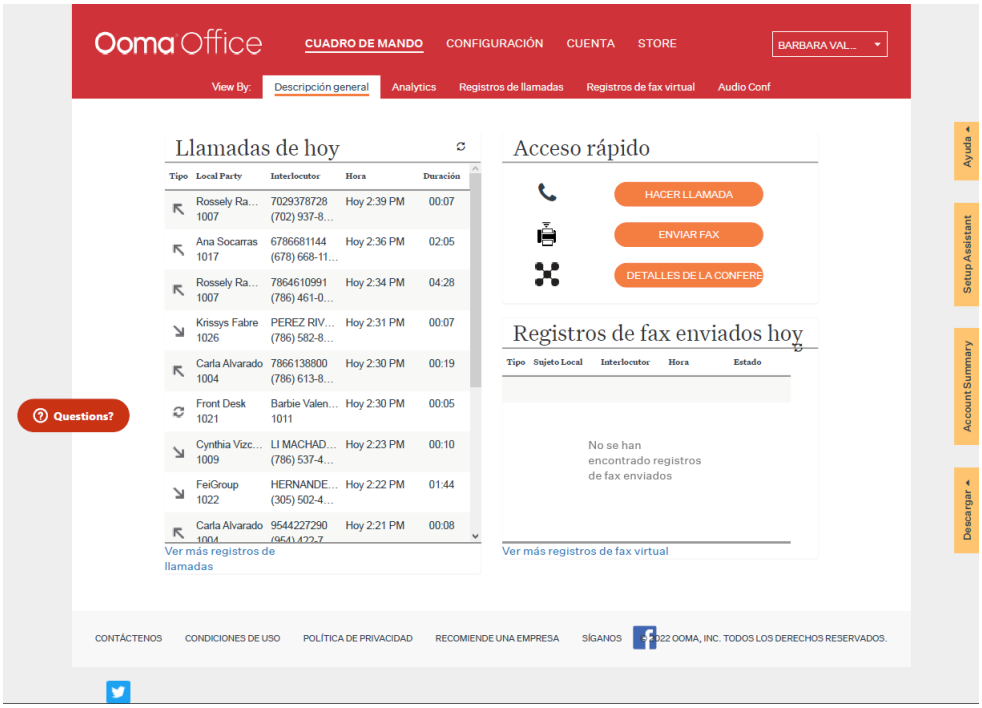


Figura 3.15: Ooma
Elaborado por: Paúl Montesdeoca

Office 365

Son un conjunto de programas de ofimática como Word, Excel, PowerPoint utilizados por FEI para la creación de documentos.

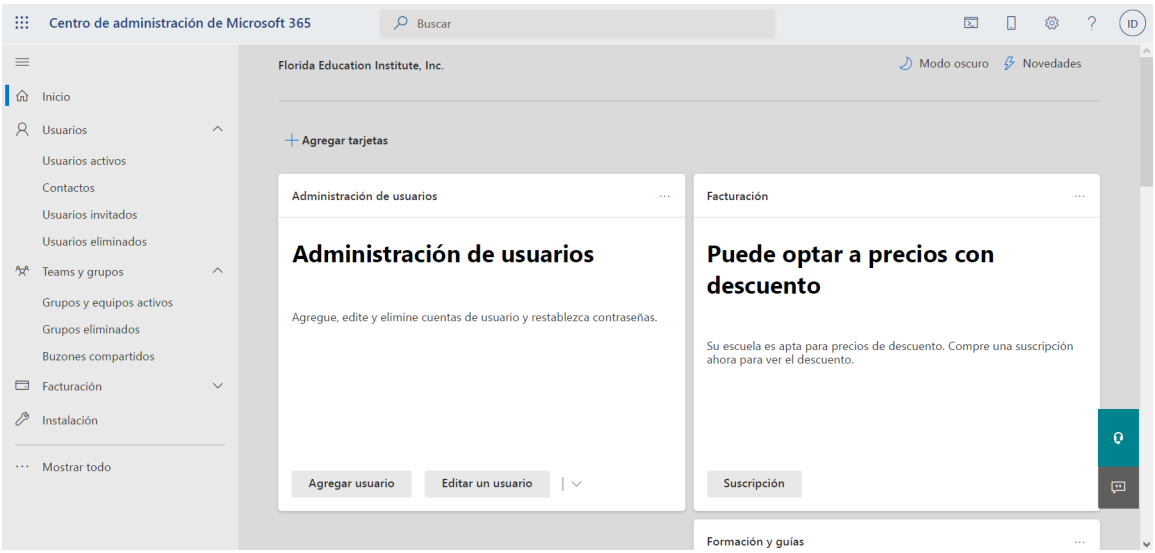


Figura 3.16: Microsoft 365
Elaborado por: Paúl Montesdeoca

QuickBooks

Es una aplicación que sirve para la administración de las cuentas financieras de la institución.

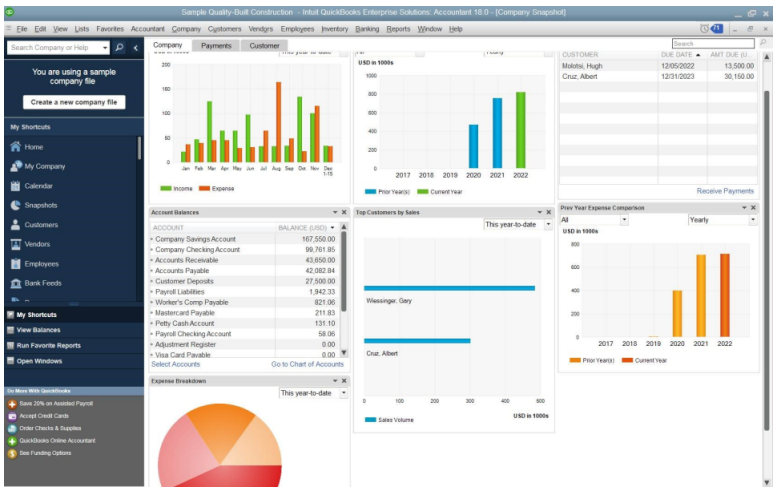


Figura 3.17: QuickBooks
Elaborado por: Paúl Montesdeoca

ADP

Es un sistema de registro de personal que FEI utiliza para registrar la entrada y salida de sus empleados.

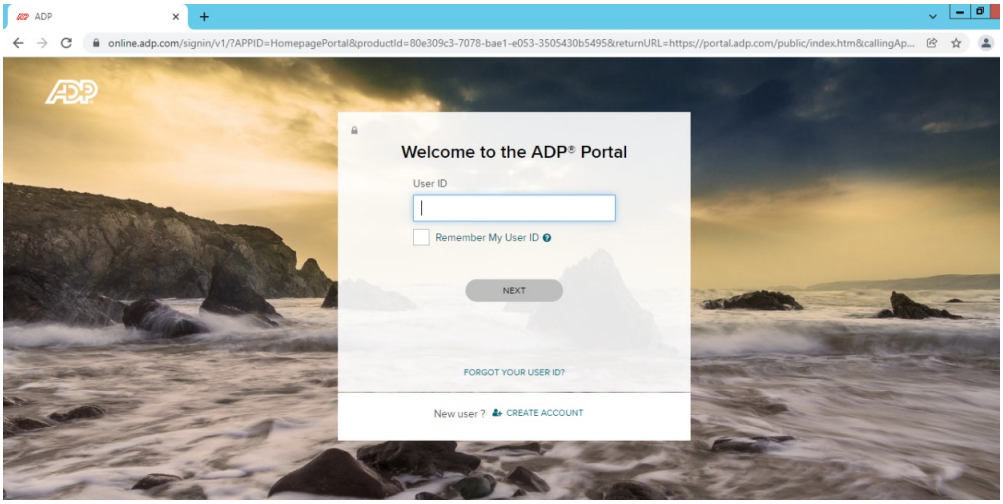


Figura 3.18: ADP
Elaborado por: Paúl Montesdeoca

Semrush

Es un sistema que se utiliza para obtener estadísticas de los datos obtenidos al momento de que una persona navega en Internet y busca palabras claves relacionadas con educación en los motores de búsqueda como google y bing.

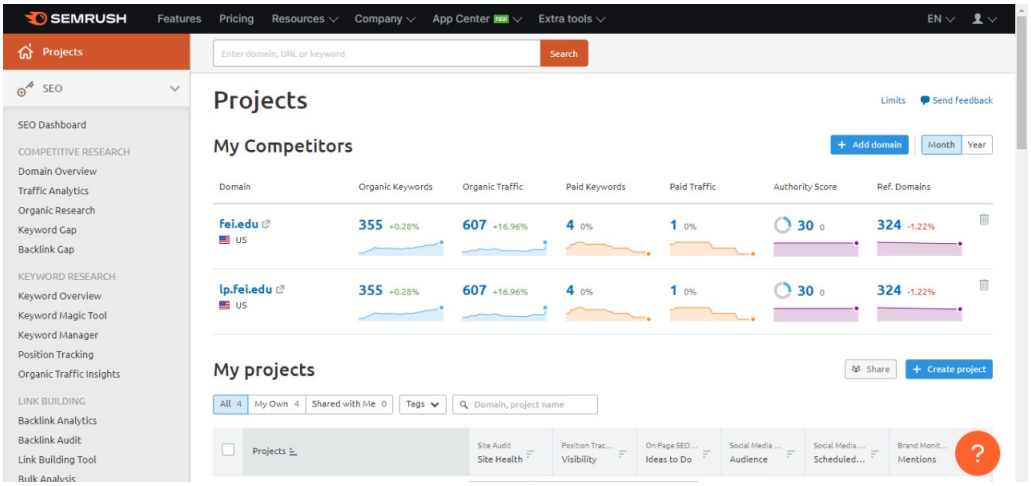


Figura 3.19: Semrush
Elaborado por: Paúl Montesdeoca

DocuSign

Es un sistema que FEI utiliza para la firma de documentos electrónicos.

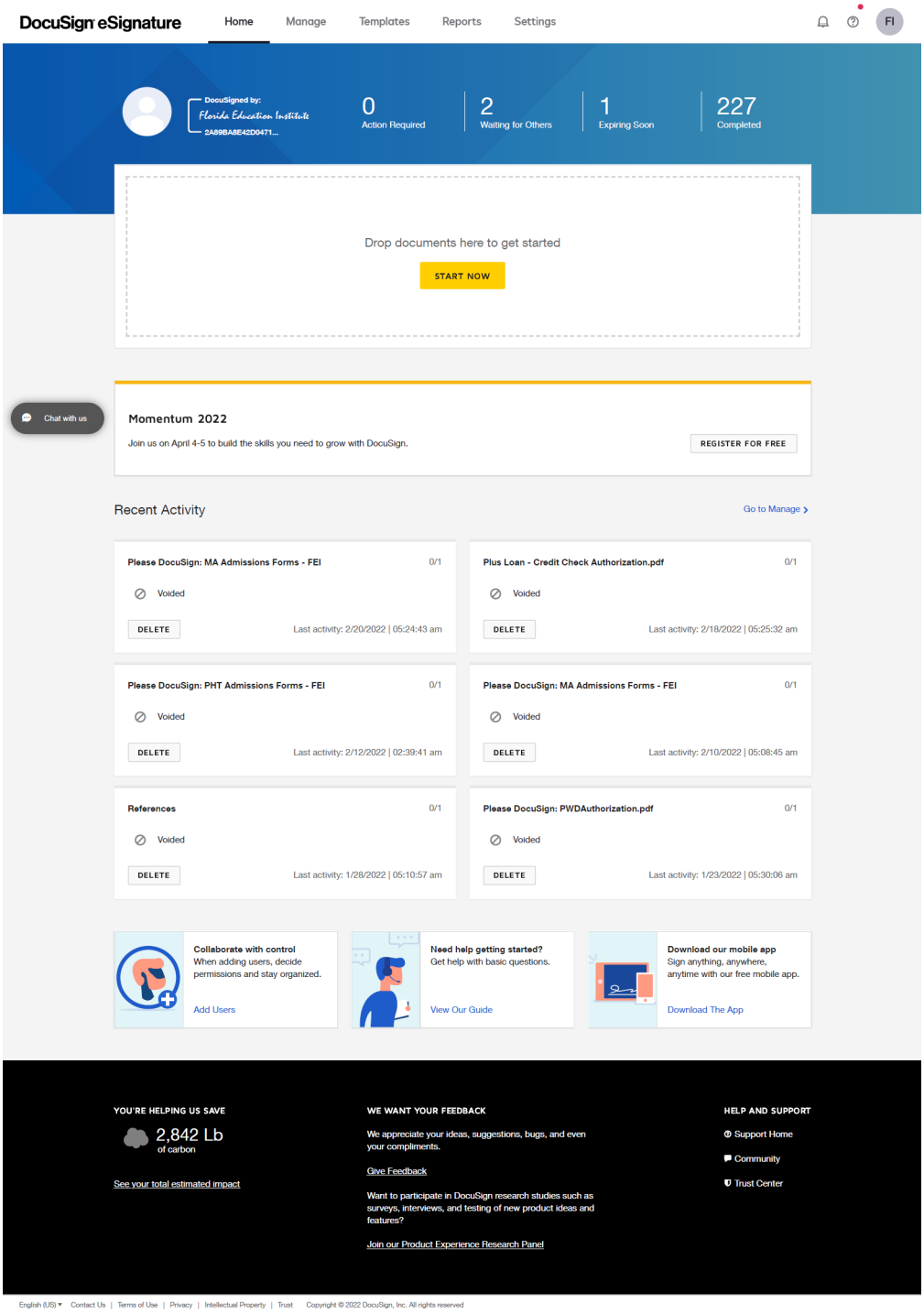


Figura 3.20: DocuSign
Elaborado por: Paúl Montesdeoca

Google Analytics

Es un servicio de Google que permite el rastreo del comportamiento de los usuarios al momento de interactuar con las páginas web de FEI, permitiendo conocer el estado de presencia en la red de la institución.

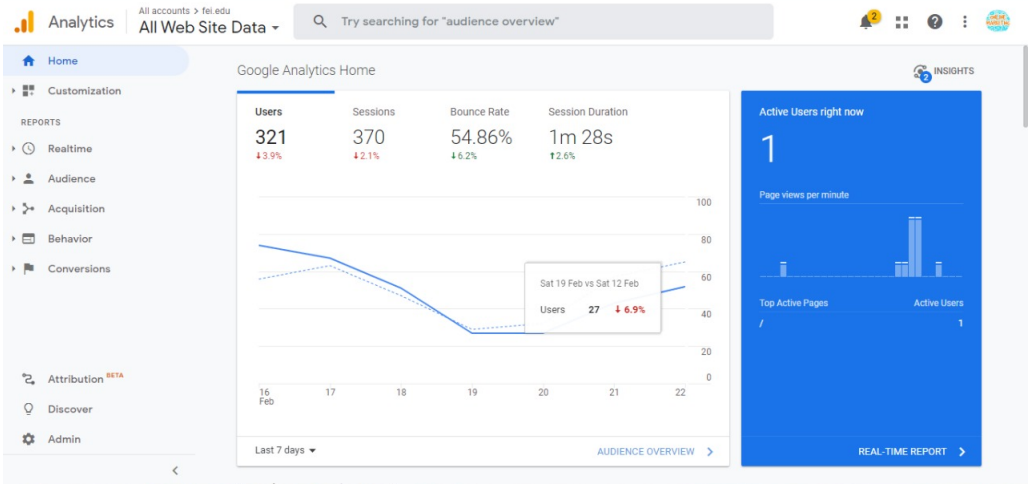


Figura 3.21: Dashboard de Google Analytics
Elaborado por: Paúl Montesdeoca

Mailchimp

Con esta herramienta se administra las campañas de marketing mediante correo.

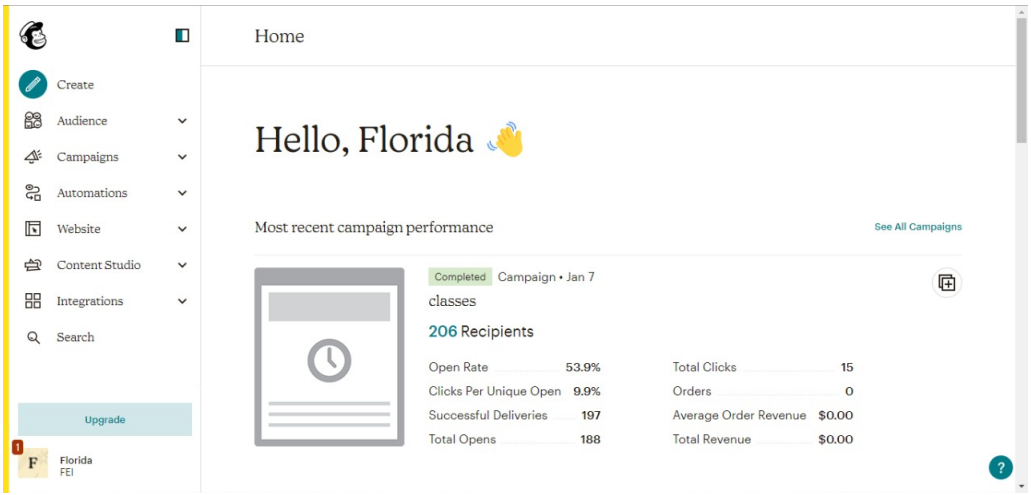


Figura 3.22: Mailchimp
Elaborado por: Paúl Montesdeoca

Zapier

Zapier es un producto que permite a los FEI integrar las aplicaciones web que utiliza, para centralizar todas sus actividades y mejorar la eficiencia del servicio.

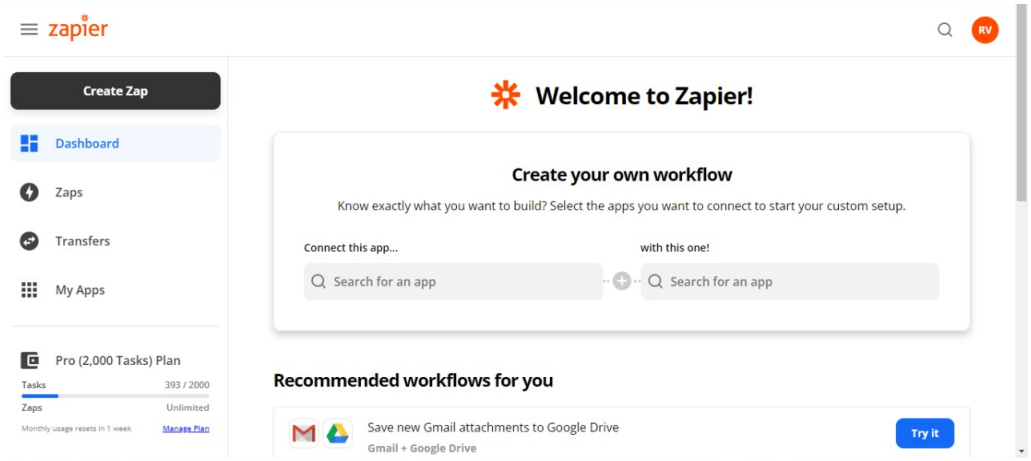


Figura 3.23: Zapier
Elaborado por: Paúl Montesdeoca

Wordpress

Con esta herramienta se administra la página web de FEI.

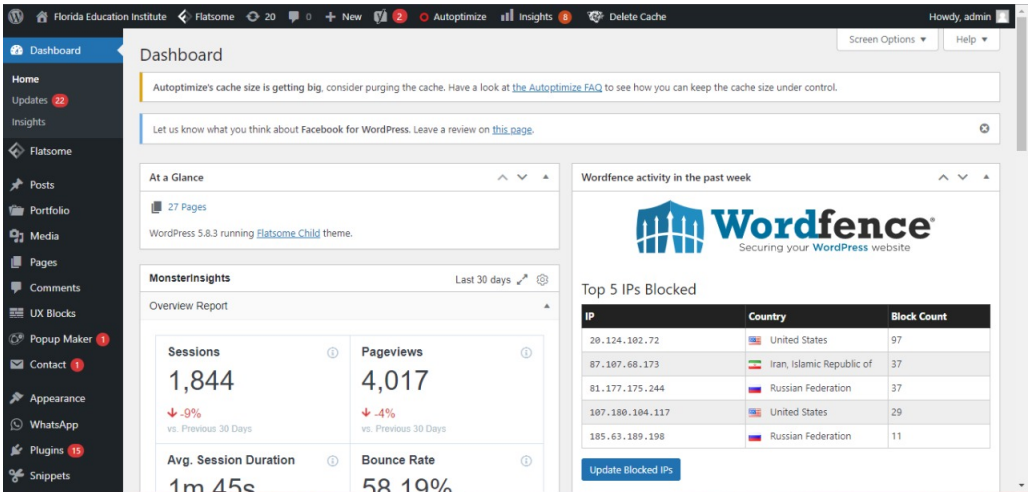


Figura 3.24: Wordpress
Elaborado por: Paúl Montesdeoca

Sendhub

Con esta herramienta se administra los mensajes de texto que reciben los teléfonos de FEI.

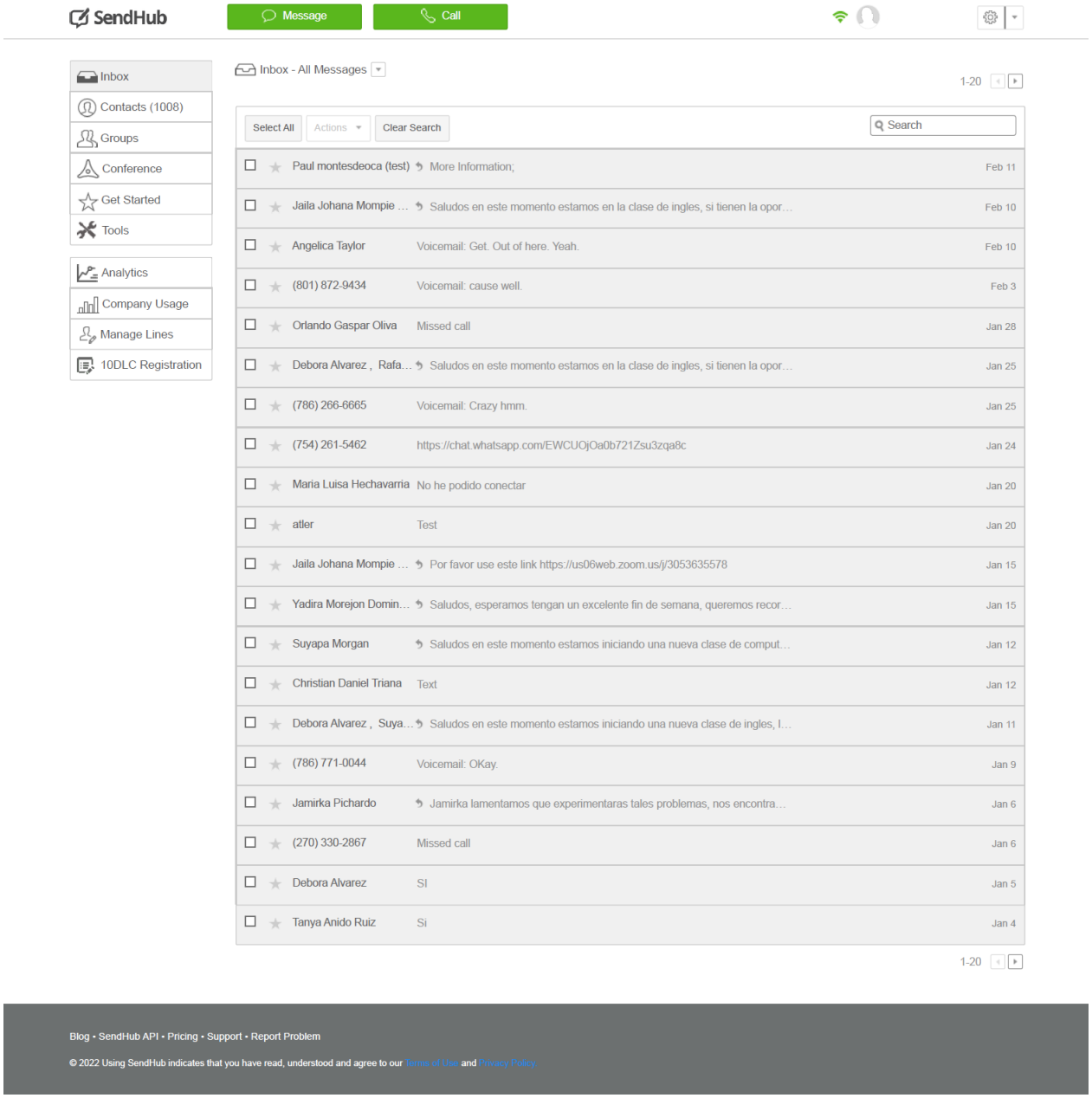


Figura 3.25: Sendhub
Elaborado por: Paúl Montesdeoca

AnyDesk

Este software permite el manejo de las máquinas virtuales de FEI.

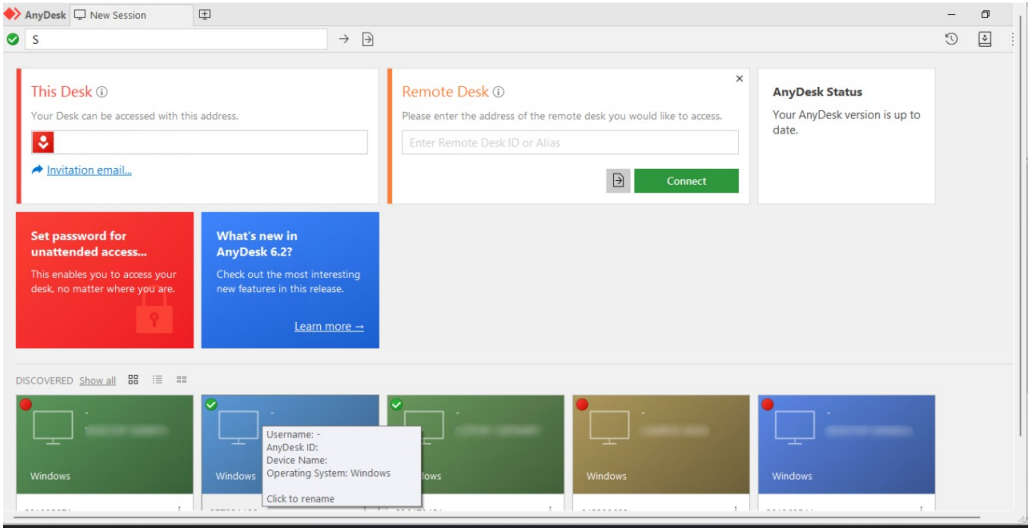


Figura 3.26: AnyDesk
Elaborado por: Paúl Montesdeoca

TawkTo

Es un servicio web que permite la interación con algún usuario que esté visitando la página web de FEI.

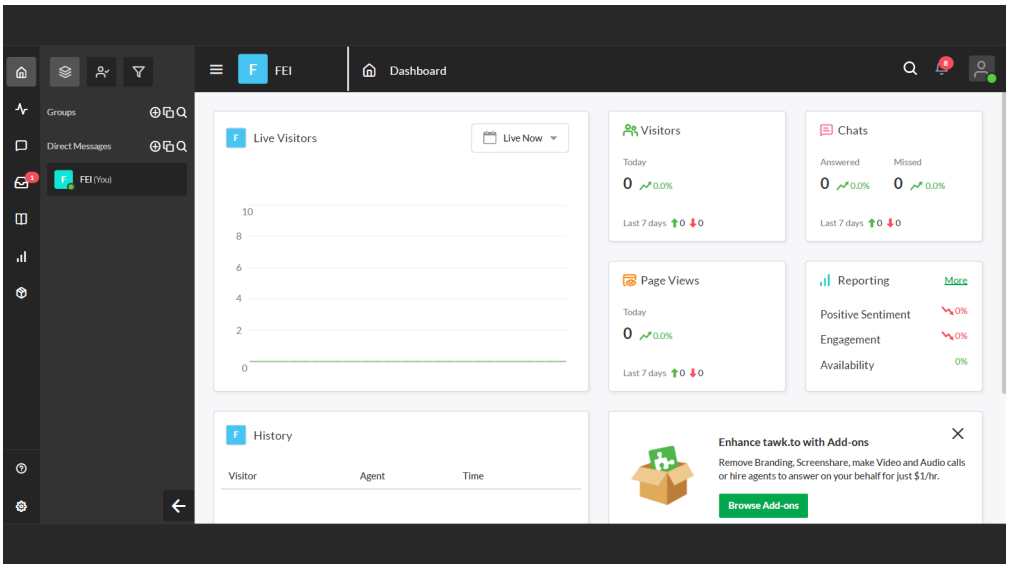


Figura 3.27: TawkTo
Elaborado por: Paúl Montesdeoca

Moodle

Es un servicio web que se utiliza como herramienta de aprendizaje donde FEI ofrece a sus estudiantes las herramientas necesarias para continuar con sus estudios de manera virtual.

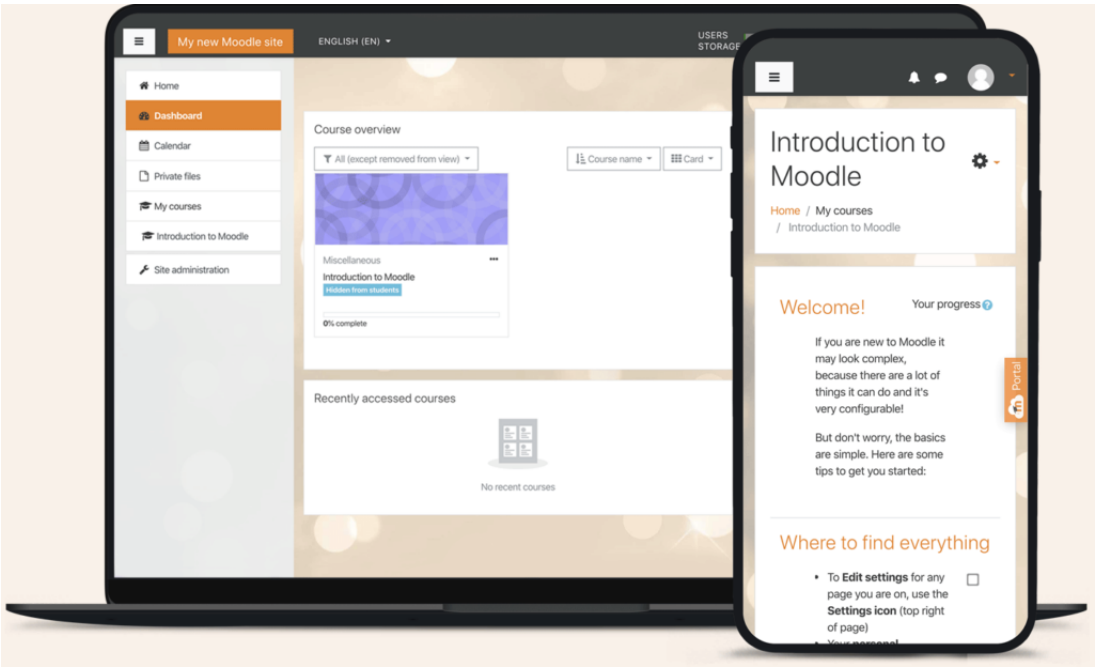


Figura 3.28: Moodle
Elaborado por: Paúl Montesdeoca

Zoom

Esta herramienta web permite las videollamadas entre personal de FEI y sus estudiantes.

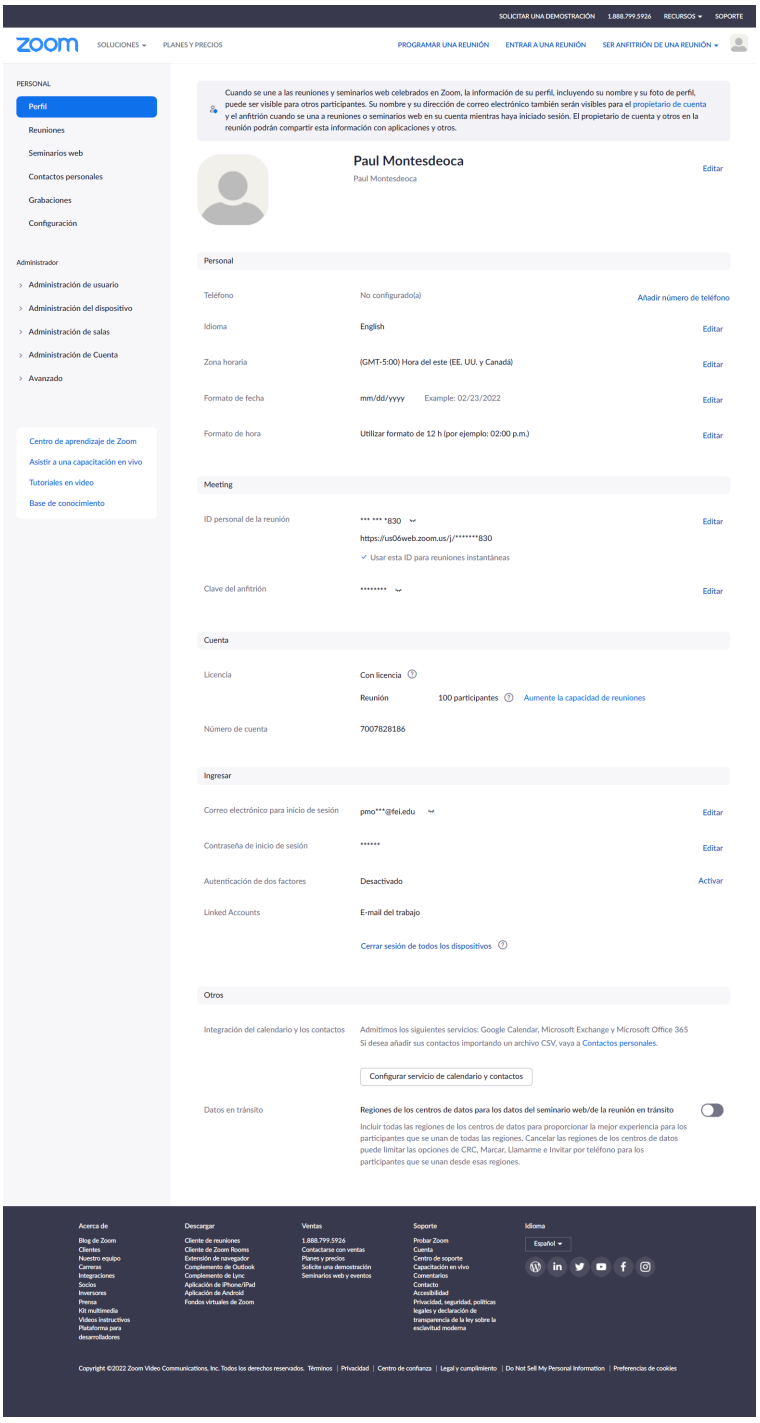


Figura 3.29: Zoom
Elaborado por: Paúl Montesdeoca

Facebook

Twitter

Tiktok

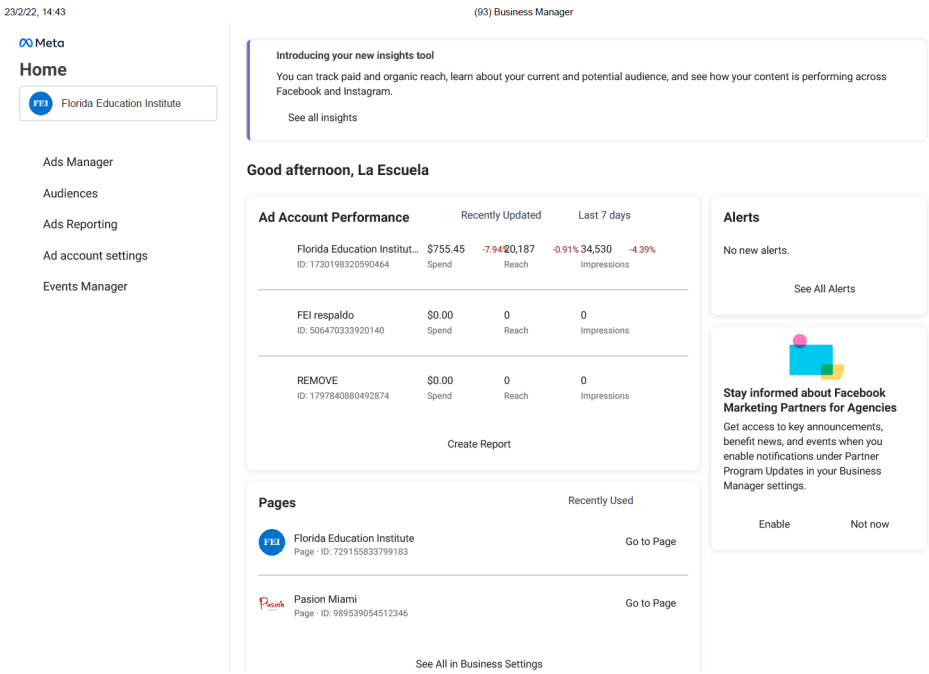


Figura 3.30: Facebook
Elaborado por: Paúl Montesdeoca

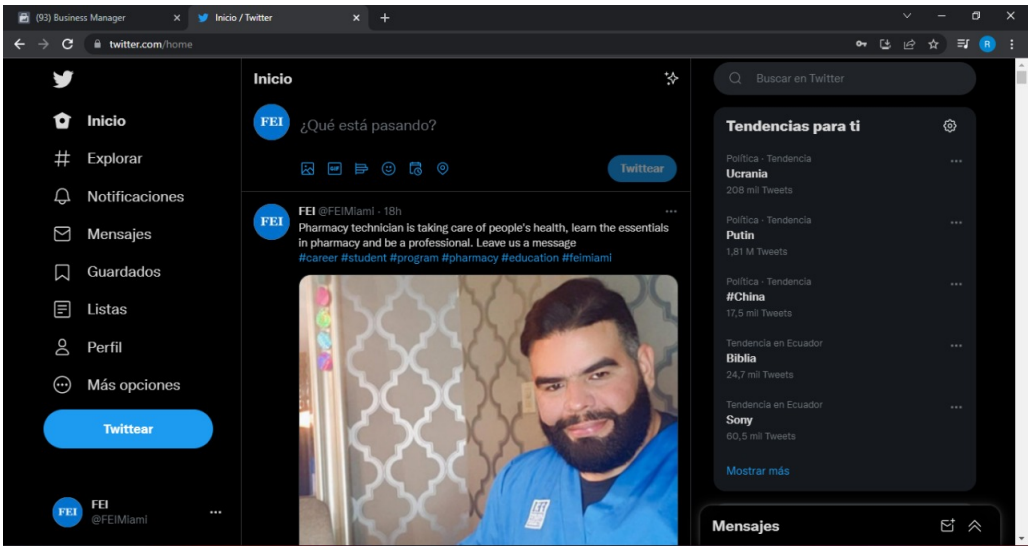


Figura 3.31: Twitter
Elaborado por: Paúl Montesdeoca

Figura 3.32: Tiktok
Elaborado por: Paúl Montesdeoca

3.1.14 Respaldos informáticos internos

FEI tiene unas estrictas políticas sobre el manejo de la información ya que es demasiado importante y vital para el correcto funcionamiento de la institución por lo cual se tiene implementado una normativa que siempre se debe cumplir.

Tipos de respaldos

En FEI se maneja dos tipos de respaldos.

- **Respaldo completo:** Se procede a realizar una copia exacta de todos los archivos y carpetas con los registro de valor con la fecha y hora en la que se completa, aunque toma bastante tiempo.
- **Respaldo incremental:** A diferencia del respaldo completo, solo se copia los archivos y carpetas que han sido modificadas desde la última copia de seguridad.

Versionamiento

- Un respaldo completo debe ser realizado diariamente con información de hasta 5 meses atrás.
- Un respaldo incremental debe ser realizado diariamente y cada vez que se crea un nuevo respaldo completo.
- Se debe realizar un respaldo mensual por el responsable de TI en el disco duro de la presidencia con la fecha de realización.
- Un respaldo incremental mensual debe ser guardado por el responsable de TI en el disco duro de la presidencia con la fecha de realización.

Responsabilidades en cuanto al respaldo

Durante el proceso de respaldo tres responsabilidades son consideradas.

- **Ejecutor:** Es la persona responsable de realizar las tareas de respaldo y registrarlos diariamente.
- **Revisor:** Es la persona encargada del seguimiento y ejecución de las copias de seguridad.
- **Custodio:** Es la persona encargada de tener una copia completa de los respaldos y máquina virtual.

Dispositivos de almacenamiento de respaldo

FEI maneja dos tipos de dispositivos:

- **Servidor NAS (almacenamiento conectado a la red).** Es una solución de almacenamiento donde se guarda la información de la institución en respaldos diarios.
- **Disco duro externo.** La presidencia tiene un disco duro, donde se guarda información adicional mensual y anual, este disco duro se encuentra en el mismo cuarto de servidores.

Personal a cargo de la recuperación de datos

- **Encargado del área de TI:** Es el responsable de identificar la magnitud de la pérdida de datos y llevar a cabo la respectiva recuperación de información. Debe existir una petición por escrito y debe ser autorizada por la presidencia.
- **Presidente:** Es el responsable de observar las tareas de recuperación de datos y asegurarse que la información sea correcta.

Seguridad de los respaldos

Las copias deben ser guardadas en dispositivos con NAS donde solo el encargado de TI y el presidente tengan acceso, la información debe estar en archivos comprimidos o carpetas con seguridad adicional, deben tener una contraseña.

Requerimientos para la recuperación de datos

Dentro de FEI, existe una normativa donde el miembro del personal que necesite restaurar información, ya sea de un archivo o directorio completo, debe enviar un correo electrónico al presidente y al encargado de TI con la siguiente información:

- Nombre de la persona
- Nombre del archivo o directorio
- Fecha de creación del archivo o directorio
- Razón por la cual pide restauración del archivo o directorio

En caso de no ser aprobado, la petición debe ser rectificada.

En caso de ser aprobada, el encargado de TI debe ejecutar la orden en la próxima hora laboral.

Si la restauración es efectiva, se debe notificar por correo electrónico a la personas involucradas.

Si la restauración no fue exitosa, se debe identificar el error y enviar los resultados por correo electrónico a las personas involucradas.

Casos en los que se llevan a cabo la recuperación de datos

- Desastres naturales: Tsunami, terremotos, huracanes, etc.
- Fallas de energía: Sobretensiones y descargas que afectan a los servidores.
- Errores humanos: Borrado involuntario o voluntario de información por parte del personal.

Observación: Se nota que el sistema de respaldo interno genera muchas copias que aumenta el uso de recursos de FEI y por lo tanto no es eficiente. Otro caso es el tiempo entre respaldo y respaldo ya sea el respaldo incremental como el completo tienen gran margen de tiempo entre ellos por lo que se puede perder mucha información entre estos periodos tan largos.

3.1.15 Respaldos informáticos externos

FEI cuenta con servicios de respaldos externos o de terceros para una mayor seguridad en el manejo de datos. Todos estos servicios se encuentran en la nube y pueden ser accedidos en cualquier parte del mundo y en cualquier momento.

Los dos servicios que se tienen utilizados son IONOS y Acronis, los dos son utilizados tanto para el manejo de servidores como de respaldo de la información. IONOS controla los servidores y mantiene un respaldo de todos los datos que maneja la institución mientras que Acronis maneja el respaldo de las máquinas virtuales creadas en los servidores y también parte de la información de FEI. Estos proveedores tienen sus centros de operaciones y servicios de respaldo tanto en Estados Unidos como en Europa, por lo tanto se tiene una doble seguridad en cuanto se trata al almacenamiento de los datos.

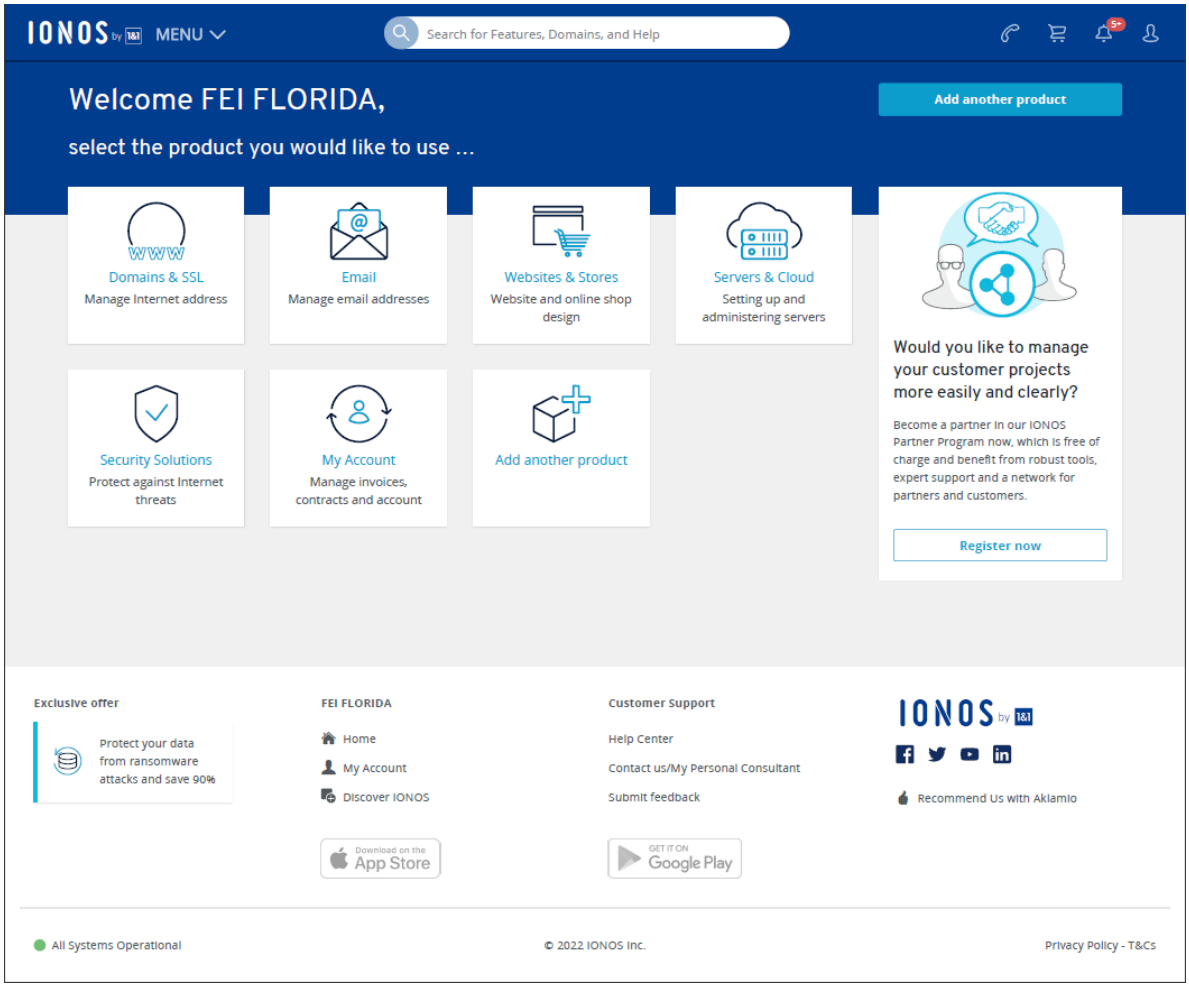


Figura 3.33: Dashboard de IONOS
Elaborado por: Paúl Montesdeoca

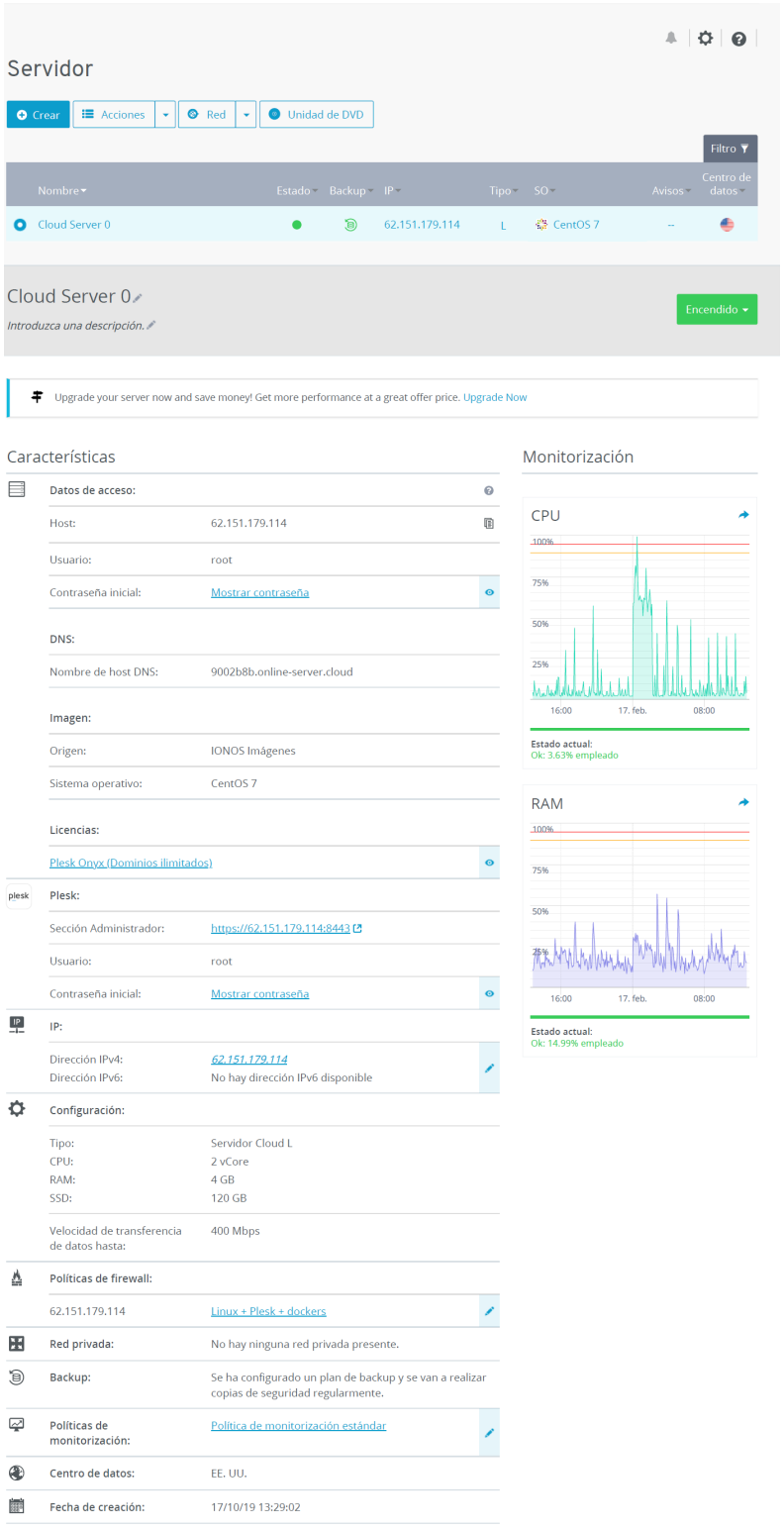


Figura 3.34: Servidor IONOS
Elaborado por: Paúl Montesdeoca

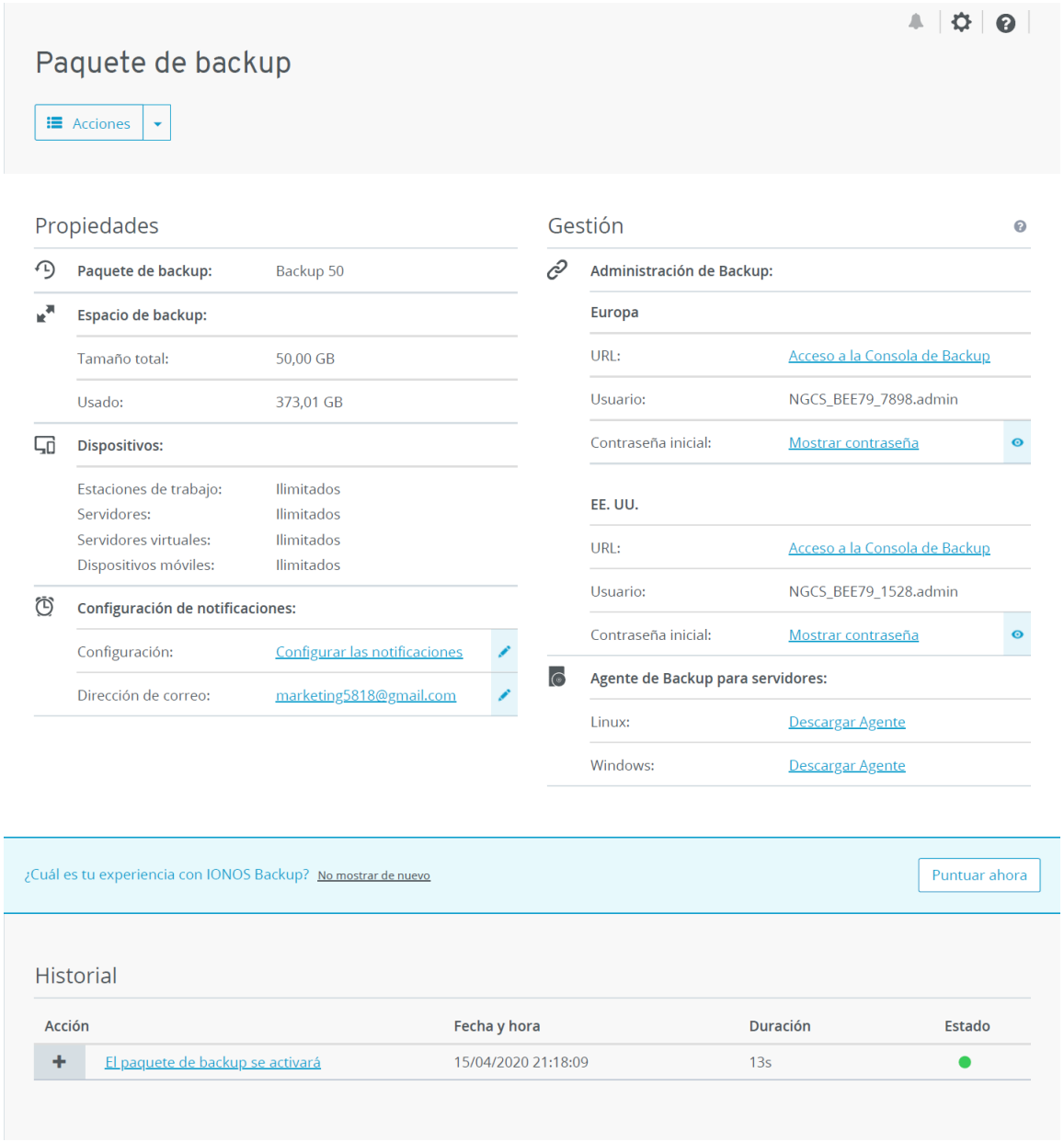


Figura 3.35: Servicio de backup de IONOS
Elaborado por: Paúl Montesdeoca

Figura 3.36: Dashboard de Acronis
Elaborado por: Paúl Montesdeoca

Figura 3.37: Servicio de backup Acronis
Elaborado por: Paúl Montesdeoca

3.1.16 Firewall

Dentro de los servidores de FEI se maneja varias políticas de Firewall para bloquear accesos no autorizados y poder seguir utilizando los demás servicios que FEI provee a sus empleados y estudiantes. Estas políticas son administradas con ayuda de los servicios de IONOS.

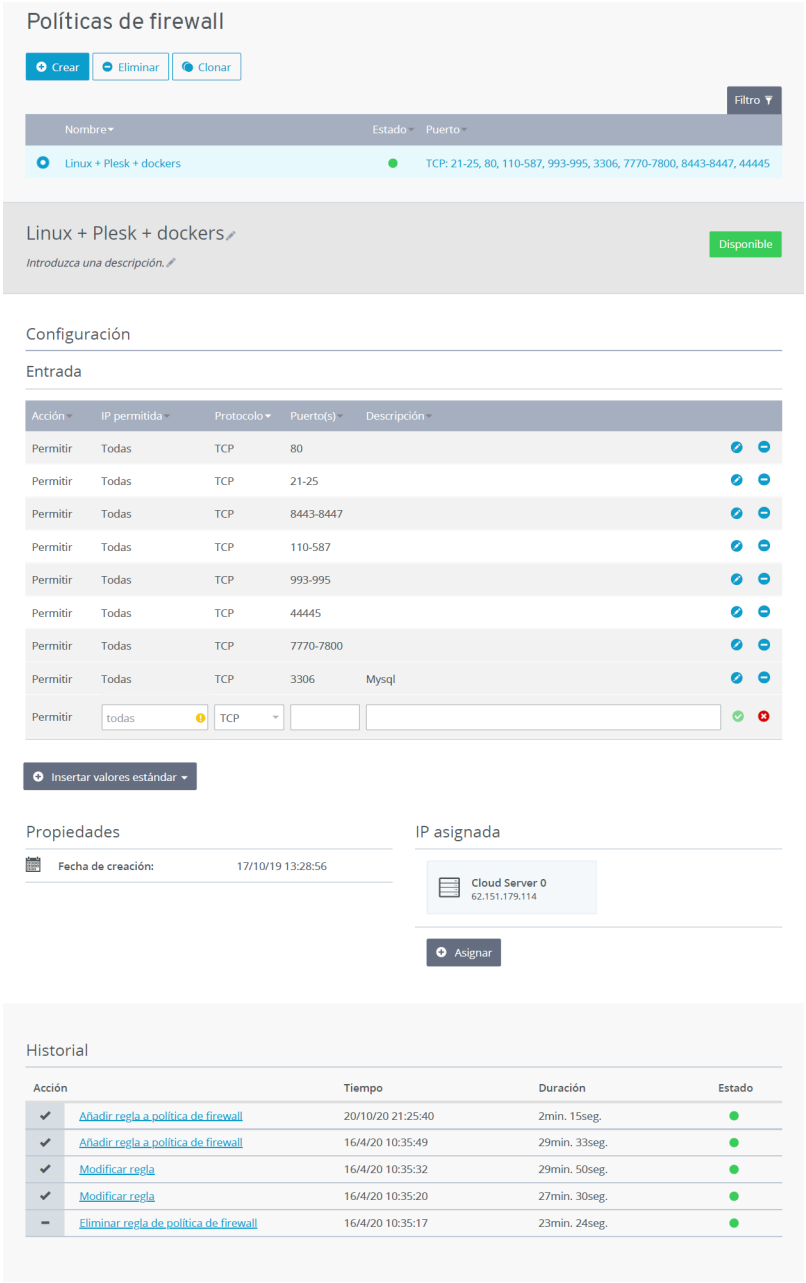


Figura 3.38: Políticas de Firewall con IONOS
Elaborado por: Paúl Montesdeoca

3.1.17 Dominios

FEI cuenta con una gran cantidad de dominios que son utilizados para proveer servicios a sus empleados y estudiantes, estos dominios son administrados en la herramienta PLESK donde solo el encargado de TI tiene acceso completo a ellos.

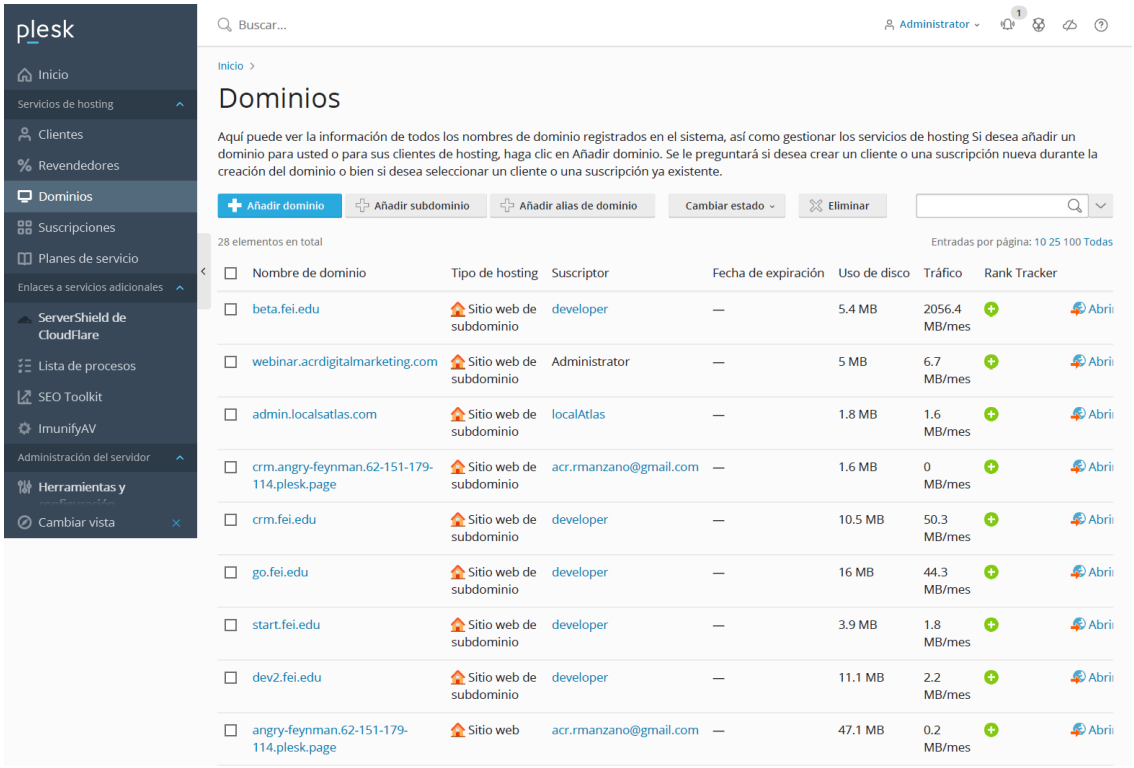


Figura 3.39: Dominios de FEI
Elaborado por: Paúl Montesdeoca

3.1.18 Restricciones y accesos al personal de la institución

Dentro de las políticas internas de la institución está el acceso restringido a ciertas funciones que solo el administrador o personal autorizado puede realizar al trabajar con los recursos informáticos.

Las funciones restringidas a nivel lógico son:

- Instalación de programas
- Navegación a sitios prohibidos por la institución
- Cambiar el nombre a archivos o carpetas que fueran creadas por el administrador
- Cambio de contraseñas

Las funciones restringidas a nivel físico son:

- Ingresar al cuarto de servidores sin previa autorización
- Mover algún dispositivo o equipo dentro de la institución
- Sacar algún dispositivo o equipo fuera de la institución

3.1.19 Topología de red de FEI

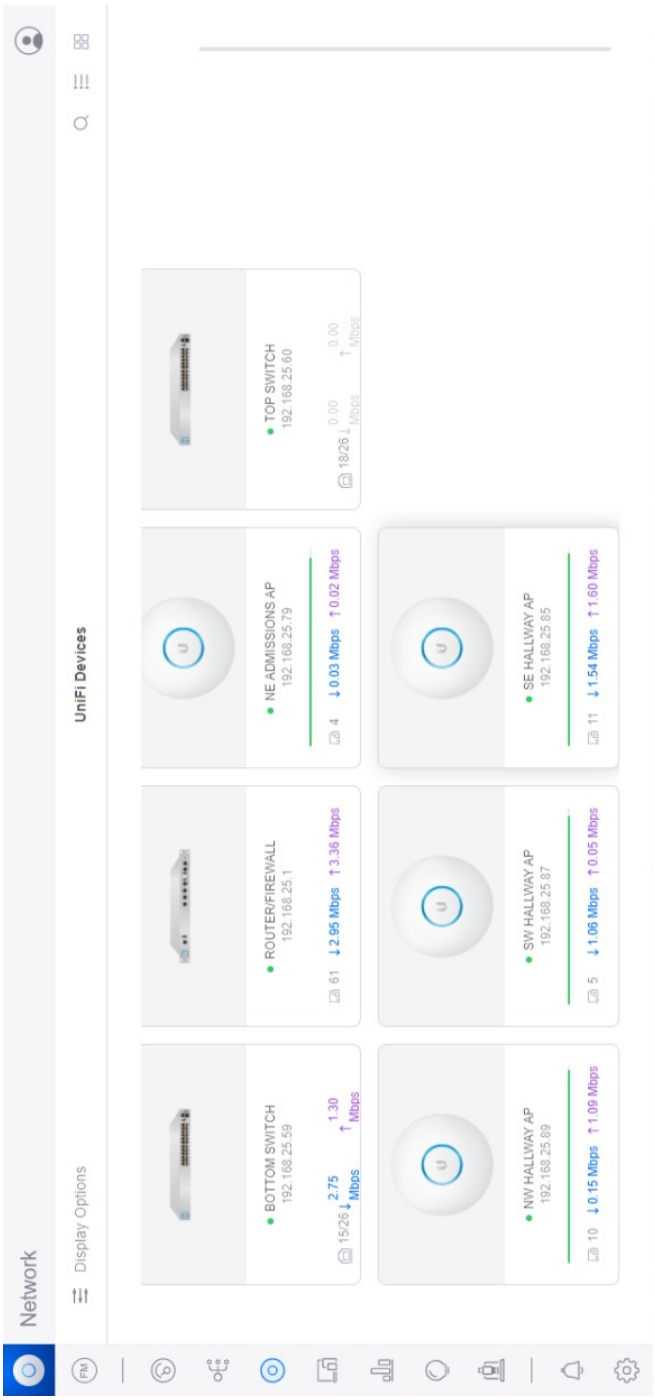


Figura 3.40: Equipos de red
Elaborado por: Paúl Montesdeoca

Figura 3.41: IP de red
Elaborado por: Paúl Montesdeoca

3.1.20 Wifi e Internet

El personal y los estudiantes de FEI tiene acceso a internet dentro de las instalaciones, el cual está monitoreado siempre para evitar posibles ataques o problemas dentro de la red de la institución.

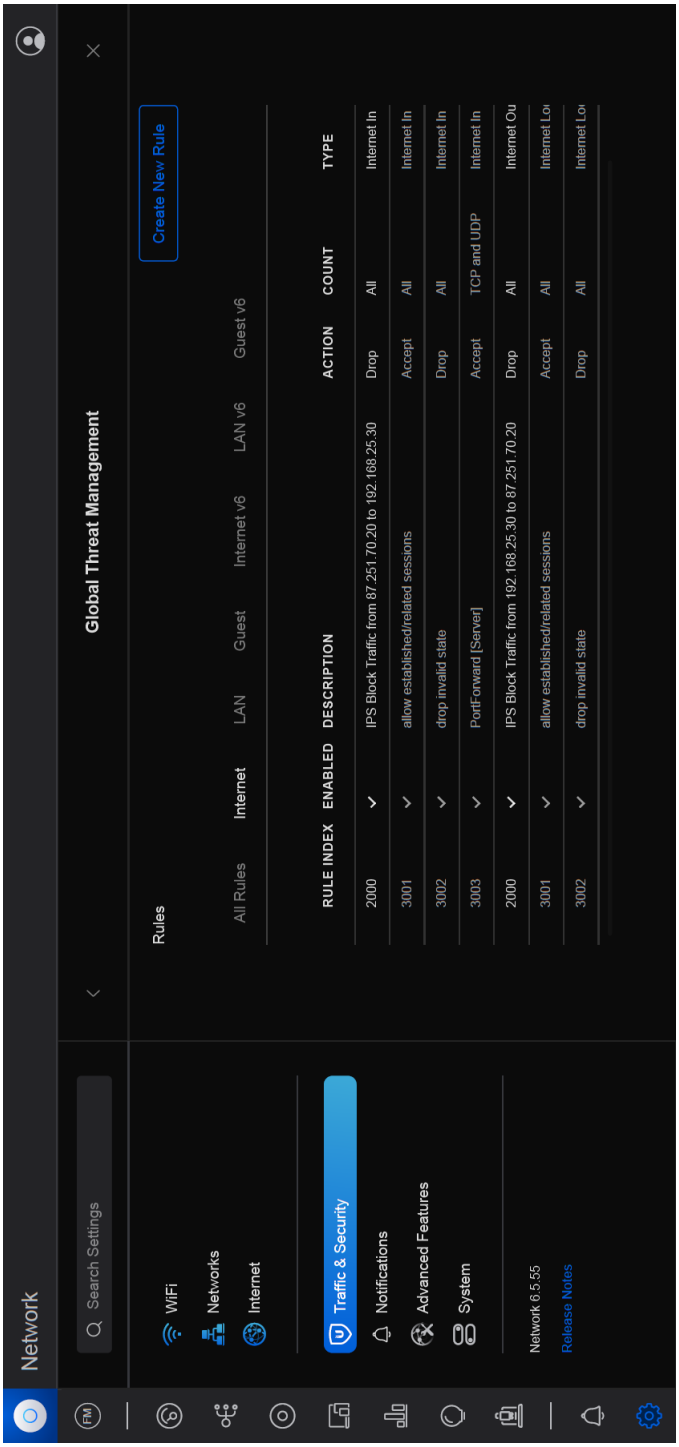


Figura 3.42: Tráfico y seguridad de red
Elaborado por: Paúl Montesdeoca

Figura 3.43: Redes de FEI
Elaborado por: Paúl Montesdeoca

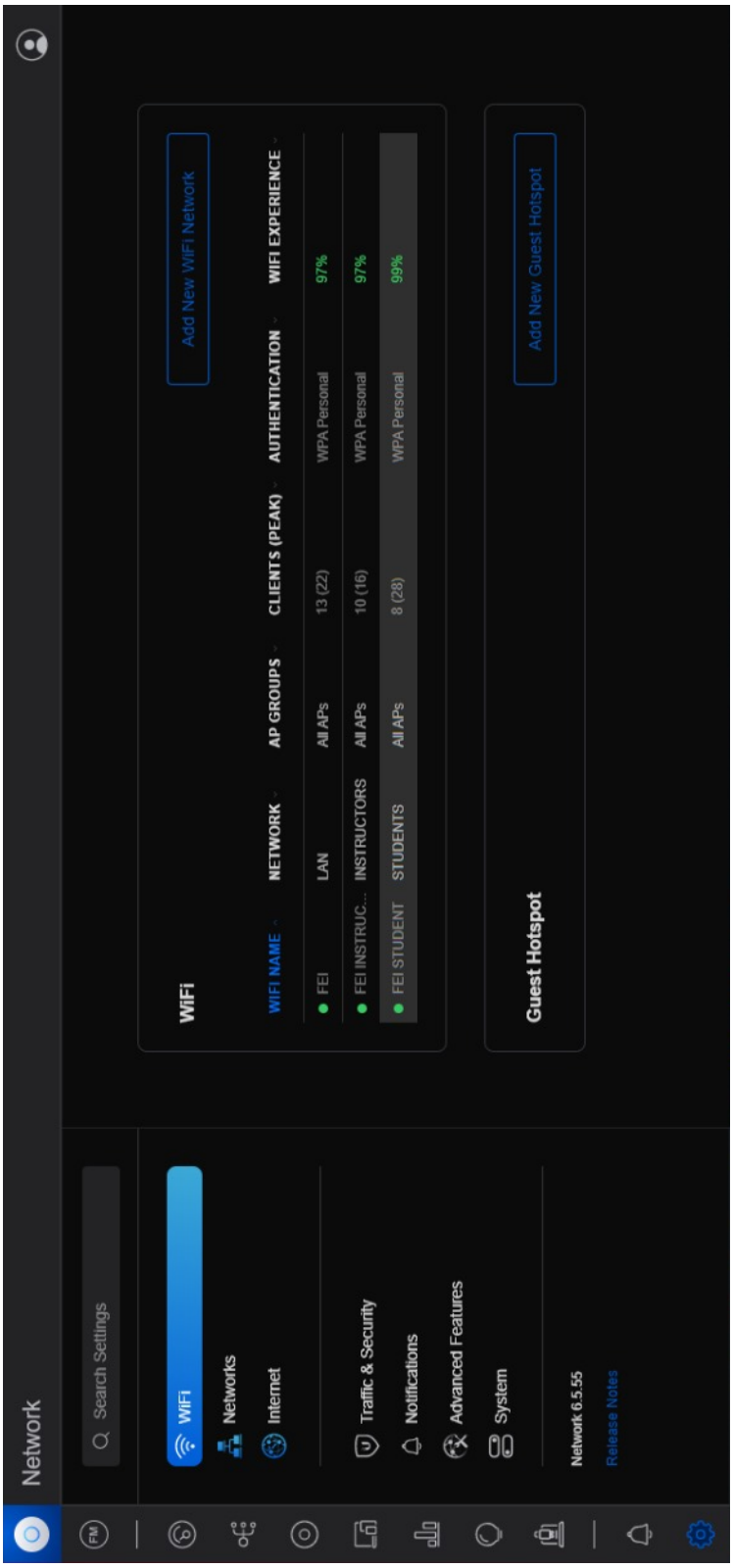


Figura 3.44: Wifi de FEI
Elaborado por: Paúl Montesdeoca

3.1.21 Contraseñas

Dentro de las políticas de FEI existen normativas sobre el uso responsable de las contraseñas de los miembros de la institución, el departamento de TI, nunca pedirá a los usuarios contraseñas personales que puedan incidir en fallas de seguridad. El personal de FEI debe seguir los siguientes estatutos.

- Las contraseñas son personales y no son transferibles
- Las contraseñas deben ser cambiadas periodicamente
- No ingresar contraseñas fáciles como: números de identificaciones personales, fechas de nacimiento, nombres de familiares o mascotas
- La nueva contraseña debe tener al menos 8 caracteres de longitud
- La nueva contraseña debe tener al menos un signo especial: $%&!/)*
- La nueva contraseña debe tener al menos un caracter numérico
- Las contraseñas de herramientas externas de cada departamento debe ser compartida con el departamento de TI y la presidencia para que tengan acceso y control

Los usuarios que no se sometan a estas políticas serán sancionados de acuerdo a las regulaciones internas de FEI

El cambio de contraseña de servicios que ofrece FEI serán hechas automáticamente y en otros casos se deberá realizar una petición por correo electrónico al encargado de TI para realizar dicho trámite.

3.1.22 File System

El File System es una herramienta que permite administrar los directorios y archivos del personal de la institución mediante varias políticas y reglas. Este sistema permite el uso correcto de los recursos informáticos al dar cierta cantidad de espacio de trabajo (espacio de memoria) dentro de los servidores, además de prevenir que en algunas carpetas los usuarios ingresen o eliminen información importante.

Observación: Este sistema fue recientemente renovado por lo tanto sus resultados han sido los esperados y se ha mejorado el manejo de la información además de su seguridad.

3.1.23 Utilización del correo institucional

FEI tiene un correo institucional el cual se utiliza para el intercambio de información interna entre los departamentos, peticiones y acceso a algunos servicios que ofrece FEI a sus empleados.

3.1.24 Políticas y normas dentro de la institución

FEI cuenta con varias políticas y normas como son: uso correcto de contraseñas, uso del correo institucional entre otras con el fin de evitar problemas como fuga de información o pérdidas de datos.

Observación: Estas normativas están escritas y repartidas con el personal de FEI pero no son revisadas periodicamente en caso de cambios o actualizaciones que son necesarias para el correcto funcionamiento de los servicios dentro de la institución.

3.1.25 Seguros

FEI cuenta con varios seguros en caso de cualquier eventualidad poder recuperar parcial o totalmente la infraestructura o los datos pérdidos en caso de desastre. La cantidad y los detalles sobre los seguros es información confidencial que solo la presidencia maneja y por motivos de seguridad no se publica en este documento.

3.1.26 Capacitaciones

FEI capacita a su personal especialmente en el uso de las herramientas y servicios internos de manera correcta, con el fin de evitar problemas y acelerar procesos para mejorar la experiencia tanto de empleados como alumnos. Entre los temas tratados se encuentran el uso correcto de contraseñas, correo institucional y uso del software institucional, además de las restricciones en el uso del WI-FI de la institución y las áreas restringidas dentro del establecimiento.

Observación: La capacitación en FEI debe ser frecuente y actualizada para que los empleados puedan resolver problemas por ellos mismos y agilizar los procesos internos de la institución. Estas capacitaciones deben realizarse en un periodo máximo de 6 meses y ser documentadas para saber que temas se trató y que áreas de la institución afectaron estas capacitaciones.

3.2 Establecimiento de las cláusulas de la norma ISO 24762:2008 en Florida Education Institute

La norma ISO 24762:2008 tiene varias cláusulas que se debe tomar en cuenta al momento de crear un plan de contigencia, las cuales se siguen para crear procedimientos que ayuden al correcto manejo de la información así como de los equipos tecnológicos de la institución

3.2.1 Recuperación de desastres de Tecnologías de la información (TIC)

Estabilidad ambiental

Florida Education Institute está expuesto a varios desastres naturales y humanos que pueden detener el trabajo continuo de la institución, por lo tanto se debe crear políticas y normas que el personal debe seguir en estos casos. En caso de:

- **Huracanes, Inundaciones y Terremotos**

  El estado de la Florida en Estados Unidos tiene protocolos para todos los ciudadanos en caso de huracanes e inundaciones, por lo tanto FEI debe seguir estas normas al pie de la letra para evitar catástrofes humanas y materiales.

  En cuanto al área de TI, en caso de perder equipos o información en estos casos se debe tener los respaldos en otros servidores en ubicaciones geográficas diferentes, ya sea contratando un servicio aparte o teniendo servidores en otra parte del mundo.

Gestión de activos

Dentro de FEI se deben crear normativas y establecer convenios con el personal para que se comprometan a usar los recursos tecnológicos de manera correcta y en favor de la institución. Además los empleados deben ser responsables de los equipos asignados y llevar un control donde conste el préstamo, asignación o devolución del activo de la institución.

Todos los activos deben ser etiquetados y asignados con un código único para luego ser ingresados en un inventario el cual va a ser actualizado constantemente para facilitar la búsqueda y el siguimiento del estado de estos equipos.

Proximidad de sitio

Cada equipo informático dentro de las instalaciones de FEI está bien equipado y protegido de varios peligros como incendios, robos etc, al tener un mejor inventario evitará que se pierdan o se substraigan activos de manera fraudulenta.

En cuanto a los servidores, la habitación donde son alojados se encuentra en buen estado y cumple todas las normas de seguridad. Y en general, FEI tiene los permisos pertinentes por parte del cuerpo de bomberos de FLorida para operar con total normalidad.

Gestion de proveedores

Existe la posibilidad de que tanto el personal, los servicios, los suministros y las soluciones de proveedores se vean afectados durante una emergencia de cualquier tipo, por los tanto se debe seguir varios protocolos para la continuidad del trabajo.

Personal: En caso de desastre natural o humano, se debe seguir los protocolos de seguridad asignados por la institución para evitar pérdidas humanas. Luego del incidente verificar que todo las personas se encuentren bien y dependiendo del estado de los equipos e infraestructura continuar el trabajo de manera normal.

Servicios: Después de una catástrofe o incidente, se debe verificar que servicios quedaron inhabilitados o fueron corrompidos durante el desastre y buscar la manera de recuperarlos, establecer cuanto durará todo el proceso e informar a todos los departamentos pertinentes.

Infraestructura: Al momento de retornar a las actvidades normales es necesario verificar que tanto la infraestructura como los equipos informáticos se encuentren en perfecto estado, caso contrario, se deberá arreglar o reemplazar dicho activo siguiendo las normas impuestas por la institución.

Acuerdos de subcontratación

FEI tiene muchos servicios contratados a terceros para mejorar la experiencia de trabajo tanto del personal como estudiantes, estos acuerdos son manejados por la presidencia de la institución y ellos deben ser los encargados de controlar el estricto cumplimiento de los convenios, realizar revisiones periódicas de los contratos y estar al pendiente de cambios en los términos de los servicios.

Seguridad de la información

La información es el bien más valioso que tiene FEI, por lo tanto es importante tener una serie de reglas que permita el uso correcto de los datos que maneja la institución.

Entre las normas que se deben implementar están:

- Los nuevos empleados que ingresen a la institución deberán recibir una capacitación previa sobre el correcto manejo de recursos y cumplimiento de tareas asignadas.
- Al momento de firmar el contrato entre el empleado y empleador debe existir una cláusula de confidencialidad para evitar la fuga de información confidencial de la institución.
- Los empleados deben manisfestar cualquier problema o acontecimiento que ocurra en el ambiente laboral.
- El encargado de TI debe monitorear a los usuarios cada 3 meses para revisar sus actividades.
- El encargado de TI está en la obligación de dar soluciones a problemas de seguridad o funcionamiento con los servicios y equipos institucionales así como salvaguardar la información que maneja.
- Mejorar las políticas, normas y reglas para proteger la información en caso de desastres naturales o humanos que comprometan la seguridad de los datos.
- Cuando un funcionario cese de trabajar en la institución deberá entregar todos los equipos que le fueron asignados para cumplir sus actividades.

- En caso de pérdida o daño de algún equipo informático de la institución el empleado deberá informar sobre este particular y el encargado de TI tomará las decisiones correspondientes informando primero a presidencia sobre este hecho.

Activación y desactivación del plan de recuperación ante desastres

FEI tiene políticas sobre almacenamiento y recuperación de datos los cuales están ordenados y documentados, así que la institución cubre de manera satisfactoria esta cláusula.

Capacitación y educación

Dentro de FEI existen manuales técnicos sobre todos los programas y servicios que usa la institución, además algunos proveedores de soluciones informáticas contratados por FEI ofrecen capacitaciones para el correcto uso de sus servicios.

Para complementar se debería realizar capacitaciones constantes por parte del departamento de TI sobre el uso correcto de los equipos informáticos y las instalaciones físicas de la institución.

Pruebas en los sistemas de TIC

Todos los sistemas dentro de la institución son probrados y el encargado de TI genera un informe con todos los datos relevantes del programa, como nombre, proveedor, funciones y características; además, de ser necesario, se adjunta un manual de usuario que sirve como material de consulta para el empleado que desee saber más sobre ese servicio.

Planificación de la continuidad del negocio para los proveedores de servicios de RC de TIC

En caso de existir algún inconveniente con los servicios que son contratados por FEI, es el encargado de sistemas de aplicar las normativas y políticas que estén a su disposición para resolver el problema de la manera más rápida y eficaz posible.

Todos los inconvenientes sucedidos deben ser documentados en un informe aprobado tanto por el encargado TI y posteriormente revisados y aprobados por presidencia. En caso de ser un error no antes visto, se debe crear una nueva planificación para mitigar que estos sucesos ocurran en el futuro. En caso de ser un error conocido, revisar todos los factores que propiciaron este escenario y determinar los cambios necesarios en la planificación actual.

Documentación y revisión periódica

Todos los programas y servicios que ofrece FEI está documentado y en caso de ser necesario tiene sus manuales de usuario para que el personal de la institución pueda consultar en caso de

tener alguna duda. Solo se debe mantener actualizados los manuales de acuerdo a los cambios que se presenten en los servicios o programas que se utiliza en FEI.

3.2.2 Instalaciones de recuperación de desastres de TIC

Ubicación de los sitios de recuperación

FEI cumple con este requisito ya que además de tener su propio sistema de backup, contrata los servicios de terceros para tener más de una copia de la valiosa información que la institución maneja.

Gracias al uso del servicios como IONOS y Acronis la información se encuentra distribuida en servidores externos dentro de Estados Unidos o Europa.

Control de acceso físico

Al contar FEI con un sistema de registro, se puede saber el ingreso y salida de las personas que trabajan dentro de la institución, sin embargo una vez dentro de FEI, no hay más filtros de seguridad, especialmente para el área de servidores.

Se debe añadir filtros de seguridad al área de servidores, verificar que las cámaras de seguridad funcionan y poner una señaletica clara y concisa para indicar al personal que no sea parte del área de TI o estudiantes que no puede ingresar a ese sitio.

Áreas dedicadas

En FEI la única área dedicada es el cuarto de servidores, no existe un departamento de TI como tal por lo tanto se recomienda que se implemente una oficina para el departamento de TI, con todos elementos necesarios que esta área requiere.

Controles ambientales

Dentro de FEI, especialmente en el cuarto de servidores las condiciones son las más optimas para trabajar y realizar las peticiones de recuperación a pesar de ser un cuarto adaptado para este fin.

Se debe documentar todas las revisiones que se hagan dentro del cuarto de servidores siendo que estas evaluaciones deben ser periódicas en un rango de seis meses para conocer el estado de los servidores.

Telecomunicaciones

FEI tiene contratos con empresas de proveedores de Internet, la cual es la más rápida de todo Miami, además por la adición de Firewall de seguridad, los datos se manejan con una seguridad extra.

Suministro de energía

La empresa contratada por FEI cumple con los requerimientos que la institución necesita no solo para el departamento de TI y los servidores sino para toda el plantel. Los cortes de energía en Miami son muy raros ya que solo ocurren cuando suceden desastres naturales.

En caso de que exista una interrupción en el servicio eléctrico, el cuarto de servidores consta con varios UPS para que no se corte el suministro de energía de golpe y dañe los equipos. Se tiene un tiempo prudencial de 30 minutos para que los sistemas puedan ser apagados de manera correcta y que vuelvan a funcionar luego de haber solucionado el imprevisto.

Gestión de cables

FEI tiene un cuarto especial donde se encuentra los paneles de control eléctrico el cual se encuentra en una ubicación distinta del cuarto de servidores. Este lugar es supervisado de manera constante para verificar que todo funcione bien dentro de la institución.

El cableado eléctrico se muestra en perfectas condiciones y no se ha tenido que hacer cambios o adecuaciones diferentes. Estos elementos también son revisados de manera periódica para que no suceda ningún inconveniente o problema mayor como incendios u otras catástrofes.

Protección contra incendios

FEI se adhiere a las normativas del cuerpo de bomberos de Miami, por lo tanto consta de un plan de evacuación en caso de incendios, además de tener toda la señalética correcta en caso de escape y los correspondientes extintores para emergencias pequeñas.

Centro de operaciones de emergencia

FEI cuenta con todas las instalaciones y servicios necesarios para sus empleados y estudiantes. Debido a que es una institución educativa debe cumplir con ciertos estándares de calidad para su funcionamiento y acreditación por parte de las autoridades de Miami.

FEI además contrata empresas externas para la limpieza y mantenimiento de las instalaciones, por lo que todos los recursos de la institución siempre se encuentran en perfecto estado y en caso de necesitar reparaciones o cambios se lo hace de inmediato, notificando siempre al personal.

Instalaciones restringidas

La única área restrigida totalmente es el área del panel eléctrico, en cambio el cuarto de servidores no está totalmente aislado al público en general y por lo tanto es un fallo de seguridad que se presenta en la institución.

Se debe crear políticas que prohiban el ingreso de personas no autorizadas a esta área además de informar a todo el personal de los nuevos cambios en los accesos a ciertos lugares.

Servicios que no son de recuperación

FEI tiene planes de riesgo en casos de desastres naturales, donde se prioriza el bienestar humano ante que el buen estado de los equipos o infraestructura física de la instución.

Se debe informar tanto al personal como a los estudiantes sobre estos planes de riesgos y en caso de ser necesario realizar varios simulacros para que todos puedan estar preparados en caso de que algún desastre real ocurra.

Ciclo de vida de las instalaciones físicas y el equipo de soporte

Se debe tener en cuenta y documentado la fecha de adquisión de los productos o herramientas que se van a utilizar dentro de la institución para tener presente el tiempo de garantía de estos y hacer reclamos en caso de ser necesario.

Las instalaciones físicas deben ser verificadas siempre para comprobar el buen estado y que no surgan problemas que puedan afectar el buen desempeño del personal, además es importante registrar que problemas han ocurrido para poder evitarlos en el futuro.

Pruebas

Todos los servicios contratados de FEI tienen garantía y son actualizados constantemente por parte de los proveedores. Estas empresas informan a la institución de cambios tanto en los servicios como en los recursos que ellos ofrecen.

Se debe realizar pruebas de estos servicios por parte de la institución y documentar cualquier anomalía que pueda afectar el buen funcionamiento de la empresa. Estas pruebas deben ser periódicas y ser autorizadas por presidencia de FEI y notificadas a todas las partes involucradas.

3.2.3 Capacidad del proveedor de servicios subcontratados

Requisitos de las instalaciones

Los proveedores de servicios de suministro eléctrico, Internet y Respaldos externos, han cumplido todos las cláusulas que FEI necesita para un buen funcionamiento de la institución.

En caso de existir algún inconveniente, FEI puede contactarse con el servicio técnico de estas empresas y pedir asesoramiento cuando ocurra algún incidente o necesite realizar un cambio en los sistemas que estas proveedores ofrecen.

Los contratos que FEI tiene con estas empresas aseguran la calidad del servicio y las garantías necesarias para un correcto funcionamiento de la institución. Estas garantías no tienen ningún costo adicional al pago mensual de los servicios.

Experiencia

Las empresas contratadas por FEI muestran una gran experiencia al brindar sus servicios a la institución ya que llevan varios años en el campo donde son expertos ahora.

Para que estas empresas fueran contratadas por FEI, tuvieron que pasar por varios filtros y cumplir las necesidades que la institución requiere para la implementación de estos servicios.

Control de acceso lógico

Los proveedores de servicios tienen controles estrictos al momento de realizar configuraciones o cambios en las políticas de recuperación de datos, siempre se necesita ingresar las credenciales que fueron creadas al momento de crear una cuenta en estas aplicaciones.

A manera de tener todas las credenciales de todos los servicios en un solo lugar se debe usar un gestor de contraseñas para aumentar la seguridad y guardar las credenciales en un solo lugar donde solo el encargado de TI y la presidencia tengan acceso a ellas.

Al ser información muy delicada no se debe compartir estas credenciales con los demás departamentos y si se necesita la recuperación de datos de algún servicio contratado por FEI se debe realizar una petición al departamento de TI conjuntamente con una petición escrita hacia presidencia.

Equipo de TIC y preparación operativa

La estructura diseñada por FEI es hasta el momento la más óptima y siempre se encuentra en total monitoreo para poder ofrecer un servicio de calidad a sus empleados y estudiantes.

Solo se debe agregar pruebas periódicas documentadas de todos los servicios y equipos para determinar su estado actual y prevenir desastres en el futuro, las revisiones diarias de los servidores son necesarias y se podría hacer una tabla donde se guarde el estado de estos componentes para poder hacer estadísticas cada cierto periodo de tiempo para saber la calidad de servicio.

Soporte de recuperación simultánea

Los servicios contratados por FEI cumplen todos los requisitos necesarios para poder realizar múltiples operaciones de recuperación de datos. Los proveedores son empresas dedicadas a trabajar en grandes escalas por lo que las operaciones de respaldo pueden ser realizadas en cualquier momento sin bajar la calidad del servicio.

Niveles de servicio

FEI puede realizar recuperación de datos masivos o solo de una parte de su información independientemente de la criticidad de los eventos ocurridos. Los servicios de respaldos están siempre disponibles para todos sus usuarios.

Tipos de servicios

FEI contrata los servicios de empresas que le pueden dar total control de su información, además de que puede extender la complejidad de sus requerimientos. Obviamente, todo depende de como esté estipulado en las cláusulas de los contratos y el aumento de precio en estos servicios.

3.2.4 Proximidad de los servicios

Los servicios contratados por FEI son capaces de proveer una respuesta rápida a las necesidades de la organización en cuanto se trata de recuperación de datos ya que son empresas con alta experiencia en esta área.

Tasa de suscripción para servicios compartidos

Las empresas de recuperación de datos contratados por FEI mantienen una buena calidad ya que son proveedores de servicios serios los cuales ofrecen planes para cada usuario dependiendo de sus necesidades y el costo que pueden pagar.

En caso de necesitar un aumento en las capacidades de servicio o algún cambio que se pueda realizar, las empresas pueden aceptar las peticiones de la institución de manera rápida y eficiente.

Activación de servicios suscritos

FEI tiene contratos estrictos y explícitos donde se indica como funciona los servicios que ofrecen las empresas y como afecta a la institución. Estos contratos solo los maneja presidencia directamente con ayuda del departamento de TI.

Prueba de la organización

Se debe implementar políticas de evaluación para probar las capacidades de los servicios contratados y documentar alguna anomalía o caso de éxito al momento de realizar estas pruebas. Todo esto con el aval de presidencia y realizado por el departamento de TI.

Cambios en la capacidad

Los proveedores de servicios de FEI están en constante actualización e innovación para ofrecer un servicio de calidad a todas las organizaciones suscritas a ellas.

Autoevaluación

Las empresas que FEI contrata tienen sus propios métodos de autoevaluación y auditoría interna.

3.2.5 Selección de sitios de recuperación

Todos los equipos, mano de obra y servicios contratados se encuentran en Estados Unidos, todos estos elementos son altamente calificados y ofrecen seguridad, eficiencia y mejora continua.

Algunos servicios de empresas contratadas se encuentran fuera de Estados Unidos para ofrecer una mayor seguridad en caso de que algún desastre natural o humano suceda en el territorio.

La fuerza de trabajo de FEI consta de profesionales en el área de TI con sus títulos universitarios y referencias laborales favorables, son personas con alta experiencia en el área de servicios informáticos y servicio al cliente.

Los equipos y la infraestructura de FEI se encuentra en óptimas condiciones y se realiza revisiones periódicas que permite la continuidad de las operaciones de la institución.

En caso de existir algún inconveniente el personal de TI se encarga de resolverlo de manera inmediata en un lapso de una hora; al terminar de evaluar y completar con la resolución del problema se realiza un informe y se informa a las partes involucradas.

3.2.6 Mejora continua

Tendencias TIC RD

Se debe seguir todos los procedimientos y tendencias que beneficien a la organización y que permiten un mejor trabajo, la mejora continua debe ser la base fundamental del equipo de TI para encontrar y evitar problemas en el futuro y crear planes de mitigación de riesgos con antelación.

Medición del desempeño

Se recomienda medir el desempeño de todos los servicios, personal y equipos de la institución para tener datos y hacer estadísticas del estado de estos elementos fundamentales de la organización.

3.2.7 Escalabilidad

Se debe preveer que toda la organización puede crecer y necesitar más elementos importantes para el buen funcionamiento de los procesos de la organización.

Todos los servicios, personal e infraestructura debe tener la capacidad de innovarse y evolucionar en favor del mejoramiento de la institución, así también se mitiga o se encuentra preparado para enfrentar los posibles problemas que vengan en el futuro.

3.2.8 Mitigación de riesgos

Al recurrir a las tendencias actuales, estableciendo medidas de desempeño y escalabilidad se puede crear políticas, normas y reglas para mitigar los riesgos.

La documentación de todos proceso y problema que surgió o puede surgir es importante para crear las políticas de mitigación de riesgos.

3.3 Definición de amenazas

Basado en toda la información recolectada hasta el momento usando las cláusulas de la norma ISO:24762:2008 se procede a realizar el cuadro de amenazas que afecta a Florida Education Institute.

Tipificación de Riesgo	**Descripción**	**Vulnerabilidad**	**Impacto**
R1	Inundación	N/A	Daño total a la infraestructura del centro de datos y pérdida de información
R2	Terremoto	N/A	Daño total a la infraestructura del centro de datos y pérdida de información
R3	Huracanes	N/A	Daño total a la infraestructura del centro de datos y pérdida de información
R4	Incendio	N/A	Daño total a la infraestructura del centro de datos y pérdida de información

R5	Daños en la Fuente de energía eléctrica	Susceptibilidad del equipamiento a alteraciones en el voltaje	Falla en los equipos
R6	Daño del UPS	Mantenimiento inadecuado	Falla en los equipos
R7	Falla en el aire acondicionado	N/A	Sobrecalentamiento de los servidores
R8	Hermetización de pasos de cables	No hay estanqueidad de la temperatura	Sobrecalentamiento de los servidores
R9	Cableado Inadecuado	Inadecuada gestión de redes	Susceptible a daños
R10	Racks y accesorios desordenados	Inadecuada ubicación del rack	Deterioro de soportes
R11	Falta de canalización y tuberías	Cableado expuesto	Susceptibilidad a daños
R12	Falta de sistema de control de acceso	Falta de registro y monitoreo de bitácora de acceso	Pérdida y robo de información
R13	Falta de sistema de gestión y monitoreo	Susceptibilidad del equipamiento a la temperatura	Susceptibilidad a daños
R14	Falta de sistema de detección y extinción de incendios	Inexistente	Incendio
R15	Tablero principal desordenado	Susceptibilidad del equipamiento a alteraciones en el voltaje y desorden en la ubicación de los equipos	Daño del centro de datos

R16	Falta de sistema de video seguridad	No existe cámaras cerca del centro de datos	Entrada de intrusos y robo de equipos
R17	Falta de puerta de seguridad	No existe ninguna puerta en el centro de datos	Robo de equipos
R18	Mala ubicación de respaldo externo de servidores	Copias en el mismo centro de datos	Pérdida de información
R19	Falta de capacitación del personal	No se tiene un plan de capacitación	Uso erróneo de sistemas de información
R20	Mala administración de recursos del centro de datos	Inadecuada separación de tareas	Omisión de responsabilidad
R21	Informes de monitoreo inexistentes	Susceptibilidad a ataques	Ataques cibernético
R22	Documentación inexistente	Falta de manuales de configuración de equipos	Indisponibilidad del servicio
R23	Falla por parte del proveedor de electricidad	Susceptibilidad del equipamiento a alteraciones en el voltaje	Daño del centro de datos
R24	Falla por parte del proveedor de internet	Mal funcionamiento de los servicios de FEI	Pérdidas de datos
R25	Instalaciones eléctricas expuestas	Susceptibilidad del equipamiento a alteraciones en el voltaje	Daño en el centro de datos y riesgo de incendio
R26	Sistema de cableado eléctrico desordenado	Susceptibilidad del equipamiento a alteraciones en el voltaje	Daño en el centro de datos y riesgo de incendio

R27	Racks expuestos	Susceptibilidad a agentes externos dañinos	Daño en el centro de datos
R28	Equipos sujetados inadecuadamente	Susceptibilidad del equipamiento a caídas	Daño en el centro de datos
R29	Falta de control acceso biométrico	Susceptibilidad del equipamiento a robos o daños	Daño en el centro de datos
R30	Exposición al polvo	Susceptibilidad del equipamiento a daños	Daño en el centro de datos
R31	Almacenamiento de equipos que no pertenecen al cuarto de servidores	N/A	Subutilización de espacio del centro de datos
R32	Piso inadecuado del centro de datos	Susceptibilidad del equipamiento a daños	Daño en el centro de datos
R33	Objetos inflamables en el centro de datos	Riesgo de incendio	Daño en el centro de datos
R34	Falta de identificación y etiquetas de equipos	N/A	Pérdida o robo de equipos
R35	No existe uniformidad en los cables de red	N/A	Posible daños en la información
R36	Obsolecencia de equipos	N/A	Posible pérdida de datos y equipos
R37	Existencia de plagas	Susceptibilidad del equipamiento a daños	Posible pérdida de datos y daños de equipos
R38	Documentación desordenada	N/A	Mala utilización de equipos y servicios
R39	Errores en las políticas de acceso a la información del servidor	N/A	Robo y destrucción de información

R40	Pandemia	N/A	Dificultad acceder a los equipos de la institución

Cuadro 3.4: Definición de riesgos
Elaborado por: Paúl Montesdeoca

3.4 Análisis de riesgos, naturales informáticos y humanos que se pueden presentar en FEI y en su Departamento de Tecnologías de la información (TI)

El análisis de riesgo se basó en el cuadro 3.4 donde todos los riesgos fueron estudiados y puestos en su respectiva zona de riesgo, este resultado se basa de acuerdo a su probabilidad e impacto dentro de la organización.

Riesgo	**Probabilidad**	**Impacto**	**Zona de riesgo**
R1	3	5	Extremo
R2	3	5	Extremo
R3	4	5	Extremo
R4	4	5	Extremo
R5	4	5	Extremo
R6	4	5	Extremo
R7	2	5	Extremo
R8	2	3	Moderado
R9	4	3	Alto
R10	3	2	Moderado
R11	2	2	Bajo
R12	4	3	Alto
R13	4	3	Alto
R14	4	3	Alto
R15	3	3	Alto
R16	3	3	Alto
R17	3	3	Alto
R18	3	2	Moderado
R19	2	1	Bajo
R20	3	3	Alto
R21	3	1	Bajo
R22	3	1	Bajo
R23	3	5	Extremo

R24	3	5	Extremo
R25	3	3	Alto
R26	3	2	Moderado
R27	3	1	Bajo
R28	3	3	Alto
R29	1	4	Alto
R30	3	2	Moderado
R31	3	1	Bajo
R32	3	1	Bajo
R33	3	3	Alto
R34	3	2	Moderado
R35	3	2	Moderado
R36	2	3	Moderado
R37	2	5	Extremo
R38	2	2	Bajo
R39	2	4	Alto
R40	1	3	Moderado

Cuadro 3.5: Matriz de riesgo
Elaborado por: Paúl Montesdeoca

3.5 Estrategia de solución tomando en cuenta la normativa ISO 24762:2008 para Florida Education Institute

Después de un análisis de todos las vulnerabilidades, riesgos y problemas dentro de Florida Education Institute (FEI), se ha determinado que no se cumplen ciertas normativas de seguridad y por lo tanto la implementación de la ISO 24762:2008 mejorará estos inconvenientes previniendo posibles escenarios catastróficos en el futuro.

El departamento de TI deberá regirse por estas nuevas normativas para tener un mejor desempeño y manejar de forma más segura la información que circula dentro de la institución, además de entrenar al personal de las demás áreas a manejar los demás datos de forma correcta, evitando posibles errores o filtraciones de información.

Otra área fundamental que se encargará el departamento de TI, es tener previsto varios escenarios donde los equipos o programas informáticos puedan fallar y tener el plan de contigencia listo para actuar de manera inmediata para que no se pierda el flujo de trabajo e informar a toda la institución de todo lo que estece pasando, encontrar el error o problema y solucionarlo.

3.6 Implantación de un plan de contingencia basado en la normativa ISO 24762:2008 para la recuperación de información en casos de desastres en el Departamento de Tecnologías de la Información (TI) de Florida Education Institute (FEI)

3.6.1 Cuadro de riesgos

Se procede a crear un cuadro de riesgos ordenados de acuerdo a probalidad e impacto para mayor claridad del lector y mejor visualización del área donde le corresponde.

PROBABILIDAD	IMPACTO				
	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
Casi seguro (5)					
Probable (4)			R9 R12 R13 R14 R15		R3 R4 R5 R6
Posible (3)	R21 R22 R27 R31 R32	R10 R18 R26 R30 R34 R35	R16 R17 R20 R25 R28 R33		R1 R2 R23 R24
Improbable (2)		R11 R38	R8 R36	R39	R7 R37
Raro (1)		R19	R40	R29	

Figura 3.45: Cuadro de riesgos
Elaborado por: Paúl Montesdeoca

Se va a tomar en cuenta los riesgos que se encuentran en zona extrema, ya que su impacto es demasiado dañino para la institución, además el presupuesto es limitado y solo se puede realizar el plan de contigencia para cubrir solo esta parte de la matriz de riesgos.

3.6.2 Definición de roles

A las siguientes personas se les asigna los siguientes roles, los cuales serán importantes al momento de ejecutar el plan de contigencia y seguir las directrices del mismo de manera ordenada y eficaz.

- Ramón Valenti - Presidente
- Ramón Valenti JR - Vicepresidente
- Paúl Montesdeoca - Asistente de soporte 1
- Orlando Goza - Asistente de soporte 2
- Yosvany Peña - Asistente de mantenimiento
- Estudiantes - Estudiantes

3.6.3 Fase de prevención

En la fase de prevención se tomará en cuenta los riesgos que se encuentren en el espectro de impacto de tipo extremo y alto de la figura 3.45, debido a que por su naturaleza es difícil de solucionarlos es mejor prevenirlos para evitar un gran impacto dentro de la institución.

R1 - Inundaciones

Procedimiento:

- Los servidores deben elevarse a una altura de más de un metro sobre el nivel del suelo, ya que en el peor de los casos el agua llegaría a subir unos 80cm de acuerdo a la posición geográfica donde se encuentra la escuela y las mediciones de los organismos de control de riegos de los Estados Unidos.
- Identificar una ruta de evacuación, y otras vías alternativas y estar preparado para evacuar.
- Colocar documentos importantes en una bolsa de plástico para que no se destruyan con el agua.
- Tener un radio para estar informado acerca de la emergencia y posibles instrucciones.
- Compra de seguros para casos de emergencia.
- Capacitación al personal involucrado.

R2 - Terremoto

Procedimiento:

- Asegurar el panel central en la pared.
- Comprar rack antísismicos para proteger los servidores.
- Tener servidores en otro lugar para en caso de caída del servicio se puede usar el servidor de respaldo.
- Colocar documentos importantes en una bolsa de plástico para que no se destruyan con el agua.
- Compra de seguros para casos de emergencia.
- Capacitación al personal involucrado.

R3 - Huracanes

Procedimiento:

- Asegurar el panel central en la pared.
- Comprar rack antísismicos para proteger los servidores.
- Tener servidores en otro lugar para en caso de caída del servicio se puede usar el servidor de respaldo.

- Compra de seguros para casos de emergencia.
- Capacitación al personal involucrado.

R4 - Incendios

Procedimiento:

- No tener materiales inflamables o que se puedan quemar con facilidad.
- Revisar las conexiones eléctricas en caso de cables sueltos o destruidos.
- Tener un sistema de detección de humo tanto en el techo como el suelo.
- Tener el cuarto de servidores en en perfecto estado de humedad y temperatura.
- Tener a la mano un extinguidor.
- Guardar documentos importantes en una caja fuerte u otro lugar fuera del datacenter.
- Compra de seguros para casos de emergencia.
- Capacitación al personal involucrado.

R9 - Cableado inadecuado

Procedimiento:

- Ordenar el cableado mediante tuberías aislantes.

R12 - Falta de sistema de control de acceso

Procedimiento:

- Mejora en el sistema de vigilancia del centro de datos.
- Registrar entradas y salidas del área de servidores.

R13 - Falta de sistema de gestión y monitoreo

Procedimiento:

- Adquisición de sistema de monitoreo para los servidores
- Monitorear los servidores todos los días en la primeras horas de la mñana y en las últimas horas de la jornada laboral.

R14 - Falta de sistema de detección y extinción de incendios

Procedimiento:

- Comprar un sistema de detección de incendios.
- Comprar un seguro en caso de existir un incendio.

R15 - Tablero principal desordenado

Procedimiento:

- Ordenar el tablero principal de control.
- Quitar cables que esten estorbando en el tablero.
- Verificar que ninguno de los cables esten rotos o tengan alguna anormalidad.

R16 - Falta de sistema de video seguridad

Procedimiento:

- Agregar cámaras de seguridad en el área de servidores.

R25 - Instalaciones eléctricas expuestas

Procedimiento:

- Revisar las toma de corriente que estén bien selladas.

R26 - Sistema de cableado eléctrico desordenado

Procedimiento:

- Revisar las toma de corriente que estén bien selladas.
- Revisar que los cables de electricidad no se encuentren entrecruzados.
- Revisar la calidad de los cables eléctricos.

R28 - Equipos sujetados inadecuadamente

Procedimiento:

- Sujetar o pegar los equipos en el panel central de manera correcta.
- Verificar que los servidores y switch esten correctamente ubicados en los racks.

R33 - Objetos inflamables en el centro de datos

Procedimiento:

- Eliminar objetos que puedan representar un posible peligro de incendio.

R34 - Falta de identificación y etiquetas de equipos

Procedimiento:

- Crear una base de datos de los equipos que tiene FEI.
- Etiquetar todos los equipos importantes que tiene la institución.

3.6.4 Fase de mitigación

En esta fase se plantean los pasos a seguir en caso de que algún posible riesgo ocurra y no se haya podido prevenir, aquí es donde se especifica que hace cada persona según su rol en la organización para mitigar los efectos negativos de la situación.

Código de riesgo	R1		
Nombre	Inundaciones		
Orden	**Responsable**	**Actividad**	**Tiempo estimado**
1	Asistente de soporte 2	Debe evaluar los daños en la estructura física, conectividad a internet y servicio LAN para luego reportar al asistente de soporte 1.	24 horas
2	Asistente de soporte 1	Con el reporte del asistente 2 y la evaluación de datos perdidos debe reportar al presidente de FEI de todos los daños.	8 horas
3	Presidente	Debe analizar el informe del asistente de soporte 1 y permitir al mismo realizar los procesos respectivos para recuperación de datos.	8 horas
4	Vicepresidente	Debe comunicarse con la compañía de seguros para informar de la catástrofe y seguir los pasos correspondientes que dicten los operadores del seguro.	2 horas
5	Encargado de mantenimiento	Conjuntamente con el asistente de soporte 2 deben limpiar el área de servidores y retirar los equipos dañados.	48 horas
6	Asistente de soporte 1	Debe realizar el presupuesto para comprar los equipos que reemplazarán a los equipos dañados e informar al presidente.	72 horas
7	Asistente de soporte 1	Mientras se limpia el centro de datos y la infraestructura en general, se debe habilitar los servicios y servidores de emergencia que se encuentran en la nube para poder continuar con el trabajo normalmente hasta la adquisión de nuevo equipo.	8 horas
8	Asistente de soporte 2	Una vez limpio todas las áreas y comprado los nuevos equipos se procede a la recolocación del centro de datos.	48 horas

9	Asistente de soporte 1	Una vez instalado todos los equipos del centro de datos se procede ha habilitar los servicios locales.	8 horas
Total de horas			226 horas

Código de riesgo	R2		
Nombre	Terremoto		
Orden	**Responsable**	**Actividad**	**Tiempo estimado**
1	Asistente de soporte 2	Debe evaluar los daños en la estructura física, conectividad a internet y servicio LAN para luego reportar al asistente de soporte 1.	24 horas
2	Asistente de soporte 1	Con el reporte del asistente 2 y la evaluación de datos perdidos debe reportar al presidente de FEI de todos los daños.	8 horas
3	Presidente	Debe analizar el informe del asistente de soporte 1 y permitir al mismo realizar los procesos respectivos para recuperación de datos.	8 horas
4	Vicepresidente	Debe comunicarse con la compañía de seguros para informar de la catástrofe y seguir los pasos correspondientes que dicten los operadores del seguro.	2 horas
5	Asistente de soporte 2	En caso de daño de la infraestructura física de FEI debe evaluar si se puede restablecer el centro de datos en el mismo lugar o cambiar a algún edificio alterno.	8 horas
6	Encargado de mantenimiento	En caso de que todo esté bien con el edificio, conjuntamente con el encargado de soporte 2 deben limpiar el área de servidores y retirar los equipos dañados.	48 horas

7	Asistente de soporte 1	Debe realizar el presupuesto para comprar los equipos que reemplazarán a los equipos dañados e informar al presidente.	72 horas
8	Asistente de soporte 1	Mientras se limpia el centro de datos y la infraestructura en general, se debe habilitar los los servicios y servidores de emergencia que se encuentran en la nube para poder continuar con el trabajo normalmente hasta la adquisión de nuevo equipo.	8 horas
9	Asistente de soporte 2	Una vez limpio todas las áreas y comprado los nuevos equipos se procede a la recolocación del centro de datos.	48 horas
10	Asistente de soporte 1	Una vez instalado todos los equipos del centro de datos se procede ha habilitar los servicios localmente.	8 horas
Total de horas			234 horas

Código de riesgo	R3		
Nombre	Huracanes		
Orden	**Responsable**	**Actividad**	**Tiempo estimado**
1	Asistente de soporte 2	Debe evaluar los daños en la estructura física, conectividad a internet y servicio LAN para luego reportar al asistente de soporte 1.	24 horas
2	Asistente de soporte 1	Con el reporte del asistente 2 y la evaluación de datos perdidos debe reportar al presidente de FEI de todos los daños.	8 horas
3	Presidente	Debe analizar el informe del asistente de soporte 1 y permitir al mismo realizar los procesos respectivos para recuperación de datos.	8 horas

4	Vicepresidente	Debe comunicarse con la compañía de seguros para informar de la catástrofe y seguir los pasos correspondientes que dicten los operadores del seguro.	2 horas
5	Asistente de soporte 2	En caso de daño de la infraestructura física de FEI debe evaluar si se puede restablecer el centro de datos en el mismo lugar o cambiar a algún edificio alterno.	8 horas
6	Encargado de mantenimiento	En caso de que todo esté bien con el edificio, conjuntamente con el encargado de soporte 2 deben limpiar el área de servidores y retirar los equipos dañados.	48 horas
7	Asistente de soporte 1	Debe realizar el presupuesto para comprar los equipos que reemplazarán a los equipos dañados e informar al presidente.	72 horas
8	Asistente de soporte 1	Mientras se limpia el centro de datos y la infraestructura en general, se debe habilitar los los servicios y servidores de emergencia que se encuentran en la nube para poder continuar con el trabajo normalmente hasta la adquisión de nuevo equipo.	8 horas
9	Asistente de soporte 2	Una vez limpio todas las áreas y comprado los nuevos equipos se procede a la recolocación del centro de datos.	48 horas
10	Asistente de soporte 1	Una vez instalado todos los equipos del centro de datos se procede ha habilitar los servicios localmente.	8 horas
Total de horas			234 horas

Código de riesgo	R4		
Nombre	Incendio		
Orden	**Responsable**	**Actividad**	**Tiempo estimado**
1	Asistente de soporte 2	Debe evaluar los daños en la estructura física, conectividad a internet y servicio LAN para luego reportar al asistente de soporte 1.	24 horas
2	Asistente de soporte 1	Con el reporte del asistente 2 y la evaluación de datos perdidos debe reportar al presidente de FEI de todos los daños.	8 horas
3	Presidente	Debe analizar el informe del asistente de soporte 1 y permitir al mismo realizar los procesos respectivos para recuperación de datos.	8 horas
4	Vicepresidente	Debe comunicarse con la compañía de seguros para informar de la catástrofe y seguir los pasos correspondientes que dicten los operadores del seguro.	2 horas
5	Asistente de soporte 2	En caso de daño de la infraestructura física de FEI debe evaluar si se puede restablecer el centro de datos en el mismo lugar o cambiar a algún edificio alterno.	8 horas
6	Encargado de mantenimiento	En caso de que todo esté bien con el edificio, conjuntamente con el encargado de soporte 2 deben limpiar el área de servidores y retirar los equipos dañados.	48 horas
7	Asistente de soporte 1	Debe realizar el presupuesto para comprar los equipos que reemplazarán a los equipos dañados e informar al presidente.	72 horas

8	Asistente de soporte 1	Mientras se limpia el centro de datos y la infraestructura en general, se debe habilitar los los servicios y servidores de emergencia que se encuentran en la nube para poder continuar con el trabajo normalmente hasta la adquisión de nuevo equipo.	8 horas
9	Asistente de soporte 2	Una vez limpio todas las áreas y comprado los nuevos equipos se procede a la recolocación del centro de datos.	48 horas
10	Asistente de soporte 1	Una vez instalado todos los equipos del centro de datos se procede ha habilitar los servicios localmente.	8 horas
Total de horas			234 horas

Código de riesgo	R5		
Nombre	Daños en la fuente de energía eléctrica		
Orden	**Responsable**	**Actividad**	**Tiempo estimado**
1	Asistente de soporte 2	Debe evaluar los daños en la estructura física, conectividad a internet y servicio LAN para luego reportar al asistente de soporte 1.	24 horas
2	Asistente de soporte 1	Con el reporte del asistente 2 y la evaluación de datos perdidos debe reportar al presidente de FEI de todos los daños.	8 horas
3	Presidente	Debe analizar el informe del asistente de soporte 1 y permitir al mismo realizar los procesos respectivos para recuperación de datos.	8 horas
4	Vicepresidente	Debe comunicarse con la compañía de seguros para informar de la catástrofe y seguir los pasos correspondientes que dicten los operadores del seguro.	2 horas
5	Asistente de soporte 1	Debe realizar el presupuesto para comprar los equipos que reemplazarán a los equipos dañados e informar al presidente.	72 horas
6	Asistente de soporte 1	Debe habilitar los los servicios y servidores de emergencia que se encuentran en la nube para poder continuar con el trabajo normalmente hasta la adquisición de nuevo equipo.	8 horas
7	Encargado de mantenimiento	Debe revisar la fuente de energía eléctrica y en caso de que sea imposible restablecer el servicio, llamar a la empresa eléctrica para que realice la evaluación y cambios respectivos.	120 horas
8	Asistente de soporte 1	Una vez instalado todos los equipos del centro de datos se procede ha habilitar los servicios localmente.	8 horas
Total de horas			250 horas

Código de riesgo	R6		
Nombre	Daño del UPS		
Orden	**Responsable**	**Actividad**	**Tiempo estimado**
1	Asistente de soporte 2	Debe evaluar los daños en la estructura física, conectividad a internet y servicio LAN para luego reportar al asistente de soporte 1.	24 horas
2	Asistente de soporte 1	Con el reporte del asistente 2 y la evaluación de datos perdidos debe reportar al presidente de FEI de todos los daños.	8 horas
3	Presidente	Debe analizar el informe del asistente de soporte 1 y permitir al mismo realizar los procesos respectivos para recuperación de datos.	2 horas
4	Asistente de soporte 1	Debe realizar el presupuesto para comprar el nuevo UPS que reemplazará al equipo dañado e informar al presidente.	72 horas
5	Asistente de soporte 1	Debe habilitar los los servicios y servidores de emergencia que se encuentran en la nube para poder continuar con el trabajo normalmente hasta la adquisión de nuevo equipo.	8 horas
6	Asistente de soporte 1	Una vez instalado todos los equipos del centro de datos se procede ha habilitar los servicios localmente.	8 horas
Total de horas			122 horas

Código de riesgo	R7		
Nombre	Falla en el aire acondicionado		
Orden	**Responsable**	**Actividad**	**Tiempo estimado**

1	Asistente de soporte 2	Debe evaluar si existe daño en la estructura física, conectividad a internet y servicio LAN para luego reportar al asistente de soporte 1.	24 horas
2	Asistente de soporte 1	Con el reporte del asistente 2 y la evaluación de datos perdidos, en caso de exitir, se debe reportar al presidente de FEI de todos los daños.	8 horas
3	Presidente	Debe analizar el informe del asistente de soporte 1 y permitir al mismo realizar los procesos respectivos para recuperación de datos.	2 horas
4	Encargado de mantenimiento	Debe contactar a la empresa responsable del aire acondicionado y pedir que cambie los equipos o realice las reparaciones necesarias e informar al presidente.	72 horas
5	Asistente de soporte 1	Debe habilitar los los servicios y servidores de emergencia que se encuentran en la nube para poder continuar con el trabajo normalmente hasta la adquisión o reparación del sistema de aire acondicionado.	8 horas
6	Asistente de soporte 1	Una vez recuperado el sistema de aire acondicionado se procede ha habilitar los servicios localmente.	8 horas
Total de horas			122 horas

Código de riesgo	R23		
Nombre	Falla por parte del proveedor de electricidad		
Orden	**Responsable**	**Actividad**	**Tiempo estimado**
1	Asistente de soporte 2	Debe evaluar si existe daño en la estructura física, conectividad a internet y servicio LAN para luego reportar al asistente de soporte 1.	24 horas

2	Asistente de soporte 1	Con el reporte del asistente 2 y la evaluación de datos perdidos, en caso de exitir, se debe reportar al presidente de FEI de todos los daños.	8 horas
3	Presidente	Debe analizar el informe del asistente de soporte 1 y permitir al mismo realizar los procesos respectivos para recuperación de datos.	2 horas
4	Encargado de mantenimiento	Debe contactar a la empresa responsable del sistema eléctrico y preguntar que sucede con el sistema eléctrico e informar al presidente.	72 horas
5	Asistente de soporte 1	Debe habilitar los los servicios y servidores de emergencia que se encuentran en la nube para poder continuar con el trabajo normalmente hasta la adquisión o reparación del sistema de aire acondicionado.	8 horas
6	Asistente de soporte 1	Una vez recuperado el sistema eléctrico se procede ha habilitar los servicios localmente.	8 horas
Total de horas			122 horas

Código de riesgo	R24		
Nombre	Falla por parte del proveedor de internet		
Orden	**Responsable**	**Actividad**	**Tiempo estimado**
1	Asistente de soporte 2	Debe evaluar si existe daño en la estructura física para verificar que los equipos de la institución funcionan correctamente.	24 horas
2	Asistente de soporte 1	Debe comunicarse con la empresa proveedora de internet y preguntar por fallas en el servicio y luego comunicar al presidente.	8 horas
3	Presidente	Debe analizar el informe del asistente de soporte 1 y permitir al mismo realizar los procesos respectivos para recuperación de datos.	2 horas
4	Asistente de soporte 1	Debe habilitar los los servicios y servidores de emergencia que se encuentran en la nube para poder continuar con el trabajo normalmente hasta la recuperación del servicio de internet	8 horas
5	Vicepresidente	Debe informar a todo el equipo de trabajo del fallo de internet dentro de las instalaciones y pedir que esperen hasta que vuelva el servicio y que si necesitan realizar alguna actividad importante procedan a realizarla mediante el servicio de red celular que también se tiene en FEI.	1 hora
6	Asistente de soporte 1	Una vez devuelto el servicio de internet debe habilitar los servicios localmente	8 horas
Total de horas			51 horas

Código de riesgo	R37
Nombre	Existencia de plagas

Orden	**Responsable**	**Actividad**	**Tiempo estimado**
1	Asistente de soporte 2	Debe evaluar si existe daño en la estructura física para verificar que los equipos de la institución funcionan correctamente e informar al presidente.	8 horas
2	Presidente	Debe analizar el informe del asistente de soporte 2 y permitir al mismo realizar los procesos respectivos para recuperación de datos.	2 horas
3	Asistente de soporte 1	En caso de daños en el centro de datos debe habilitar los los servicios y servidores de emergencia que se encuentran en la nube para poder continuar con el trabajo normalmente y además preparar un presupuesto en caso de necesitar cambiar algún equipo.	8 horas
4	Vicepresidente	Debe contactar con alguna empresa de manejo de plagas para la eliminación de las misma.	2 horas
5	Asistente de soporte 1	Una vez eliminada las plagas del centro de datos y comprobado que los equipos funcionen bien debe habilitar los servicios localmente.	8 horas
Total de horas			28 horas

Capítulo 4

Conclusiones y recomendaciones

4.1 Conclusiones

Al evaluar el estado de la organización se puede dar cuenta de los aciertos y errores que cometía el área de TI y ahora es responsabilidad de sus encargados encontrar las soluciones más óptimas que beneficien no solo a la institución sino tambien a los estudiantes que utilizan los servicios de FEI. El área de TI a pesar de haber trabajado de manera diligente y eficiente tiene algunas falencias como el hecho de no documentar todos los procesos que ocurren dentro de la organización y no llevar de manera más ordenada los inventarios físicos de la institución.

Al realizar el análisis de riegos naturales, informáticos y humanos se descubrió que FEI no estaba preparado para afrontar tales amenazas, a pesar de tener algunas políticas de seguridad y prevención de riesgos era necesario investigar más a fondo todos los posibles problemas que la institución llevaba a cuestas durante varios años y que la hacían vulnerable, ahora con la debida utilización de metodologías y normas se puede estar preparado para cualquier contrariedad venidera.

La implantación de un plan de riesgos informáticos se lo ha realizado parcialmente en la institución ya que además del trabajo propuesto a FEI, este debe acoplarlo a las leyes y estatutos que las normas del estado de Florida en Estados Unidos obliga a seguir a todas las instituciones de educación ocupacional como es el caso de FEI. Sin embargo, hasta el momento se ha visto buenos resultados de la implantación parcial del plan de riesgos, siendo así, ya se han realizado los respectivos correctivos en algunas áreas de la institución y se han actualizado viejas políticas para que todo el personal y estudiantes deban seguir con el fin de tener una mayor seguridad y protección de datos.

4.2 Recomendaciones

El departamento de TI debe crear las políticas de seguridad necesarias que crea conveniente y difundirlas con toda la organización para incentivar buenos hábitos y prácticas en el manejo y gestión de la información.

El departamento de TI debe contar siempre de un técnico encargado para que lleve a cabo todo tipo de monitoreo de las áreas importantes de la organización, realice pruebas periódicas de todos los sistemas y mejore las áreas que crea necesarias para el buen funcionamiento de la institución.

Se debe capacitar constamente a los empleados y estudiantes para que tengan un conocimiento sólido sobre seguridad informática para evitar posibles fugas de información, ingreso de virus a los sistemas, vulnerabilidades en las contraseñas, spam en los correos institucionales y otros problemas que puede afectar a la institución.

Presidencia debería asignar una mayor cantidad de presupuesto para el plan de contigencia, ya que quedan otros problemas que no son muy graves dentro de la institución pero con la oportuna intervención podrían ser prevenidos.

Bibliografía

[1] Byron Vicente Nieto Muñoz. Análisis y evaluación para el diseño de un plan de recuperación ante desastres (drp) aplicado en un centro de datos para empresas municipales basado en la norma iso/iec 24762:2008. 2015.

[2] John José Chamba Mera, Luis Ignacio Delgado álvarez, and Espol. Desarrollo de un plan de recuperación ante desastres (drp) para la unidad de t.i. de la corporación amco. 11 2017.

[3] Colosal ciberataque golpea a cientos de empresas en EE.UU - BBC News Mundo. [Online] https://www.bbc.com/mundo/noticias-57706437, 2021.

[4] Terremotos y centros de datos. [Online] https://directortic.es/reportajes/terremotos-y-centros-de-datos-2014092512128.htm, 2021.

[5] Ciberataques en América Latina crecen un 24% durante los primeros ocho meses de 2021. [Online] https://latam.kaspersky.com/blog/ciberataques-en-america-latina-crecen-un-24-durante-los-primeros-ocho-meses-de-2021/22718/, 2021.

[6] Los Ciberataques más famosos del 2021 en Colombia y el mundo. [Online] www.nsit.com.co/los-ciberataques-mas-famosos-del-2021-en-colombia-y-el-mundo/, 2021.

[7] Se declara el estado de emergencia institucional en CNT; Telecomunicaciones anunció siete medidas tras ataques informáticos - El Comercio. [Online] https://www.elcomercio.com/actualidad/negocios/cnt-hackers-ataques-informaticos-modernizacion.html, 2021.

[8] La ANT informa sobre ataque cibernético a sus sistemas. [Online] www.ant.gob.ec/la-ant-informa-sobre-ataque-cibernetico-a-sus-sistemas/, 2021.

[9] Florida Education Institute. [Online] https://www.fei.edu, 2022.

[10] ISO/IEC 24762:2008. [Online] https://www.iso.org/obp/ui/iso:std:iso-iec:24762:ed-1:v1:en, 2022.

[11] Carlos Mellado Erices. Plan de contingencia informático. 2014.

[12] ¿Qué son las normas ISO y cuál es su finalidad? [Online] https://www.isotools.org/2015/03/19/que-son-las-normas-iso-y-cual-es-su-finalidad/, 2022.

[13] ¿Qué es la Seguridad Informática? — UNIR Ecuador. [Online] https://ecuador.unir.net/actualidad-unir/que-es-seguridad-informatica/, 2022.

[14] R.C.S. Alonso. *Tecnologías de la información y la comunicación: Introducción a los sistemas de información y de telecomunicación.* Manuales transversales. Ideaspropias Editorial, 2007.

[15] ¿En qué consiste una matriz de riesgos? — RSM. [Online] https://www.rsm.global/peru/es/aportes/blog-rsm-peru/en-que-consiste-una-matriz-de-riesgos, 2020.

[16] ISO 24762:2008 — Disaster Recovery. [Online] https://www.disasterrecovery.org/iso-24762-2008/, 2022.