

**MÁSTER UNIVERSITARIO EN SEGURIDAD DE
LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS
COMUNICACIONES**

TRABAJO FIN DE MÁSTER

**Resiliencia TIC microPYMEs y
hogares**

Autores

**Erik Arencón García - 222A8925
Javier González González - 21838024**

**Director del Trabajo Fin de Máster
Dr. Carlos Bachmaier Johanning**

CURSO 2022-2023

RESUMEN

El Trabajo de Fin de Máster (TFM) plantea resolver problemas de resiliencia en entornos de bajos recursos cómo microPYMEs y hogares.

Existe la necesidad de poder asegurar en lo posible la continuidad de negocio en cualquier tipo de organización. Mientras que en organizaciones de cierto tamaño este problema está resuelto en mayor o menor medida, las empresas de menor tamaño y recursos no están preparadas para conseguirla. El objetivo principal de este proyecto es aportar una solución accesible para este tipo de organizaciones, pudiendo extrapolar la solución a hogares familiares.

Primero se realizará un análisis de los posibles puntos de ruptura de la continuidad de negocio y cómo proteger y solucionar estos problemas. Después de haber identificado los problemas a grandes rasgos, se estudiará en detalle aquellos que sean críticos para el desarrollo de las actividades diarias de los clientes (creación de BIA). Por último se desarrollará el plan de acción que consiga el objetivo de resiliencia buscado.

Este proyecto es de tipo industrial aportando una solución a un problema planteado para microPYMEs y hogares.

ABSTRACT

The Master's Final Project (MFP) aims to solve resilience problems in low resource environments such as micro-SMEs and households.

There is a need to ensure as much business continuity in any type of organization. While in organizations of a certain size this problem is solved to a greater or lesser extent, companies of smaller size and resources are not prepared to achieve it. The main objective of this project is to provide an accessible solution for this type of organizations, being able to extrapolate the solution to family homes.

First, an analysis of the possible breakpoints of business continuity and how to protect and solve these problems will be carried out. After having identified the problems in broad terms, we will study in detail those that are critical for the development of the daily activities of the clients (creation of BIA). Finally, an action plan will be developed to achieve the desired resilience objective.

This is an industrial project providing a solution to a problem posed for micro-SMEs and households.

AGRADECIMIENTOS

Expresar agradecimiento a todas las personas que, de una u otra forma, nos han apoyado a lo largo de este viaje académico. A familia y amigos por la paciencia y comprensión a lo largo de este periodo.

En segundo lugar, agradecer por su compromiso a nuestro tutor Carlos por orientarnos y aconsejarnos en lo necesario, siendo de gran ayuda, impulsando nuestro interés y curiosidad por el tema de desarrollo.

Por último, agradecer a nuestro compañero de TFM por llevar a cabo este trabajo de manera conjunta, manteniendo la calma en medio del caos, compartiendo y apoyándonos en lo necesario para alcanzar los objetivos.

ÍNDICE DE CAPÍTULOS Y ANEXOS

| | |
|--|-----------|
| 1 INTRODUCCIÓN | 12 |
| 2 ESTADO DE LA CUESTIÓN | 14 |
| 2.1 Marcos, normativas y metodologías | 14 |
| 2.2 Productos relacionados con resiliencia (aplicables en entornos de pymes) | 16 |
| 2.3 Trabajos relacionados | 20 |
| 3 DESCRIPCIÓN DEL PROBLEMA | 22 |
| 4 SOLUCIÓN PROPUESTA | 24 |
| 4.1 OBJETIVOS | 24 |
| 4.2 LOGROS A ALCANZAR | 26 |
| 4.3 PLANIFICACIÓN | 26 |
| 4.3.1 PLANIFICACIÓN DE TAREAS | 27 |
| 5 DESARROLLO DE LA SOLUCIÓN GENERAL EN MICROPYMES | 31 |
| 5.1 Conectividad de red | 31 |
| 5.1.2 Riesgos, Impactos y Vulnerabilidades | 31 |
| 5.1.3 Estrategia de redundancia | 35 |
| 5.1.4 Conclusión | 46 |
| 5.2 Electricidad | 47 |
| 5.2.1 Introducción | 47 |
| 5.2.2 Riesgos, Impactos y Vulnerabilidades | 48 |
| 5.2.3 Estrategia de redundancia | 50 |
| 5.2.4 Conclusión | 58 |
| 5.3 DATOS | 59 |
| 5.3.2 Riesgos, Impactos y Vulnerabilidades | 59 |
| 5.3.3 Estrategia de redundancia | 61 |
| 5.3.4 Conclusión | 68 |
| 6 APLICACIÓN PRÁCTICA A UN CASO CONCRETO | 69 |
| 6.1 Definición de la empresa | 69 |
| 6.2 Análisis de impacto de negocio | 72 |
| 6.2.1 Introducción | 72 |
| 6.2.2 Alcance | 73 |
| 6.2.3 Definiciones y terminología | 74 |
| 6.2.4 Activos | 75 |
| 6.2.5 Árbol de dependencias | 76 |
| 6.2.6 Análisis de riesgos | 77 |
| 6.2.7 Análisis de impacto | 78 |
| 6.2.8 Recomendaciones | 80 |
| 7 PRUEBAS Y VALIDACIÓN | 81 |
| 7.1 Demostrativo para resiliencia de Datos | 81 |
| 7.2 Demostrativo para resiliencia Eléctrica | 82 |
| 7.3 Demostrativo para resiliencia de Red | 84 |
| 7.3.1 Demostrativo de resiliencia de red en clases online | 84 |
| 7.3.2 Demostrativo para resiliencia de red en aplicación web | 84 |

| | |
|---|-----------|
| 8 CONCLUSIONES | 85 |
| 8.1 Conclusiones del trabajo | 85 |
| 8.2 Conclusiones personales | 85 |
| 9 TRABAJOS FUTUROS | 86 |
| 10 DECLARACIÓN DE COLABORACIÓN | 87 |
| 11 APÉNDICES | 88 |
| 11.1 BIBLIOGRAFÍA | 88 |
| 11.2 CONFIGURACIÓN DE TAREAS PROGRAMADAS EN WINDOWS | 91 |
| 11.3 CONFIGURACIÓN DE GOOGLE CLOUD PARA ALMACENAMIENTO DE COPIAS DE SEGURIDAD | 95 |
| 11.4 INSTALACIÓN PASO A PASO POWERCHUTE | 100 |
| 11.5 CONFIGURACIÓN AUTOMATIZACIONES SAI | 106 |
| 11.6 GUIA DE PRUEBAS SEMESTRALES DE FUNCIONAMIENTO DEL SAI | 113 |
| 11.7 FORMACIÓN ANUAL RELACIONADA CON EVENTOS DISRUPTIVOS | 114 |
| 11.8 CONFIGURACIÓN DE DISPOSITIVO MÓVIL COMO PUNTO DE ACCESO | 116 |
| 11.9 CONFIGURACIÓN DE RED EN DISPOSITIVOS PORTÁTILES | 120 |
| 11.10 CREACIÓN DE PÁGINA WEB SECUNDARIA | 122 |
| 11.11 SCRIPTS | 126 |
| 11.11.1 COPIAS DE SEGURIDAD | 128 |
| 11.11.2 SUBIDA DE COPIAS DE SEGURIDAD A GOOGLE DRIVE | 129 |
| 11.11.3 ROTADO DE COPIAS DE SEGURIDAD EN GOOGLE DRIVE | 130 |
| 11.11.4 DESCARGA DE COPIAS DE SEGURIDAD EN GOOGLE DRIVE | 130 |
| 11.11.5 RESTAURAR LOS DATOS DE LA COPIA DE SEGURIDAD | 131 |

ÍNDICE TABLAS

| | |
|---|-----------|
| Tabla 1: Tabla con los objetivos principales del proyecto | 25 |
| Tabla 2: Tabla con los objetivos secundarios del proyecto | 25 |
| Tabla 3: Planificación de tareas | 28 |
| Tabla 4: Planificación de tareas - calendario | 30 |
| Tabla 5: Tabla de calificación del impacto según la pérdida reputacional | 78 |
| Tabla 6: Tabla de análisis de impacto | 79 |

ÍNDICE FIGURAS

| | |
|--|------------|
| Figura 1: SAI Salicru One Inline (SPS 1100 ONE, n.d.) y SAI APC Back-UPS BX1600MI-GR (APC Back-UPS BX1600MI-GR, n.d.) | 16 |
| Figura 2: Router Netgear Nighthawk LAX20 - AX4 4G Lte (Silveira, n.d.) | 17 |
| Figura 3: Generador Electrico Gasolina 5500W, Leelbox con 2 tomas (Generador Electrico Gasolina 5500W Leelbox, n.d.) | 18 |
| Figura 4: Panel Solar de 410 W 31,6V (LEICKE Panel Solar, n.d.) | 19 |
| Figura 5: Diagrama SAI Offline | 52 |
| Figura 6: Diagrama SAI Interactivo | 53 |
| Figura 7: Diagrama SAI Online | 54 |
| Figura 8: Plano de la distribución de la oficina de la microPYME | 70 |
| Figura 9: Esquema de red de microPYME | 71 |
| Figura 10: Árbol de dependencias de la microPYME | 76 |
| Figura 11: Página de descarga de PowerChute con las distintas versiones | 82 |
| Figura 12 - 11.2 Programador de tareas | 91 |
| Figura 13 - 11.2 Elementos para crear nueva tarea | 92 |
| Figura 14 - 11.2 Creación de una nueva tarea | 92 |
| Figura 15 - 11.2 Desencadenador de tarea | 93 |
| Figura 16 - 11.2 Iniciar un programa desde una tarea | 93 |
| Figura 17 - 11.2 Ejecutar una tarea manualmente | 94 |
| Figura 18 - 11.2 Resultados de tareas programadas | 94 |
| Figura 19 - 11.3 Comando instalación SDK Google | 95 |
| Figura 20 - 11.3 Instalador SDK(1) | 95 |
| Figura 21 - 11.3 Instalador SDK(2) | 96 |
| Figura 22 - 11.3 Instalador SDK(3) | 96 |
| Figura 23 - 11.3 Consola principal Google Cloud | 97 |
| Figura 24 - 11.3 Creación de un nuevo proyecto en Google Cloud | 97 |
| Figura 25 - 11.3 Datos de nuevo proyecto Google Cloud | 97 |
| Figura 26 - 11.3 Login desde la máquina a Google Cloud | 98 |
| Figura 27 - 11.3 Selección de proyecto | 98 |
| Figura 28 - 11.3 Creación de un bucket | 99 |
| Figura 29 - 11.4 Descarga del programa | 100 |
| Figura 30 - 11.4 Archivos de programa | 101 |
| Figura 31 - 11.4 Comprobación/Instalación MV C++ 2017 | 101 |
| Figura 32 - 11.4 Selección del SAI | 102 |
| Figura 33 - 11.4 Selección comunicación del SAI | 102 |
| Figura 34 - 11.4 Creación de cuenta de acceso a la consola de SAI | 103 |
| Figura 35 - 11.4 Permisos en el firewall de Windows | 104 |
| Figura 36 - 11.4 Acceso a la consola PowerChute | 104 |
| Figura 37 - 11.4 Aceptación de términos | 105 |
| Figura 38 - 11.5 Tipo de contraseña | 106 |
| Figura 39 - 11.5 Contraseña de aplicación | 107 |

| | |
|---|------------|
| Figura 40 - 11.5 Historial de uso de contraseña de aplicación | 107 |
| Figura 41 - 11.5 Apartado de configuración de envío de correos | 108 |
| Figura 42 - 11.5 Datos servidor SMTP | 108 |
| Figura 43 - 11.5 Destinatarios | 109 |
| Figura 44 - 11.5 Contraseñas de aplicación | 109 |
| Figura 45 - 11.5 Datos de contacto | 109 |
| Figura 46 - 11.5 Notificación de envío de correo de prueba | 110 |
| Figura 47 - 11.5 Ejemplo de correo electrónico recibido | 110 |
| Figura 48 - 11.5 Eventos Críticos | 111 |
| Figura 49 - 11.5 Eventos Medios | 111 |
| Figura 50 - 11.5 Eventos Información | 111 |
| Figura 51 - 11.5 Selección de scripts para una alerta específica | 112 |
| Figura 52 - 11.5 Selección de scripts a ejecutar | 112 |
| Figura 53 - 11.8 Uso de datos | 116 |
| Figura 54 - 11.8 Activación de datos móviles | 117 |
| Figura 55 - 11.8 Zona Wi-Fi/Compartir conexión | 118 |
| Figura 56 - 11.8 Datos Zona Wi-Fi | 119 |
| Figura 57 - 11.9 Administrar redes conocidas | 120 |
| Figura 58 - 11.9 Datos de la red | 120 |
| Figura 59 - 11.9 Histórico de redes conocidas | 121 |
| Figura 60 - 11.10 Aplicación AWebServer | 122 |
| Figura 61 - 11.10 Permisos AWebServer | 123 |
| Figura 62 - 11.10 Pestaña principal AWebServer | 124 |
| Figura 63 - 11.10 Ejemplo de web secundaria | 125 |
| Figura 64 - 11.11 Powershell | 126 |
| Figura 65 - 11.11 Ejecución fallido de script Powershell | 127 |
| Figura 66 - 11.11 Modificación de política en Powershell | 127 |
| Figura 67 - 11.11 Ejecución de Script en Powershell | 127 |
| Figura 68 - Código copias de seguridad | 128 |
| Figura 69 - Código subidas copias de seguridad | 129 |
| Figura 70 - Código rotado copias de seguridad | 130 |
| Figura 71 - Código descarga copias de seguridad | 130 |
| Figura 72 - Código restauración copias de seguridad | 131 |

1 INTRODUCCIÓN

La resiliencia es la capacidad de un sistema para resistir y recuperarse de situaciones adversas, manteniendo sus funciones y servicios críticos en funcionamiento. En la actualidad, la resiliencia es un tema de gran importancia en diversos ámbitos, ya que permite garantizar la continuidad y sostenibilidad de diferentes sistemas y organizaciones, incluso en situaciones de crisis o desastres naturales.

Las microPYMEs diariamente se enfrentan a problemas de resiliencia que pueden afectar enormemente a su negocio ya que son mucho más vulnerables que otras empresas de mayor tamaño. Existen varios factores que contribuyen a los problemas de resiliencia en las microPYMEs como la escasez de recursos, escasez o falta de planificación estratégica, dependencia de factores externos (proveedores, clientes, socios), dependencia de mercado o falta de conocimiento, dificultando la posibilidad de realizar inversiones o mejoras en la infraestructura y complicando la recuperación ante situaciones excepcionales.

En este documento se expondrá el problema de una manera genérica que aplican a la gran mayoría de las microPYMEs y, posteriormente, se estudiará en detalle la aplicación del problema de manera específica, exponiendo los objetivos a alcanzar con el fin de encontrar soluciones que mejoren la resiliencia de estos sistemas.

La metodología seguida para llevar a cabo este proyecto será descrita con detalle, desde la identificación del problema, pasando por el análisis de las causas que lo provocan, hasta el planteamiento de soluciones para mejorarlo. También se explicará la planificación que se ha seguido para la ejecución del proyecto y los recursos necesarios para llevarlo a cabo.

Se analizarán diferentes soluciones para mejorar la resiliencia de los sistemas estudiados y se describe cómo se han desarrollado y puesto a prueba estas soluciones. Se indicarán demostradores que apliquen las distintas soluciones propuestas.

Finalmente, se presentarán las conclusiones obtenidas en el proyecto, destacando los resultados más relevantes y proponiendo posibles líneas de investigación futura. En definitiva,

este documento tiene como objetivo proporcionar una guía para aquellos interesados en mejorar la resiliencia de diferentes sistemas, ofreciendo una visión general del problema y de las soluciones disponibles.

2 ESTADO DE LA CUESTIÓN

En la actualidad, existen varias alternativas para analizar e implementar resiliencia en empresas. Para la investigación de este proyecto, se han estudiado estas herramientas, metodologías, estándares y proyectos previos, con el fin de analizar las distintas posibilidades que existen y seleccionar la más adecuada, partiendo de las características y recursos de microPYMEs y hogares.

2.1 Marcos, normativas y metodologías

- **ISO 22317 (*ISO 22317:2021 - Security and Resilience — Business Continuity Management Systems — Guidelines for Business Impact Analysis, 2021*)**: Esta norma internacional proporciona pautas y recomendaciones para desarrollar un proceso de evaluación de la capacidad de respuesta de la organización y mejorarlo, fortaleciendo su resiliencia y capacidad de sobreponerse a eventos disruptivos. Ofrece un marco para evaluaciones de la capacidad de respuesta de cada etapa de una situación de emergencia en la empresa, desde la prevención y preparación hasta la respuesta y recuperación.
- **ISO 22301 (*ISO 22301:2019 - Security and Resilience — Business Continuity Management Systems — Requirements, 2019*)**: Esta norma internacional establece los requisitos sobre un SGCN (sistema de gestión de la continuidad del negocio). Proporciona un marco para identificar riesgos, para la planificación de la continuidad del negocio y para la respuesta ante situaciones de crisis, permitiendo a las empresas establecer medidas adecuadas para mantener sus operaciones y minimizar el impacto de interrupciones.
- **ISO/IEC 27001 (*IEC 27001 Standard — Information Security Management Systems, 2022*)**: Para la gestión de la seguridad conforme la norma, se especifican una serie de requisitos. Pretende asegurar la confidencialidad, integridad y disponibilidad de la información de una organización. La norma define de manera genérica cómo se planifica, implanta, verifica y controla un Sistema de Gestión de Seguridad de la Información (SGSI).

- **Plan de Recuperación, Transformación y Resiliencia (PRTR):** programa de políticas del gobierno de España que aborda los desafíos económicos y sociales causados por la pandemia de COVID-19, impulsando la transición hacia una economía más sostenible y resiliente. Uno de sus pilares es la transformación digital y la digitalización de pymes (impulso a la pyme, componente 13). Se facilita la financiación, digitalización, pero solo se menciona resiliencia medioambiental y resiliencia del apoyo, por lo que queda fuera del alcance del TFM.
- **Plan de continuidad de negocio:** describe mediante un conjunto de acciones y medidas diseñadas de forma que, cuando surja una anomalía que pudiera dar lugar a una interrupción del negocio, se asegure en lo requerido la continuidad de las operaciones, minimizando el impacto negativo en situaciones de crisis o de desastres. Un plan de continuidad de negocio debe identificar los riesgos, implementar prevenciones y crear estrategias de mitigaciones, asignar los responsables para cada caso, elaborar un plan de contingencia y probar todo esto mediante pruebas y entrenamientos. Según el Incibe, tiene varias perspectivas: “infraestructura TIC, recursos humanos, mobiliario, sistemas de comunicación, logística, sistemas industriales, infraestructuras físicas, etc”.

2.2 Productos relacionados con resiliencia (aplicables en entornos de pymes)

- **SAI:** En el mercado actual, para abordar cortes de suministro eléctrico, existen varios tipos de SAI (Sistemas de Alimentación Ininterrumpida) diseñados para cubrir las necesidades de los negocios. Los SAI se clasifican en tres categorías principales: SAI de línea interactiva, SAI en línea y SAI en paralelo (cada categoría ofrece unas prestaciones de nivel diferente en cuanto a cortes y microcortes). Es importante tener en cuenta que el precio de los SAI puede variar considerablemente dependiendo de la capacidad de respaldo, (de la cual depende el tiempo de suministro en caso de corte), la marca y las características de cada modelo. Al elegir un SAI, es fundamental evaluar las necesidades del negocio en cuanto a la protección de la energía y encontrar un equilibrio entre la funcionalidad y el presupuesto disponible. Esto a veces es lo más complicado, ya que o no se llegan a concretar las necesidades o partes críticas, o debido a la alta variedad, no se llega a decidir cuál es el apropiado. Requiere un mantenimiento regular para asegurar que las baterías que incorpora se mantengan operativas.



Figura 1: SAI Salicru One Inline (SPS 1100 ONE, n.d.) y SAI APC Back-UPS BX1600MI-GR (APC Back-UPS BX1600MI-GR, n.d.)

- **Router:** se suele optar por utilizar un router de conexión normal de fibra como conexión a Internet debido a su alta velocidad y estabilidad. Sin embargo, para garantizar la continuidad del servicio en caso de fallo de la conexión principal, se puede utilizar un router con doble entrada de internet (doble proveedor) o se puede utilizar un router SIM como backup. Estos routers SIM pueden activarse automáticamente en caso de que se produzca una interrupción en la conexión de fibra, asegurando una conexión a Internet confiable y sin interrupciones a través de la red móvil. El precio de estos routers de backup con conexión SIM dependerá de factores como la capacidad de respaldo, la compatibilidad con diferentes bandas de frecuencia y las características adicionales que ofrecen.



Figura 2: Router Netgear Nighthawk LAX20 - AX4 4G Lte (Silveira, n.d.)

- **Generadores eléctricos de gasolina:** existen generadores portátiles y generadores estacionarios o industriales. Estos generadores están marcados por la capacidad de generación, la marca, la eficiencia energética y las características adicionales. Además, la funcionalidad de los generadores eléctricos siempre está limitada por la capacidad de gasolina o combustible que puedan tener en el momento del uso. La autonomía y el tiempo de funcionamiento de un generador depende de la capacidad del tanque del combustible, esté incorporado o sea externo, y de la eficiencia con la que consume el combustible. Es fundamental evaluar las necesidades energéticas del negocio y encontrar un equilibrio entre la capacidad requerida, la duración del suministro y el presupuesto disponible al elegir un generador eléctrico adecuado. Requiere un mantenimiento regular para asegurar su operatividad, verificando que las baterías que incorpora se mantengan operativas así como la disponibilidad de combustible.



Figura 3: Generador Electrico Gasolina 5500W, Leelbox con 2 tomas (*Generador Electrico Gasolina 5500W Leelbox, n.d.*)

- **Placas solares:** la capacidad de generación, la eficiencia del dispositivo y la tecnología implementada son elementos que debemos tener en cuenta en la decisión de la compra de placas. Además, la funcionalidad de las placas solares siempre es dependiente de las condiciones climáticas, principalmente la disponibilidad de luz solar. Los días soleados y claros proporcionan una mayor generación de energía, mientras que condiciones nubladas o con poca luz solar afectarán la producción energética. Es fundamental evaluar los requisitos eléctricos del negocio, considerar las condiciones climáticas predominantes en la zona. Es importante destacar que es necesario, no solo la compra de placas solares, sino si se quiere tener dependencia de la hora del día, también la compra de acumuladores.



Figura 4: Panel Solar de 410 W 31,6V (*LEICKE Panel Solar*, n.d.)

2.3 Trabajos relacionados

- "How to set up backup internet connections for home offices" (Froehlich, 2022) explica la importancia de contar con conexiones a Internet de reserva en oficinas domésticas y ofrece una guía paso a paso para que el personal informático sea capaz de configurar un acceso fiable a Internet. Es esencial disponer de una conexión a Internet de reserva para garantizar que los empleados puedan seguir trabajando sin interrupciones. El artículo sugiere dos métodos para asegurar la estabilidad que son utilizar un router con conexión móvil independiente o un router que también admite conexiones móviles para crear una conexión a Internet de reserva. También recomienda utilizar una tecnología diferente a la de la conexión principal y añadir un SAI al router de Internet para garantizar el acceso a Internet durante un corte de electricidad. El artículo también destaca la importancia de asegurar el acceso a los recursos digitales de una empresa a través de una conexión de reserva.
- "¿Qué es la resiliencia empresarial?" (Romero & García, 2021) publicado en Expok News, desarrolla el concepto de resiliencia empresarial y su importancia en la actualidad. El artículo explica la resiliencia empresarial como la capacidad de una empresa para adaptarse y recuperarse de acontecimientos inesperados como pueden ser catástrofes naturales, ciberataques y pandemias entre otros. Cabe destacar la importancia de contar con un plan que garantice la continuidad de la empresa ante situaciones límite. El artículo hace hincapié en la necesidad de la flexibilidad y agilidad de las empresas en sus operaciones para responder a circunstancias cambiantes.
- "Cómo lograr una empresa más resiliente y sufrir menos ante una crisis" (Alonso, 2021) analiza la importancia de la resiliencia e indica consejos para que las empresas aumenten su resiliencia. Destaca la importancia de tener un plan que garantice la continuidad de la empresa ante situaciones adversas. El artículo sugiere que las empresas deberían centrarse en crear una cultura resistente, invertir en tecnología y desarrollar una plantilla flexible. Además, el artículo subraya la importancia de la ciberseguridad y la protección de datos para garantizar la continuidad de la empresa.

- "Cómo transformar a mi compañía en una organización resiliente" (*¿Cómo Transformar a Mi Compañía En Una Organización Resiliente?*, 2021) analiza la importancia de la resiliencia empresarial y ofrece consejos para que las empresas sean más resilientes. Destaca la importancia de contar con un plan que garantice la continuidad de la empresa en tiempos de crisis. El artículo sugiere que las empresas deberían centrarse en cambiar el enfoque del negocio y sobre todo digitalizando.

3 DESCRIPCIÓN DEL PROBLEMA

En el entorno empresarial actual, las microPYMEs desempeñan un papel vital en la economía. Estas pequeñas empresas contribuyen significativamente al crecimiento económico, la generación de empleo y la innovación. Sin embargo, a pesar de su importancia, las microPYMEs enfrentan numerosos desafíos que pueden amenazar su supervivencia y crecimiento a largo plazo. Uno de los desafíos más críticos es la falta de resiliencia, es decir, la capacidad de adaptarse y recuperarse rápidamente ante eventos adversos.

Las microPYMEs son especialmente vulnerables a eventos imprevistos que pueden afectar negativamente sus operaciones comerciales. Estos eventos pueden incluir desastres naturales, como terremotos, inundaciones o incendios, así como eventos socioeconómicos, como crisis económicas o cambios en la demanda del mercado. Las microPYMEs a menudo carecen de los recursos financieros, tecnológicos y de personal necesarios para hacer frente a estas situaciones de manera efectiva, lo que agrava su vulnerabilidad.

Las consecuencias de estos eventos pueden ser devastadoras para una microPYME. Pueden experimentar interrupciones en la cadena de suministro, daños a sus activos físicos, pérdida de clientes y oportunidades de negocio, así como dificultades financieras. La falta de resiliencia puede llevar a una recuperación lenta y costosa o, en el peor de los casos, al cierre de la empresa.

Las microPYMEs operan con recursos limitados en comparación con las empresas más grandes. Estas limitaciones incluyen personal, tecnología, infraestructura y capital. La falta de recursos financieros y tecnológicos dificulta la implementación de medidas de resiliencia adecuadas, ya que se priorizan otras inversiones o gastos por encima de la resiliencia al no ser considerado como un problema o riesgo principal.

Por ejemplo, las microPYMEs pueden carecer de fondos para invertir en sistemas de respaldo avanzados, contratar personal especializado en gestión de riesgos o mantener inventarios de emergencia. La falta de acceso a financiamiento y recursos adecuados limita su capacidad para implementar estrategias de resiliencia y los deja expuestos a riesgos significativos.

Además, las microPYMEs a menudo dependen en gran medida de un solo proveedor o socio comercial para el suministro de materiales, servicios o tecnología. Si alguno de estos proveedores o socios enfrenta dificultades o interrupciones en su operación, las microPYMEs pueden sufrir un impacto directo en sus propias operaciones.

Otra de las razones fundamentales por las que las microPYMEs luchan con la resiliencia es la falta de conciencia de riesgos. Muchas microPYMEs no cuentan con planes formales de gestión de riesgos y continuidad del negocio. No tienen un enfoque estructurado para identificar, evaluar y mitigar los riesgos potenciales a los que están expuestas.

La falta de conciencia sobre los riesgos potenciales dificulta su capacidad para responder y recuperarse ante eventos adversos. Sin una planificación adecuada, las microPYMEs se encuentran desprevenidas y pueden sufrir daños significativos en caso de una interrupción. La falta de un plan de contingencia claro y la falta de capacitación en la implementación de dicho plan son obstáculos adicionales para la resiliencia de las microPYMEs.

Las microPYMEs a menudo enfrentan limitaciones en su infraestructura tecnológica, lo que afecta su capacidad para mantener la continuidad operativa y proteger sus activos digitales. Pueden tener redes informáticas inadecuadas, falta de medidas de seguridad de ciberseguridad, sistemas de respaldo insuficientes y falta de capacidades de recuperación ante desastres.

Estas limitaciones tecnológicas dificultan la implementación de prácticas de resiliencia efectivas. La falta de inversión en tecnología y sistemas de respaldo puede dejar a las microPYMEs expuestas a ataques cibernéticos, pérdida de datos críticos y tiempos de inactividad prolongados. La falta de conocimiento y comprensión de las soluciones tecnológicas disponibles también contribuye a la falta de resiliencia en el ámbito digital.

La falta de capacitación y conocimientos especializados en gestión de riesgos y resiliencia es otro desafío común para las microPYMEs. Muchos propietarios de microPYMEs no tienen experiencia ni recursos para dedicarse a la gestión de riesgos o para implementar prácticas de resiliencia efectivas.

La falta de capacitación y conocimientos limita su capacidad para identificar y abordar proactivamente los riesgos. Carecen de la comprensión necesaria para desarrollar estrategias y planes de resiliencia sólidos. Además, no cuentan con personal capacitado para llevar a cabo evaluaciones de riesgos, implementar medidas de seguridad y recuperación, y coordinar las actividades necesarias durante y después de una crisis.

La falta de resiliencia es un problema crítico que enfrentan las microPYMEs en su búsqueda de supervivencia y éxito en un entorno empresarial cada vez más complejo y volátil. La vulnerabilidad a eventos imprevistos, la dependencia de recursos limitados, la falta de planificación y conciencia de riesgos, la dependencia de proveedores y socios externos, las limitaciones en infraestructura tecnológica, y la falta de capacitación y conocimientos especializados son desafíos clave que deben abordarse para mejorar la resiliencia de las microPYMEs.

Es fundamental que las microPYMEs reconozcan la importancia de la resiliencia y adopten medidas proactivas para fortalecerla. Esto incluye la implementación de planes de gestión de riesgos y continuidad del negocio, la diversificación de proveedores y socios, la mejora de la infraestructura tecnológica, la capacitación del personal en resiliencia y la búsqueda de apoyo externo a través de asociaciones y programas gubernamentales.

Solo al abordar estos desafíos y mejorar su capacidad de adaptación y recuperación, las microPYMEs podrán desarrollar una mayor resiliencia y sentar las bases para su crecimiento a futuro.

4 SOLUCIÓN PROPUESTA

4.1 OBJETIVOS

El objetivo de este TFM es resolver el problema de resiliencia en varios ámbitos en microPYMEs y hogares.

Para alcanzar este objetivo se identificaron, inicialmente los objetivos específicos recogidos en la siguiente tabla:

| ID | Objetivo | Resultado |
|----|---|---|
| O1 | Análisis de la estructura y contexto de microPYMEs y hogares | Descripción de las empresas y entornos |
| | | Arquitectura tecnológica |
| | | Identificación del estado actual de la resiliencia en microPYMEs |
| O2 | Análisis del problema de resiliencia aplicable de manera genérica en microPYMEs | Comparativa de elementos de mejora de resiliencia existentes, y riesgos asociados a estos |
| O3 | Creación de BIA | Identificación de los servicios críticos, activos, amenazas, vulnerabilidades, posibles medidas de mitigación y recomendaciones |
| | | Documento de análisis de impacto de negocio |

| | | |
|----|-------------------------|---|
| O4 | Modelado de la solución | Estrategias y medidas a implantar de resiliencia ante disruptores |
|----|-------------------------|---|

Tabla 1: Tabla con los objetivos principales del proyecto

Si se completan los objetivos principales y las horas asignadas al proyecto lo permiten, se desarrollará los siguientes objetivos:

| | | |
|-----|---|-------------------------------|
| Os1 | Estudio y posible implementación física de medidas de contención con bajos recursos | Maqueta física de la solución |
|-----|---|-------------------------------|

Tabla 2: Tabla con los objetivos secundarios del proyecto

4.2 LOGROS A ALCANZAR

El objetivo final es establecer los mecanismos de resiliencia que dispone una microPYME, mostrando las distintas opciones existentes. Uno de los principales logros de esta investigación es identificar y describir las estrategias de resiliencia aplicables a microPYMEs.. Otro logro importante será la evaluación de los factores clave que contribuyen a la resiliencia en las microPYMEs, al comprender estos factores, se identificarán áreas de mejora y recomendaciones para fortalecer la resiliencia de las microPYMEs. Por último, este trabajo pretende contribuir al conocimiento existente sobre la resiliencia en microPYMEs.

4.3 PLANIFICACIÓN

A continuación, se adjunta un plan detallado del trabajo que permitirá el seguimiento y la valoración continua del mismo, indicando las distintas fases de desarrollo y la estimación de tiempo. Este plan de trabajo consta de un diagrama Gantt.

El plan de trabajo consta de un análisis previo y general del proyecto, donde se establecerán las bases del mismo. Una definición y planificación de proyecto, un análisis e inicio de recogida de datos y un cierre de proyecto, donde se documentaron todos los anteriores apartados en una memoria TFM.

Se han llevado a cabo varias reuniones de revisión con el tutor.

4.3.1 PLANIFICACIÓN DE TAREAS

| NÚMERO EDT | TÍTULO DE LA TAREA | RESPONSABLE DE LA TAREA | FECHA DE INICIO | FECHA DE ENTREGA | DURACIÓN |
|------------|--|-------------------------|-----------------|------------------|----------|
| 1 | Análisis e inicio del proyecto | | | | |
| 1.1 | Revisión de TFMs | Ambos | 30/01/23 | 01/02/23 | 1 |
| 1.1.1 | Selección de TFM | Ambos | 30/01/23 | 02/02/23 | 2 |
| 1.2 | Reunión de presentación de proyecto | Ambos | 02/02/23 | 09/02/23 | 7 |
| 1.3 | Petición de información adicional | Erik Arencón | 13/02/23 | 20/02/23 | 7 |
| 1.4 | Planificación del proyecto | Ambos | 20/02/23 | 23/02/23 | 3 |
| 1.5 | Inicio del proyecto | Ambos | 24/02/23 | 27/02/23 | 3 |
| 1.6 | Creación de PPFM | Ambos | 28/02/23 | 02/03/23 | 2 |
| 2 | Definición y planificación del proyecto | | | | |
| 2.1 | Definición del alcance y de los objetivos | Pendiente | 03/03/23 | 09/03/23 | 6 |
| 2.2 | Plan de comunicación | Pendiente | 10/03/23 | 17/03/23 | 7 |
| 2.3 | Gestión de riesgos | Pendiente | 20/03/23 | 29/03/23 | 9 |
| 2.4 | Modelación de empresa | Pendiente | 23/03/23 | 19/04/23 | 26 |
| 2.5 | Creación de BIA | Pendiente | 31/03/23 | 19/04/23 | 19 |
| 3 | Análisis e inicio del proyecto | | | | |
| 3.1 | Análisis del estado del arte | Pendiente | 20/04/23 | 26/04/23 | 6 |

| | | | | | |
|----------|---|-----------|----------|----------|----|
| 3.2 | Análisis de puntos de fallo | Pendiente | 27/04/23 | 18/05/23 | 21 |
| 3.2.1 | Soluciones para prevenir caídas de servicio | Pendiente | 03/05/23 | 09/05/23 | 6 |
| 3.2.2 | Servicios en la empresa | Pendiente | 10/04/23 | 18/05/23 | 38 |
| 3.3 | Contextualización de servicios | Pendiente | 19/05/23 | 07/06/23 | 18 |
| 3.3.1 | Definición de servicios y salvaguardas | Pendiente | 26/05/23 | 07/06/23 | 11 |
| 4 | Cierre del proyecto | | | | |
| 4.1 | Objetivos del proyecto | Pendiente | 08/06/23 | 22/06/23 | 14 |
| 4.2 | Realización memoria final | Pendiente | 23/06/23 | 04/07/23 | 11 |
| 4.3 | Reunión de revisión de proyecto | Pendiente | 18/07/23 | 18/07/23 | 1 |
| 4.4 | Arreglos memoria post-revisión | Pendiente | 05/07/23 | 11/07/23 | 6 |
| 4.5 | Preparación defensa TFM | Pendiente | 12/07/23 | 14/07/23 | 2 |

Tabla 3: Planificación de tareas

Estas tareas van asociadas al siguiente diagrama, separándolos en dos con el fin de facilitar su visualización.

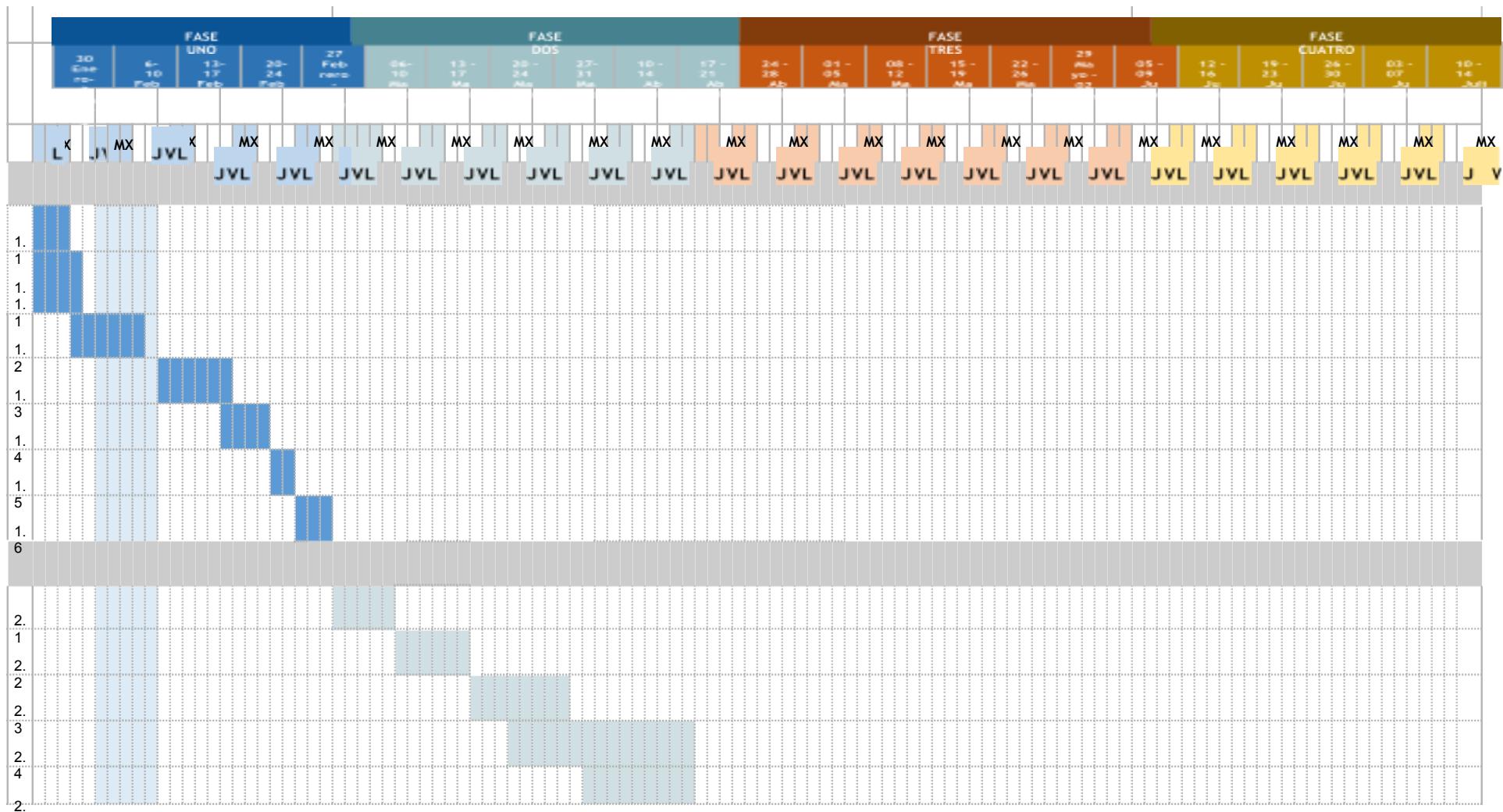


Tabla 4: Planificación de tareas - calendario

5 DESARROLLO DE LA SOLUCIÓN GENERAL EN MICROPYMEs

Cuando se trata de abordar el problema de la resiliencia, una empresa, sin importar sus características, debe considerar diversos aspectos que pueden influir en su capacidad para enfrentar y superar desafíos. Algunos de los elementos de su árbol de dependencia que tendrán que tratar son el personal, electricidad, datos, internet, infraestructura, proveedores o equipamiento entre otros. Estos elementos comparten riesgos y vulnerabilidades en algunas circunstancias, implicando diferentes impactos dependiendo del propio elemento que sea afectado.

En este apartado, nos centraremos en tres de estos elementos: internet, electricidad y datos, con el objetivo de explorar cómo las microPYMEs pueden fortalecer su resiliencia en estas áreas críticas.

5.1 Conectividad de red

5.1.1 Introducción

Cada vez existen más microPYMEs que se dedican al negocio online o tecnológico o que dependen de la tecnología y el internet para desarrollar sus actividades diarias. Por ello la pérdida parcial o total de la conectividad red en la actualidad supone un impacto significativo en su productividad y la continuidad de su negocio.

La resiliencia de red es la capacidad que tienen dichas microPYMEs para resistir, adaptarse y recuperarse de una manera rápida y eficiente ante la pérdida de conectividad. La pérdida de conectividad puede deberse a diversos problemas como desastres naturales, fallos en el hardware, cortes de energía o ataques cibernéticos, con ocurrencia en la propia pyme o su(s) suministrador(es). A continuación se describirán diversos riesgos que se derivan de la pérdida de conexión y las medidas de resiliencia que se pueden adoptar para mitigar, contener y recuperarse de este problema.

5.1.2 Riesgos, Impactos y Vulnerabilidades

Dependencia de servicios en la nube: Si la microPYME utiliza servicios en la nube para almacenar datos, aplicaciones o sistemas de gestión empresarial, la falta de internet puede impedir el acceso a estos servicios. Esto puede generar problemas de funcionamiento, pérdida de datos (información del cliente, registros financieros, documentos comerciales y otros datos críticos necesarios para la operación y toma de decisiones) o interrupción en la continuidad del negocio.

Problemas de cumplimiento normativo: Si la microPYME opera en una industria regulada, es posible que deba cumplir con ciertas normativas relacionadas con la protección de datos, privacidad, seguridad cibernética, entre otras. La falta de acceso a internet puede dificultar el cumplimiento de estas regulaciones y exponer a la empresa a riesgos legales y sanciones.

Riesgo de pérdida de datos: Si la microPYME utiliza servicios de almacenamiento en la nube o respaldos en línea, la falta de internet puede dificultar la sincronización y el respaldo de datos, lo que aumenta el riesgo de pérdida de información importante en caso de fallas o daños en los sistemas locales.

Riesgo de interrupción en los servicios de pago en línea: Si la microPYME utiliza servicios de pago en línea, la falta de internet puede interrumpir la capacidad de aceptar pagos electrónicos, lo que puede resultar en una disminución de las ventas y afectar la experiencia del cliente.

Riesgo de falta de actualización de software y aplicaciones: Sin conexión a internet, la microPYME puede tener dificultades para acceder a actualizaciones de software y aplicaciones, lo que puede resultar en problemas de compatibilidad, vulnerabilidades de seguridad y pérdida de funcionalidad.

Impacto en la reputación de la empresa: Si la microPYME depende de una presencia en línea, la pérdida de internet puede afectar negativamente su reputación. Los clientes pueden percibir la falta de conexión como una falta de fiabilidad o capacidad para satisfacer sus necesidades. Esto puede dañar la imagen de la empresa y afectar la confianza de los clientes en el negocio. Además puede dificultar el monitoreo de la reputación en línea de la microPYME, incluyendo la supervisión de reseñas, comentarios y menciones en redes sociales y plataformas de reseñas. Esto puede afectar la capacidad de la empresa para responder y gestionar adecuadamente su reputación en línea, la interacción con los clientes y la promoción de la marca.

Incapacidad para acceder a información crítica: Si la microPYME almacena datos o utiliza aplicaciones en línea para acceder a información crítica, como inventarios, registros de clientes o información de proveedores, la falta de internet puede dificultar el acceso a esta información. Esto puede afectar la toma de decisiones, la planificación y la capacidad de respuesta rápida a situaciones comerciales.

Retrasos en la resolución de problemas técnicos: Muchas microPYMEs dependen del soporte técnico en línea para resolver problemas de software, configuración de redes o cualquier otro inconveniente relacionado con la tecnología. Sin acceso a internet, puede ser más difícil o demorado buscar ayuda y solucionar problemas técnicos, lo que afecta la eficiencia y el rendimiento operativo.

Impacto en la colaboración y trabajo remoto: En la actualidad, muchas microPYMEs se apoyan en el trabajo remoto y la colaboración en línea para llevar a cabo sus actividades. La pérdida de internet dificulta la colaboración a distancia, el intercambio de archivos, la comunicación en tiempo real y otras actividades necesarias para mantener la eficiencia y la productividad.

Interrupción de operaciones: Si una microPYME depende en gran medida del acceso a internet para llevar a cabo sus operaciones diarias, la pérdida de conexión puede interrumpir el flujo de trabajo y afectar la productividad. Las tareas que requieren acceso a sistemas en la nube, comunicación por correo electrónico, procesamiento de pagos en línea o uso de aplicaciones web pueden detenerse o

retrasarse.

Dificultades en la gestión financiera: Si la microPYME utiliza herramientas en línea para la gestión financiera, como la banca en línea, sistemas de facturación electrónica o servicios de contabilidad en la nube, la pérdida de internet puede dificultar la administración de las finanzas de la empresa. Esto puede llevar a retrasos en los pagos, problemas de facturación y dificultades en el control de los flujos de efectivo.

Dificultades en la investigación y desarrollo: Si la microPYME se dedica a la investigación y desarrollo, la falta de internet puede limitar el acceso a recursos en línea, bases de datos científicas, herramientas de colaboración y otras fuentes de información necesarias para la innovación y el desarrollo de productos.

Impacto en la logística y el seguimiento de envíos: Si la microPYME se dedica al comercio electrónico o tiene una cadena de suministro dependiente del acceso a internet, la pérdida de conexión puede dificultar el seguimiento de envíos, la coordinación con proveedores y la gestión de inventarios. Esto puede causar demoras en las entregas y problemas en la gestión de la cadena de suministro.

Interrupción de servicios de soporte y atención al cliente: Si la microPYME depende de servicios de atención al cliente en línea, como centros de llamadas o chats en vivo, la pérdida de internet puede interrumpir la capacidad de brindar soporte o asistencia a los clientes, lo que afecta la satisfacción del cliente y la reputación de la empresa.

Pérdida de oportunidades de colaboración y asociación: Sin acceso a internet, una microPYME puede perder oportunidades de colaborar con otras empresas o asociarse con proveedores, lo que puede limitar su crecimiento y expansión en el mercado.

Dificultades en el reclutamiento y contratación de personal: Si la microPYME depende de plataformas en línea para el reclutamiento y contratación de personal, la falta de internet puede dificultar el proceso y limitar las opciones disponibles para encontrar y contratar nuevos empleados.

Dificultades en el acceso a recursos de aprendizaje y capacitación en línea: Si la microPYME utiliza recursos en línea para el aprendizaje y la capacitación de sus empleados, la falta de conexión a internet puede limitar el acceso a cursos en línea, tutoriales y otras herramientas educativas, limitando las oportunidades de crecimiento y desarrollo de habilidades para el personal, lo que puede afectar su satisfacción y retención.

Impacto en la continuidad del negocio: Si la pérdida de internet es prolongada, puede tener un impacto significativo en la continuidad del negocio de una microPYME. La falta de acceso a servicios críticos en línea puede resultar en la pérdida de clientes, daños financieros y dificultades para recuperarse.

Impacto en la imagen de marca y percepción del cliente: Si la microPYME tiene una presencia en línea importante y pierde el acceso a internet, puede afectar negativamente la imagen de la marca y la percepción del cliente. Los clientes pueden percibir a la empresa como poco confiable o desactualizada, lo que puede afectar la confianza y la relación con los clientes.

Impacto en la gestión de la comunicación interna: La falta de acceso a internet puede dificultar la comunicación interna de la microPYME, especialmente si se depende de herramientas de mensajería en línea, correo electrónico o intranets para la colaboración y la transmisión de información entre los miembros del equipo.

Problemas en la gestión de la reputación y crisis de relaciones públicas: Si surge una situación de crisis o un problema de relaciones públicas que requiere una gestión en línea, la falta de internet puede dificultar la respuesta rápida y efectiva, lo que puede empeorar la situación y afectar negativamente la reputación.

Limitaciones en el acceso a herramientas de gestión empresarial: Si la microPYME utiliza herramientas en línea para la gestión de proyectos, la planificación, la gestión del tiempo o la gestión de tareas, la pérdida de internet puede afectar la eficiencia y la productividad de la empresa al limitar el acceso a estas herramientas.

Dificultades en la gestión de inventario y control de stock: Si la microPYME utiliza sistemas en línea para la gestión de inventario y control de stock, la pérdida de conexión puede dificultar la actualización en tiempo real de los niveles de inventario, lo que puede resultar en problemas de disponibilidad de productos y pérdida de ventas.

Impacto en la gestión de eventos y marketing promocional: Si la microPYME organiza eventos o depende del marketing promocional en línea, la falta de internet puede dificultar la planificación, promoción y ejecución de estos eventos, lo que puede afectar la participación y el éxito de las iniciativas de marketing.

Dificultades en el acceso a servicios gubernamentales en línea: Si la microPYME interactúa con agencias gubernamentales y utiliza servicios en línea para trámites, presentación de impuestos o solicitudes de licencias, la pérdida de internet puede interrumpir la capacidad de cumplir con los requisitos legales y administrativos.

Vulnerabilidad a ciberataques: Cuando una microPYME pierde el acceso a internet, puede resultar más vulnerable a ciberataques. Sin una conexión estable, las medidas de seguridad en línea, como cortafuegos, actualizaciones de software y monitoreo de amenazas, pueden volverse ineficaces. Esto aumenta el riesgo de sufrir ataques de malware, ransomware u otros tipos de ataques.

Problemas de seguridad física: La falta de internet puede interrumpir la conectividad con los sistemas de seguridad física, como cámaras de videovigilancia en línea o sistemas de control de acceso. Esto puede afectar la capacidad de la microPYME para monitorear sus instalaciones y

proteger sus activos físicos.

Incapacidad para realizar actualizaciones y parches de seguridad: Sin acceso a internet, puede resultar difícil o imposible para una microPYME aplicar actualizaciones de software y parches de seguridad críticos. Esto deja los sistemas y dispositivos vulnerables a brechas de seguridad y ataques informáticos.

Dificultades en la colaboración y comunicación con proveedores y socios comerciales: La falta de acceso a internet puede dificultar la comunicación y colaboración con proveedores y socios comerciales que dependen de herramientas en línea para la coordinación y la gestión conjunta de proyectos o actividades comerciales.

5.1.3 Estrategia de redundancia

Redundancia de enlaces: La implementación de múltiples proveedores de servicios de Internet o conexiones de Internet por enlaces alternantes (cableado/inalámbrico) puede ser una opción relativamente asequible, ya que existen diferentes opciones de ISP y de enlaces con precios competitivos en el mercado.

- **Redundancia activa-pasiva:** Consiste en tener un enlace principal activo que se utiliza normalmente y un enlace de respaldo pasivo que se activa solo si el enlace principal falla. En caso de una interrupción en el enlace principal, algunos esquemas permiten que el enlace de respaldo se active automáticamente para mantener la conectividad.

Ventajas:

Comutación automática: En caso de una falla en el enlace principal, el enlace de respaldo se activa automáticamente sin interrupciones significativas en la conectividad, por tanto no requiere intervención humana.

Menor costo: En comparación con la redundancia activa-activa, tener un enlace de respaldo pasivo suele ser más económico, ya que no requiere la misma capacidad de ancho de banda.

Desventajas:

Recursos subutilizados: Durante el funcionamiento normal, el enlace de respaldo no se utiliza, lo que significa que parte de los recursos de conexión están inactivos y subutilizados.

Tiempo de comutación: En comparación con la redundancia activa-activa, la comutación al enlace de respaldo puede tomar más tiempo, lo que puede causar una breve interrupción en la conectividad.

- **Redundancia activa-activa:** Este enfoque implica utilizar múltiples enlaces que están activos simultáneamente y que pueden configurarse para equilibrar la carga de tráfico entre ellos. Si uno de los enlaces falla, el tráfico se redistribuye automáticamente a través de los enlaces restantes.

Ventajas:

Mayor capacidad de tráfico: Al utilizar múltiples enlaces activos simultáneamente, se puede aprovechar la capacidad combinada de todos los enlaces, lo que permite un mayor rendimiento y ancho de banda disponible.

Tolerancia a fallas mejorada: Si uno de los enlaces falla, en ciertos sistemas el tráfico se redistribuye automáticamente a través de los enlaces restantes, lo que minimiza las interrupciones en la conectividad.

Desventajas:

Mayor costo: La implementación de múltiples enlaces activos implica un costo adicional, ya que se deben pagar los servicios de todos los enlaces y se requiere un mayor nivel de capacidad de ancho de banda.

Configuración y gestión más complejas: La configuración y el monitoreo de múltiples enlaces activos puede ser más complejo y requerir una administración más rigurosa.

- **Protocolo de enrutamiento dinámico con redundancia:** Mediante el uso de protocolos de enrutamiento dinámico, como el Border Gateway Protocol (BGP) o el Open Shortest Path First (OSPF), se pueden configurar rutas redundantes en los dispositivos de red. Estos protocolos permiten que los enlaces de respaldo se activen automáticamente en caso de una falla en el enlace principal.

Ventajas:

Automatización de la conmutación: Los protocolos de enrutamiento dinámico permiten la conmutación automática de rutas en caso de una falla en el enlace principal, lo que minimiza las interrupciones en la conectividad.

Flexibilidad en la configuración: Los protocolos de enrutamiento dinámico ofrecen flexibilidad para configurar diferentes rutas y prioridades de enrutamiento.

Desventajas:

Requiere configuración y mantenimiento avanzados: La implementación de protocolos de enrutamiento dinámico puede requerir un conocimiento técnico más avanzado y una configuración más compleja.

Possible impacto en el rendimiento: En redes de menor escala, la sobrecarga generada por los protocolos de enrutamiento dinámico puede afectar el rendimiento general de la red.

- **Comutación por error:** Este método implica utilizar dispositivos de red con capacidades de comutación por error, como switches capa 3 o routers con capacidades de comutación por error. Estos dispositivos pueden detectar una falla en un enlace y redirigir automáticamente el tráfico hacia un enlace de respaldo sin interrupciones.

Ventajas:

Comutación rápida: Los dispositivos de red con capacidades de comutación por error pueden detectar rápidamente una falla en un enlace y redirigir el tráfico hacia un enlace de respaldo sin interrupciones perceptibles.

Mayor tolerancia a fallas: La comutación por error mejora la resiliencia de la red al proporcionar una comutación automática en caso de una falla en el enlace principal.

Desventajas:

Costo adicional: Los dispositivos de red con capacidades de comutación por error pueden ser más costosos en comparación con los dispositivos estándar.

Configuración y gestión más complejas: La configuración y el mantenimiento de la comutación por error pueden requerir un mayor nivel de experiencia técnica y supervisión constante.

Implementación de políticas de seguridad y cortafuegos: Configurar políticas de seguridad adecuadas y utilizar soluciones de cortafuegos basadas en software puede ser una inversión más económica en comparación con otras soluciones de alta disponibilidad.

- **Cortafuegos de red perimetral:** Un cortafuegos de red perimetral se coloca en la frontera entre la red interna y la red externa, generalmente en el borde del enlace de Internet. Este dispositivo se encarga de filtrar el tráfico entrante y saliente, y aplicar políticas de seguridad para proteger la red interna contra posibles amenazas externas.

Ventajas:

Protección en la frontera de la red: El cortafuegos de red perimetral proporciona una barrera de seguridad en el punto de entrada de la red, protegiendo contra amenazas externas antes de que lleguen a la red interna.

Filtrado de tráfico granular: Permite filtrar y controlar el tráfico entrante y saliente en función de políticas de seguridad específicas.

Desventajas:

Riesgo de ataques internos: El cortafuegos de red perimetral no protege contra amenazas internas, por lo que es importante implementar medidas de seguridad adicionales para mitigar este riesgo.

Possible impacto en el rendimiento: El procesamiento del tráfico a través del cortafuegos puede generar una sobrecarga de recursos y afectar el rendimiento de la red.

- **Segmentación de red:** Mediante la segmentación de red, se dividen las redes internas en segmentos lógicos más pequeños. Cada segmento se coloca detrás de un cortafuegos o dispositivo de seguridad, lo que permite aplicar políticas específicas para cada segmento y limitar la propagación de amenazas dentro de la red.

Ventajas:

Mayor seguridad: La segmentación de red ayuda a limitar la propagación de amenazas dentro de la red y a aislar los segmentos comprometidos, mejorando la seguridad global de la red.

Control y políticas específicas: Permite aplicar políticas de seguridad específicas para cada segmento, lo que facilita la gestión y el control de los recursos de red.

Desventajas:

Configuración y gestión más complejas: La segmentación de red puede requerir una configuración y gestión más complejas, especialmente en redes más grandes, lo que puede aumentar la carga de trabajo para los administradores de red.

Possible impacto en la conectividad: Una segmentación inadecuada puede afectar la conectividad entre los segmentos y dificultar la colaboración y el acceso a los recursos de red.

- **Cortafuegos de host:** Los cortafuegos de host se instalan en los dispositivos finales, como servidores o estaciones de trabajo, para protegerlos individualmente. Estos cortafuegos controlan el tráfico entrante y saliente del dispositivo y aplican políticas de seguridad específicas para proteger los recursos locales.

Ventajas:

Protección específica para dispositivos finales: Los cortafuegos de host brindan una capa adicional de protección al nivel del dispositivo final, lo que ayuda a proteger los servidores y las estaciones de trabajo individualmente.

Mayor control y políticas personalizadas: Permite aplicar políticas de seguridad específicas para cada dispositivo, lo que permite un mayor control y personalización de las medidas de seguridad.

Desventajas:

Requisito de instalación en cada dispositivo: Los cortafuegos de host deben instalarse y configurarse en cada dispositivo individualmente, lo que puede ser una tarea laboriosa y requerir una administración y actualización constantes.

Possible impacto en el rendimiento del dispositivo: La implementación de cortafuegos de host puede generar una carga adicional en los dispositivos, lo que puede afectar su rendimiento.

- **Listas de control de acceso (ACL):** Las listas de control de acceso son reglas configuradas en los dispositivos de red para permitir o denegar el flujo de tráfico según criterios específicos, como direcciones IP, puertos o protocolos. Las ACL se utilizan comúnmente en routers, switches y firewalls para filtrar el tráfico y aplicar políticas de seguridad.

Ventajas:

Filtrado de tráfico granular: Las ACL permiten un control preciso sobre qué tipo de tráfico se permite o se bloquea en función de criterios específicos, lo que mejora la seguridad y protege contra amenazas conocidas.

Configuración flexible: Las ACL se pueden configurar en dispositivos de red como routers y switches, lo que permite adaptar las políticas de seguridad a las necesidades y requisitos específicos de la red.

Desventajas:

Gestión compleja en redes grandes: En redes grandes y complejas, la gestión de múltiples ACL puede volverse complicada y propensa a errores si no se realiza adecuadamente. Esto solo se aplicaría si la PYME requiriese una infraestructura grande para su negocio.

Requiere un mantenimiento constante: Las ACL deben actualizarse y ajustarse regularmente para reflejar los cambios en la red y las necesidades de seguridad, lo que puede requerir una dedicación continua de recursos.

- **Sistemas de prevención de intrusiones (IPS):** Los sistemas de prevención de intrusiones se utilizan para monitorear y analizar el tráfico de red en busca de actividades maliciosas o comportamientos sospechosos. Estos sistemas pueden bloquear o tomar medidas correctivas automáticamente cuando se detecta una amenaza, ayudando a proteger la red contra intrusiones.

Ventajas:

Detección y respuesta en tiempo real: Los IPS monitorean activamente el tráfico de red y pueden detectar y responder a actividades maliciosas en tiempo real, lo que ayuda a mitigar amenazas y ataques.

Protección avanzada contra intrusiones: Los IPS utilizan técnicas sofisticadas para identificar patrones de ataque conocidos y desconocidos, lo que proporciona una capa adicional de seguridad para la red.

Desventajas:

Possible impacto en el rendimiento: El procesamiento de tráfico adicional realizado por los IPS puede tener un impacto en el rendimiento de la red, especialmente en redes con recursos limitados.

Posibles falsos positivos o negativos: Los IPS pueden generar falsas alarmas (positivos falsos) o no detectar ciertos ataques (negativos falsos), lo que requiere una configuración y afinación adecuadas para reducir estos errores.

- **Actualizaciones y parches de seguridad:** Además de los métodos mencionados anteriormente, es fundamental mantener actualizados los sistemas y aplicar los parches de seguridad relevantes. Esto ayuda a asegurar que las vulnerabilidades conocidas están corregidas y que la red esté protegida contra las últimas amenazas conocidas.

Ventajas:

Protección contra vulnerabilidades conocidas: Las actualizaciones y parches de seguridad ayudan a corregir las vulnerabilidades conocidas en los sistemas y aplicaciones, lo que reduce el riesgo de explotación por parte de atacantes.

Mejora continua de la seguridad: Mantener los sistemas actualizados con las últimas actualizaciones y parches ayuda a garantizar una protección continua y mantenerse al día con las últimas amenazas y soluciones.

Desventajas:

Possibles incompatibilidades o interrupciones: Las actualizaciones y parches pueden tener conflictos con otras aplicaciones o sistemas, lo que puede provocar incompatibilidades o interrupciones temporales en la funcionalidad.

Dependencia de los proveedores: La disponibilidad de actualizaciones y parches depende de los proveedores de software y puede haber retrasos en la entrega o falta de soporte para ciertas versiones.

- **Balanceo de carga:** Distribuye el tráfico entrante entre varios servidores o dispositivos de red utilizando soluciones de balanceo de carga. Esto ayuda a evitar la saturación de un solo punto de entrada y distribuye la carga de manera equitativa para mitigar los efectos de un ataque DOS.

Ventajas:

Mejor rendimiento y capacidad de respuesta: El balanceo de carga distribuye el tráfico entre múltiples servidores, lo que mejora el rendimiento y la capacidad de respuesta de las aplicaciones y servicios.

Mayor disponibilidad: Si uno de los servidores falla, el balanceo de carga redirige el tráfico a los servidores restantes, lo que garantiza la continuidad del servicio.

Desventajas:

Configuración y gestión más complejas: La implementación y configuración del balanceo de carga puede ser más compleja en comparación con una infraestructura de servidor única, lo que requiere un conocimiento técnico adecuado.

Requisito de recursos adicionales: El balanceo de carga puede requerir recursos adicionales, como hardware o software especializado, lo que puede generar un costo adicional.

- **Configuración de umbrales y límites de tráfico:** Establece umbrales y límites de tráfico en los dispositivos de red para detectar y bloquear patrones de tráfico anormalmente alto o sospechoso. Esto puede incluir limitar la tasa de conexiones por segundo, el número máximo de solicitudes por cliente o el ancho de banda asignado a determinados tipos de tráfico.

Ventajas:

Protección contra tráfico anormal: La configuración de umbrales y límites de tráfico permite detectar y bloquear patrones de tráfico anormalmente alto o sospechoso, lo que ayuda a prevenir ataques de saturación o abusos de recursos. **Control y gestión del tráfico:** Establecer límites de tráfico permite controlar y gestionar el flujo de datos, evitando el consumo excesivo de ancho de banda y asegurando una distribución equitativa de los recursos de red.

Desventajas:

Possible afectación del tráfico legítimo: Una configuración inadecuada de umbrales y límites puede afectar el tráfico legítimo y limitar el rendimiento de las aplicaciones o servicios, lo que requiere un ajuste y monitoreo cuidadosos.

Possible falta de adaptabilidad: Los umbrales y límites de tráfico pueden ser estáticos y no adaptarse automáticamente a cambios en las necesidades de la red, lo que puede requerir ajustes manuales periódicos.

- **Protección de capa de aplicación:** Utiliza soluciones de protección de capa de aplicación, como firewalls de aplicaciones web (WAF), para identificar y bloquear los ataques DOS específicos dirigidos a las aplicaciones web. Estas soluciones pueden detectar patrones de tráfico malicioso y filtrar el tráfico no deseado antes de que llegue a los servidores.

Ventajas:

Protección específica para aplicaciones web: Los firewalls de aplicaciones web (WAF) proporcionan una capa adicional de seguridad en la capa de aplicación, protegiendo contra ataques específicos dirigidos a aplicaciones web y ayudando a mitigar riesgos.

Filtrado avanzado y detección de amenazas: Los WAF utilizan técnicas sofisticadas de filtrado y detección de amenazas para identificar y bloquear actividades maliciosas en tiempo real, lo que ayuda a proteger las aplicaciones y los datos.

Desventajas:

Possible impacto en el rendimiento de las aplicaciones: El procesamiento adicional realizado por los WAF puede afectar el rendimiento de las aplicaciones web, especialmente en situaciones de alto tráfico o con recursos limitados.

Configuración y afinación adecuadas: Los WAF requieren una configuración y afinación adecuadas para evitar falsos positivos y asegurar una protección efectiva sin afectar negativamente la funcionalidad de las aplicaciones.

Monitorización y gestión proactiva de la red: Utilizar herramientas de monitorización de red, muchas de las cuales ofrecen opciones gratuitas o de bajo costo, puede ayudar a detectar problemas y tomar medidas antes de que se conviertan en interrupciones importantes.

- **Supervisión de red:** Utilizar herramientas de supervisión de red, como Nagios, Zabbix o PRTG, que permiten monitorear constantemente la salud y el rendimiento de los dispositivos de red, como routers, switches, firewalls y servidores. Estas herramientas generan alertas en tiempo real cuando se detectan problemas, lo que permite tomar acciones de manera proactiva.

Ventajas:

Monitoreo constante: Las herramientas de supervisión de red monitorean constantemente la salud y el rendimiento de los dispositivos de red, lo que permite detectar problemas en tiempo real y tomar medidas inmediatas.

Alertas y notificaciones en tiempo real: Las herramientas de supervisión generan alertas y notificaciones instantáneas cuando se detectan problemas, lo que permite una respuesta rápida y una solución proactiva.

Desventajas:

Requiere una configuración y mantenimiento adecuados: Configurar y mantener las herramientas de supervisión de red puede requerir un conocimiento técnico adecuado y una gestión constante para garantizar un monitoreo efectivo.

Possible sobrecarga de información: Con una supervisión constante, puede generarse una gran cantidad de datos e información, lo que puede dificultar el análisis y la identificación de los problemas más importantes.

- **Análisis de registros y registros de eventos:** Los registros y registros de eventos de los dispositivos de red contienen información detallada sobre las actividades y los eventos que ocurren en la red. Mediante el análisis de estos registros, se pueden identificar patrones, detectar anomalías y tomar medidas preventivas antes de que se conviertan en problemas importantes.

Ventajas:

Identificación de patrones y anomalías: El análisis de registros permite identificar patrones de comportamiento normal y detectar anomalías o actividades sospechosas en la red.

Acceso a información detallada: Los registros y registros de eventos proporcionan información detallada sobre las actividades y eventos en la red, lo que facilita el análisis y la identificación de problemas.

Desventajas:

Requiere herramientas de análisis adecuadas: El análisis de registros puede requerir el uso de herramientas de análisis especializadas para extraer información relevante, lo que puede implicar una inversión adicional.

Necesidad de conocimientos avanzados: El análisis de registros puede requerir conocimientos avanzados en la interpretación de los datos y la identificación de patrones o anomalías, lo que puede limitar su accesibilidad para usuarios menos técnicos.

- **Supervisión de ancho de banda:** La supervisión del ancho de banda permite monitorear y analizar el uso del ancho de banda en la red. Esto ayuda a identificar cuellos de botella, aplicaciones o usuarios que consumen demasiado ancho de banda, y tomar medidas para optimizar el rendimiento de la red.

Ventajas:

Identificación de cuellos de botella: La supervisión del ancho de banda permite identificar los puntos de congestión y los cuellos de botella en la red, lo que ayuda a tomar medidas para optimizar el rendimiento y garantizar una distribución equitativa del ancho de banda.

Control y gestión del uso del ancho de banda: La supervisión del ancho de banda permite identificar las aplicaciones o usuarios que consumen demasiado ancho de banda, lo que permite tomar medidas para evitar un uso excesivo y asegurar un rendimiento óptimo de la red.

Desventajas:

Possible impacto en el rendimiento: Las herramientas de supervisión del ancho de banda pueden generar una sobrecarga adicional en la red y afectar su rendimiento, especialmente en entornos con recursos limitados.

Necesidad de una configuración adecuada: La supervisión del ancho de banda requiere una configuración adecuada de las herramientas de supervisión para capturar los datos relevantes y evitar la generación de datos innecesarios o inexactos.

- **Supervisión de disponibilidad de servicios:** Es importante monitorear la disponibilidad y el rendimiento de los servicios críticos en la red, como servidores de correo electrónico, servidores web o servicios en la nube. Mediante la supervisión de estos servicios, se pueden detectar problemas de rendimiento o tiempo de inactividad y tomar acciones para restaurar la funcionalidad rápidamente.

Ventajas:

Detección temprana de problemas de servicio: La supervisión de la disponibilidad de servicios permite identificar problemas de rendimiento o tiempo de inactividad en los servicios críticos, lo que permite una respuesta rápida y la resolución de problemas antes de que afecten a los usuarios o clientes.

Mantenimiento de la satisfacción del cliente: Al monitorear la disponibilidad y el rendimiento de los servicios, se puede garantizar una experiencia positiva para los

usuarios y mantener la satisfacción del cliente.

Desventajas:

Requiere una configuración y mantenimiento adecuados: La supervisión de servicios requiere la configuración y el mantenimiento de herramientas de supervisión adecuadas, así como la definición de umbrales y métricas de rendimiento relevantes.

Possibles falsas alarmas o falta de detección: Las herramientas de supervisión pueden generar falsas alarmas o no detectar ciertos problemas de rendimiento o tiempo de inactividad, lo que requiere una afinación adecuada para reducir los errores.

- **Gestión de configuraciones:** La gestión de configuraciones implica mantener un registro actualizado de las configuraciones de los dispositivos de red, como routers y switches. Esto ayuda a garantizar que las configuraciones estén correctas y coherentes, y permite revertir rápidamente los cambios en caso de problemas o errores.

Ventajas:

Control y consistencia de las configuraciones: La gestión de configuraciones ayuda a mantener un registro actualizado de las configuraciones de los dispositivos de red, lo que garantiza que las configuraciones estén correctas y coherentes en toda la red.

Reversión rápida de cambios: En caso de problemas o errores, la gestión de configuraciones permite revertir rápidamente los cambios a una configuración anteriormente funcional, lo que reduce el tiempo de inactividad y los impactos negativos.

Desventajas:

Requiere una gestión constante: La gestión de configuraciones implica una gestión y supervisión constantes para asegurar que las configuraciones estén actualizadas y reflejen los requisitos y cambios de la red.

Possible impacto en la compatibilidad o interoperabilidad: Al realizar cambios en las configuraciones, puede haber riesgos de incompatibilidad o problemas de interoperabilidad con otros dispositivos o sistemas, lo que requiere pruebas y validaciones adecuadas.

- **Pruebas de rendimiento y carga:** Realizar pruebas periódicas de rendimiento y carga en la red permite identificar posibles puntos débiles y evaluar la capacidad de la red para manejar cargas de trabajo intensivas. Esto ayuda a identificar problemas antes de que se vuelvan críticos y permite realizar ajustes preventivos.

Ventajas:

Identificación de puntos débiles y limitaciones: Las pruebas de rendimiento y carga permiten identificar los puntos débiles de la red y evaluar su capacidad para manejar cargas de trabajo intensivas, lo que ayuda a identificar y solucionar problemas antes de que se vuelvan críticos.

Ajuste preventivo: Las pruebas de rendimiento y carga proporcionan información sobre el comportamiento de la red en diferentes condiciones, lo que permite realizar ajustes preventivos y optimizar el rendimiento de la red.

Desventajas:

Requiere recursos y planificación adecuados: Realizar pruebas de rendimiento y carga puede requerir recursos adicionales, como herramientas de prueba y tiempo dedicado, así como una planificación adecuada para minimizar el impacto en la operación normal de la red.

Possible interrupción o impacto en el rendimiento: Las pruebas de rendimiento y carga pueden generar una carga adicional en la red y afectar su rendimiento durante el proceso de prueba, lo que requiere una consideración cuidadosa y una programación adecuada.

Configuración de rutas alternativas: Establecer rutas alternativas en los dispositivos de red utilizando protocolos de enrutamiento dinámico o configuraciones estáticas no implica costos adicionales, aunque puede requerir conocimientos técnicos para su implementación.

- **Enrutamiento estático con rutas de respaldo:** En este método, se configuran manualmente rutas estáticas de respaldo en los dispositivos de red. Si el enlace principal falla, el dispositivo de red cambiará automáticamente al enlace de respaldo para enrutar el tráfico.

Ventajas:

Cambio automático sin intervención humana: En caso de fallo en el enlace principal, el enrutamiento estático con rutas de respaldo permite que el dispositivo de red cambie automáticamente al enlace de respaldo sin necesidad de intervención humana, lo que reduce el tiempo de inactividad.

Control total sobre las rutas: Al configurar manualmente las rutas de respaldo, se tiene un control completo sobre las rutas utilizadas y se puede adaptar a las necesidades específicas de la red.

Desventajas:

Mayor complejidad de configuración: Configurar y mantener manualmente rutas estáticas de respaldo puede ser más complejo y propenso a errores en comparación con otros métodos de enrutamiento.

Limitado a configuraciones estáticas: El enrutamiento estático con rutas de respaldo no se adapta automáticamente a cambios en la red, por lo que requiere una actualización manual de las rutas en caso de cambios en la topología de la red.

- **Túneles VPN:** Mediante la configuración de túneles VPN (Virtual Private Network), se puede establecer una conexión segura a través de una red pública, como Internet, para enrutar el tráfico a través de una ruta alternativa. Esto es especialmente útil si se utiliza

una conexión de respaldo, como una conexión de banda ancha o un enlace celular, para garantizar la conectividad cuando falla el enlace principal.

Ventajas:

Conexión segura: Los túneles VPN proporcionan una conexión segura a través de una red pública, lo que protege la privacidad y la integridad de los datos transmitidos.

Utilización de rutas alternativas: Al establecer un túnel VPN, se puede utilizar una ruta alternativa, como una conexión de respaldo, para enrutar el tráfico en caso de fallos en los enlaces principales, lo que garantiza la conectividad continua.

Desventajas:

Sobrecarga de procesamiento: El establecimiento y mantenimiento de los túneles VPN puede generar una sobrecarga adicional en los dispositivos de red, lo que puede afectar el rendimiento general de la red.

Posibles limitaciones de ancho de banda: La utilización de una conexión de respaldo, como una conexión de banda ancha o un enlace celular, puede implicar limitaciones de ancho de banda en comparación con los enlaces principales, lo que puede afectar la velocidad y el rendimiento de la red.

5.1.4 Conclusión

La resiliencia de la red es de vital importancia para garantizar la continuidad de las operaciones en una microPYME en caso de pérdida de conexión. En aquellas microPYMEs dedicadas al negocio tecnológico u online incluso puede afectar e incluso romper totalmente la continuidad de su negocio. Al ser normalmente contratados los servicios de red a una compañía telefónica este servicio depende de tener un suministro eléctrico estable por lo que varios riesgos y soluciones son comunes en ambos casos.

Para poder evitar, o en su caso mitigar el impacto lo máximo posible es necesario realizar un análisis previo de los procesos críticos de la empresa para poder determinar cuales son las acciones y medidas que se pueden tomar. En el caso de las microPYMEs, al ser empresas de poco tamaño con recursos limitados además es importante tener en cuenta que muchas de estas soluciones se pueden aplicar con herramientas de distribución libre o con soluciones de bajo coste.

5.2 Electricidad

5.2.1 Introducción

La electricidad juega un papel fundamental en el funcionamiento de las microPMEs. Su disponibilidad constante es esencial para mantener las operaciones diarias y garantizar la continuidad del negocio. Desde la perspectiva de la infraestructura y el equipo técnico, la empresa depende de la electricidad para alimentar los dispositivos electrónicos, como computadoras, servidores y otros equipos necesarios para brindar servicios en línea.

La resiliencia eléctrica es la capacidad que tienen dichas microPMEs para resistir, adaptarse y recuperarse de una manera rápida y eficiente ante la pérdida de electricidad. Esta pérdida puede deberse a un fallo en la infraestructura eléctrica debido a condiciones climáticas adversas, mantenimiento de la infraestructura tanto del proveedor como interna, fallos en las estaciones de distribución, sobrecargas eléctricas, o daños físicos en las instalaciones como incendios, inundaciones o cualquier otro tipo de desastre natural.

La resiliencia eléctrica implica adoptar medidas proactivas para garantizar un suministro eléctrico confiable y contar con planes de contingencia eficientes para hacer frente a las interrupciones. Esto puede incluir la implementación de sistemas de respaldo de energía, la diversificación de fuentes de suministro, la optimización de la eficiencia energética y la capacitación del personal en medidas de seguridad y respuesta ante emergencias.

En resumen, la electricidad es una necesidad crucial para las pymes con recursos limitados. Su pérdida tendría efectos devastadores en la productividad, la seguridad, la comunicación, la calidad de los productos y servicios, así como en los esfuerzos de sostenibilidad de estas empresas. Es fundamental que las pymes tengan acceso confiable a la electricidad para garantizar su funcionamiento continuo y su éxito en un entorno empresarial.

A continuación, se describirán diversos riesgos que se derivan de la pérdida de conexión eléctrica y las medidas de resiliencia que se pueden adoptar para mitigar, contener y recuperarse de este problema.

5.2.2 Riesgos, Impactos y Vulnerabilidades

Riesgo de seguridad: La falta de electricidad dejaría los sistemas de seguridad inoperables, aumentando el riesgo de robos, vandalismo y otros delitos, lo que podría tener un impacto negativo en la seguridad de la empresa y de su personal.

Riesgos para la salud y seguridad de los empleados: La falta de electricidad puede generar riesgos para la salud y seguridad de los empleados en la empresa. La iluminación deficiente puede aumentar el riesgo de accidentes. Además, si la empresa opera en un entorno donde se requiere electricidad para equipos de seguridad, como extintores de incendios, sistemas de ventilación o maquinaria pesada, la falta de energía puede comprometer la seguridad de los empleados en caso de emergencias.

Interrupción de operaciones: La falta de electricidad paraliza las operaciones de la empresa, lo que resultaría en la pérdida de productividad y en la imposibilidad de cumplir con los plazos y compromisos establecidos.

Pérdida de ingresos: Sin electricidad, las pymes no podrían generar ingresos, lo que podría llevar a dificultades financieras y afectar su sostenibilidad a largo plazo.

Daño a la reputación: La incapacidad para satisfacer las necesidades de los clientes debido a la falta de electricidad puede dañar la reputación de la empresa y llevar a la pérdida de clientes existentes y potenciales.

Problemas de comunicación: Sin electricidad, los sistemas de comunicación, como el acceso a Internet y los sistemas telefónicos, se verían afectados, dificultando la comunicación con clientes, proveedores y otros socios comerciales, lo que podría llevar a la pérdida de oportunidades de negocio.

Pérdida de refrigeración: Muchas pymes dependen de sistemas de refrigeración y almacenamiento controlados por electricidad para mantener la calidad y la seguridad de sus productos. La falta de electricidad podría llevar a la pérdida de temperaturas constantes, conllevando a apagados de equipos electrónicos o elementos perecederos.

Dificultades en la gestión de inventario: Sin electricidad, las pymes tendrían dificultades para realizar un seguimiento preciso del inventario y administrar eficientemente sus existencias, lo que podría resultar en pérdidas y desperdicios.

Retrasos en el cumplimiento de contratos y compromisos: La falta de electricidad dificultará el cumplimiento de contratos y compromisos con clientes y proveedores, lo que podría llevar a multas, demandas y pérdida de relaciones comerciales.

Impacto en la sostenibilidad ambiental: La pérdida de electricidad interrumpiría los esfuerzos de las pymes por adoptar prácticas empresariales sostenibles, como el uso de energías renovables, lo que podría afectar negativamente su imagen y reputación ambiental.

Pérdida de clientes: Si la microPYME no puede cumplir con los pedidos o brindar servicios debido a la falta de electricidad, es probable que los clientes busquen otras opciones. La pérdida de clientes puede ser tanto a corto plazo como a largo plazo, ya que pueden optar por cambiar a competidores más confiables y consistentes en su suministro de productos o servicios.

Pérdida de datos: Si la electricidad se interrumpe abruptamente, existe el riesgo de pérdida de datos en los sistemas informáticos. Esto puede resultar en la eliminación de información crítica, como registros de clientes, datos financieros o información operativa. La pérdida de datos puede ser costosa de recuperar y puede tener implicaciones legales y de cumplimiento.

Costos adicionales: La pérdida de electricidad puede generar costos adicionales para la empresa. Por ejemplo, si se utilizan generadores de respaldo, esto implica un gasto adicional en combustible y mantenimiento. Además, es posible que se requieran reparaciones o reemplazos de equipos dañados debido a apagones de energía, lo que aumenta los costos.

Impacto en la seguridad: La falta de electricidad puede afectar la seguridad de la empresa. Los sistemas de seguridad electrónicos, como cámaras de vigilancia y alarmas, pueden dejar de funcionar, lo que aumenta el riesgo de robos, vandalismo u otros incidentes. Además, la iluminación insuficiente puede crear un entorno inseguro para los empleados, lo que aumenta el riesgo de accidentes laborales.

Dependencia de recursos externos: En caso de pérdida prolongada de electricidad, las pymes podrían depender de generadores de energía diésel u otros recursos externos costosos para mantener sus operaciones, lo que representaría una carga financiera adicional.

5.2.3 Estrategia de redundancia

Grupo electrógeno: Los grupos electrógenos portátiles son una solución común para proporcionar energía durante interrupciones de electricidad, adaptándose a todo tipo de pymes dependiendo de las necesidades debido a la variedad de productos. Debemos tener clara la necesidad, ya que, dependiendo de la necesidad del tipo de arranque, se deberá elegir entre manual, eléctrico simple (botón) o automático. Las principales diferencias que encontraremos a rasgos generales entre los distintos grupos son las siguientes:

Según su tensión: dependiendo del consumo que se tenga en la pyme, y de las necesidades de resiliencia, existen dos principales tipos de generadores según su tensión

- **Grupos electrógenos monofásicos:** Estos grupos electrógenos generan una tensión de salida monofásica. La tensión monofásica es comúnmente utilizada en hogares y pequeñas empresas. Estos grupos electrógenos suelen tener una tensión de salida de 120 o 240 voltios y son adecuados para aplicaciones con cargas de baja potencia.
- **Grupos electrógenos trifásicos:** Estos grupos electrógenos generan una tensión de salida trifásica. La tensión trifásica es utilizada en aplicaciones comerciales, industriales y en sistemas de distribución de energía a gran escala. Los grupos electrógenos trifásicos tienen tres corrientes de salida que se desfasan entre sí en 120 grados. La tensión de salida puede variar dependiendo de la configuración y el tamaño del grupo electrógeno.

Según su combustible: dependiendo de la aplicación específica que tenga el grupo electrógeno se adecuará mejor a las características de la pyme uno de los siguientes tipos de grupo:

- **Grupos electrógenos diésel:** Estos grupos electrógenos utilizan motores diésel para generar electricidad. Son adecuados para aplicaciones comerciales, industriales y residenciales, y son especialmente útiles en situaciones de emergencia o como respaldo durante apagones.

Ventajas:

Mayor eficiencia: Los motores diésel son generalmente más eficientes que los de gasolina, lo que resulta en un menor consumo de combustible y mayores horas de funcionamiento continuo.

Durabilidad y vida útil: Los motores diésel tienden a ser más robustos y duraderos, lo que los hace adecuados para un uso intensivo y prolongado.

Mayor densidad energética: El diésel contiene más energía por volumen en comparación con la gasolina, lo que permite un almacenamiento más compacto.

Combustible más estable: El diésel tiene una vida útil más larga y es menos propenso a degradarse con el tiempo.

Desventajas:

Costo inicial más elevado: Los grupos electrógenos diésel suelen tener un costo inicial más alto en comparación con los de gasolina.

Mayor ruido y vibración: Los motores diésel tienden a ser más ruidosos y vibrantes en comparación con otros tipos de grupos electrógenos.

Emisiones más altas: Los motores diésel emiten mayores cantidades de gases de escape, incluidos los contaminantes atmosféricos y las emisiones de gases de efecto invernadero.

- **Grupos electrógenos de gasolina:** Estos grupos electrógenos funcionan con motores de gasolina. Son más comunes en aplicaciones residenciales o pequeñas empresas, aportando una baja potencia en comparación, pero una movilidad sencilla.

Ventajas:

Amplia disponibilidad: La gasolina es fácilmente accesible en estaciones de servicio en la mayoría de las áreas.

Menor costo inicial: Los grupos electrógenos de gasolina suelen ser más económicos en comparación con otros tipos.

Facilidad de transporte y manejo: Al ser dispositivos de menor tamaño y más compactos, es más sencillo el desplazamiento y uso.

Fácil mantenimiento: Los motores de gasolina suelen requerir menos mantenimiento que los diésel.

Desventajas:

Mayor costo operativo: El precio de la gasolina puede ser más alto que otros combustibles, lo que puede resultar en un costo operativo más elevado a largo plazo.

Menor eficiencia: Los motores de gasolina tienden a ser menos eficientes en términos de consumo de combustible en comparación con los diésel.

Duración limitada del combustible: La gasolina tiene una vida útil más corta en comparación con otros combustibles, lo que puede dificultar el almacenamiento a largo plazo.

- **Grupos electrógenos de gas natural o propano:** Estos grupos electrógenos utilizan gas natural o propano como combustible. Son populares en aplicaciones residenciales y comerciales debido a su menor impacto ambiental.

Ventajas:

Combustible limpio: El gas natural y el propano son combustibles más limpios y producen emisiones más bajas en comparación con la gasolina y el diésel.

Menor mantenimiento: Los motores que funcionan con gas natural o propano tienden a requerir menos mantenimiento debido a la combustión más limpia.

Mayor disponibilidad continua de combustible: Si tienes acceso a una red de suministro de gas natural o a una fuente de propano, puedes contar con un suministro constante de

combustible.

Menor ruido y vibración: Estos grupos electrógenos suelen ser más silenciosos y generan menos vibraciones que los diésel.

Desventajas:

Costo inicial más elevado: Los grupos electrógenos de gas natural/propano suelen ser más costosos en comparación con los de gasolina.

Requiere una infraestructura de suministro: Para utilizar gas natural, necesitarás una conexión a una red de gas, lo cual puede requerir una instalación adicional. Para el propano, se necesita un tanque de almacenamiento adecuado.

Menor densidad energética: El gas natural y el propano tienen una menor densidad energética en comparación con la gasolina y el diésel, lo que implica un mayor volumen de almacenamiento.

SAI (Sistema de Alimentación Ininterrumpida): Es un dispositivo diseñado para proporcionar energía eléctrica continua y sin interrupciones a equipos electrónicos o sistemas en caso de fallos en el suministro de energía principal. Consiste en una batería recargable y un circuito de conversión de energía que permite que los dispositivos conectados continúen funcionando incluso en situaciones de cortes de energía o fluctuaciones en la red eléctrica. Además de proporcionar energía de respaldo, los SAI también protegen los equipos conectados contra sobretensiones, picos de voltaje y otros problemas eléctricos que podrían dañarlos. Los SAI son ampliamente utilizados en entornos como oficinas, centros de datos, hospitales y cualquier lugar donde la continuidad del suministro eléctrico sea crucial para garantizar el funcionamiento adecuado de los sistemas electrónicos.

- **Offline o Standby:** funciona con el equipo conectado directamente a la red eléctrica en condiciones normales. Cuando la energía de la red se interrumpe, el SAI conmuta rápidamente a la batería interna para proporcionar energía de respaldo. En este tipo de SAI, no hay conversión de energía continua (CC) a corriente alterna (CA) en el modo de espera. Sin embargo, cuando se produce un corte de energía, hay un tiempo de conmutación donde puede haber una breve interrupción en la alimentación. La protección contra fluctuaciones de voltaje es limitada y no se realizan funciones avanzadas de filtrado de ruidos en la línea de energía.

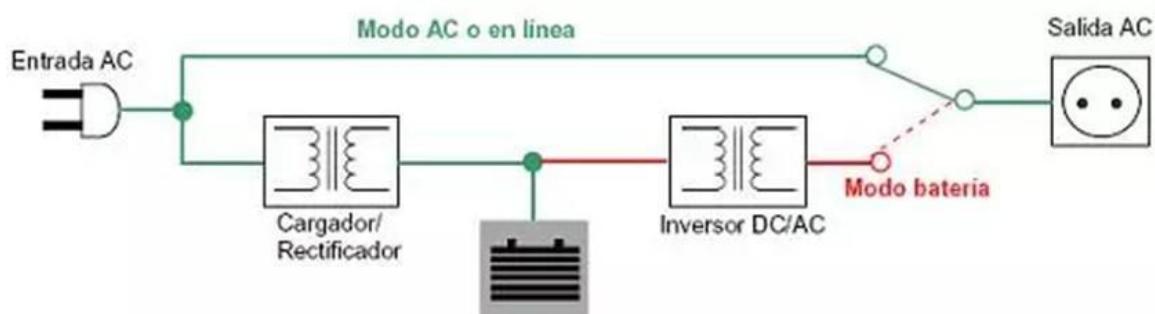


Figura 5: Diagrama SAI Offline

Ventajas:

Costo económico: El SAI Offline es generalmente más asequible en comparación con otros tipos de SAI, lo que lo hace adecuado para usuarios con presupuestos limitados.

Fácil instalación y mantenimiento: La configuración y el mantenimiento de este tipo de SAI son simples y no requieren conocimientos técnicos avanzados.

Adecuado para cargas no críticas de menor potencia: El SAI Offline es ideal para equipos de oficina y computadoras personales que no requieren una protección y tiempo de respaldo prolongados.

Desventajas:

Protección limitada contra variaciones de voltaje: El SAI Offline no proporciona una regulación activa del voltaje y, por lo tanto, ofrece una protección limitada contra variaciones y problemas en la línea de energía.

Falta de filtrado de ruidos: Este tipo de SAI no tiene la capacidad de filtrar ruidos y distorsiones en la línea de energía, lo que puede afectar el rendimiento de los equipos conectados.

Tiempo de conmutación mayor: Cuando se produce un corte de energía, el tiempo de conmutación del SAI Offline es ligeramente más largo, lo que puede causar una breve interrupción en la alimentación y afectar la continuidad de los dispositivos conectados.

- **Interactivo o In-line:** agrega una función adicional al SAI Offline: el regulador automático de voltaje (AVR). El AVR monitorea constantemente el voltaje de entrada y, en caso de alteraciones o caídas de tensión, ajusta automáticamente el voltaje de salida para mantenerlo dentro de un rango seguro. Esto protege los equipos conectados contra alteraciones de voltaje y evita la conmutación a la batería en situaciones donde solo se producen fluctuaciones menores en la red eléctrica. Cuando se produce un corte de energía, el SAI comuta a la batería interna para continuar suministrando energía. El tiempo de conmutación es ligeramente mayor que en el caso del SAI Offline. Sin embargo, la protección contra fluctuaciones de voltaje es mejor y proporciona un tiempo de respaldo más largo.

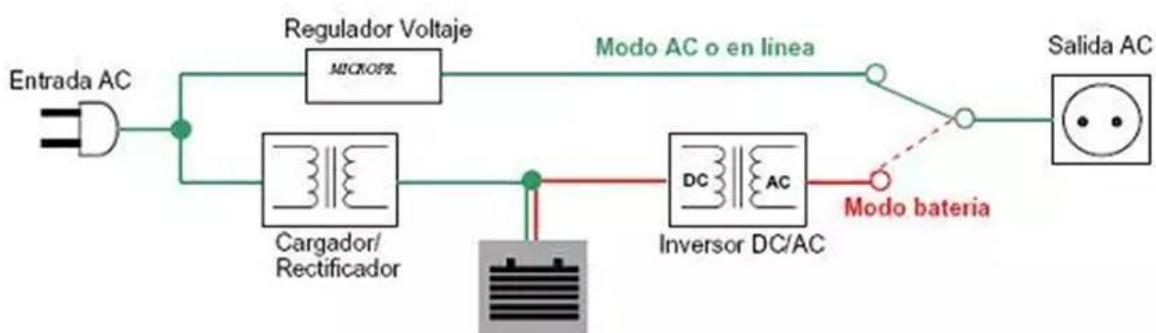


Figura 6: Diagrama SAI Interactivo

Ventajas:

Protección contra fluctuaciones de voltaje: Gracias al regulador automático de voltaje (AVR), el SAI Line Interactive puede mantener un voltaje de salida constante incluso ante fluctuaciones y caídas de tensión en la red eléctrica, lo que protege los equipos conectados.

Mayor tiempo de respaldo: En comparación con el SAI Offline, el SAI Line Interactive ofrece un tiempo de respaldo más prolongado durante los cortes de energía, lo que proporciona una mayor continuidad en la operación de los dispositivos.

Adecuado para áreas con suministro eléctrico irregular: Este tipo de SAI es especialmente útil en áreas donde el suministro eléctrico es inestable, ya que protege los equipos de las variaciones de voltaje y las caídas de tensión.

Desventajas:

Tiempo de conmutación: Aunque el tiempo de conmutación del SAI Line Interactive es menor en comparación con el SAI Offline, aún puede haber una breve interrupción en la alimentación cuando se produce un corte de energía.

Capacidad de filtrado limitada: Aunque el SAI Line Interactive proporciona cierta protección contra fluctuaciones de voltaje, su capacidad de filtrar ruidos y distorsiones en la línea de energía sigue siendo limitada en comparación con otros tipos de SAI.

- **Doble Conversión o Online:** es el tipo más avanzado y ofrece la máxima protección y calidad de energía. En este tipo de SAI, la energía de la red eléctrica se convierte de CA a CC y luego nuevamente a CA a través de un proceso de doble conversión. La energía de entrada siempre pasa por la etapa de conversión de CC a CA, lo que garantiza un suministro estable y de alta calidad en todo momento. Además, el SAI Online también tiene un backup de baterías que alimenta los equipos en caso de un corte de energía, sin interrupción ni tiempo de conmutación perceptible. Incluye filtrado activo de ruidos y distorsiones en la línea de energía, lo que brinda una protección completa contra fluctuaciones de voltaje, sobretensiones, picos y otros problemas eléctricos. Este tipo de SAI, utiliza un modo llamado "Bypass" para la realización de mantenimientos o en caso de producirse fallo en el propio dispositivo SAI.

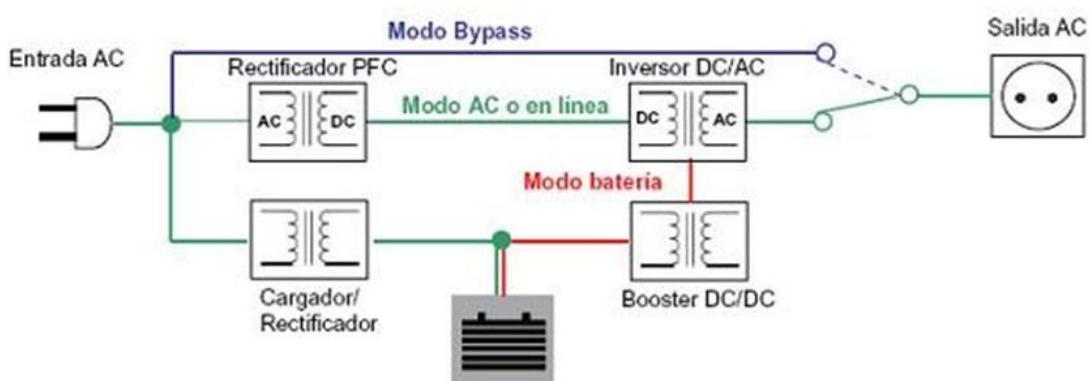


Figura 7: Diagrama SAI Online

Ventajas:

Suministro eléctrico ininterrumpido y de alta calidad: garantiza un suministro continuo y estable de energía mediante la conversión constante de energía de CC a CA, lo que proporciona una alimentación ininterrumpida incluso en casos de cortes de energía prolongados.

Protección completa contra problemas eléctricos: Al realizar una doble conversión de energía, este tipo de SAI ofrece una protección completa contra fluctuaciones de voltaje, sobretensiones, picos y otros problemas eléctricos, lo que asegura una alimentación de alta calidad para equipos sensibles.

Filtrado activo de ruidos y distorsiones: El SAI Online incluye funciones avanzadas de filtrado, lo que permite eliminar ruidos y distorsiones de la línea de energía, brindando una alimentación más limpia y estable a los dispositivos conectados.

Desventajas:

Mayor costo: El SAI Online es generalmente más costoso en comparación con otros tipos de SAI debido a su diseño y funcionalidades avanzadas.

Menor eficiencia energética: Debido a la doble conversión de energía, el SAI Online tiene una eficiencia energética ligeramente menor en comparación con otros tipos de SAI, lo que significa que puede consumir más energía durante el funcionamiento normal.

Mayor tamaño y peso: El SAI Online tiende a ser más grande y pesado en comparación con otros tipos de SAI, lo que puede requerir un espacio adicional y hacer que su instalación sea complicada.

- **Modular:** consta de módulos individuales que se pueden agregar o quitar según las necesidades de carga. Cada módulo incluye su propia batería y sistema de conversión de energía. Los módulos se conectan en paralelo para aumentar la capacidad y redundancia del SAI. Si se produce una falla en un módulo, los demás continúan suministrando energía sin interrupción. Esto brinda alta disponibilidad y escalabilidad. Además, los módulos pueden adaptarse a la carga actual, lo que resulta en una mayor eficiencia.

Ventajas:

Escalabilidad: El SAI Modular permite agregar o quitar módulos según las necesidades de carga, lo que proporciona flexibilidad y la posibilidad de adaptarse a cambios futuros.

Alta disponibilidad: Debido a la modularidad, si un módulo falla, los otros módulos continúan funcionando sin interrupciones, lo que garantiza una alta disponibilidad y continuidad de energía.

Mayor eficiencia energética: Al adaptarse a la carga actual, los módulos del SAI Modular evitan el consumo excesivo de energía, lo que aumenta la eficiencia y reduce los costos operativos.

Desventajas:

Mayor costo inicial: tiende a tener un mayor costo inicial debido a la necesidad de adquirir múltiples módulos y componentes adicionales para la configuración inicial.

Configuración y mantenimiento más complejos: La modularidad del SAI requiere una configuración y un mantenimiento más cuidadosos, lo que puede resultar en una mayor complejidad operativa.

Requiere planificación adecuada: La elección y el dimensionamiento correcto de los módulos y la capacidad del SAI Modular requieren una planificación cuidadosa y una comprensión detallada de los requisitos de carga, lo que puede ser más desafiante en comparación con otros tipos de SAI.

Sistema de energía solar: Está compuesto principalmente por tres componentes clave: los paneles solares, el inversor y el sistema de almacenamiento de energía. Aprovecha la energía solar para generar electricidad mediante paneles solares, la convierte en corriente alterna utilizando un inversor y la almacena en un sistema de almacenamiento de energía, como baterías. Esto proporciona una fuente de electricidad confiable y sostenible, reduciendo la dependencia de la red eléctrica convencional y mejorando la capacidad de la micropyme para hacer frente a posibles cortes de energía.

- **Sistema híbrido (solar + almacenamiento):** Un sistema híbrido combina paneles solares fotovoltaicos con almacenamiento de energía, comúnmente utilizando baterías. Estos sistemas permiten aprovechar la energía solar tanto para alimentar la carga directamente como para almacenar el exceso de energía generada durante el día para su uso posterior, incluso en horas sin sol. El almacenamiento de energía proporciona resiliencia y capacidad de respaldo durante cortes de electricidad, lo que garantiza un suministro continuo de energía. Además, estos sistemas pueden estar conectados a la red eléctrica, permitiendo la venta del exceso de energía generada y la compra de electricidad en caso de necesidad al no producir suficiente.

Ventajas:

Resiliencia eléctrica: El almacenamiento de energía permite contar con un respaldo durante cortes de electricidad, lo que garantiza un suministro continuo de energía.

Autonomía: Puedes utilizar la energía almacenada durante la noche o en días nublados, reduciendo la dependencia de la red eléctrica.

Ahorro en la factura eléctrica: Almacenar y utilizar la energía solar generada reduce la cantidad de energía que debes comprar de la red, lo que se traduce en ahorros a largo plazo.

Sostenibilidad: El uso de energía solar reduce la dependencia de los combustibles fósiles y contribuye a la reducción de emisiones de carbono.

Desventajas:

Costo inicial más alto: La inclusión de sistemas de almacenamiento de energía aumenta el costo inicial de instalación en comparación con otros sistemas solares.

Mantenimiento: Las baterías requieren un mantenimiento adecuado para garantizar su funcionamiento óptimo y su vida útil.

- **Sistema fuera de la red (autónomo o aislado):** Un sistema fuera de la red es independiente de la red eléctrica convencional. Utiliza paneles solares para generar electricidad, que se almacena en baterías para su uso posterior. Este tipo de sistema se utiliza comúnmente en áreas remotas donde no hay acceso a la red eléctrica o donde la conexión a la red resulta costosa o poco práctica. Los sistemas fuera de la red son autosuficientes y proporcionan electricidad para todas las necesidades de la carga, lo que incluye la iluminación, los electrodomésticos y otros equipos. Suelen requerir una mayor capacidad de almacenamiento de energía para garantizar un suministro continuo durante períodos prolongados sin sol.

Ventajas:

Independencia energética: No dependes de la red eléctrica, lo que es especialmente útil en áreas remotas donde el acceso a la red no es viable.

Suministro continuo: Con el almacenamiento de energía en baterías, puedes tener electricidad incluso durante períodos prolongados sin sol.

Sostenibilidad: Utilizar energía solar en sistemas fuera de la red reduce la necesidad de generación de energía a través de fuentes no renovables.

Desventajas:

Alto costo inicial: La necesidad de paneles solares y baterías de mayor capacidad puede incrementar el costo de instalación en comparación con sistemas conectados a la red.

Dimensionamiento adecuado: Es necesario calcular correctamente la capacidad de almacenamiento y generación para asegurarse de satisfacer la demanda energética incluso en condiciones adversas.

- **Sistema conectado a la red:** Un sistema conectado a la red, también conocido como sistema de energía solar en la red o interconectado, está diseñado para funcionar en combinación con la red eléctrica convencional. Los paneles solares generan electricidad que se consume inmediatamente en la carga y, si la demanda es mayor que la generación solar, se obtiene la electricidad adicional de la red. Si la generación solar es mayor que el consumo, el exceso de energía se envía a la red eléctrica, lo que permite al propietario del sistema venderla y obtener una compensación económica. Estos sistemas no incorporan almacenamiento de energía y dependen de la red para el suministro continuo en caso de insuficiencia de generación solar, como durante la noche o en días nublados. Este sistema no aporta resiliencia, sino que serviría, en combinación con otros sistemas para la mejora de las

condiciones de la microPYME.

Ventajas:

Acceso a energía continua: Puedes aprovechar tanto la energía solar generada como la electricidad de la red, asegurando un suministro constante y evitando interrupciones en el servicio.

Ahorro en la factura eléctrica: Al generar parte de la electricidad consumida, se reducen los costos de la energía comprada a la red.

Contribución a la red eléctrica: Si generas un exceso de energía, puedes enviarla a la red y recibir compensación económica o créditos en tu factura eléctrica.

Desventajas:

Dependencia de la red: Durante cortes de electricidad, el sistema conectado a la red no proporcionará energía, a menos que se incorpore un sistema de respaldo adicional.

No es autónomo: En caso de interrupción en la red, el sistema conectado a la red no podrá suministrar electricidad sin un sistema de almacenamiento adicional.

5.2.4 Conclusión

En conclusión, la resiliencia eléctrica es de gran importancia para las microPYMEs debido a su impacto directo en la continuidad operativa y el éxito. Estas empresas, que a menudo operan con recursos muy limitados, enfrentan riesgos significativos ante la pérdida de electricidad. Los efectos de la interrupción del suministro eléctrico pueden ser amplios y perjudiciales, incluyendo la interrupción de la producción, la pérdida de clientes, daños a la reputación, pérdida de datos, costos adicionales y problemas de seguridad, entre otros.

Al invertir en resiliencia eléctrica, las microPYMEs pueden reducir los riesgos asociados con la pérdida de electricidad y minimizar los impactos negativos en sus operaciones, clientes, empleados y reputación. La capacidad de mantenerse en funcionamiento y cumplir con los compromisos comerciales, incluso en situaciones adversas, fortalece la confianza de los clientes, mejora la imagen de la empresa y brinda una ventaja competitiva.

Además, la resiliencia eléctrica puede abrir oportunidades para el crecimiento y la expansión empresarial. Las microPYMEs que pueden garantizar una continuidad operativa confiable están en mejores condiciones para aprovechar oportunidades comerciales, cumplir con los plazos de entrega, ofrecer un servicio de calidad y mantener relaciones sólidas con clientes y proveedores.

En resumen, la resiliencia eléctrica es esencial para el éxito y la supervivencia de las microPYMEs. La capacidad de hacer frente a las interrupciones del suministro eléctrico y mantener la operación de manera eficiente y confiable puede marcar la diferencia entre el crecimiento sostenible y la lucha por sobrevivir. Al tomar medidas proactivas para garantizar la resiliencia eléctrica, las microPYMEs pueden proteger su negocio y estar preparadas para enfrentar los desafíos energéticos en un entorno empresarial en constante cambio.

5.3 DATOS

5.3.1 Introducción

La resiliencia de datos se ha convertido en un aspecto crucial para el éxito y la supervivencia de las microPYMEs en la era digital. En un mundo donde la información se ha convertido en un activo invaluable, las empresas, sin importar su tamaño, enfrentan constantemente amenazas como pérdida de datos, ciberataques, desastres naturales y fallos técnicos que podrían poner en peligro su funcionamiento y, en última instancia, su viabilidad.

La necesidad de no perder los datos de los que dispongan se convierte en una prioridad crucial para el éxito y la continuidad de cualquier negocio.

Una microPYME, por su tamaño reducido y limitados recursos, puede parecer menos susceptible a estos riesgos en comparación con una gran empresa. Sin embargo, la realidad es que las consecuencias de la pérdida de datos pueden ser peores debido a su incapacidad para recuperarse rápidamente.

La resiliencia de datos se refiere a la capacidad de una empresa para mantener y proteger su información crítica frente a cualquier adversidad. Implica la implementación de medidas preventivas. Además, implica la planificación y preparación para hacer frente a posibles desastres, como inundaciones, incendios o fallas de hardware.

En resumen, la resiliencia de datos se ha vuelto esencial para las microPYMEs, ya que garantiza la continuidad de sus operaciones, protege la información vital y ayuda a cumplir con las regulaciones vigentes. Invertir en medidas de seguridad y preparación puede parecer un desafío, pero es un costo insignificante en comparación con las consecuencias de no hacerlo. La resiliencia de datos se convierte así en un pilar fundamental para la supervivencia y el éxito a largo plazo de una microPYME en un entorno empresarial cada vez más digitalizado y amenazante.

5.3.2 Riesgos, Impactos y Vulnerabilidades

Incumplimiento legal: Dependiendo del tipo de datos perdidos, una microPYME puede enfrentar consecuencias legales. Si se trata de información personal o financiera de clientes, existen regulaciones de privacidad y protección de datos que deben cumplirse. El incumplimiento de estas regulaciones puede resultar en multas y sanciones financieras que pueden ser especialmente onerosas para una microPYME con recursos limitados.

Pérdida de productividad: La incapacidad de acceder a los datos necesarios puede ralentizar las operaciones diarias y dificultar la toma de decisiones, lo que resulta en una disminución de la productividad y eficiencia.

Consecuencias financieras: La pérdida de datos confidenciales puede dar lugar a costosos litigios, multas regulatorias y daños a la reputación de la empresa, lo que puede tener un impacto significativo en las finanzas de la pyme.

Interrupción de negocio: En caso de desastres naturales, ciberataques u otros eventos imprevistos, la falta de un plan de respaldo y recuperación de datos puede llevar a interrupciones prolongadas y poner en peligro la continuidad del negocio.

Dificultad para el crecimiento: La falta de datos confiables puede obstaculizar la toma de decisiones estratégicas y limitar la capacidad de la pyme para identificar oportunidades de crecimiento y adaptarse a un entorno empresarial en constante cambio.

Pérdida de confianza y lealtad del cliente: La pérdida de datos de clientes puede afectar negativamente la experiencia del cliente, dando lugar a errores en los pedidos, falta de comunicación y una disminución general de la satisfacción del cliente. Esto puede resultar en la pérdida de confianza y lealtad de los clientes.

Pérdida de información crítica: La falta de una estrategia sólida de respaldo y recuperación de datos puede llevar a la pérdida irreversible de información crítica para el funcionamiento de la empresa, como registros financieros, datos de clientes y otros activos valiosos.

Daño a la reputación: La pérdida de datos puede dañar la reputación de una pyme, especialmente si se trata de información confidencial o sensible. Esto puede afectar negativamente la percepción de los clientes, socios comerciales y otras partes interesadas, lo que a su vez puede tener un impacto duradero en la imagen y credibilidad de la empresa.

Costos de recuperación: La recuperación de datos perdidos puede ser costosa para una microPYME. Dependiendo de la magnitud de la pérdida y la complejidad de los sistemas, puede ser necesario recurrir a servicios de recuperación de datos especializados, lo que implica gastos adicionales. Además, la pérdida de tiempo y la interrupción de las operaciones también pueden generar costos indirectos.

Impacto en la continuidad del negocio: La pérdida de datos puede tener un impacto directo en la continuidad del negocio de una PYME. Si la información es esencial para el funcionamiento diario y no se puede recuperar de manera oportuna, la PYME puede enfrentar dificultades significativas para retomar las operaciones normales y cumplir con las expectativas de los clientes.

Daño a las relaciones con socios y proveedores: La pérdida de datos puede afectar las relaciones con socios comerciales y proveedores. Si la microPYME no puede acceder a información clave compartida con socios estratégicos o si la pérdida de datos afecta las operaciones conjuntas, la confianza y la colaboración pueden verse comprometidas, lo que puede tener un impacto negativo en la cadena de suministro y las asociaciones comerciales.

Vulnerabilidad a amenazas de seguridad: La pérdida de datos puede dejar a una pyme vulnerable a ciberataques y otras amenazas de seguridad. Sin una adecuada protección y medidas de respaldo, los datos empresariales están expuestos a riesgos como el robo de información confidencial o la manipulación de datos.

5.3.3 Estrategia de redundancia

Local: La resiliencia en datos físicos se refiere a la implementación de medidas de protección y recuperación de datos en infraestructuras locales, como servidores, discos duros y otros dispositivos de almacenamiento. Se centra en garantizar la disponibilidad y la integridad de los datos en caso de fallos o desastres.

- **NAS:** El Network Attached Storage (NAS) es un dispositivo de almacenamiento conectado a la red local de la empresa. Proporciona una solución centralizada para almacenar y acceder a datos desde diferentes dispositivos. Los usuarios pueden acceder a los archivos almacenados en el NAS a través de la red local o incluso de forma remota a través de Internet.

Ventajas:

Facilidad de acceso: Los empleados pueden acceder a los datos almacenados en el NAS desde cualquier dispositivo conectado a la red. Esto permite un flujo de trabajo más flexible y colaborativo.

Copias de seguridad automáticas: Muchos sistemas NAS ofrecen la opción de programar copias de seguridad automáticas. Esto garantiza que los datos se respalden regularmente sin necesidad de intervención manual, lo que brinda una mayor protección contra la pérdida de datos.

Funciones de seguridad avanzadas: Los dispositivos NAS suelen ofrecer características de seguridad adicionales, como encriptación de datos, autenticación de usuarios y control de acceso. Esto ayuda a proteger los datos almacenados contra accesos no autorizados y asegura su confidencialidad.

Desventajas:

Costo inicial: La adquisición de un dispositivo NAS y los discos duros necesarios puede ser una inversión inicial significativa para una microPYME con recursos limitados.

Limitación de capacidad: Algunos dispositivos NAS tienen una capacidad de almacenamiento limitada en comparación con otras soluciones de almacenamiento a gran escala. Esto puede ser un problema si tu microPYME maneja grandes volúmenes de datos.

Dependencia de la red: La velocidad de transferencia de datos hacia y desde el NAS está sujeta a las limitaciones de la red local. Si la red experimenta congestión o baja velocidad, puede afectar el rendimiento del acceso a los datos.

- **Copias de seguridad a dispositivos físicos:** Esta opción implica realizar copias de seguridad periódicas de los datos en dispositivos físicos, como discos duros externos, unidades USB o cintas magnéticas.

Ventajas:

Accesibilidad y control: Las copias de seguridad físicas se pueden almacenar en un lugar seguro dentro de la empresa y los propietarios tienen un control directo sobre ellas. Esto proporciona una sensación de seguridad y permite un acceso rápido en caso de necesidad.

Baja inversión inicial: Los dispositivos físicos utilizados para copias de seguridad, como discos duros externos o unidades USB, suelen ser más económicos en comparación con otras soluciones. Esto puede ser beneficioso para una microPYME con recursos limitados.

Portabilidad: Los dispositivos físicos de copias de seguridad se pueden transportar fuera de la empresa, lo que proporciona una capa adicional de protección en caso de desastres o emergencias locales.

Desventajas:

Dependencia de la gestión manual: Las copias de seguridad físicas deben realizarse de forma regular y manual, lo que implica un esfuerzo adicional y la posibilidad de olvidar hacerlo. Si no se realiza una copia de seguridad actualizada y se produce un fallo o pérdida de datos, podrías perder información importante.

Riesgo de pérdida o daño: Los dispositivos físicos utilizados para copias de seguridad pueden extraviarse, dañarse o ser robados. Esto puede resultar en la pérdida permanente de datos y comprometer la recuperación de información vital.

Limitaciones de capacidad: La capacidad de almacenamiento de los dispositivos físicos es limitada. Si tu microPYME genera grandes volúmenes de datos, es posible que necesites adquirir varios dispositivos para cubrir todas las necesidades de respaldo.

- **Redundancia en hardware (RAID):** RAID (Redundant Array of Independent Disks) es una tecnología que combina múltiples discos duros físicos en una única unidad lógica para mejorar el rendimiento y la resiliencia de datos.

Ventajas:

Mayor rendimiento: La configuración RAID distribuye los datos en varios discos duros, lo que permite un acceso y transferencia más rápidos. Esto puede mejorar el rendimiento general del sistema, especialmente en entornos con una alta carga de trabajo de datos.

Tolerancia a fallos: Dependiendo del nivel de RAID implementado, si un disco duro falla, los datos se pueden recuperar a través de la redundancia de información almacenada en los otros discos. Esto asegura la disponibilidad continua de los datos y reduce el tiempo de inactividad del sistema.

Reemplazo en caliente: Algunas configuraciones RAID permiten el reemplazo de discos defectuosos mientras el sistema sigue en funcionamiento. Esto minimiza el tiempo de inactividad y facilita el mantenimiento del sistema sin interrupciones significativas.

Desventajas:

Costo adicional: Configurar una matriz RAID requiere la adquisición de múltiples discos duros y una controladora RAID. Esto puede aumentar los costos iniciales de hardware, especialmente si se desea implementar configuraciones RAID más avanzadas.

Complejidad de configuración y gestión: La configuración y el mantenimiento de una configuración RAID pueden ser complejos, especialmente para usuarios no técnicos. Se requiere un conocimiento adecuado de las distintas configuraciones RAID y la configuración correcta para maximizar el rendimiento y la resiliencia.

Limitaciones de protección: Aunque RAID brinda protección contra fallos de disco, no ofrece una protección completa contra otros tipos de desastres, como incendios, inundaciones o errores humanos. Es importante considerar otras medidas de resiliencia para proteger los datos en caso de eventos catastróficos.

- **Protección ciberseguridad:** La protección de ciberseguridad implica la implementación de medidas y herramientas para proteger los datos contra amenazas ciberneticas, como ataques de malware, ransomware o piratería informática.

Ventajas:

Protección contra amenazas ciberneticas: Las soluciones de ciberseguridad ayudan a detectar, prevenir y mitigar ataques maliciosos, como malware, ransomware y piratería informática. Esto protege los datos y la infraestructura de la empresa contra posibles daños y pérdidas.

Integridad y confidencialidad de los datos: Las medidas de seguridad cibernetica aseguran que los datos se mantengan íntegros y sólo sean accesibles por personas autorizadas. Esto protege la confidencialidad y evita la manipulación no autorizada de los datos.

Variedad de opciones: Existen soluciones de ciberseguridad disponibles para diferentes presupuestos y necesidades. Desde software antivirus básico hasta soluciones de seguridad avanzadas, como firewalls y sistemas de detección de intrusiones, hay opciones adecuadas para diferentes entornos empresariales.

Desventajas:

Configuración y gestión técnica: Algunas soluciones de ciberseguridad pueden requerir conocimientos técnicos para su correcta configuración y gestión. Esto puede suponer un

desafío para una microPYME con recursos limitados o falta de experiencia en ciberseguridad.

Evolución constante de las amenazas: Las amenazas ciberneticas evolucionan rápidamente y los métodos de ataque se vuelven más sofisticados. Esto requiere una actualización y adaptación constante de las soluciones de seguridad para mantener la resiliencia de los datos. El seguimiento de estas amenazas y mantenerse al día puede ser un desafío en sí mismo.

- **Equipamiento de respaldo:** Esta opción implica tener dispositivos duplicados para respaldar los datos críticos de la empresa, como tener dos ordenadores idénticos, permitiendo crear redundancia en los dispositivos.

Ventajas:

Alta disponibilidad de datos: En caso de fallo de uno de los dispositivos, los datos siguen estando disponibles en el dispositivo duplicado. Esto minimiza el tiempo de inactividad y asegura la continuidad de las operaciones comerciales.

Recuperación rápida: Al tener un equipo duplicado, la recuperación de datos y la continuidad del negocio pueden ser más rápidas y fluidas. Simplemente se puede cambiar al dispositivo duplicado mientras se soluciona el problema en el equipo principal.

Redundancia de hardware: La duplicación del equipo proporciona una capa adicional de protección contra fallos de hardware. Si un componente falla, el otro dispositivo puede continuar funcionando sin interrupciones significativas.

Desventajas:

Costo adicional: Adquirir y mantener dispositivos duplicados implica una inversión adicional en hardware y licencias de software si es necesario. Esto puede ser un desafío para una microPYME con recursos financieros limitados.

Sincronización y gestión: La sincronización y la gestión de los datos entre los dispositivos duplicados pueden requerir herramientas y configuraciones específicas para asegurar la integridad de los datos. Es importante mantener los dispositivos actualizados y asegurarse de que ambos estén sincronizados adecuadamente.

No protección completa contra desastres: Si ambos dispositivos están ubicados en la misma ubicación física, aún existe el riesgo de pérdida de datos en caso de desastres naturales o eventos catastróficos. Es recomendable tener una estrategia adicional de respaldo fuera del sitio para mitigar este riesgo.

Cloud: La resiliencia en la nube se refiere a la implementación de medidas de protección y recuperación de datos en entornos de computación en la nube. Los datos se almacenan y procesan en servidores remotos y se accede a ellos a través de Internet.

- **Servicio de almacenamiento en la nube:** Un servicio de almacenamiento en la nube permite a los usuarios almacenar y acceder a sus datos a través de servidores remotos en lugar de utilizar almacenamiento local. Los datos se almacenan en centros de datos gestionados por proveedores de servicios en la nube. Algunos ejemplos populares de servicios de almacenamiento en la nube son Dropbox, Google Drive y OneDrive.

Ventajas:

Acceso conveniente a los datos desde cualquier lugar con conexión a Internet: Los servicios de almacenamiento en la nube permiten a los usuarios acceder a sus archivos y datos desde diferentes dispositivos, como computadoras, teléfonos inteligentes o tabletas, siempre que tengan acceso a Internet. Esto facilita la colaboración y el trabajo en equipo, ya que múltiples personas pueden acceder y editar los mismos archivos de forma simultánea.

No se requiere inversión en hardware adicional: Al utilizar un servicio de almacenamiento en la nube, no es necesario invertir en hardware adicional, como servidores o unidades de almacenamiento local. Esto es especialmente beneficioso para una microPYME con recursos limitados, ya que evita los gastos iniciales de adquisición de equipos y su mantenimiento.

Redundancia y copias de seguridad de los datos: Los proveedores de servicios en la nube suelen implementar medidas de seguridad y copias de seguridad automatizadas para proteger los datos de sus usuarios. Esto implica que los datos se almacenan en múltiples ubicaciones y se crean copias de seguridad periódicas, lo que aumenta la seguridad y la resiliencia de los datos frente a posibles pérdidas.

Desventajas:

Dependencia de la conexión a Internet: Para acceder a los datos almacenados en la nube, es necesario tener una conexión a Internet estable y confiable. Si la conexión a Internet es lenta o se interrumpe, puede haber dificultades para acceder a los archivos y trabajar de manera eficiente.

Costos continuos a medida que se aumenta el almacenamiento: Aunque los servicios de almacenamiento en la nube suelen ofrecer un espacio inicial gratuito o de bajo costo, a medida que se requiere más capacidad de almacenamiento, es posible que se deba pagar una tarifa adicional. Esto puede convertirse en un factor a considerar en términos de presupuesto a largo plazo.

Control y seguridad de los datos: Al utilizar un servicio de almacenamiento en la nube, los datos de la empresa se encuentran bajo el control y la responsabilidad del proveedor de servicios. Esto puede generar preocupaciones en términos de confidencialidad y seguridad de los datos, especialmente si se trata de información sensible o regulada. Es importante investigar y seleccionar un proveedor confiable que cumpla con los requisitos de seguridad y privacidad de la empresa.

- **Copias de seguridad:** Las copias de seguridad en la nube implica almacenar copias de seguridad de los datos de una empresa en servidores remotos. Estas copias de seguridad se pueden programar y automatizar para garantizar la disponibilidad y recuperación de los datos en caso de pérdida, daño o falla del hardware local.

Ventajas:

Mayor seguridad de los datos en comparación con el almacenamiento local: Al realizar copias de seguridad en la nube, los datos se protegen de eventos adversos locales, como incendios, robos o daños en el hardware. Los proveedores de servicios en la nube suelen implementar medidas de seguridad robustas, como cifrado de datos y redundancia, para garantizar la integridad de las copias de seguridad.

Protección contra pérdida de datos: Las copias de seguridad en la nube aseguran que los datos estén respaldados y disponibles para su recuperación en caso de pérdida accidental, falla del hardware o ataques cibernéticos. Esto reduce el riesgo de interrupciones comerciales y permite una rápida recuperación de datos críticos en situaciones de emergencia.

Posibilidad de automatizar el proceso de copia de seguridad: Los servicios de copias de seguridad en la nube suelen ofrecer la capacidad de programar y automatizar las copias de seguridad. Esto ahorra tiempo y garantiza que los datos se respaldan regularmente sin la necesidad de intervención manual.

Desventajas:

Costos asociados con el almacenamiento en la nube y la transferencia de datos:

Dependiendo de la cantidad de datos que se deban respaldar y el proveedor de servicios en la nube elegido, puede haber costos asociados con el almacenamiento y la transferencia de datos. Es importante evaluar y comparar las tarifas de diferentes proveedores para encontrar la opción más adecuada en función de las necesidades y el presupuesto de la micropyme.

Dependencia de la conexión a Internet para realizar y restaurar las copias de seguridad: Al realizar copias de seguridad en la nube, es necesario contar con una conexión a Internet confiable para cargar los datos en los servidores remotos y para restaurarlos cuando sea necesario. Una conexión a Internet lenta o inestable puede afectar la eficiencia de las copias de seguridad y la recuperación de datos.

Restricciones de almacenamiento: Los proveedores de servicios en la nube suelen ofrecer diferentes límites de capacidad de almacenamiento en función del plan seleccionado. Si los requisitos de almacenamiento de la empresa exceden estos límites, es posible que se deba pagar una tarifa adicional o buscar alternativas de almacenamiento.

- **Infraestructura en la nube:** La migración a la infraestructura en la nube implica trasladar completamente los recursos de TI de una empresa, como servidores, aplicaciones y datos, a servidores remotos gestionados por proveedores de servicios en la nube. Esto implica una transición completa de un entorno de TI local a uno basado en la nube.

Ventajas:

Eliminación de la necesidad de mantener y administrar infraestructura local: Al migrar a la infraestructura en la nube, la empresa se libera de la responsabilidad de mantener y administrar servidores locales, lo que reduce la carga de trabajo y los costos asociados. La infraestructura en la nube es administrada por el proveedor de servicios, lo que permite a la empresa enfocarse en sus operaciones principales.

Escalabilidad y flexibilidad: La infraestructura en la nube permite escalar los recursos de manera flexible según las necesidades del negocio. Se pueden agregar o reducir rápidamente recursos como capacidad de almacenamiento, potencia de procesamiento o memoria, lo que permite adaptarse a los cambios en la demanda sin incurrir en costos excesivos.

Mayor fiabilidad y redundancia: Los proveedores de servicios en la nube suelen ofrecer una infraestructura altamente confiable y redundante. Esto significa que los datos y las aplicaciones están respaldados por sistemas y ubicaciones redundantes, lo que reduce el riesgo de interrupciones y pérdidas de datos debido a fallas de hardware o desastres naturales.

Desventajas:

Costos iniciales y continuos asociados con los servicios en la nube: La migración a la infraestructura en la nube puede implicar costos iniciales significativos, como la reestructuración de los sistemas y la formación del personal. Además, existen costos continuos por el uso de los servicios en la nube, como el consumo de recursos, el almacenamiento y las transferencias de datos. Estos costos deben considerarse en el presupuesto de la empresa.

Complejidad en la migración de datos y aplicaciones existentes: La migración de una infraestructura local a la nube puede ser un proceso complejo. Requiere planificación, evaluación y posiblemente modificaciones en las aplicaciones existentes y en los flujos de trabajo. Además, la transferencia de grandes volúmenes de datos a la nube puede llevar tiempo y requerir una conexión a Internet rápida y estable.

- **Dependencia de la conexión a Internet:** Al migrar a la infraestructura en la nube, la conexión a Internet se vuelve crucial para acceder a los recursos y servicios en la nube. Si la conexión a Internet falla o es lenta, puede afectar la productividad y la disponibilidad de los sistemas y datos en la nube.

5.3.4 Conclusión

En conclusión, la resiliencia de datos ya sea en formato físico o en la nube, es de vital importancia para las microPYMEs. La pérdida de datos puede tener consecuencias devastadoras, como interrupciones operativas, pérdida de clientes, daño a la reputación y costos financieros significativos. En un mundo donde la información se ha convertido en un activo crítico, las microPYMEs deben reconocer la necesidad de proteger y preservar sus datos.

La resiliencia de datos implica implementar medidas preventivas y estrategias de recuperación para proteger la información crítica de la empresa. Al hacerlo, las microPYMEs pueden minimizar la posibilidad de pérdida de datos y reducir el impacto negativo en sus operaciones y reputación.

Además, en un contexto de creciente regulación y preocupación por la privacidad de los datos, la resiliencia de datos se vuelve aún más importante. Cumplir con las leyes y regulaciones de protección de datos es esencial para evitar multas y sanciones legales que podrían poner en peligro la viabilidad financiera de una microPYME.

Ya sea que los datos se almacenen en formato físico o en la nube, es esencial tener en cuenta la importancia de la resiliencia. Si bien la nube ofrece ventajas en términos de accesibilidad, escalabilidad y redundancia, también es necesario implementar medidas de seguridad y realizar copias de seguridad regulares para proteger los datos almacenados en línea. Por otro lado, si se utilizan medios físicos para el almacenamiento de datos, es necesario asegurarlos adecuadamente y contar con planes de recuperación.

En última instancia, invertir en la resiliencia de datos no solo es una medida de protección, sino también una ventaja competitiva. Las microPYMEs que pueden demostrar que tienen sólidas políticas y prácticas de resiliencia de datos generan confianza en sus clientes, proveedores y socios comerciales. Esto fortalece la reputación de la empresa y la posiciona como una entidad confiable y segura para hacer negocios.

En resumen, la resiliencia de datos es esencial para el funcionamiento continuo y exitoso de una microPYME. Protege la información vital, garantiza la continuidad del negocio, cumple con las regulaciones y fomenta la confianza. Al priorizar la resiliencia de datos, las microPYMEs pueden salvaguardar su futuro y estar preparadas para afrontar los desafíos en el entorno empresarial cada vez más digitalizado y amenazante de hoy en día.

6 APPLICACIÓN PRÁCTICA A UN CASO CONCRETO

6.1 Definición de la empresa

Para el desarrollo de este proyecto se ha sintetizado una empresa, esto es, analizando diferentes empresas se ha modelizado una que semeja empresas microPYMEs reales. La microPYME se dedica al negocio de clases online. Imparte clases de apoyo a cursos correspondiente a la educación primaria del sistema educativo español. Además, imparte clases particulares fuera de estos cursos. Los clientes de la empresa son principalmente padres o tutores legales de niños comúnmente entre los seis y los doce años de edad que necesitan refuerzo para sus estudios oficiales.

Está compuesta por cuatro empleados fijos que trabajan a media jornada, distribuyendo su tiempo y adaptando el horario entre las distintas tareas y reuniones que tienen asignadas.

El fundador actúa como director y contable de la compañía, sus funciones incluyen la propia dirección y toma de decisiones de la empresa, realizar todas las tareas relacionadas con la contabilidad, la contratación y dirección del personal así como llevar la cuenta bancaria de la empresa y las cuentas de las redes sociales. Durante el periodo de admisiones será el encargado de llevar el proceso de matriculación. El informático se encarga de crear, actualizar y mantener la web de la empresa, así como la infraestructura y solucionar todos los problemas técnicos de los sistemas de la compañía. Por último hay dos profesores encargados de realizar las clases de los cursos. Ellos se encargan de organizar el material y los temas de las clases que imparten además de llevar el contacto tanto con los alumnos como familiares una vez empezadas las clases. A la incorporación/sustitución de un nuevo profesor, el director le formará internamente sobre las metodologías y funcionamiento de la empresa mientras que el resto de personal docente le dará apoyo en sus tareas durante el proceso de adaptación.

Se sitúa en un piso de un grupo de viviendas residenciales antiguas, convirtiendo el piso a oficina. La oficina cuenta con las instalaciones preexistentes de un piso como electricidad básica y acceso de red. Se tiene contratado con el proveedor de red una tarifa de fibra con una velocidad de 500 Mb/s simétrica además de un servicio de IP fija para poder hacer público su servicio web. Adicionalmente para el acceso a la página web se utiliza un servicio de DNS gratuito. Se tiene contratado con el proveedor de electricidad una potencia de 10kw, para tener la capacidad de utilizar los dispositivos principales de manera simultánea. El consumo medio del lugar es de 860W aproximadamente, teniendo en cuenta todos los dispositivos electrónicos. El domicilio se ha dividido en distintas zonas siendo cada zona una habitación diferente del piso, donde cada trabajador tendrá un lugar fijo de trabajo debido a que la conexión de red es completamente cableada, situándose en esa sala los elementos necesarios y relacionados con sus tareas. El informático dispondrá en su sala de un ordenador de sobremesa con sistema operativo Windows que actúa como servidor. La distribución del personal puede identificarse mejor en el siguiente plano de la casa adaptada a oficina.

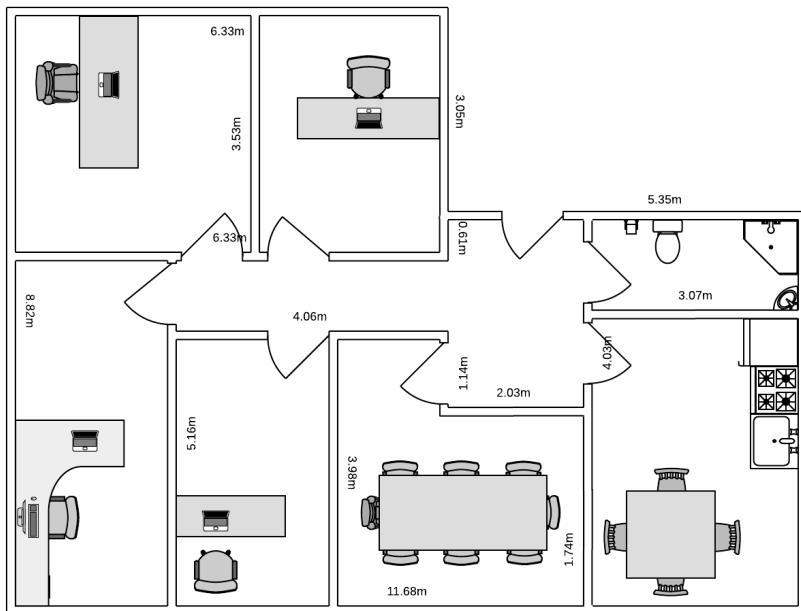


Figura 8: Plano de la distribución de la oficina de la microPYME

El informático de la empresa es responsable de mantener el sitio web y la plataforma de enseñanza en línea, asegurándose de que todo funcione correctamente. También está a cargo de garantizar la seguridad de los datos y de los sistemas de la empresa.

Todo el personal utilizará su dispositivo personal con sistema operativo Windows para sus labores. Todos los datos utilizados por la web como cuentas, archivos, clases, documentos, están almacenados en la base de datos de la web mientras que todos los documentos que contienen información personal como información de los empleados, nóminas, datos privados de los alumnos, estarán directamente almacenados en el equipo del director.

Para proporcionar un soporte informático rápido y eficiente se precisa de la presencialidad de todos los empleados durante el transcurso de sus actividades laborales en la oficina. En casos de fuerza mayor como pandemias o nevadas, los profesores podrán impartir de manera excepcional las clases desde sus domicilios.

La web de la empresa creada internamente por el informático se aloja en dicho servidor. Dentro de las funcionalidades de la web se encuentra el sistema de matriculación donde los alumnos se registran para los cursos y clases que deseen y un sistema de acceso a la plataforma para poder visualizar los contenidos de los cursos matriculados. Por su lado, los profesores dispondrán de un rol específico con el que pueden gestionar los contenidos, alumnos y calificaciones de los cursos que imparten.

No se tiene una pasarela de pago en la web, ya que los pagos se realizan directamente mediante transferencia bancaria a la cuenta de la empresa. Esta web no tiene excesivo tráfico, aunque se han detectado picos de conexiones durante las semanas de matriculación a los cursos y periodos de exámenes. El servidor web utiliza apache para el frontal de la página y mysql como base de datos.

Con esta configuración, obtenemos el siguiente esquema de dispositivos y red, donde se identifican el servidor donde se aloja la Web y la BBDD, y la conectividad de los dispositivos de la oficina. Se ha deshabilitado la conexión inalámbrica a la red por lo que no se contempla que se conecte a ella ningún otro dispositivo diferente a los indicados en el siguiente esquema de red.

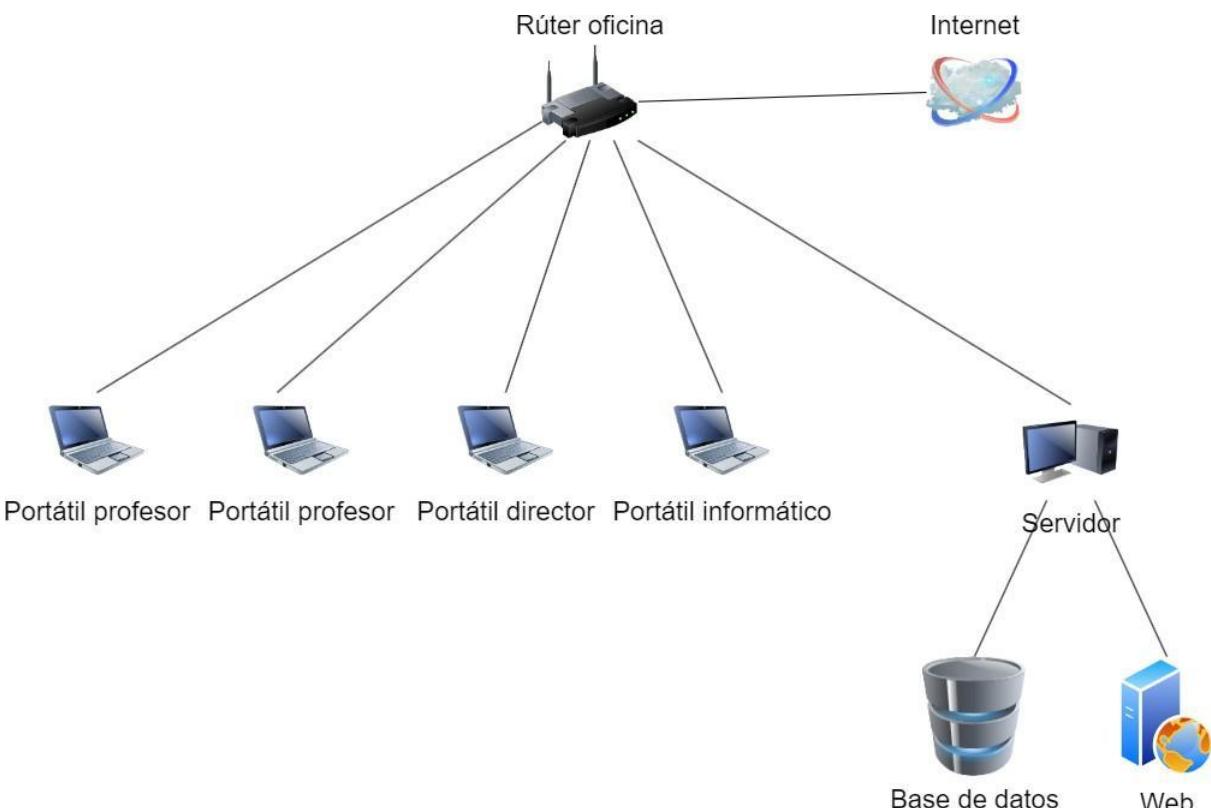


Figura 9: Esquema de red de microPYME

Para las clases se utiliza la herramienta de Teams de forma gratuita. Para ello agendan llamadas que servirán cómo las clases e invitarán a los alumnos a unirse a ellas. Se planificarán las llamadas mediante un calendario, donde se establecerán grupos de alumnos por clases, y horarios fijos de estas sesiones.

La empresa ha obtenido un total de ingresos de 80.000€, donde se incluyen matrículas y servicios de formación en línea. Mientras que los gastos ascienden a un total de 47.000€, que incluyen el salario de los profesores y el informático, el alquiler del local, los servicios de internet y los suministros y otros gastos. El beneficio de la empresa en el previo año es igual a 33.000€, teniendo la opción de la ampliación del negocio. El sueldo del director es establecido en un 80% de los beneficios totales de la pyme, quedando así margen para la ampliación del negocio.

Actualmente la empresa está bien consolidada y se plantea en el futuro expandirse tanto en tamaño como en sector, contratando nuevo personal docente que sea capaz de impartir clases de apoyo para estudios superiores. Las clases son solo online, no se ha planteado en un futuro cercano proporcionar clases presenciales.

Dado a la facilidad que proporcionan, la empresa utilizará sus propias redes sociales gestionadas por el fundador para darse a conocer y publicitar la empresa. En estas redes no solo se incluirá publicidad de las clases, sino publicaciones interesantes relacionadas con los temas de estudios que estén tratando.

Se dispondrá de un sistema de bonificaciones para los profesores, dependiendo del número de alumnos a los que imparten clase. A su vez, se dispondrá de un horario “flexible”, siempre que se avise con un tiempo de margen, dando todas las facilidades posibles al alcance de la empresa.

6.2 Análisis de impacto de negocio

6.2.1 *Introducción*

El presente documento presenta el Análisis de Impacto en el Negocio (BIA, por sus siglas en inglés) para la micropyme dedicada al negocio de clases online. El objetivo de este BIA es evaluar los posibles impactos y riesgos que podrían afectar la continuidad del negocio de la micropyme y, en consecuencia, su capacidad para continuar con las clases en línea de manera efectiva. Mediante este análisis, se van a identificar las áreas críticas de la empresa y los recursos clave necesarios para su funcionamiento, así como establecer las estrategias de mitigación para minimizar los efectos de cualquier interrupción en el negocio.

Durante el análisis, se considerarán los riesgos potenciales sobre la infraestructura tecnológica, la conectividad a internet, la seguridad de los datos, así como otros aspectos relevantes para la continuidad del negocio. Asimismo, se evaluará el impacto de posibles interrupciones en los procesos críticos de la micropyme, como la matriculación de alumnos, la planificación y preparación de clases, la impartición de clases en línea, y la comunicación con los alumnos y sus familiares.

El resultado de este BIA permitirá identificar los riesgos clave, evaluar los impactos potenciales y proponer recomendaciones específicas para mejorar la resiliencia del negocio y reducir los riesgos identificados. Además, se establecerá un plan de acción que detalle las medidas necesarias para implementar

6.2.2 Alcance

El alcance del Análisis de Impacto de Negocio se enfoca en evaluar los posibles impactos y riesgos en los procesos de la microPYME que afecten a la continuidad de su negocio. Entre dichos procesos se encuentran:

Matriculación: Los tutores legales de los alumnos ya sea mediante la web o contactando directamente con el director registran a los alumnos en el curso que deseen. Después mediante transferencia bancaria a la cuenta de la empresa se realiza el pago del curso. Una vez realizado, se da el acceso a la web a la cuenta del alumno teniendo así visibilidad sobre todos los recursos educativos además de añadirles a las reuniones en Teams donde se imparten las clases de su curso.

Web educativa: En la web educativa es donde se suben y se pueden consultar todos los recursos educativos de los cursos impartidos. En ella se encuentran, documentos, videos y todo lo necesario para que los alumnos puedan realizar los cursos. Este material es subido por los profesores que imparten el curso. Además en ella se pueden realizar entregas que los profesores pueden puntuar.

Clases online: Las clases online se realizan a través de la herramienta Teams. Las reuniones se programan a principio de curso y se invita a todos los alumnos matriculados en el curso.

Gestión interna

Aquí se recoge todas aquellas tareas que afectan a la empresa internamente como la gestión de las finanzas, nóminas, personal.

El alcance de este BIA no abarca los siguientes aspectos:

Clases presenciales: Dado que la micropyme se enfoca exclusivamente en clases en línea, no se evaluarán los posibles impactos en las clases presenciales.

Pasarela de pago en la web: Como los pagos se realizan directamente mediante transferencia bancaria, no se incluirá la evaluación de una pasarela de pago en este documento.

6.2.3 Definiciones y terminología

Análisis de Impacto en el Negocio (BIA): Proceso sistemático para identificar y evaluar los posibles impactos de interrupciones en los procesos críticos de una organización y determinar las medidas necesarias para su recuperación.

Continuidad del Negocio: Capacidad de una organización para continuar con sus operaciones y cumplir con sus objetivos, incluso en situaciones de interrupción o crisis.

Riesgo: Posibilidad de que ocurra un evento que tenga un impacto negativo en la organización, sus procesos o sus recursos.

Impacto: Consecuencia o efecto resultante de una interrupción en los procesos críticos de la organización, que puede afectar la operatividad, la reputación, la seguridad, la economía u otros aspectos del negocio.

Proceso Crítico: Actividad o función dentro de la organización que es esencial para el logro de sus objetivos y cuya interrupción tendría un impacto significativo en la continuidad del negocio.

Tiempo de Recuperación Objetivo (RTO): Período de tiempo máximo permitido para recuperar un proceso crítico después de una interrupción, establecido en función de los requisitos de negocio y la tolerancia a la interrupción.

Punto de Recuperación Objetivo (RPO): El punto en el tiempo hasta el cual se pueden aceptar las pérdidas de datos durante la recuperación de un proceso crítico, determinado por las necesidades de la organización y la capacidad de recuperación de datos.

Vulnerabilidad: Debilidad o fallo en los controles o sistemas de una organización que puede ser explotado por amenazas, aumentando el riesgo de una interrupción o compromiso de la continuidad del negocio.

Amenaza: Fuente potencial de daño o peligro que puede afectar a la organización, sus procesos o sus recursos. Puede ser interna o externa.

Infraestructura Tecnológica: Conjunto de componentes y sistemas tecnológicos utilizados por la organización para respaldar sus operaciones, como servidores, redes, sistemas de almacenamiento y software.

Gestión de Crisis: Conjunto de acciones y procedimientos establecidos para gestionar y responder de manera efectiva a situaciones de emergencia o interrupciones que puedan afectar la continuidad del negocio.

Plan de Acción: Documento que detalla las medidas específicas que se deben tomar para implementar las recomendaciones del BIA, incluyendo las responsabilidades, los plazos y los recursos necesarios.

6.2.4 Activos

- Datos
 - Base de datos de la web
 - Nóminas
 - Documentación financiera y administrativa
 - Cuentas de aplicación
- Aplicaciones
 - Web educativa
 - Paquete de aplicaciones de oficina (word, excel, etc...)
 - Aplicación de videollamada (Teams)
- Hardware
 - Equipos windows de profesores
 - Equipo windows del informático
 - Equipo windows del director
 - Servidor
- Red
 - Router
- Tecnología
 - Cableado de red
- Personal
 - Profesores
 - Director/contable
 - Informático
- Instalaciones
 - Oficina
- Suministros
 - Conectividad a internet
 - Electricidad
 - Servicio de DNS externo

6.2.5 Árbol de dependencias

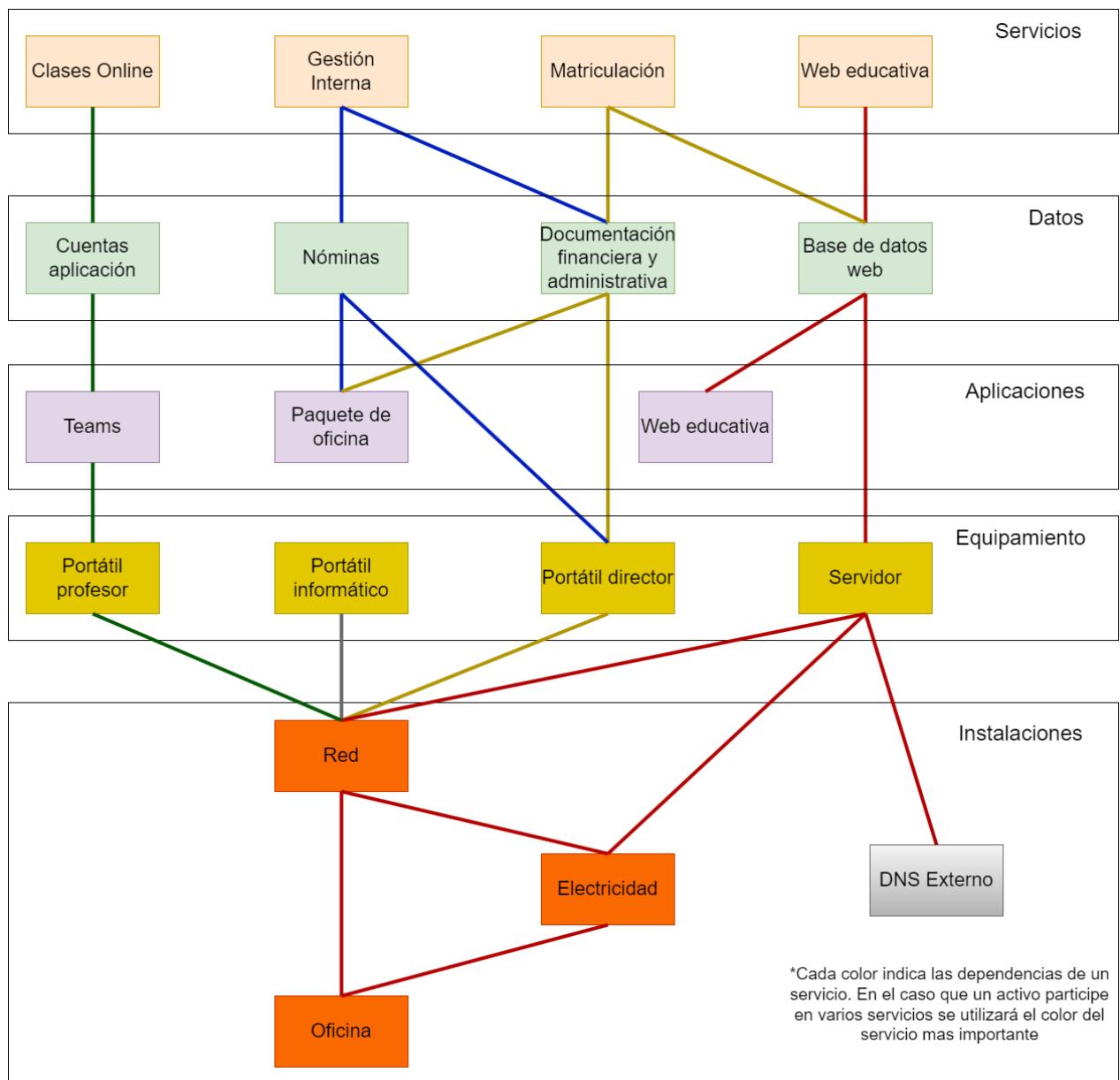


Figura 10: Árbol de dependencias de la microPYME

6.2.6 Análisis de riesgos

Amenazas:

Interrupción del servicio de internet: La microPYME depende de una conexión a internet estable para la impartición de clases en línea. Cualquier interrupción en el servicio de internet, ya sea causada por problemas técnicos o fallas en el proveedor, podría afectar la capacidad de ofrecer las clases de manera efectiva.

Además, al estar la web alojada en un servidor físicamente dentro de las instalaciones de la microPYME, dicha interrupción de servicio también puede afectar al acceso de los recursos educativos de la web o el registro de nuevos estudiantes a la hora de realizar la matriculación.

Interrupción del servicio de nombres: La web de la microPYME para que sea fácilmente accesible mediante su nombre de dominio depende del proveedor de DNS gratuito que le proporciona el servicio. Por ello una interrupción en dicho servicio supondría que la web solamente fuese accesible mediante el uso de la IP pública lo que no es comúnmente conocido, haciendo que los clientes puedan tener problemas de acceso.

Interrupción en el servicio eléctrico: La oficina desde donde se realizan todas las actividades de la compañía depende del suministro eléctrico para su funcionamiento. Sin electricidad tanto las salas donde se encuentran los empleados como el servidor físico dejarían de funcionar dejando la web fuera de servicio. Además aunque las clases se realizan desde dispositivos portátiles que no dependen directamente de estar enchufados a la corriente, sí dependen de la conexión por red al router, lo que supone que se pierda la conexión en estos dispositivos provocando que no se puedan realizar las clases online.

Interrupción del servicio web: El servidor web se aloja en un servidor de manera local por lo que existen varios factores que puedan afectar a dicho servicio. La web puede ser afectada por fallos en el propio software, fallos en la configuración, fallos en el hardware del servidor, indisponibilidad de conectividad, errores humanos o ataques cibernéticos (denegación de servicios, malware, etc ...)

Vulnerabilidades:

Falta de redundancia en la conectividad a internet: Si la microPYME no tiene una conexión a internet secundaria o medidas de respaldo, una pérdida de conectividad a internet prolongada podría dejar a la empresa sin acceso a los recursos y servicios en línea necesarios para llevar a cabo las clases o el acceso a la página web. Esto podría resultar en la insatisfacción de los alumnos y la pérdida de ingresos.

Falta de redundancia del servicio de nombres (DNS): La microPYME al depender de un único proveedor de DNS de carácter gratuito, es susceptible a pérdidas del servicio dejando a la empresa sin acceso a la web mediante su nombre de dominio.

Falta de redundancia de la infraestructura eléctrica: La microPYME depende de la energía eléctrica para alimentar los equipos y dispositivos necesarios para la impartición de clases en línea. La falta de un suministro eléctrico confiable y la ausencia de un sistema de respaldo, como un generador o baterías de respaldo, podrían interrumpir las operaciones y generar pérdida de tiempo y recursos.

Falta de redundancia de datos: La empresa no realiza copias de seguridad por lo que en caso de ser afectada por una pérdida de los datos no sería capaz de recuperarlos provocando una interrupción de sus servicios.

6.2.7 Análisis de impacto

Debido al modelo de negocio de la PYME, los ingresos que recibe la empresa se producen enteramente por las matriculaciones de los alumnos por lo que es importante mantener un número alto de alumnos matriculados cada año. Por ello para realizar el análisis de impactos, se ha tenido en cuenta el impacto reputacional por encima del económico ya que este está afectado directamente por la reputación del servicio que se ofrece.

| Impacto | Pérdida reputacional |
|---------|---|
| Bajo | No hay pérdida |
| Medio | Pérdida de hasta el 20% de los clientes |
| Alto | Pérdida mayor del 20% de los clientes |

Tabla 5: Tabla de calificación del impacto según la pérdida reputacional

Se define como “A” al único área de negocio que es el de la educación online.

A_1: Proceso de negocio de las clases online.

A_2: Proceso de la web educativa.

A_3: Proceso de matriculación.

A_4: Proceso de gestión interna.

Para poder cuantificar el impacto, la prioridad y los tiempos se ha realizado una entrevista con el director de la microPYME. Tras la entrevista y en base a sus respuestas se han llegado a las siguientes conclusiones:

Debido al hecho de ser una empresa pequeña, todo tipo de gestión interna no sufre de demasiados problemas ya que se pueden adaptar a todo tipo de problemas y a la situación de cada uno de los empleados. Por ejemplo en el caso de no disponer del equipo portátil, siempre puede apuntar toda gestión realizada durante ese tiempo en papel y posteriormente trasladarlo al portátil.

Para la matriculación, el pago se realiza mediante transferencia bancaria por lo que lo más importante del proceso es el registro del pago y el registro en la web. El registro del pago se puede consultar en la propia cuenta bancaria o se puede apuntar manualmente para posteriormente añadirlo al archivo del portátil.

Este proceso es importante ya que de él dependen los ingresos de la empresa pero al tratarse de un proceso simple, con facilidad de utilizar métodos alternativos y sobre todo transparente para el usuario la pérdida del servicio no supone un gran impacto siempre y cuando se tenga cuidado de no perder los datos del proceso.

El registro en la web depende de la propia web y a su vez, el proceso de negocio de la web educativa es una parte importante del negocio ya que es donde los profesores suben el contenido de las materias y los alumnos acceden a ellas y realizan las entregas de sus tareas. Por ello es necesario que la web esté habilitada el mayor tiempo posible aunque no se considera grave que haya caídas puntuales.

Por último el proceso que se considera el más importante es el de las clases online ya que son la cara de la empresa y lo que los clientes buscan al contratar sus servicios. Que se pierdan las clases periódicamente o de manera prolongada supone un grave problema para la empresa y es algo a evitar a toda costa.

Teniendo en cuenta estas conclusiones se considera:

Que el negocio más prioritario es el de las clases online. Estas clases podrían sufrir caídas pero deben ser poco habituales y con una duración corta. Los datos proporcionados en las clases se consideran menos importantes ya que los profesores pueden proporcionarlos de nuevo posteriormente.

La web educativa se considera con prioridad media ya que no es necesario que se consulte diariamente y siempre y cuando los períodos de caída no sean demasiado altos ni frecuentes no afecta muy negativamente a la empresa. En cambio los datos de esta web sí que son algo más importantes ya que ahí se almacenan las tareas de los alumnos así como las correcciones y materiales proporcionados por los profesores. Estos datos pueden volver a ser subidos por parte de los profesores y alumnos pero es importante que no suceda con frecuencia.

Después se considera también con prioridad media el proceso de matriculación. Normalmente la matriculación no afecta directamente al cliente ya que aunque el servicio esté caído mientras no haya pérdida de los datos de matriculación no supone un problema para una vez reestablecido el servicio se pueda seguir realizando la gestión.

Por último el proceso menos importante, y por ello el menos prioritario es el proceso de gestión interna. Al tener tan pocos trabajadores existe cercanía y conocimiento de la situación de cada uno por lo que aunque el servicio no esté disponible pueden seguir realizando las gestiones por otros medios sin que se vean afectados. Con respecto a los datos de estas gestiones aunque sí tienen más importancia que la disponibilidad del servicio, también pueden ser recuperados fácilmente hablando con el empleado del que se necesiten los datos.

| Área de negocio | Proceso | Prioridad | RTO | RPO |
|-----------------|---------|-----------|----------|----------|
| A | A_1 | Alta | 1 Hora | 1 Día |
| A | A_2 | Media | 1 Semana | 1 Día |
| A | A_3 | Medio | 1 Semana | 1 Hora |
| A | A_4 | Baja | 1 Mes | 1 Semana |

Tabla 6: Tabla de análisis de impacto

6.2.8 Recomendaciones

Para evitar y mitigar la pérdida de la información tanto de los procesos de gestión interna como matriculación o contenido de la página web y su base de datos se recomienda la realización de copias de seguridad de manera regular que pueden ser almacenadas en la nube. Al no disponer de una cantidad demasiado grande de información es posible almacenar todos esos datos en las cuentas cloud de bajo coste asociadas a cada trabajador, donde se almacenarán los datos que se utilicen por estos trabajadores. También existirá una copia a nivel del ordenador “servidor” de la empresa en otra cuenta diferente.

En cuanto al problema eléctrico la recomendación es instalar un sistema de alimentación ininterrumpida (SAI). Como solo es necesario alimentar tres dispositivos (Router, dispositivo de red redundada y Servidor físico) no se requiere mucha potencia y hay soluciones que no suponen un coste muy elevado y pueden cubrir esta necesidad. El consumo medio de estos dispositivos es de unos 530 W (500 W la torre, 10 W el dispositivo de red redundada y 20 W el router aproximadamente) proporcionando unos 15 min de carga, tiempo suficiente para cambiar a los métodos alternativos.

Para mitigar el impacto de la pérdida de red se propone utilizar en caso de fallo de la red fija durante una clase un dispositivo con acceso a una red móvil que se pueda levantar de manera rápida y así poder cubrir las clases. A su vez, esta red se utilizará para continuar con la disponibilidad de la página web, levantando una web secundaria de bajo recursos en el dispositivo que provee la red móvil donde se avise de la caída del servicio y se indique un método de contacto en caso de ser necesario.

Para cubrir fallos en el servicio de DNS y la parte del servicio web durante el uso de esta red móvil es posible utilizar un servicio de DDNS (DNS dinámico) lo que soluciona temporalmente la disponibilidad de la web. Existen servicios de DDNS gratuitos o de bajo coste. Los DDNS resuelven como dirección IP aquella que el usuario indica que está operativa en el momento, siendo esta la IP fija del servidor o la IP fija asignada a la red móvil. Esto tiene que estar contemplado por el propio servidor web, implementando el código proporcionado por el proveedor del DDNS para actualizar su IP en tiempo real.

La mayor parte de los mecanismos contemplados entrará a funcionar de forma automática y transparente para los profesores, salvo la necesidad de conectar a la red móvil alternativa en caso de pérdida de conectividad. Habrá que instruir a los profesores en cómo actuar en caso de pérdida de internet por cable, y refrescar periódicamente, mediante ejercicios sin alumnos. En una etapa posterior se puede evaluar automatizar este aspecto también, si se producen disruptiones en frecuencia o impacto suficiente del proveedor de internet por cable, mediante la colocación de un encaminador con SIM.

Por último es importante que la implementación de las soluciones quede bien documentada desde su implementación hasta su manual de uso y pruebas realizadas.

Se debe establecer un plan de pruebas periódico, al menos una vez al año, que el responsable de informática debe ejecutar a fin de comprobar que los mecanismos (respaldo de datos, SAI, acceso móvil y operativa DDNS) y del conocimiento adecuado de los profesores (formación y ejercicios periódicos).

7 PRUEBAS Y VALIDACIÓN

7.1 Demostrativo para resiliencia de Datos

Primero, ya que el servidor es un equipo Windows, se debe crear un script en powershell que realice la copia de seguridad de los datos deseados (Consultar anexo [COPIAS DE SEGURIDAD](#)). Despues es necesario programar una tarea para que la copia se realice periódicamente (Consultar anexo [CONFIGURACIÓN DE TAREAS PROGRAMADAS EN DISPOSITIVOS WINDOWS](#)). Con ello ya tendríamos configurado la realización de copias de seguridad de manera periódica de los datos de interés en el servidor.

El siguiente paso sería poder almacenar esas copias en un lugar diferente y accesible, en este caso se utilizará el servicio de nube gratuito de Google Cloud. Para ello se debe crear una cuenta gratuita de Google para tener tanto un correo como un almacenamiento gratuito en la nube. Para crear la cuenta se deben seguir los pasos indicados en "<https://support.google.com/accounts/answer/27441?hl=es>" Una vez esté la cuenta creada, se necesita crear y configurar un proyecto para poder almacenar las copias de seguridad (Consultar anexo [CONFIGURACIÓN DE GOOGLE CLOUD PARA ALMACENAMIENTO DE COPIAS DE SEGURIDAD](#)). Debemos añadir un segundo factor de autenticación como método adicional de seguridad. Podemos encontrar como hacerlo en "<https://support.google.com/accounts/answer/185839>".

Una vez configurado y disponiendo de las credenciales, se debe crear un script en powershell que realice la subida de las copias de seguridad al drive (Consultar anexo [SUBIDA DE COPIAS DE SEGURIDAD A GOOGLE DRIVE](#)). Al igual que con el script que realiza las copias, es necesario crear una tarea periódica que se ejecute justo después de la copia de seguridad para asegurarse que se sube la última versión.

Como el almacenamiento de las cuentas gratuitas de Google Cloud es limitado es necesario mantener un número pequeño de copias en la nube, por ello es necesario crear otro script que compruebe el número de archivos que hay subidos y en caso de superar el número de copias determinado por la empresa (recomendable siempre que sea posible tener al menos 2) que elimine la copia más antigua (Consultar anexo [ROTADO DE COPIAS DE SEGURIDAD EN GOOGLE DRIVE](#)). Al igual que con los anteriores se debe crear una tarea periódica, en este caso antes de que se realice la subida de la copia, para así mantener controlado el uso del almacenamiento en la nube.

Después, es necesario también disponer de un script para recuperar la copia de seguridad en caso de requerirse (Consultar anexo [DESCARGA DE COPIAS DE SEGURIDAD EN GOOGLE DRIVE](#)). Este script solo se ejecuta en momentos puntuales por lo que no requiere crear una tarea para él.

Por último, una vez recuperada la copia de seguridad es necesario aplicarla en el servidor. Para ello se crea otro script que extraiga todos los archivos y los coloque en su respectiva ruta original (Consultar anexo [RESTAURAR LOS DATOS DE LA COPIA DE SEGURIDAD](#)).

7.2 Demostrativo para resiliencia Eléctrica

Utilizaremos el SAI “APC Back-UPS BX1600MI-GR” (*APC Back-UPS BX1600MI-GR*, n.d.). Instalaremos el SAI cerca de donde se encuentra el ordenador y el dispositivo de backup de red, que en el caso de la microPYME desarrollada será en la habitación del informático.

Se debe conectar la entrada de alimentación del SAI a una toma de corriente cercana. Se conectarán todos los dispositivos (en este caso el ordenador y el dispositivo móvil al SAI en una de las 4 conexiones de salida).

Una vez conectados ambos dispositivos, encenderemos el ordenador en primer lugar. En segundo lugar se encenderá el SAI desde el botón de encendido en la parte frontal. Verificar que tanto el ordenador como el dispositivo móvil están recibiendo electricidad a través del SAI.

Instalar el software asociado al SAI específico. En nuestro caso, instalaremos PowerChute, software asociado a esta versión de SAI. Para instalarlo, se conecta el SAI al ordenador mediante el cable de datos. Vamos a la web “<http://www.apc.com/tools/download>” y buscamos por el modelo que estamos instalando “BX1600MI-GR”. Una vez en la web, descargamos el primer software “Software, PowerChute Serial Shutdown, v1.0, unattended, graceful shutdown, UPS Monitoring & Configuration, Energy Management”.

Software, PowerChute Serial Shutdown, v1.0, unattended, graceful shutdown, UPS Monitoring & Configuration, Energy Management

Software, PowerChute Serial Shutdown, v1.0, unattended, graceful shutdown, UPS Monitoring & Configuration, Energy Management

SFPCSS10

Operating System: Windows 8, Windows 10

Updated on: 03/03/2023

[Documentation](#)¹²

[Download](#)

PowerChute Personal Edition v3.1

PowerChute Personal Edition v3.1

SFPCPE31

Operating System: Windows 10

Updated on: 11/06/2019

[Documentation](#)⁵

[Download](#)

Figura 11: Página de descarga de PowerChute con las distintas versiones

Para ver la instalación paso a paso, consultar Anexo [INSTALACIÓN PASO A PASO POWERCHUTE](#).

Con todo instalado, ya tendremos el SAI montado y con el software necesario para su funcionamiento instalado.

Vamos a configurar el SAI para notificar los cortes o caídas eléctricas. Se va a configurar de tal forma en la que, en caso de detectarse pérdida en la red eléctrica, se envíe un Email notificando a todo el personal de la empresa, y se envíe un mail a la automatización de despliegue de la web de resiliencia, con el fin de reducir el consumo eléctrico. Se creará una copia de seguridad de los datos del dispositivo y, posteriormente, se apagará el servidor de manera controlada automáticamente. Para ver el proceso de configuración con estos requisitos, ver Anexo [CONFIGURACIÓN AUTOMATIZACIONES SAI](#)

Con el fin de mantener el funcionamiento óptimo y correcto del sistema, se deberá seguir el Anexo [GUIA DE PRUEBAS SEMESTRALES DE FUNCIONAMIENTO DEL SAI](#). Se deberán realizar 2 pruebas anualmente para comprobar:

- El correcto funcionamiento de las automatizaciones configuradas para la microPYME.
- La comprobación del estado del SAI y de las baterías, con el fin de mantener el estado óptimo de los dispositivos físicos.

A su vez, y con el fin de que todo el personal de la empresa se encuentre al tanto del funcionamiento de resiliencia se deberá realizar y seguir el Anexo [FORMACIÓN ANUAL RELACIONADA CON EVENTOS DISRUPTIVOS](#).

7.3 Demostrativo para resiliencia de Red

7.3.1 Demostrativo de resiliencia de red en clases online

Para poder continuar con las clases online en caso de una interrupción en el servicio de red primero necesitaremos un dispositivo móvil con una tarifa de datos contratada. Debe configurarse como punto de acceso (Consultar anexo [CONFIGURACIÓN DE DISPOSITIVO MÓVIL COMO PUNTO DE ACCESO](#)), en este caso usando un Android, para que sea capaz de proveer de red a los portátiles de los profesores. Después hay que añadir como conexión esta nueva red en los propios portátiles (consultar anexo [CONFIGURACIÓN DE RED EN DISPOSITIVOS PORTÁTILES](#)). Es importante que esta red quede guardada y recordada por los equipos para que cuando se active esta red secundaria los equipos y desconectar el cable de red, automáticamente se conecten y así reducir el tiempo sin conectividad y la necesidad de tener que realizar esta configuración con cada interrupción de la red.

7.3.2 Demostrativo para resiliencia de red en aplicación web

Para poder cubrir la pérdida de la web a causa del fallo de red es necesario disponer de un contrato de red móvil con servicio de IP fija o pública, además para poder realizar correctamente la resolución de nombres de dominio de manera rápida y eficaz es necesario utilizar un proveedor de DDNS. Primero se configura el dispositivo móvil como punto de acceso (Consultar anexo [CONFIGURACIÓN DE DISPOSITIVO MÓVIL COMO PUNTO DE ACCESO](#)). Después utilizando para el demostrativo la aplicación android de KSWEB creamos una web con un mensaje simple que indique la indisposición de la página principal y al menos una forma de contacto en caso de necesidad (Consultar anexo [CREACIÓN DE PÁGINA WEB SECUNDARIA](#)) y lo configuramos dentro de la consola del proveedor de DDNS para que se muestre esta nueva web en lugar de la anterior.

8 CONCLUSIONES

8.1 Conclusiones del trabajo

El objetivo del presente Trabajo de Fin de Máster (TFM) es analizar posibles maneras de añadir resiliencia dentro del campo de las microPYMEs y que puede ser aplicable en el ámbito del hogar. Se ha definido cómo el perímetro del análisis la resiliencia en tres de las áreas: red, electricidad y datos.

Una vez realizado el análisis de los problemas y sus posibles soluciones en casos genéricos se ha hecho una aplicación a un caso práctico basado en una microPYME típica, que se ha descrito de forma detallada, pudiendo trasladar los conocimientos adquiridos a dicho caso. Para este caso práctico se ha realizado un análisis detallado de las amenazas y desafíos a la continuidad de la microPYME para poder realizar un documento de análisis de impacto de negocio (BIA) que permita abordar los problemas de resiliencia sobre la empresa. Posteriormente se han formulado propuestas de mecanismos para dotar de resiliencia frente a las vulnerabilidades de conectividad, servicio de nombres y electricidad.

El proyecto ha sido desarrollado completamente por dos alumnos durante todas las etapas del desarrollo, realizando tanto tareas conjuntas como haciendo reparto del trabajo para después realizar una puesta en común y llegar a una solución satisfactoria y consensuada por ambos.

Por último, se han cumplido los objetivos propuestos durante el anteproyecto siendo estos adaptados y mejorados para el desarrollo del proyecto dejando posibilidad de realizar mejoras a futuro así como expandir el alcance del proyecto propuesto en el alcance.

8.2 Conclusiones personales

A día de hoy, existe una gran cantidad de información sobre los riesgos de seguridad a los que se encuentran expuestas las pymes. Entre las prioridades no se encuentran la seguridad o la creación de resiliencia, concluyendo que la resiliencia es un desafío crítico para las microPYMEs y hogares. Esta información indica que las PYMEs y hogares están muy expuestos al no tener personal con conocimiento para la protección o recursos que poder destinar a mejorar su infraestructura y resiliencia.

Se ha determinado, que existe documentación para la mejora de la resiliencia en hogares y MicroPYMEs, pero que se encuentra muy separada por categorías específicas dependiendo del elemento que quieras proteger, no encontrando distintas opciones de manera sencilla.

Uno de los objetivos principales fue abordar estos desafíos para poder ofrecer una solución accesible para mejorar la resiliencia de las microPYMEs y los hogares. Después de haber realizado un análisis de posibles puntos de ruptura, y ver la gran cantidad de ellos en estas infraestructuras, se han destacado 3 de los principales. Esto ha permitido investigar estos puntos de fallo, conocer mejor el entorno de micropymes y llegar a poder realizar un plan de acción factible para llevar a cabo en estas situaciones.

Por último, ambos integrantes queremos destacar la aplicación de los conocimientos adquiridos durante el máster, llegando a poder aplicar estos conocimientos no solo dentro de un marco lectivo, sino de un marco realista de infraestructuras de micropymes y hogares.

9 TRABAJOS FUTUROS

En este capítulo se recogen los trabajos futuros que han surgido a partir del trabajo desarrollado.

Aún existen áreas de mejora que se pueden abordar en el futuro para expandir el trabajo desarrollado.

En primer lugar, se propondrá la implementación de un cifrado sólido para las copias de seguridad, asegurando la confidencialidad de los datos almacenados. Además de la posibilidad de agrupar y mejorar los scripts que realizan las copias de seguridad y las gestionan.

Se plantea la creación de un demostrativo de red para mejorar la resiliencia. La integración de todos los demostrativos en una solución completa permitirá evaluar de manera práctica el comportamiento del sistema completo.

A su vez, se busca aumentar el alcance añadiendo más elementos de resiliencia del árbol de dependencia, ya que para el alcance del proyecto se han contemplado electricidad, datos y red.

Por último, se enfoca en añadir elementos de seguridad adicionales a las soluciones implementadas, así como a los demostrativos. Estas mejoras y desarrollos futuros fortalecerán la solución, garantizando su resiliencia y seguridad ante desafíos tecnológicos cambiantes.

10 DECLARACIÓN DE COLABORACIÓN

El trabajo se ha dividido de forma equitativa entre ambos autores.

Cada párrafo en la memoria ha sido bien escrito, revisado, comentado y discutido por ambos autores. Lo mismo se aplica a las actividades para la creación de la memoria, incluida búsqueda documental, análisis y estructuración de la información y planteamiento de soluciones, así como de los demostradores: si un autor ha efectuado una actividad el otro la ha revisado y rematado, y estos roles se han distribuido equitativamente en el proyecto.

Erik ha sido el preparador inicial del demostrativo relacionado con las copias de seguridad y Javier el demostrativo relacionado con pérdida de electricidad y tanto la investigación, cómo el desarrollo del problema general y la aplicación específica se han preparado de forma conjunta.

11 APÉNDICES

11.1 BIBLIOGRAFÍA

. (2023, June 13). . - YouTube. Retrieved July 14, 2023, from

https://download.schneider-electric.com/files?p_Doc_Ref=SPD_BU-UM-990-6291_ES&p_enDocType=User+guide&p_File_Name=BU-UM-990-6291B-ES.pdf

Alonso, R. (2021, September 8). *Medidas para convertirse en una empresa resiliente*. Think Big Empresas. Retrieved July 4, 2023, from

<https://empresas.blogthinkbig.com/como-lograr-una-empresa-mas-resiliente/>

APC Back-UPS BX1600MI-GR. (n.d.). APC. Retrieved July 14, 2023, from

<https://www.apc.com/es/es/product/BX1600MI-GR/apc-backups-1600va-230v-avr-tomas-schuko/>

Ciurans, R. (n.d.). *SAIS MODULARES ¿SON REALMENTE MÁS FIABLES?* Salicru. Retrieved July 5, 2023, from

https://www.salicru.com/files/pagina/72/276/jn003a00_whitepaper-3rc_salicru.pdf

¿Cómo transformar a mi compañía en una organización resiliente? (2021, March 25). EY.

Retrieved July 4, 2023, from

https://www.ey.com/es_es/resilient-enterprise/rebuild-a-lean-company/como-transformar-a-mi-compania-en-una-organizacion-resiliente

COMPONENTE 13. (2021, June 16). La Moncloa. Retrieved July 5, 2023, from

<https://www.lamoncloa.gob.es/temas/fondos-recuperacion/Documents/16062021-Componente13.pdf>

¿Cuál es el mejor grupo electrógeno para tu vivienda? Y como escogerlo. (2019, May 10).

Generadores Eléctricos. Retrieved July 5, 2023, from

<https://www.generadoreselectricos.org/blog/mejor-grupo-electrogeno-para-la-vivienda/>

Froehlich, A. (2022, November). *How to set up backup internet connections for home offices*.

TechTarget. Retrieved July 3, 2023, from

<https://www.techtarget.com/searchnetworking/answer/How-to-set-up-backup-internet-connections-for-home-offices>

Generador Electrico Gasolina 5500W Leelbox. (n.d.). Amazon. Retrieved July 15, 2023, from

<https://www.amazon.es/Generador-Electrico-Leelbox-Emergencia-Dispositivos/dp/B0BM42Y4ZP>

IEC 27001 Standard – Information Security Management Systems. (2022). ISO. Retrieved July 21, 2023, from <https://www.iso.org/standard/27001>

ISO 22301:2019 - Security and resilience — Business continuity management systems — Requirements. (2019). ISO. Retrieved July 21, 2023, from

<https://www.iso.org/standard/75106.html>

ISO 22317:2021 - Security and resilience — Business continuity management systems — Guidelines for business impact analysis. (2021). ISO. Retrieved July 21, 2023, from

<https://www.iso.org/standard/79000.html>

LEICKE Panel Solar. (n.d.). Amazon. Retrieved July 15, 2023, from

<https://www.amazon.es/LEICKE-Monocristalino-Eficiencia-Resistencia-Jard%C3%ADN/dp/B0BYS3V334>

Plan Contingencia Continuidad Negocio | Empresas. (n.d.). INCIBE. Retrieved June 26, 2023, from

<https://www.incibe.es/empresas/que-te-interesa/plan-contingencia-continuidad-negocio>

Plan de contingencia y continuidad de negocio. (n.d.). INCIBE. Retrieved June 26, 2023, from

https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_plan_de_contingencia_y_continuidad_de_negocio.pdf

Plan de Recuperación, Transformación y Resiliencia Gobierno de España. (n.d.). Plan de Recuperación, Transformación y Resiliencia Gobierno de España. Retrieved July 21,

2023, from <https://planderecuperacion.gob.es/>

Policy routing, multihoming and all that jazz « I. (2012, October 7). backreference.org.

Retrieved July 3, 2023, from

<https://backreference.org/2012/10/07/policy-routing-multihoming-and-all-that-jazz/index.html>

Preguntas frecuentes acerca de grupos electrógenos estacionarios PRAMAC. (n.d.). Pramac.

Retrieved July 5, 2023, from https://www.pramac.com/es_ES/aboutstationarygenerators

¿Qué es un plan de continuidad de negocio (BCP)? (2020, November 25). IBM. Retrieved July 5, 2023, from <https://www.ibm.com/es-es/services/business-continuity/plan>

Qué es un SAI y tipos de SAI (Online, Interactivo, Offline, AVR). (n.d.). Rackonline. Retrieved

July 5, 2023, from <https://www.rackonline.es/content/que-es-un-sai-y-tipos-de-sai>

Rodríguez, E. (2022, November 17). *Qué SAI comprar, ¿cuál es mejor?* Xataka. Retrieved July 5, 2023, from

<https://www.xataka.com/seleccion/guia-compra-sai-que-como-funcionan-tipos-13-sistema-s-alimentacion-ininterrumpida-39-euros>

Romero, M., & García, R. M. (2021, November 4). *¿Qué es la resiliencia empresarial?*

ExpokNews. Retrieved July 3, 2023, from

<https://www.expoknews.com/que-es-la-resiliencia-empresarial/>

Silveira, J. (n.d.). *Nighthawk 4G LTE Router - LAX20.* Netgear. Retrieved July 15, 2023, from

<https://www.netgear.com/home/mobile-wifi/routers/lax20/>

SPS 1100 ONE. (n.d.). Salicru. Retrieved July 15, 2023, from

<https://www.salicru.com/ve-es/sps-1100-one-a-1.html>

Sylkat. (2022, February 3). *AWebServer (Http Web Server A - Apps en Google Play.* Google Play.

Retrieved July 21, 2023, from

https://play.google.com/store/apps/details?id=com.sylkat.apache&hl=es_MX

11.2 CONFIGURACIÓN DE TAREAS PROGRAMADAS EN WINDOWS

Para poder ejecutar un script periódicamente es necesario programar una tarea en Windows. Para ello accedemos al “Programador de tareas de Windows”.

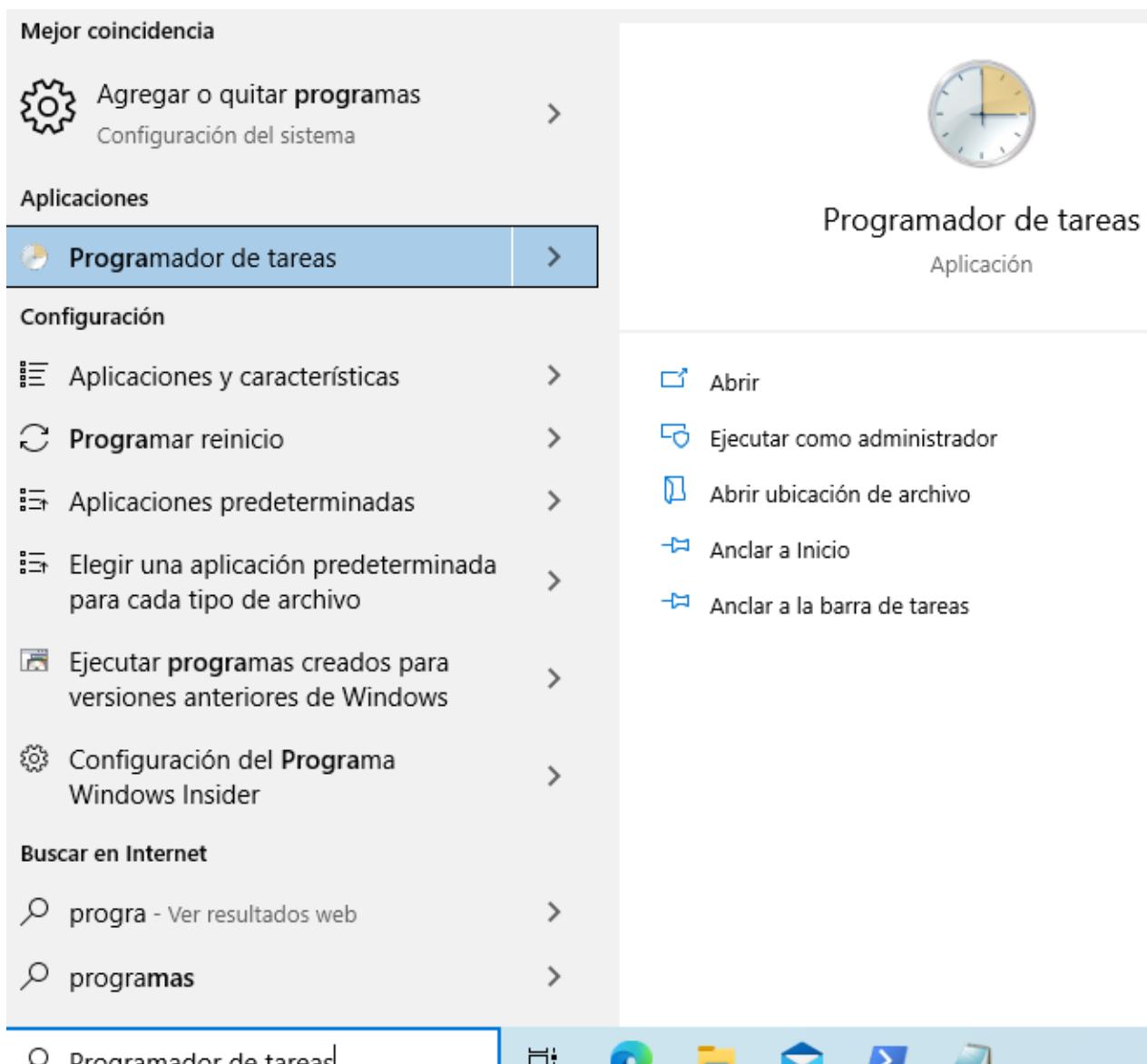


Figura 12 - 11.2 Programador de tareas

Una vez dentro seleccionamos “Crear tarea...”.

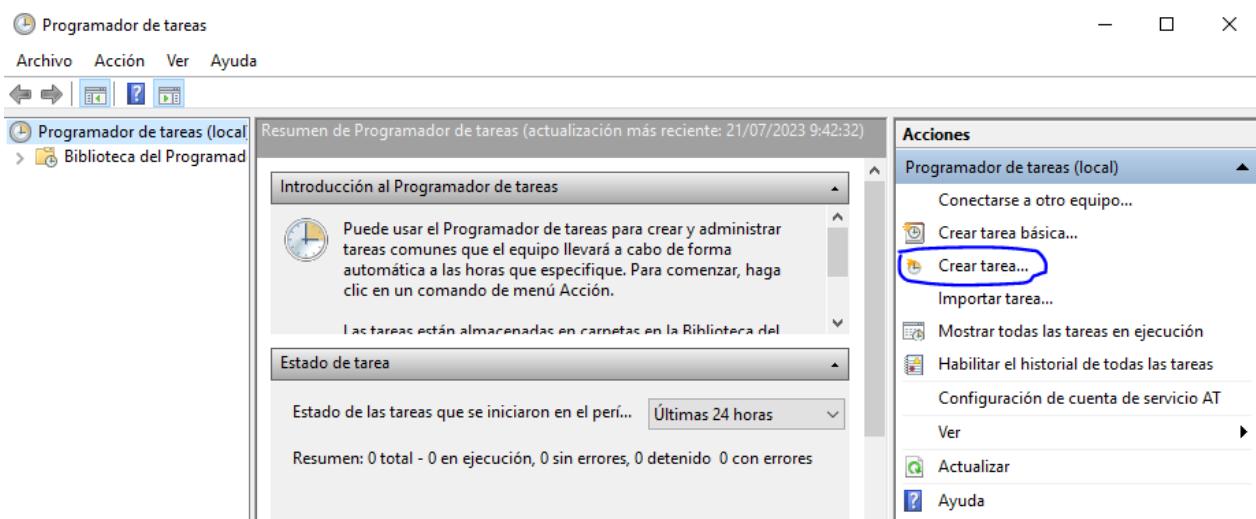


Figura 13 - 11.2 Elementos para crear nueva tarea

Seleccionamos un nombre para la tarea y le asignamos una descripción. Se marcan los campos de “Ejecutar tanto sí el usuario inició sesión cómo sí no” y “Ejecutar con privilegios más altos”

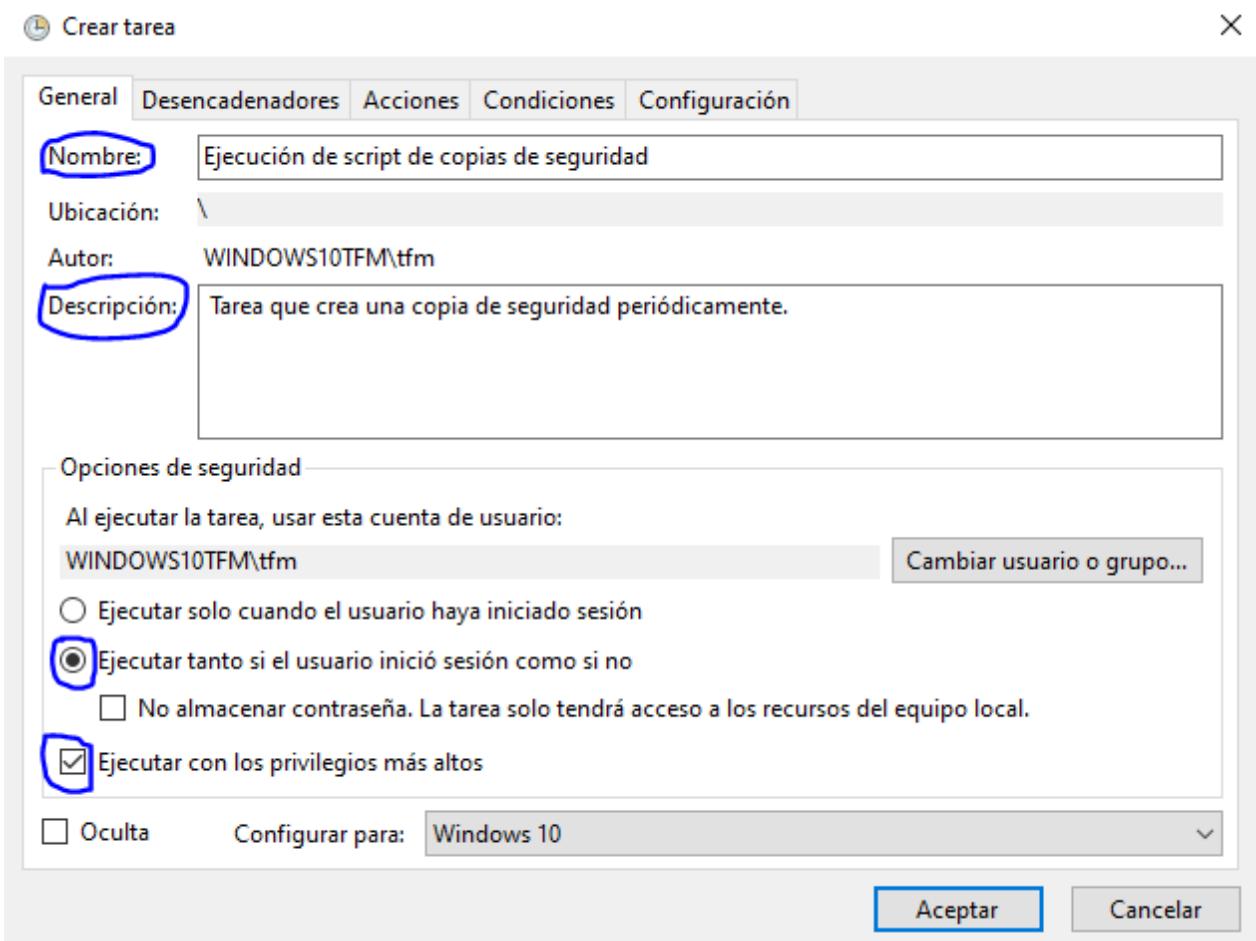


Figura 14 - 11.2 Creación de una nueva tarea

En el apartado de “Desencadenadores” seleccionamos “Nuevo” y modificamos las opciones según la necesidad de la tarea.

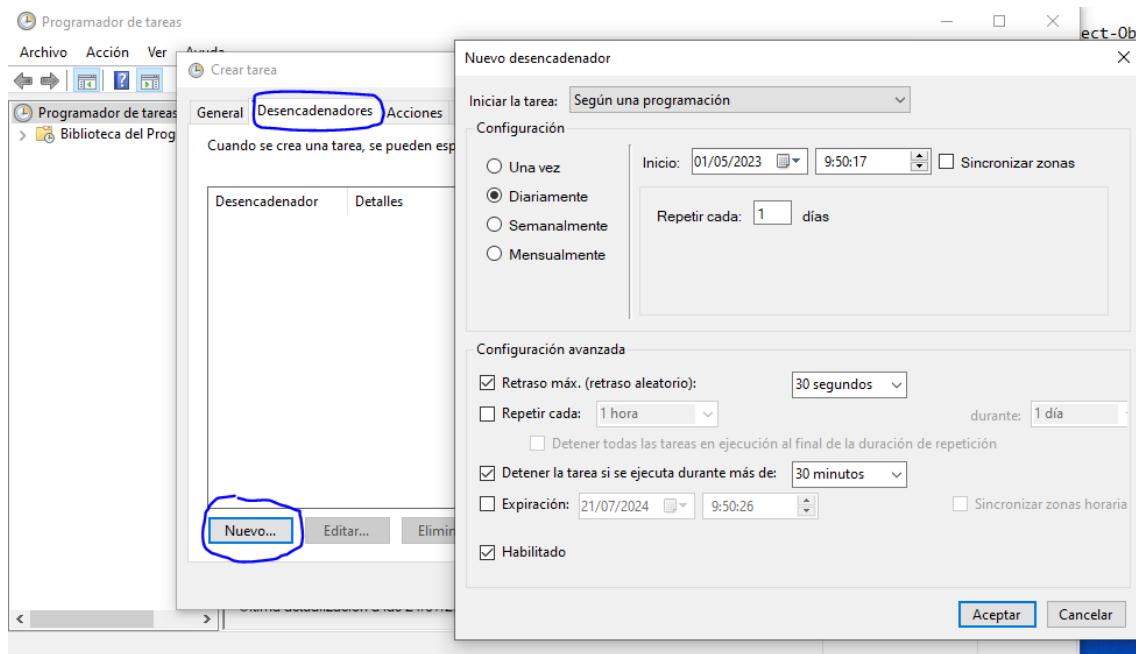


Figura 15 - 11.2 Desencadenador de tarea

En el apartado “Acciones” seleccionamos “Nueva” y especificamos como acción “Iniciar un programa” y en “Programa o script” Añadimos la ruta de ejecución de PowerShell
“C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe” y en “Agregar argumentos” añadimos el comando de ejecución del script en PowerShell con
“-command “Path_Del_Script\Nombre_Del_Script.ps1””

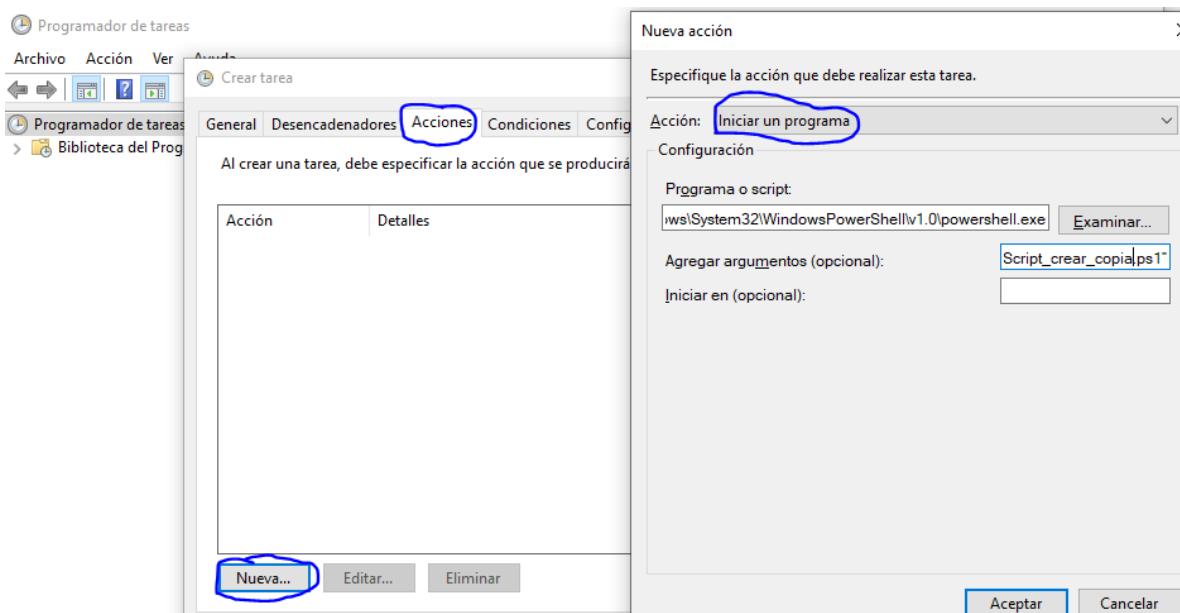


Figura 16 - 11.2 Iniciar un programa desde una tarea

Para comprobar que la tarea se ejecuta correctamente podemos lanzarla manualmente accediendo a “Biblioteca del programador de tareas” seleccionando la tarea que acabamos de crear y haciendo clic en “Ejecutar”

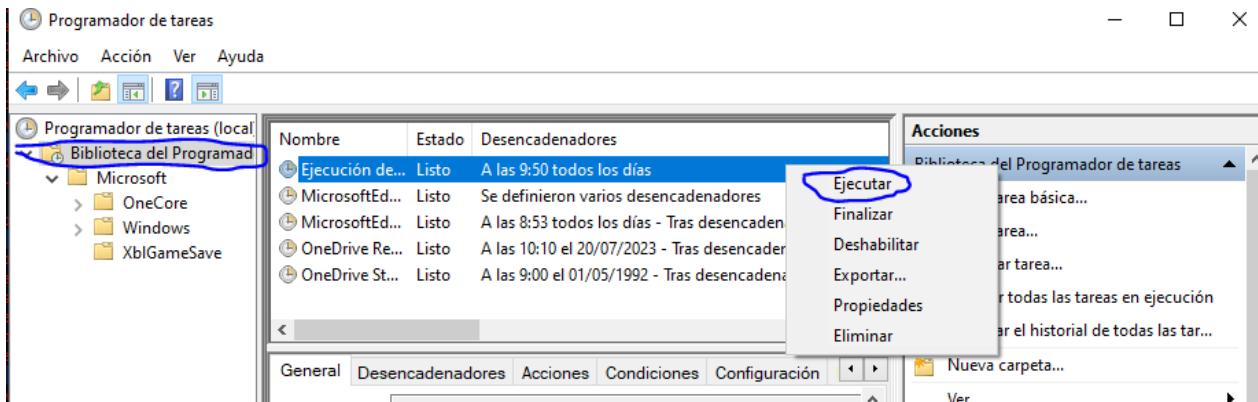


Figura 17 - 11.2 Ejecutar una tarea manualmente

En “Programador de tareas (local)” Podemos observar tanto las ejecuciones manuales como las programadas realizadas.

Introducción al Programador de tareas

Puede usar el Programador de tareas para crear y administrar tareas comunes que el equipo. Las tareas están almacenadas en carpetas en la Biblioteca del Programador de tareas. Para más información, haga clic en un comando en el menú Acción.

Estado de tarea

Estado de las tareas que se iniciaron en el período de tiempo siguiente:

Resumen: 4 total - 0 en ejecución, 4 sin errores, 0 detenido 0 con errores

| Nombre de tarea | Resultado... | Desencadenado por |
|---|--------------|------------------------|
| Ejecución de script de copias de seguridad... | Correcto | Programación de tiempo |
| Ejecución de script de copias de seguridad... | Correcto | |
| Ejecución de script de copias de seguridad... | Correcto | |

Figura 18 - 11.2 Resultados de tareas programadas

11.3 CONFIGURACIÓN DE GOOGLE CLOUD PARA ALMACENAMIENTO DE COPIAS DE SEGURIDAD

Primero instalamos el SDK de Google Cloud mediante “Install-Module GoogleCloud”

```
PS C:\Windows\system32> Install-Module GoogleCloud
```

Figura 19 - 11.3 Comando instalación SDK Google

Se abrirá el instalador, seleccionamos tipo de instalación “Single User” y dejamos el resto de valores por defecto.

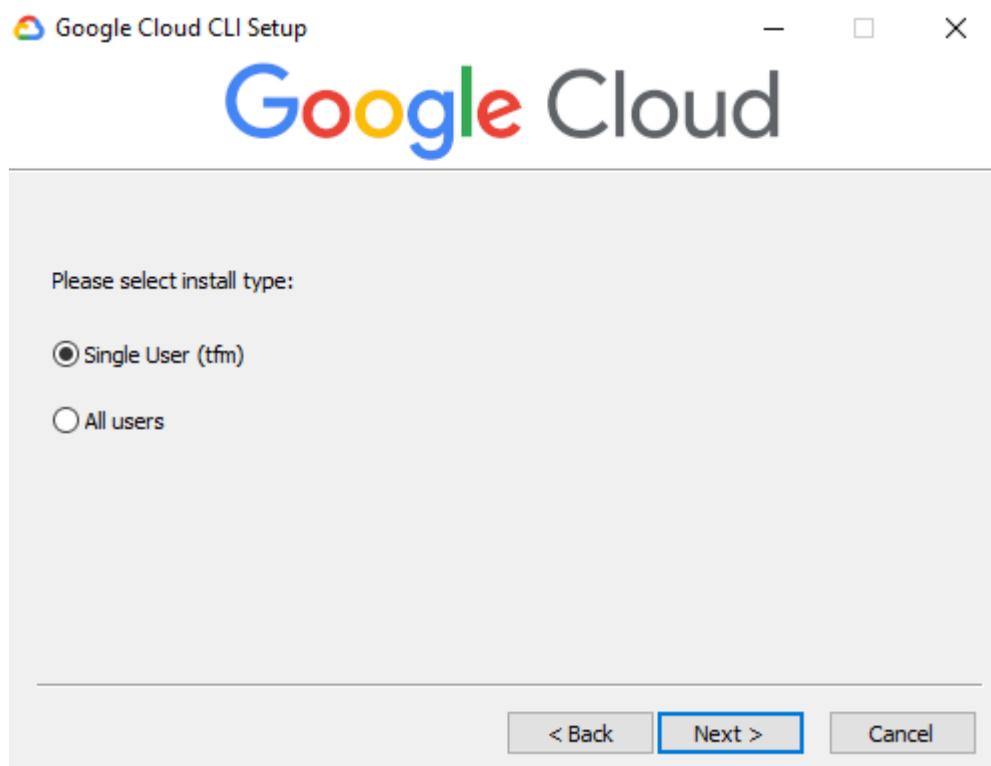


Figura 20 - 11.3 Instalador SDK(1)

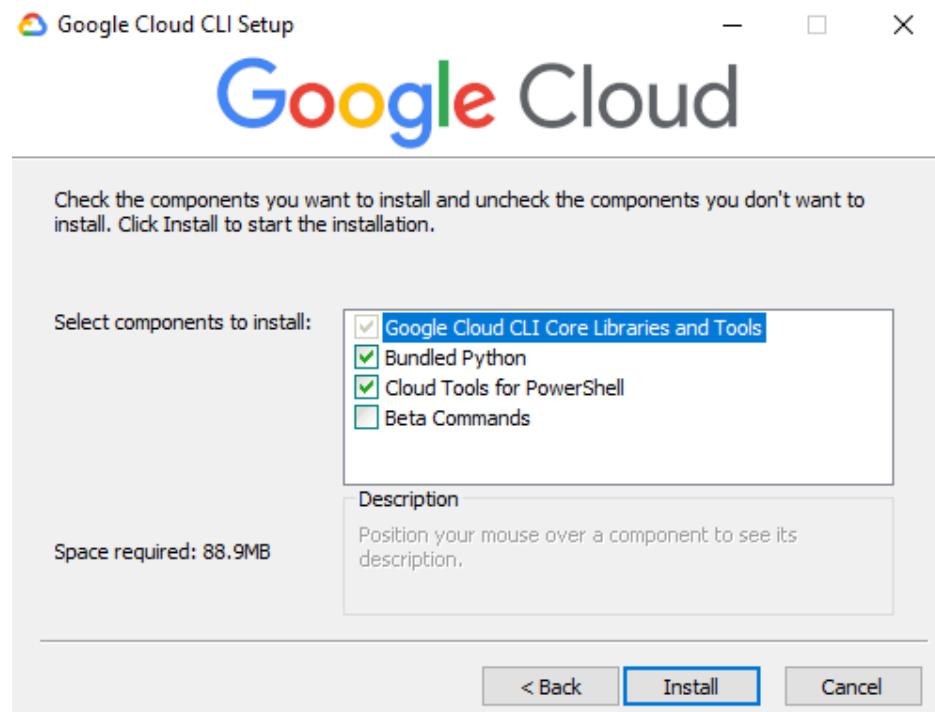


Figura 21 - 11.3 Instalador SDK(2)

Una vez llegado al último paso, elegimos “Install” y esperamos a que termine la instalación.

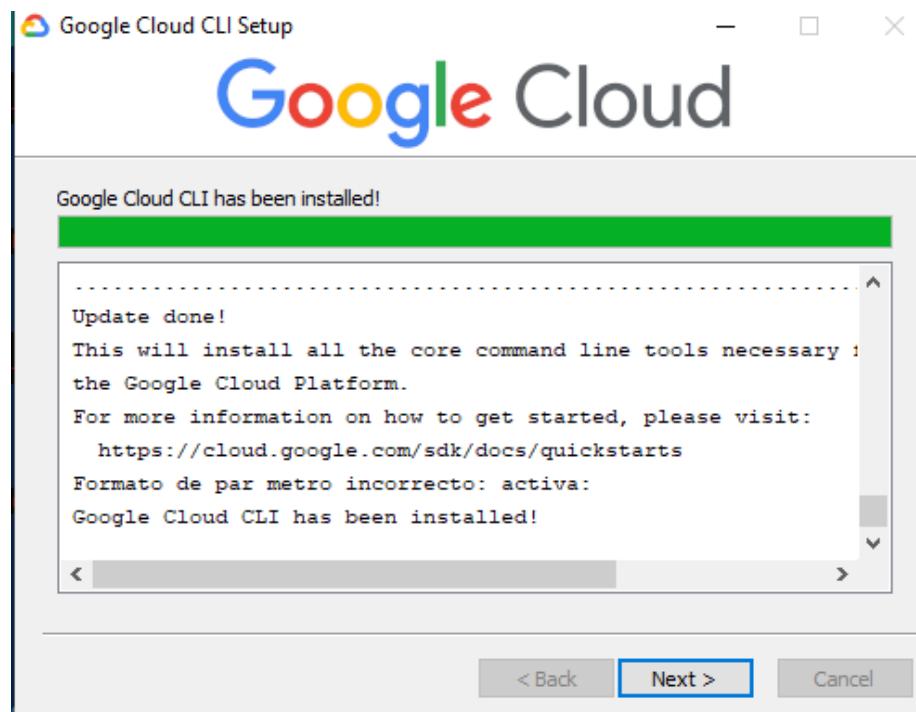


Figura 22 - 11.3 Instalador SDK(3)

Accedemos a la consola de google cloud en “<https://console.cloud.google.com>” y seleccionamos “Crea o selecciona un nuevo proyecto” y “Proyecto nuevo”

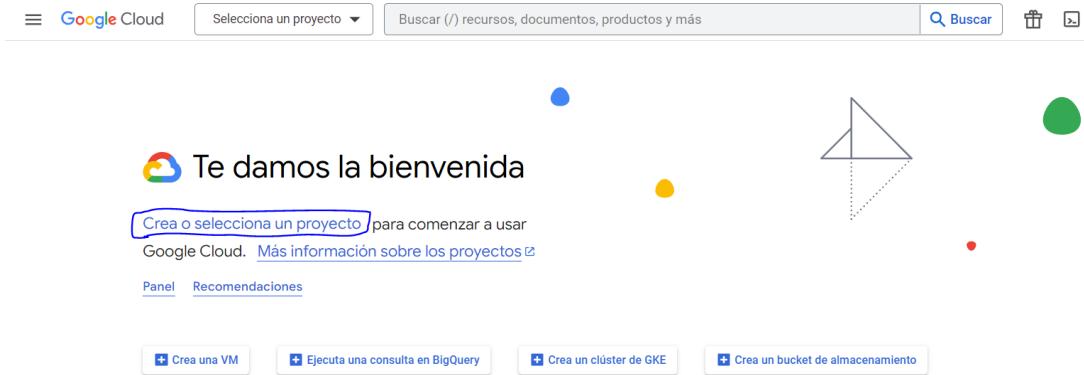


Figura 23 - 11.3 Consola principal Google Cloud



Figura 24 - 11.3 Creación de un nuevo proyecto en Google Cloud

Introducimos el nombre del proyecto y en caso de desearlo editamos el ID de proyecto.

The image shows the 'Proyecto nuevo' (New project) creation form. It includes a warning message about quota limits: 'Tienes 10 projects restantes en tu cuota. Solicita un incremento o borra algunos proyectos.' with a link to 'Más información'. The 'Nombre del proyecto' field is filled with 'TFM|Resiliencia2023'. The 'ID de proyecto' field shows 'tfm-resiliencia2023' with an 'EDITAR' link. The 'Ubicación' field shows 'Sin organización' with an 'EXPLORAR' button. At the bottom are 'CREAR' and 'CANCELAR' buttons.

Figura 25 - 11.3 Datos de nuevo proyecto Google Cloud

Desde PowerShell ejecutamos “gcloud init” y nos solicitará hacer login.

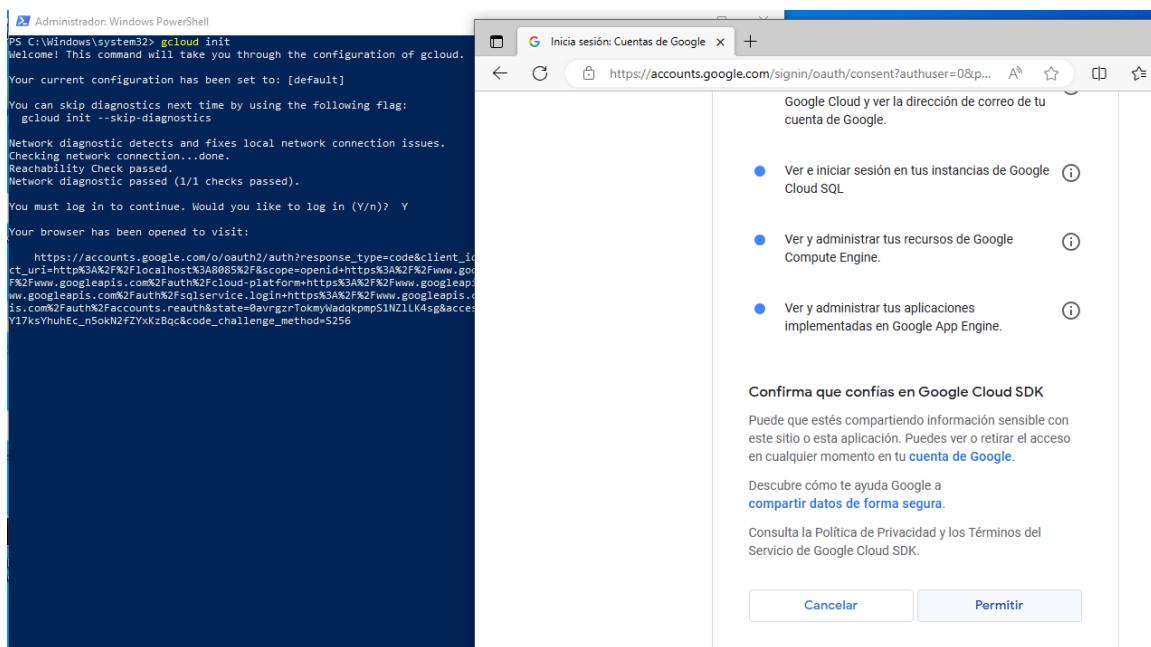


Figura 26 - 11.3 Login desde la máquina a Google Cloud

Una vez aceptemos, nos pedirá que seleccionemos el proyecto.

```
You are logged in as: [tfmresiliencia@gmail.com].  
Pick cloud project to use:  
[1] tfm-resiliencia2023  
[2] Enter a project ID  
[3] Create a new project  
Please enter numeric choice or text value (must exactly match list item): 1  
Your current project has been set to: [tfm-resiliencia2023].  
  
Not setting default zone/region (this feature makes it easier to use  
[gcloud compute] by setting an appropriate default value for the  
--zone and --region flag).  
See https://cloud.google.com/compute/docs/gcloud-compute section on how to set  
default compute region and zone manually. If you would like [gcloud init] to be  
able to do this for you the next time you run it, make sure the  
Compute Engine API is enabled for your project on the  
https://console.developers.google.com/apis page.  
  
Created a default .boto configuration file at [C:\Users\tfm\.boto]. See this file and  
[https://cloud.google.com/storage/docs/gsutil/commands/config] for more  
information about configuring Google Cloud Storage.  
Your Google Cloud SDK is configured and ready to use!  
  
* Commands that require authentication will use tfmresiliencia@gmail.com by default  
* Commands will reference project `tfm-resiliencia2023` by default  
Run `gcloud help config` to learn how to change individual settings  
  
This gcloud configuration is called [default]. You can create additional configurations if you work with multiple accounts and/or projects.  
Run `gcloud topic configurations` to learn more.  
  
Some things to try next:  
* Run `gcloud --help` to see the Cloud Platform services you can interact with. And run `gcloud help COMMAND` to get help on any gcloud command.  
* Run `gcloud topic --help` to learn about advanced features of the SDK like arg files and output formatting  
* Run `gcloud cheat-sheet` to see a roster of go-to `gcloud` commands.  
PS C:\Windows\system32>
```

Figura 27 - 11.3 Selección de proyecto

Creamos el bucket que contendrá nuestras copias de seguridad con “gcloud storage buckets create gs://{nombre}/ --uniform-bucket-level-access”.

```
PS C:\Windows\system32> gcloud storage buckets create gs://tfm_resiliencia_copias_de_seguridad/ --uniform-bucket-level-access
Creating gs://tfm_resiliencia_copias_de_seguridad/...
PS C:\Windows\system32>
```

Figura 28 - 11.3 Creación de un bucket

11.4 INSTALACIÓN PASO A PASO POWERCHUTE

En nuestro caso, instalaremos PowerChute, software asociado a esta versión de SAI. Para instalarlo, se conecta el SAI al ordenador mediante el cable de datos. Vamos a la web “<http://www.apc.com/tools/download>” y buscamos por el modelo que estamos instalando “BX1600MI-GR”. Una vez en la web, descargamos el primer software “Software, PowerChute Serial Shutdown, v1.0, unattended, graceful shutdown, UPS Monitoring & Configuration, Energy Management”.

Software, PowerChute Serial Shutdown, v1.0, unattended, graceful shutdown, UPS Monitoring & Configuration, Energy Management



Software, PowerChute Serial Shutdown, v1.0, unattended, graceful shutdown, UPS Monitoring & Configuration, Energy Management

SFPCSS10

Operating System: Windows 8, Windows 10

Updated on: 03/03/2023

[Documentation¹²](#)

[Download](#)

PowerChute Personal Edition v3.1



PowerChute Personal Edition v3.1

SFPCPE31

Operating System: Windows 10

Updated on: 11/06/2019

[Documentation⁵](#)

[Download](#)

Figura 29 - 11.4 Descarga del programa

Una vez descargado, descomprimimos el archivo.

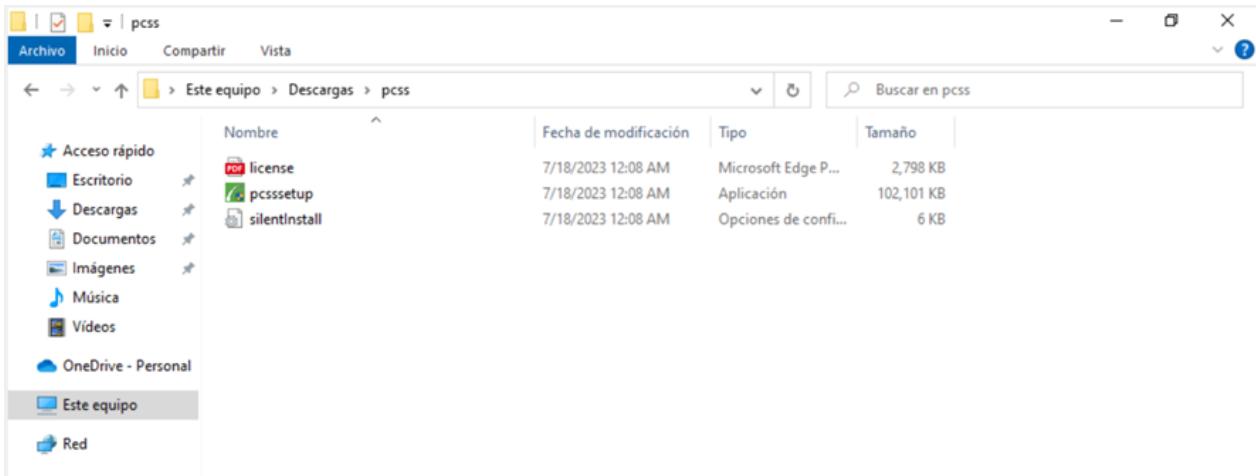


Figura 30 - 11.4 Archivos de programa

Ejecutaremos el archivo “pcsssetup”. Y seguimos paso a paso el instalador. Es posible que no tengamos algunos de los paquetes necesarios para instalar el programa. En este caso, automáticamente nos aparecerá la siguiente pantalla, donde haremos clic en “Aceptar”.



Figura 31 - 11.4 Comprobación/Instalación MV C++ 2017

Continuaremos con el instalador. Cuando se nos pregunte si deseamos que se busque automáticamente un SAI en los puertos, haremos clic en “Si”.

Como tenemos conectado el SAI al pc, haremos clic en “Detección automática”. En caso de no encontrarse, en base al SAI que estamos utilizando, seleccionaremos el modelo “Back-UPS”.



Figura 32 - 11.4 Selección del SAI

Seleccionaremos USB como puerto de conexión.

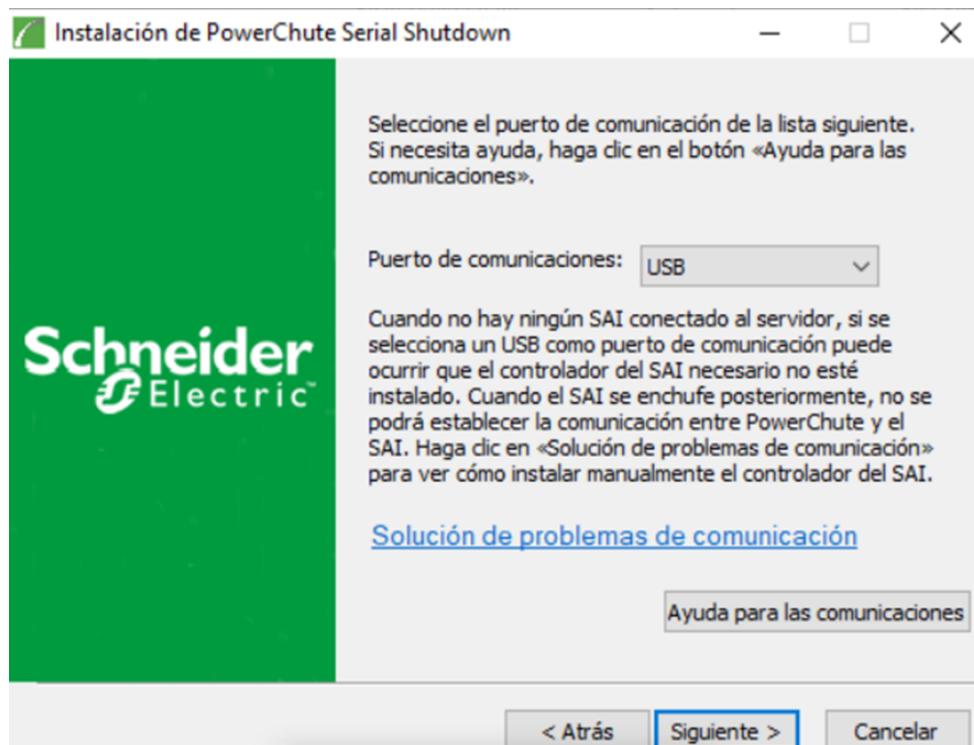


Figura 33 - 11.4 Selección comunicación del SAI

Dejaremos la ruta de instalación por defecto, que será "C:\Program Files\APC\PowerChute Serial Shutdown\"

En el siguiente paso, estableceremos un usuario y una contraseña. Es importante guardar estos datos, ya que serán los que utilicemos posteriormente.

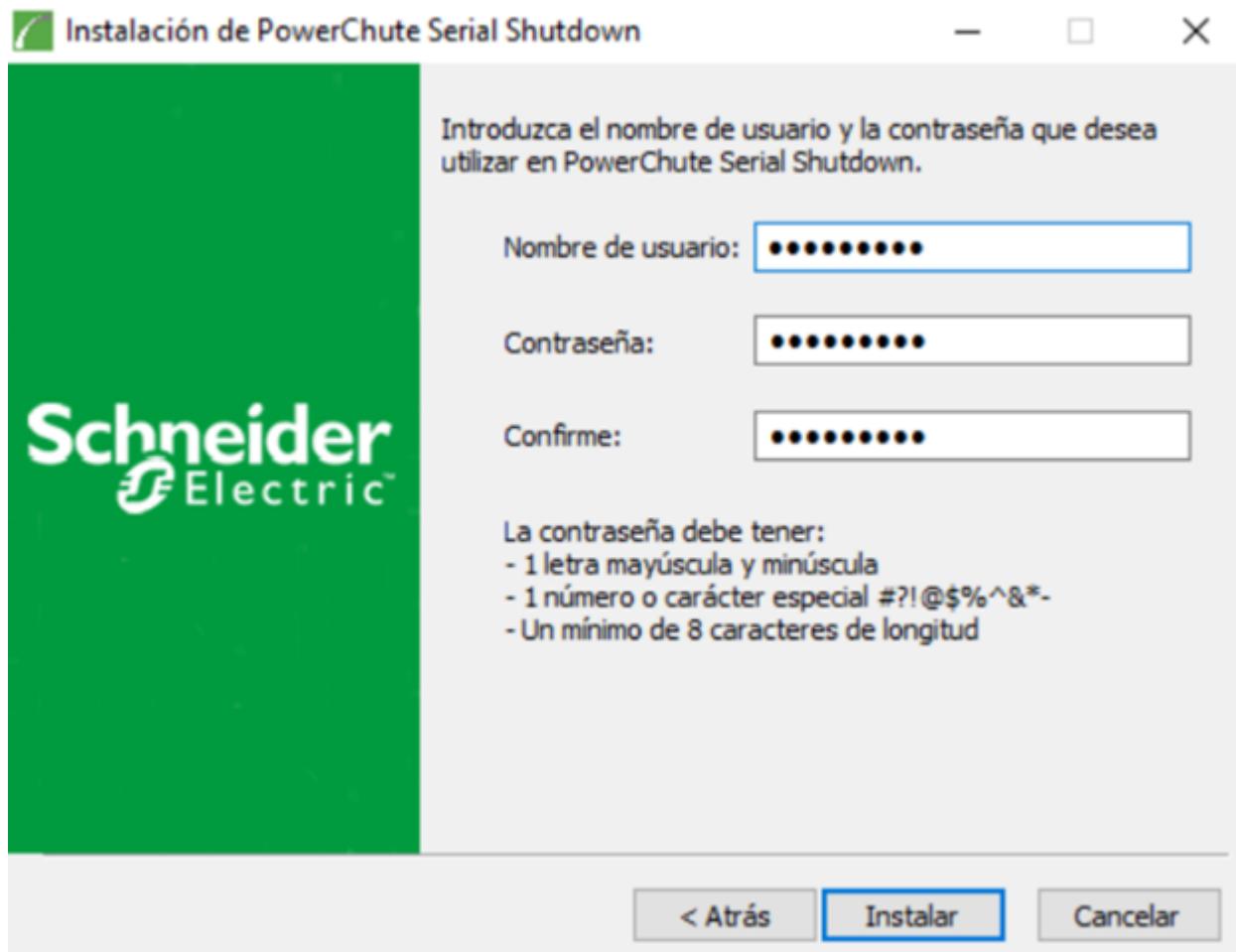


Figura 34 - 11.4 Creación de cuenta de acceso a la consola de SAI

Se nos indicará que se debe excluir este servicio en el firewall de Windows. Haremos clic en “Sí”.

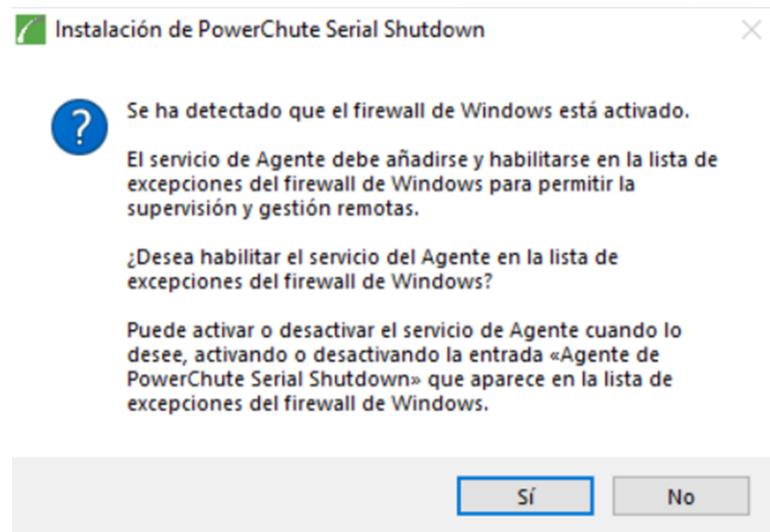


Figura 35 - 11.4 Permisos en el firewall de Windows

Para terminar, haremos clic en Finalizar. Con esto el software estará instalado correctamente.

Para acceder a la interfaz del software, deberemos ir a “localhost:6547”.

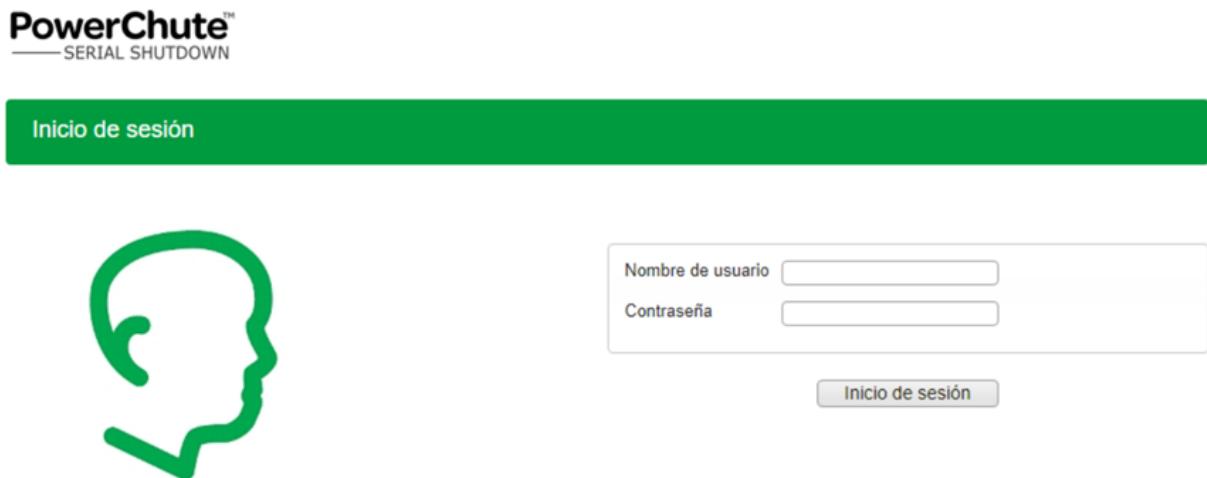


Figura 36 - 11.4 Acceso a la consola PowerChute

Una vez aquí, aceptaremos las preferencias en el botón de “Aplicar”.

The screenshot shows the 'Preferencias' (Preferences) window of the PowerChute Serial Shutdown software. At the top, it displays the logo 'PowerChute™ SERIAL SHUTDOWN' and the system information 'Win10gen'. On the right, there's a navigation bar with links like 'Estado del sistema' (System Status), 'www.apc.com | Cerrar sesión | Acerca de | Ayuda' (www.apc.com | Log out | About | Help), and a language switcher for 'Español' (Spanish). Below the header, there are two main sections: 'Programa de mejora de la experiencia del cliente de PowerChute' (Customer Experience Improvement Program) and 'Actualizaciones de PowerChute' (PowerChute Updates).

Programa de mejora de la experiencia del cliente de PowerChute

El Programa de mejora de la experiencia del cliente (CEIP) de PowerChute nos proporciona la información que nos permite mejorar nuestro producto y servicios, y nos ayuda a asesorarle sobre la mejor manera de implementar y configurar PowerChute.

Como parte del CEIP, recopilaremos cierta información sobre cómo configura y utiliza PowerChute Serial Shutdown en su entorno. Esta información es completamente anónima y no puede utilizarse para identificar personalmente a ningún individuo. Para obtener más información, consulte nuestro [Preguntas frecuentes sobre el CEIP](#).

Si prefiere no participar en el CEIP de PowerChute, desmarque la casilla a continuación. Puede unirse o abandonar el CEIP cuando lo deseé.

Únase al programa de mejora de la experiencia del cliente de PowerChute(CEIP)

Actualizaciones de PowerChute

PowerChute Serial Shutdown comprobará si hay actualizaciones y le informará si hay una nueva versión del software disponible. Esta comprobación de actualización envía datos anónimos del entorno de PowerChute al servidor de actualización de Schneider Electric.

Si no quiere que se comprueben las actualizaciones, desmarque la casilla que aparece a continuación.

Habilitar actualizaciones de PowerChute

Figura 37 - 11.4 Aceptación de términos

Con esto tendremos instalado el software y acceso a la consola principal de PowerChute.

11.5 CONFIGURACIÓN AUTOMATIZACIONES SAI

Contraseña de aplicación de Google - POWERCHUTE

En primer lugar, crearemos una cuenta de aplicación en la cuenta de la organización. Para esto iremos a Gestión de tu cuenta de Google. Desde allí, en la sección Seguridad encontraremos una sección llamada iniciar sesión en Google que tiene una parte donde pone “contraseñas de aplicación”. Crearemos una nueva cuenta. Tenemos que seleccionar “Otra (nombre personalizado) con el fin de poder seguir los movimientos de esta cuenta. Para nuestro caso llamaremos a la contraseña de aplicación “POWERCHUTE_NOTIFICACIONES” (en el ejemplo se visualizará con el nombre “PRUEBA_POWERCHUTE”).

← Contraseñas de aplicaciones

Las contraseñas de aplicación te permiten iniciar sesión en tu cuenta de Google desde aplicaciones instaladas en dispositivos que no admiten la verificación en dos pasos. No tendrás que recordarlas porque solo tienes que introducirlas una vez. [Más información](#)

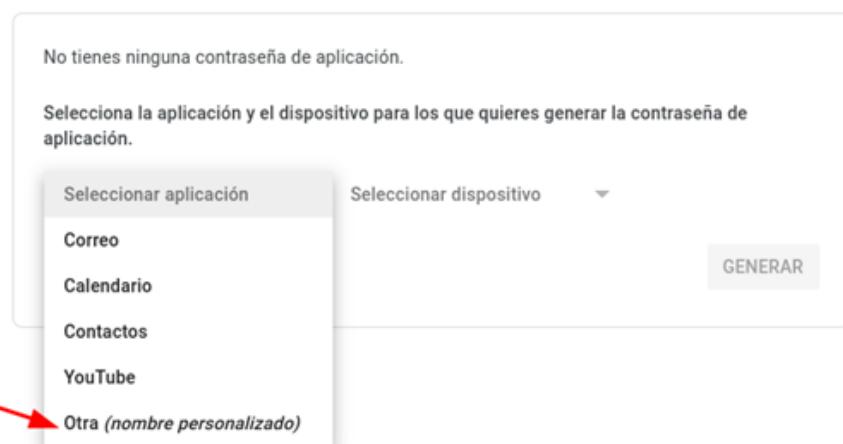


Figura 38 - 11.5 Tipo de contraseña

Una vez hacemos clic en crear, nos aparecerá la contraseña de la aplicación. ES IMPORTANTE GUARDAR BIEN ESTA CONTRASEÑA, YA QUE NO SE VOLVERÁ A PODER VISUALIZAR.

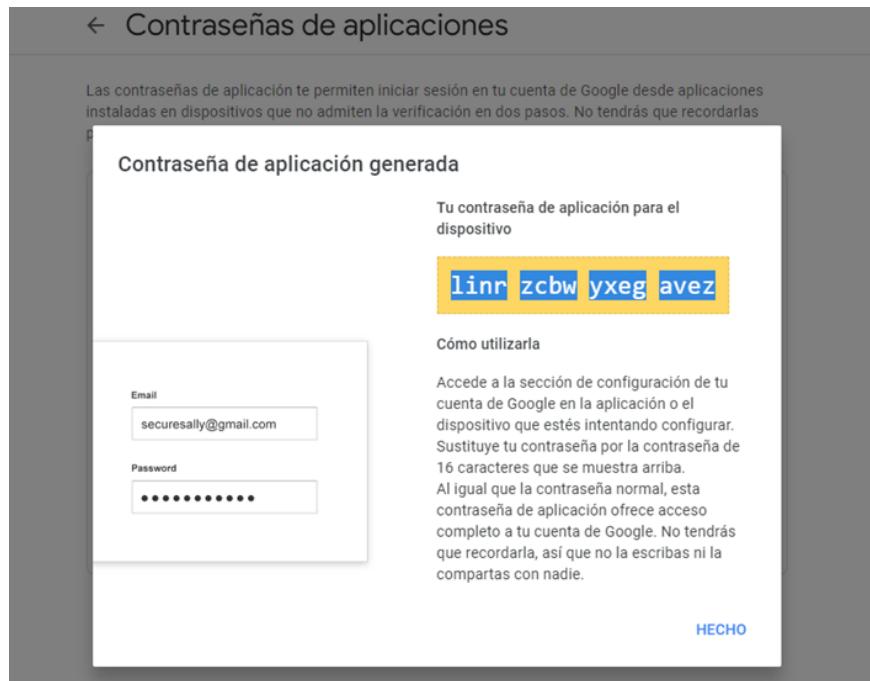


Figura 39 - 11.5 Contraseña de aplicación

Una vez creada, podremos ver todas las cuentas de aplicaciones creadas, junto con la fecha de creación y de último uso.

← Contraseñas de aplicaciones

Las contraseñas de aplicación te permiten iniciar sesión en tu cuenta de Google desde aplicaciones instaladas en dispositivos que no admiten la verificación en dos pasos. No tendrás que recordarlas porque solo tienes que introducirlas una vez. [Más información](#)

| Tus contraseñas de aplicación | | | |
|---|-------------------|-------------------------|---|
| Nombre | Fecha de creación | Último uso | |
| PRUEBA_POWERCHUTE | 21:13 | 21:14 | |
| Selecciona la aplicación y el dispositivo para los que quieras generar la contraseña de aplicación. | | | |
| Seleccionar aplicación | ▼ | Seleccionar dispositivo | ▼ |
| GENERAR | | | |

Figura 40 - 11.5 Historial de uso de contraseña de aplicación

Envío de correos electrónicos

Se va a configurar el software asociado al SAI para que envíe correos electrónicos ante determinados sucesos que ocurran. Desde la pestaña principal del navegador, iremos al menú “PowerChute”, al submenú “Configuración de correo electrónico”.

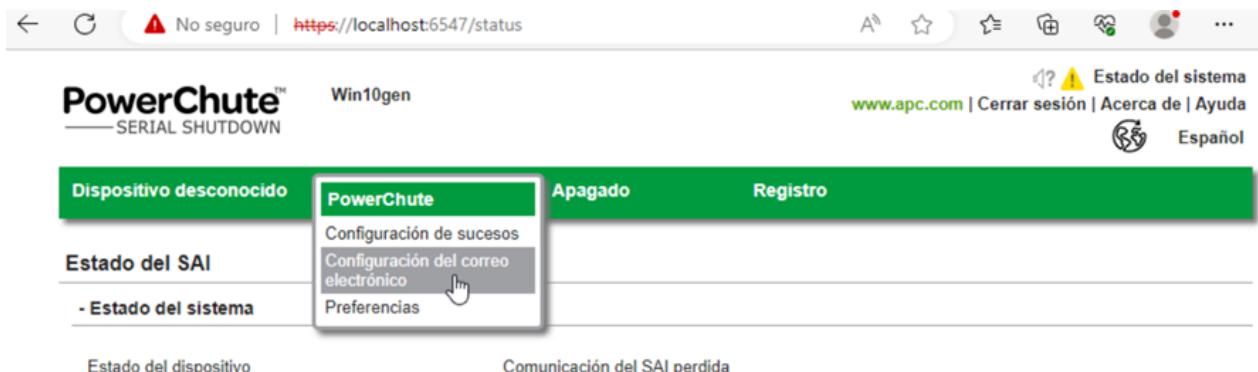


Figura 41 - 11.5 Apartado de configuración de envío de correos

En esta pestaña, tenemos todos los datos para configurar el envío de correos electrónicos de manera automática cuando ocurran determinadas situaciones. Aquí vamos a configurar los datos de la cuenta desde la que se enviarán los correos electrónicos de notificación, así como los destinatarios de los correos.

Los datos que se deben introducir son:

Apartado Configuración del servidor SMTP

- Servidor SMTP: “smtp.gmail.com” (Utilizaremos la cuenta de Google creada para la organización)
- Desde la dirección de correo: “tfmresiliencia@gmail.com” (cuenta de correo de la organización)
- Puerto: “365” (Puerto por defecto de Gmail)
- Usar SSL/TLS: “SSL”

- Configuración del servidor SMTP *

Servidor SMTP (nombre de host, IPv4 o IPv6)

smtp.gmail.com

Desde la dirección de correo electrónico

tfmresiliencia@gmail.com

Puerto

465

Usar SSL/TLS

SSL

Habilitar la comprobación de identidad del servidor

Figura 42 - 11.5 Datos servidor SMTP

Apartado Añadir/eliminar destinatarios de correo electrónico

En este apartado se debe añadir UNO A UNO las direcciones de correo que queremos que sean notificadas ante la caída de la red eléctrica. Cada vez que escribamos una, debemos hacer clic en el botón “Aplicar”. En este caso, se deberán añadir todas las direcciones de los profesores, del director de la microPYME y del informático.

- Añadir/eliminar destinatarios de correo electrónico *

Añada cada destinatario de correo electrónico en el campo «A la dirección de correo electrónico» de uno en uno y pulse Aplicar. Se puede agregar un máximo de diez direcciones de correo electrónico.

A la dirección de correo electrónico

Para eliminar un destinatario de correo electrónico, seleccione la casilla correspondiente y pulse Aplicar.

tfmresiliencia@gmail.com

Figura 43 - 11.5 Destinatarios

Apartado Autenticación básica de correo electrónico

- Habilitar autenticación: Debe estar marcado
- Nombre del usuario del servidor: “tfmresiliencia@gmail.com” (cuenta de correo de la organización)
- Contraseña del servidor y confirmar contraseña: Se debe introducir la contraseña de aplicación creada para el envío de correos del SAI.

- Autenticación básica de correo electrónico

Habilitar autenticación



Nombre de usuario del servidor (opcional)

tfmresiliencia@gmail.com

Contraseña del servidor (opcional)

Confirmar contraseña

Figura 44 - 11.5 Contraseñas de aplicación

Apartado Información de contacto

Este apartado es opcional. Estos datos se verán indicados en el correo que recibiremos, por lo que es recomendable indicar como nombre de contacto el nombre del informático y como ubicación del sistema “Oficina” en el caso de la microPYME, al ser donde se encuentra el SAI.

- Información de contacto

Nombre de contacto

ADMIN_TEST

Ubicación del sistema

TEST

Prueba

Aplicar

Figura 45 - 11.5 Datos de contacto

Una vez terminemos con la configuración, haremos clic en “Aplicar”.

Para realizar una prueba de que la configuración es correcta, hacemos clic en “Prueba”. Nos aparecerá una ventana donde confirmaremos con “Si” el envío de la prueba de correo. Si hemos introducido todos los datos necesarios, se mostrará por pantalla el siguiente mensaje.

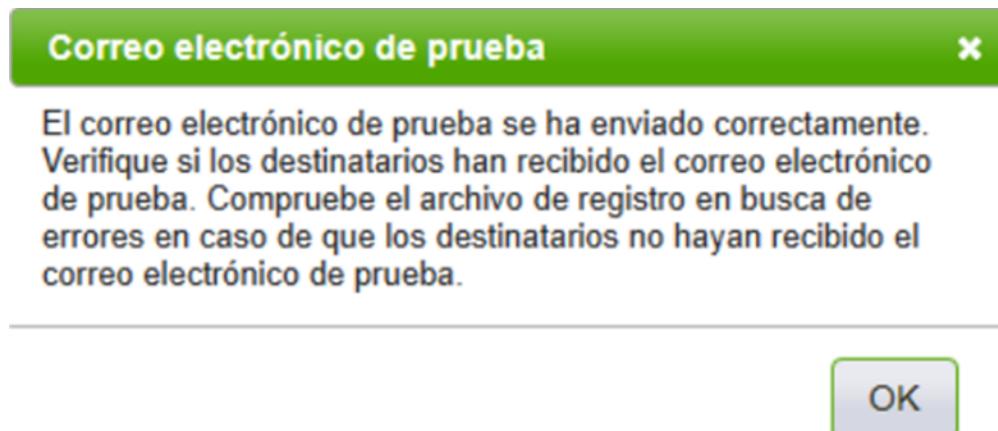


Figura 46 - 11.5 Notificación de envío de correo de prueba

Si los datos son correctos, en los correos que hayamos indicado como destinatarios recibiremos el siguiente mensaje, quedando la configuración del envío de correos correcta.

Correo electrónico de prueba de PowerChute Serial Shutdown

Nombre de la red: Win10gen

Nombre de contacto: ADMIN_TEST

Ubicación del dispositivo: TEST

URL: <https://Win10gen:6547>

Figura 47 - 11.5 Ejemplo de correo electrónico recibido

Ahora tenemos que configurar qué tipo de eventos se notificarán mediante correo electrónico. En la pestaña de “PowerChute -> Configuración de sucesos” aparecerá un listado con las acciones que pueden ocurrir y que desencadenan una alerta. Para la correcta configuración, del envío de notificaciones ante la pérdida de corriente eléctrica y la recuperación de la corriente y la baja batería restante, se deben marcar las opciones marcadas en la columna “Correo electrónico” en las siguientes imágenes.

| Evento | Registro | Correo electrónico | Apagado | Archivo de comandos |
|--|-------------------------------------|-------------------------------------|-------------------------------------|---|
| Pérdida de comunicación cuando funcionaba con la batería | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |  |
| Batería baja | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |  |

Figura 48 - 11.5 Eventos Críticos

| ⚠ Evento | Registro | Correo electrónico | Apagado | Archivo de comandos |
|---|-------------------------------------|-------------------------------------|--------------------------|---|
| Funcionamiento con batería | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |  |
| Batería descargada | <input checked="" type="checkbox"/> | <input type="checkbox"/> | |  |
| Sobrecarga | <input checked="" type="checkbox"/> | <input type="checkbox"/> | |  |
| Autocomprobación fallida | <input checked="" type="checkbox"/> | <input type="checkbox"/> | |  |
| Se perdió la comunicación | <input checked="" type="checkbox"/> | <input type="checkbox"/> | |  |
| Se ha superado el umbral de tiempo en batería | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |  |
| Tiempo de ejecución insuficiente disponible | <input checked="" type="checkbox"/> | <input type="checkbox"/> | |  |
| Es necesario reemplazar la batería | <input checked="" type="checkbox"/> | <input type="checkbox"/> | |  |
| Batería desconectada | <input checked="" type="checkbox"/> | <input type="checkbox"/> | |  |
| Archivo de configuración no válido | <input checked="" type="checkbox"/> | <input type="checkbox"/> | |  |
| Inicio de sesión de usuario no válido | <input checked="" type="checkbox"/> | <input type="checkbox"/> | |  |

Figura 49 - 11.5 Eventos Medios

- Información

| ℹ Evento | Registro | Correo electrónico |
|--|-------------------------------------|-------------------------------------|
| Ya no funciona con batería | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Sobrecarga resuelta | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Inicio del apagado | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Communication Established (Comunicación establecida) | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Supervisión iniciada | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Usuario conectado | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Usuario desconectado | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Supervisión detenida | <input checked="" type="checkbox"/> | |
| Tiempo de ejecución suficiente disponible | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Autocomprobación superada | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Autocomprobación iniciada | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Batería reemplazada | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Batería reconectada | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Archivo de configuración cambiado | <input checked="" type="checkbox"/> | <input type="checkbox"/> |

Figura 50 - 11.5 Eventos Información

Con esta configuración, se recibirán alertas en los correos indicados como destinatarios cada vez que ocurran estos eventos.

Ejecución de scripts de manera automática ante un evento

Dentro de la pestaña “PowerChute -> Configuración de sucesos” tenemos el listado completo de eventos. Buscamos el evento “Funcionamiento con batería”. El objetivo es asignar la ejecución de un script cuando este evento sea detectado. Para esto, haremos clic en el botón “Archivo de comandos”.

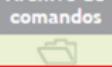
| Evento | Registro | Correo electrónico | Apagado | Archivo de comandos |
|----------------------------|-------------------------------------|-------------------------------------|--------------------------|---|
| Funcionamiento con batería | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |  |

Figura 51 - 11.5 Selección de scripts para una alerta específica

Nos saltará una pestaña en la que tendremos que seleccionar el script deseado.

Es importante destacar que TODOS los scripts de deben encontrar dentro de la carpeta de “C:\Program Files\APC\PowerChute Serial Shutdown\agent\cmdfiles”, siendo esta la ruta de instalación por defecto. Aquí marcaremos el check de “Habilitar la ejecución de archivos de comandos” y seleccionaremos el comando que queremos ejecutar. Dejaremos los valores de tiempo por defecto.

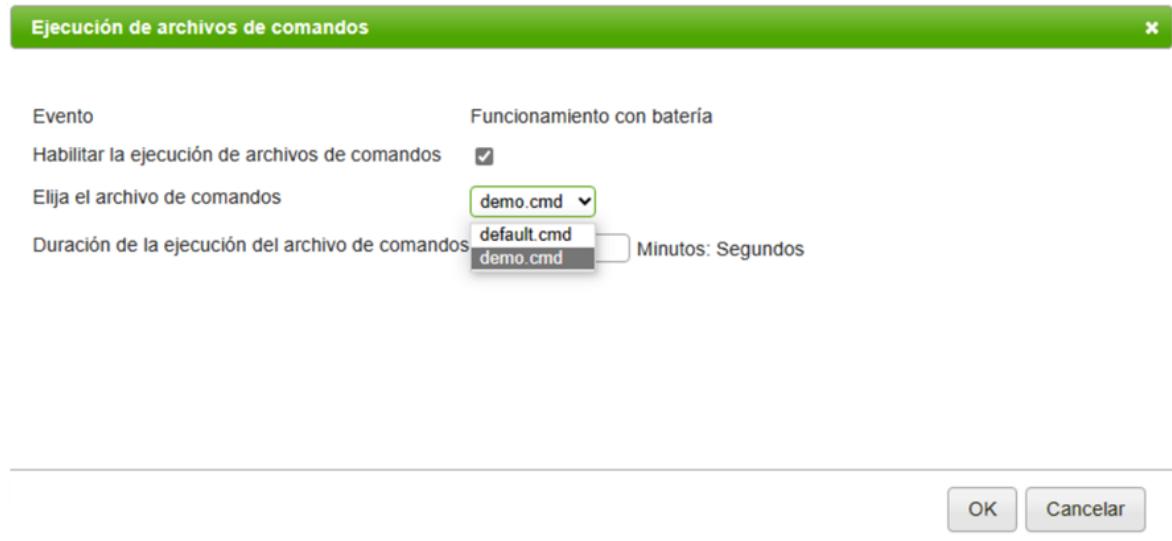


Figura 52 - 11.5 Selección de scripts a ejecutar

Una vez realizada esta configuración, cuando el evento suceda, se ejecutará el script que tenga habilitado.

11.6 GUIA DE PRUEBAS SEMESTRALES DE FUNCIONAMIENTO DEL SAI

Este procedimiento ha sido diseñado para verificar el correcto funcionamiento del SAI, su capacidad para detectar y responder ante pérdidas de electricidad, y también la revisión del estado de las baterías del dispositivo. Asegúrate de seguir las precauciones de seguridad mientras realizas estas pruebas. Se deben realizar al menos 2 pruebas al año. Para comprobar el SAI, seguiremos los siguientes pasos:

- **Paso 1: Preparación**

Lea detenidamente el manual del usuario del SAI.

Informa al personal afectado acerca de las pruebas para evitar interrupciones innecesarias durante el transcurso de la realización de las pruebas.

- **Paso 2: Verificación del estado físico**

Inspecciona visualmente el SAI en busca de daños, conexiones sueltas o cualquier anomalía. Si encuentras algún problema, detén las pruebas. Será necesario realizar las reparaciones necesarias para solucionar estos daños, o en su defecto, reemplazar el dispositivo.

- **Paso 3: Prueba de pérdida de energía**

Con el SAI en modo de funcionamiento normal, simula una pérdida de energía desconectando el suministro eléctrico que llega al SAI.

Observa cómo el SAI responde al corte de energía. Debe cambiar automáticamente al modo de batería y proporcionar energía continua a los dispositivos conectados, así como notificar mediante los canales establecidos del corte del suministro.

Verifica que el tiempo de transferencia sea adecuado y que no haya interrupciones significativas durante el cambio de modo. Verifica que las notificaciones hayan llegado correctamente.

- **Paso 4: Prueba del estado de las baterías**

Con el SAI todavía funcionando en modo de batería, revisa la aplicación del SAI para verificar el estado de las baterías. Asegúrate de que la carga de la batería no esté demasiado baja y comprueba otras anomalías resaltadas en la aplicación.

- **Paso 5: Restauración**

Una vez finalizadas las pruebas, restablece el suministro eléctrico del SAI y verifica que regrese al modo de funcionamiento normal, así como que las baterías se estén recargando.

- **Paso 6: Registro y documentación**

Registra los resultados de las pruebas, incluyendo detalles sobre la duración del modo de batería, el estado de las baterías y cualquier otra observación relevante.

Documenta cualquier problema encontrado durante las pruebas.

- **Paso 7: Mantenimiento**

Una vez terminadas completamente las pruebas, estos problemas deberán ser notificados y solucionados.

Programe la siguiente fecha para la realización de las pruebas del SAI en 6 meses como máximo desde la fecha de la revisión.

11.7 FORMACIÓN ANUAL RELACIONADA CON EVENTOS DISRUPTIVOS

Anualmente se realizará una formación y concienciación para el personal sobre cómo actuar frente a determinados eventos disruptivos y sobre cómo se debe actuar durante estos.

- **Evento 1:** Notificación de corte de electricidad y/o cambio a baterías en el SAI, cambio a entorno de emergencia.

1. Concienciación:

Al inicio del año, se llevará a cabo una sesión de capacitación para todo el personal de la microPYME sobre la importancia de estar preparados ante cortes de electricidad.

Se explicará la relevancia de mantener la continuidad de las operaciones y cómo un corte eléctrico puede tener un gran impacto en el trabajo y los equipos.

2. Identificación del evento:

El informático será el encargado de monitorear el estado del suministro eléctrico y la duración de las baterías en el Sistema de Alimentación Ininterrumpida (SAI).

3. Acciones frente al corte de electricidad:

Cuando se reciba la notificación del corte de electricidad, el responsable designado activará el plan de contingencia.

Todo el personal será alertado mediante una comunicación inmediata mediante correo electrónico de manera automática para que comiencen el proceso de cambio al entorno de emergencia.

4. Cambio al entorno de emergencia:

Se instruirá al personal sobre cómo cambiar de red y asegurarse de que todos los datos y archivos importantes estén guardados.

Se proporcionarán pautas claras sobre qué tareas se pueden continuar y cómo realizarlas en el entorno de emergencia y qué acciones se deben tomar al entrar en el modo de baterías del SAI.

- **Evento 2:** Corte en los servicios de internet. Cambio de la red por cable a la red Wifi de la oficina.

1. Concienciación:

Al comienzo del año, se llevará a cabo una sesión de capacitación para todo el personal sobre la importancia de tener planes alternativos en caso de interrupciones en el servicio de internet.

Se destacará como afectaría el trabajo diario y la necesidad de cambiar a una conexión de respaldo, como la red Wifi de la oficina.

2. Identificación del evento:

El personal de IT será responsable encargado de monitorear el estado del servicio de internet y comunicar rápidamente cualquier interrupción al personal y de realizar cualquier acción de cambio entre redes.

3. Acciones frente al corte de internet:

Cuando detecte el corte de internet, el responsable activará el plan de contingencia.

Todo el personal será alertado sobre la necesidad de cambiar a la red Wifi de la oficina para mantener la conectividad y poder continuar con las tareas diarias, por lo que

deberán desconectar el cable de red.

4. Cambio a la red Wifi de la oficina:

Se instruirá al personal sobre cómo cambiar a la red Wifi de la oficina de manera rápida y segura.

Se proporcionarán pautas claras sobre cómo acceder a la red Wifi y asegurarse de que los dispositivos estén conectados correctamente.

5. Verificación y seguimiento:

Una vez realizado el cambio a la red Wifi, se terminará con las actividades que se estén realizando y se realizarán las acciones necesarias para terminar con las tareas que puedan ser afectadas por el corte, notificando a clientes en caso necesario.

Se supervisará el rendimiento de la red Wifi durante el evento disruptivo y se tomarán medidas correctivas si es necesario.

11.8 CONFIGURACIÓN DE DISPOSITIVO MÓVIL COMO PUNTO DE ACCESO

Para configurar un dispositivo móvil, en este caso un dispositivo Android, como punto de acceso debemos realizar estos dos pasos:

1. Comprobar que los datos están activos en un dispositivo Android.
2. Configurar un móvil Android como punto de acceso para compartir la conexión de datos con otros dispositivos.

- **Parte 1:** Comprobar que los datos están activos

Antes de configurar el dispositivo móvil como punto de acceso, debemos asegurarnos de que los datos móviles están activados. Podemos comprobarlo de la siguiente manera:

Abre la "Configuración" en el dispositivo Android.

Desplázate hacia abajo y selecciona "Redes e internet" o "Conexiones inalámbricas y redes" o "Conexiones", dependiendo de la versión de Android.

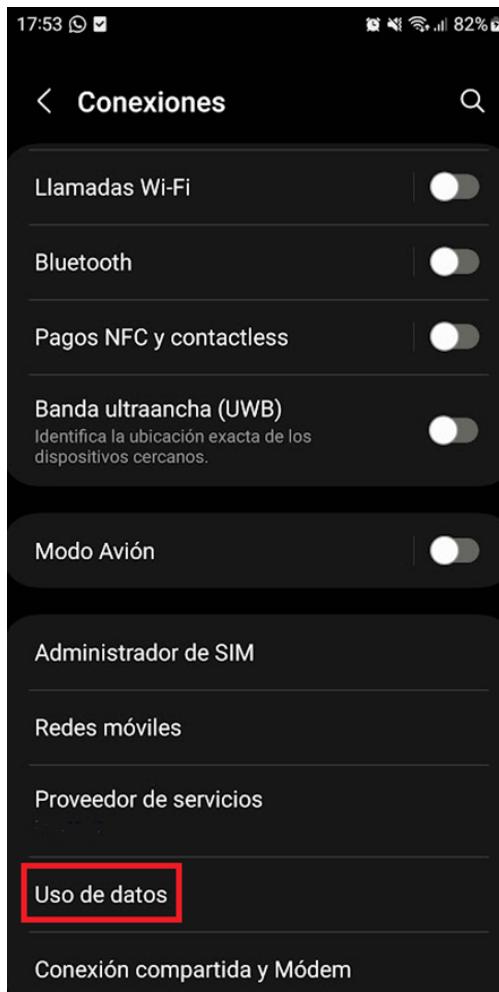


Figura 53 - 11.8 Uso de datos

Si el dispositivo tiene la opción "Datos móviles" o "Uso de datos", actívala. Si ya está activada, deberías ver un ícono en la barra de estado de tu teléfono que indica que los datos móviles están en uso.

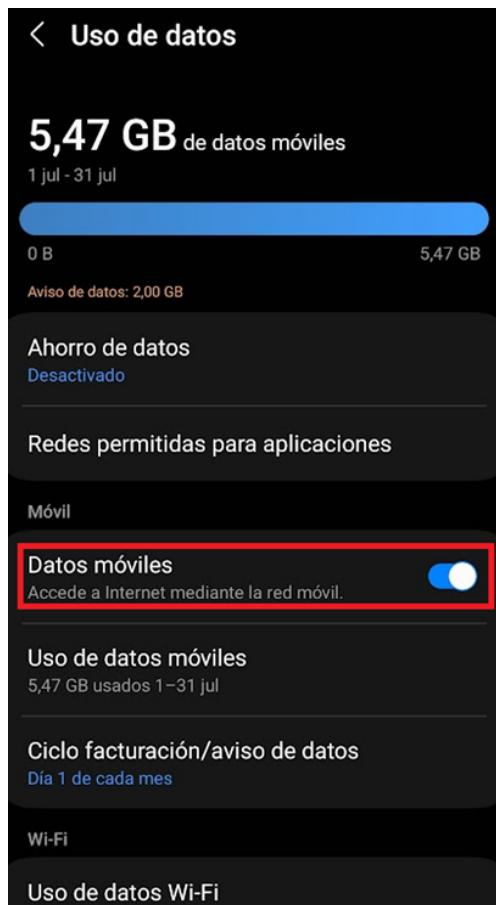


Figura 54 - 11.8 Activación de datos móviles

Con esto, ya has verificado que los datos móviles están activados en tu dispositivo.

- **Parte 2:** Configurar un móvil Android como punto de acceso

Una vez que hemos verificado que los datos móviles están activos, procedemos a configurar el dispositivo Android como punto de acceso para que otros dispositivos puedan conectarse a él y compartir la conexión de datos. Para ello, seguiremos estos pasos:

Ve a la "Configuración" en tu móvil Android.

Busca y selecciona "Punto de acceso y zona Wi-Fi" o "Tethering y zona Wi-Fi" (el nombre puede variar según la versión de Android).



Figura 55 - 11.8 Zona Wi-Fi/Compartir conexión

Una vez dentro, activa la opción "Punto de acceso Wi-Fi" o "Zona Wi-Fi portátil".

Ahora, el móvil Android se convertirá en un punto de acceso inalámbrico y otros dispositivos podrán verlo en la lista de redes Wi-Fi disponibles.

Podemos configurar la seguridad, cambiando la contraseña entre otras cosas para proteger y configurar este punto de acceso. Para ello, dentro de la configuración de "Punto de acceso y zona Wi-Fi", busca la opción "Configurar punto de acceso Wi-Fi" o "Configurar zona Wi-Fi".

Se establecerá un nombre para la red Wi-Fi (SSID). Este es el nombre que verán los otros dispositivos cuando busquen redes disponibles. Elige un tipo de seguridad para tu red Wi-Fi. Se recomienda usar WPA2. Se pedirá que establezcas una contraseña para la red. Elije una contraseña segura y anótala para que puedas compartirla con los dispositivos que deseen conectarse.

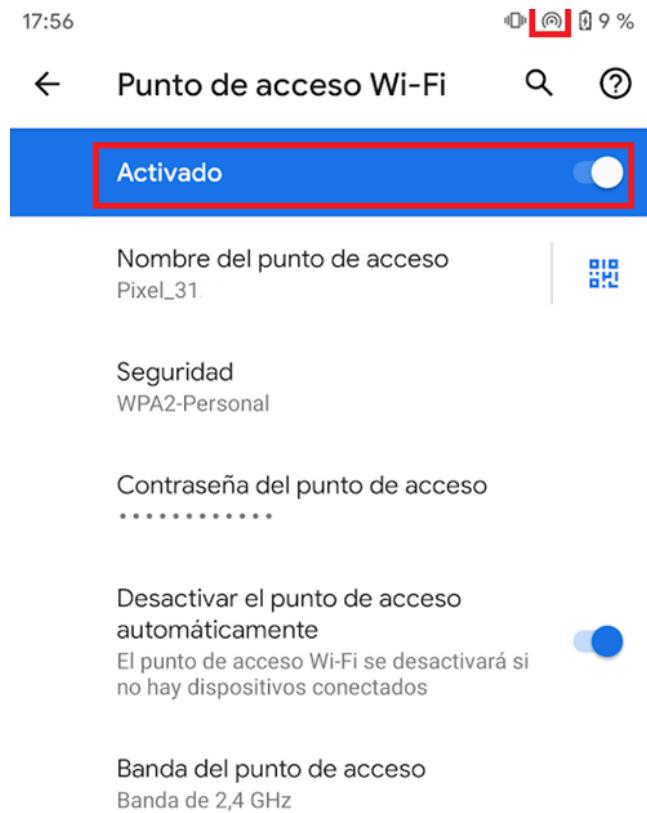


Figura 56 - 11.8 Datos Zona Wi-Fi

Con esto queda configurado el móvil Android como un punto de acceso Wi-Fi y otros dispositivos podrán conectarse a él usando la contraseña que hayas establecido.

11.9 CONFIGURACIÓN DE RED EN DISPOSITIVOS PORTÁTILES

Se deberá seguir el siguiente procedimiento para configurar manualmente la red Wifi secundaria, ya que no siempre estará encendida y nos aparecerá como disponible.

En el ordenador, abrir el centro de redes y recursos. Para esto presiona las teclas "Win + X" y selecciona "Configuración de red e Internet" o "Conexiones de red" o "Centro de redes y recursos compartidos". Una vez en esta pestaña, debemos irnos al apartado de "Wifi" y "Administrar redes conocidas".

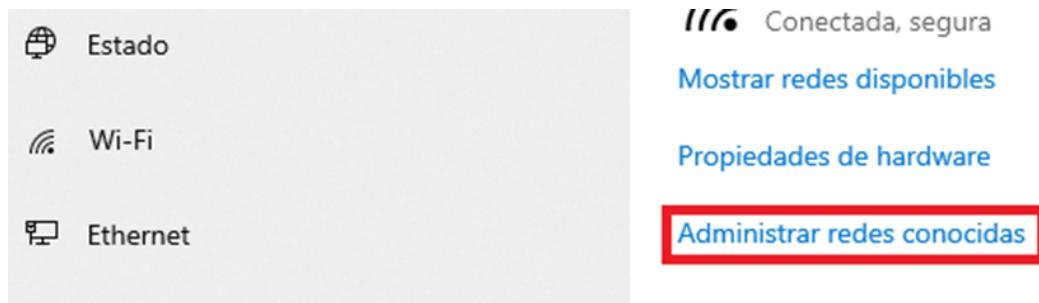


Figura 57 - 11.9 Administrar redes conocidas

Una vez dentro, agregaremos una nueva red. En este apartado deberemos introducir los datos que nos sean proporcionados con los datos de la red. Se debe especificar el nombre, el tipo de seguridad, la contraseña de la red, y MUY IMPORTANTE, marcar la opción de "Conectar automáticamente".

Agregar una nueva red

Nombre de red

TFM_resiliencia

Tipo de seguridad

AES WPA2-Personal

Llave de seguridad

Conectar automáticamente

Conectarse aunque esta red no esté retransmitiendo

Guardar

Cancelar

Figura 58 - 11.9 Datos de la red

Una vez guardemos esta configuración, nos aparecerá la red en el listado de la página de “Administrar redes conocidas”, conectándose sin tener que volver a introducir los datos de autenticación cuando exista un problema en la red principal y sea necesario cambiar a esta.

Administrar redes conocidas

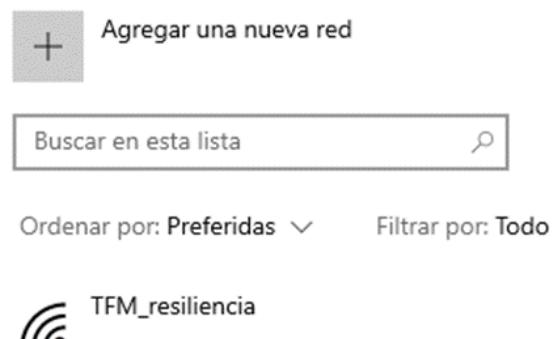


Figura 59 - 11.9 Histórico de redes conocidas

11.10 CREACIÓN DE PÁGINA WEB SECUNDARIA

En el dispositivo Android preparado para levantar la red secundaria abriremos Play Store y buscaremos y instalaremos la aplicación “AWebServer (Http Web Server A” (Sylkat, 2022).



Figura 60 - 11.10 Aplicación AWebServer

Una vez instalada abrimos la aplicación. Nada más abrir, nos pedirá permisos a fotos, contenido multimedia y archivos del dispositivo. Concedemos estos permisos con “Permitir”.



Figura 61 - 11.10 Permisos AWebServer

En el propio dispositivo, se ha creado una carpeta con el nombre de html_TFMresiliencia que contendrá la página web de contingencia. El código de la web de ejemplo está accesible en (<https://github.com/TFMResiliencia/TFMResiliencia2023/blob/main/index.html>). Habrá que crear un archivo llamado “index.html” en la ruta objetivo.

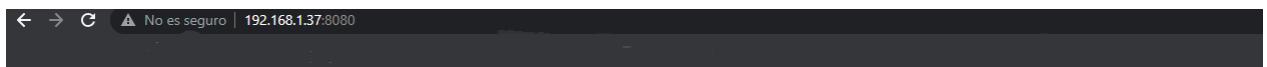
Una vez creado el archivo y colocado en la ruta, en la aplicación cambiaremos la Carpeta Web. Haremos clic en el botón “Selecciona” e indicaremos la ruta a la carpeta objetivo.



Figura 62 - 11.10 Pestaña principal AWebServer

Al hacer clic sobre iniciar, nos aparecerá un mensaje para elegir desde donde queremos que la web sea accesible. Para el procedimiento o pruebas se utilizará “Interno”, para que sea accesible desde la red interna en la que estemos. Cuando tengamos que levantar la web secundaria en caso de contingencia, se indicará “Externo”, donde utilizará la IP pública que tenga el dispositivo.

Una vez iniciado, podremos acceder a una web que nos indicará que hay un problema con la web normal.



Ejemplo de Web de Formación

Estamos teniendo problemas de conectividad y la web no se encuentra disponible. Vuelva a intentarlo en unos minutos

Para cualquier consulta o problema, póngase en contacto mediante uno de los medios previamente proporcionados o a alguno de los medios públicos de la empresa.

Teléfono: 123456789

Email: tfmresiliencia@tfmresiliencia.com

Gracias y perdonen por las molestias.

Figura 63 - 11.10 Ejemplo de web secundaria

11.11 SCRIPTS

Estos scripts se encontrarán almacenados en Github y en la cuenta de almacenamiento y copias de seguridad de la organización.

Para poder ejecutar Scripts primero accedemos a PowerShell y ejecutamos como administrador.

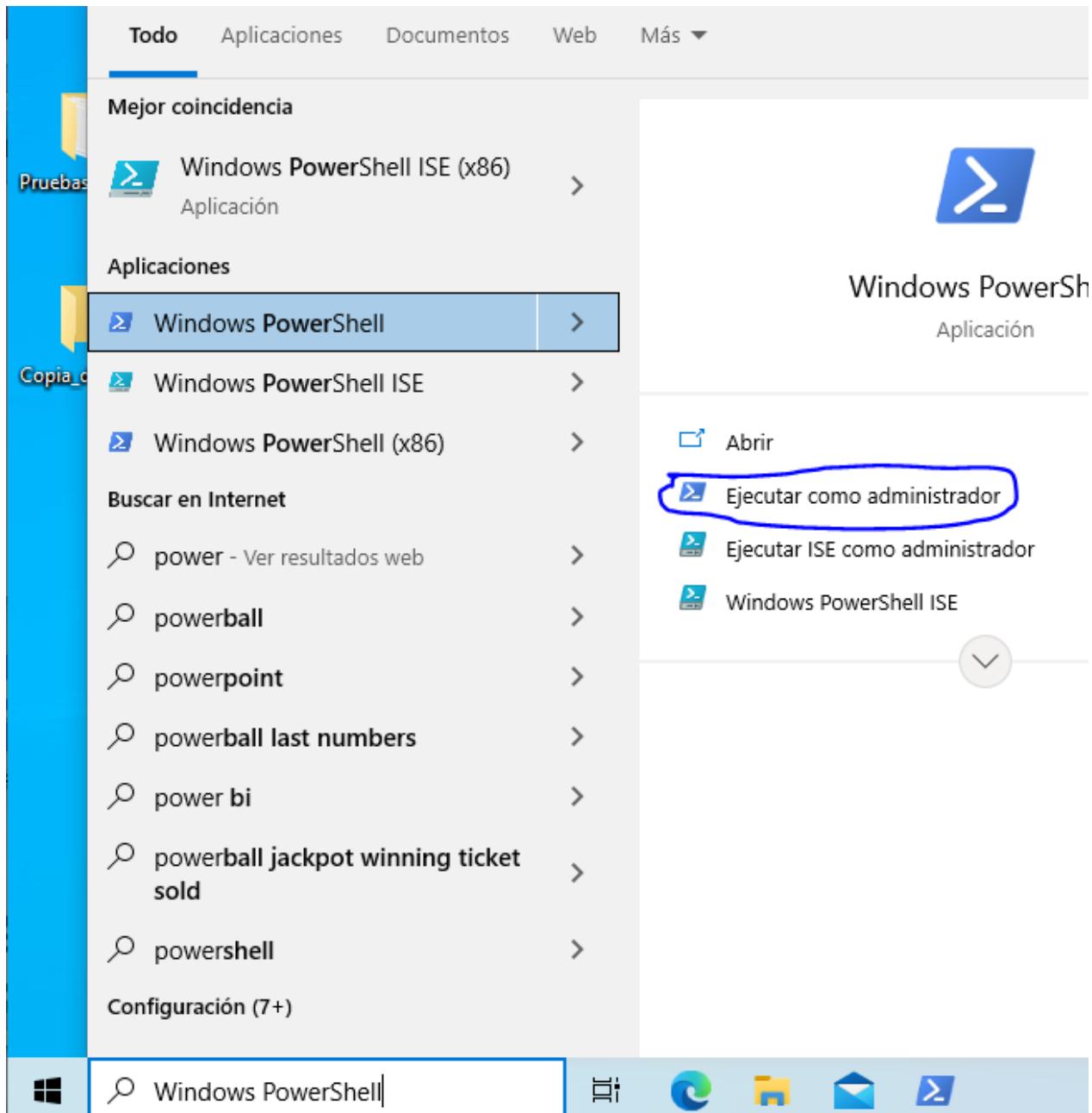
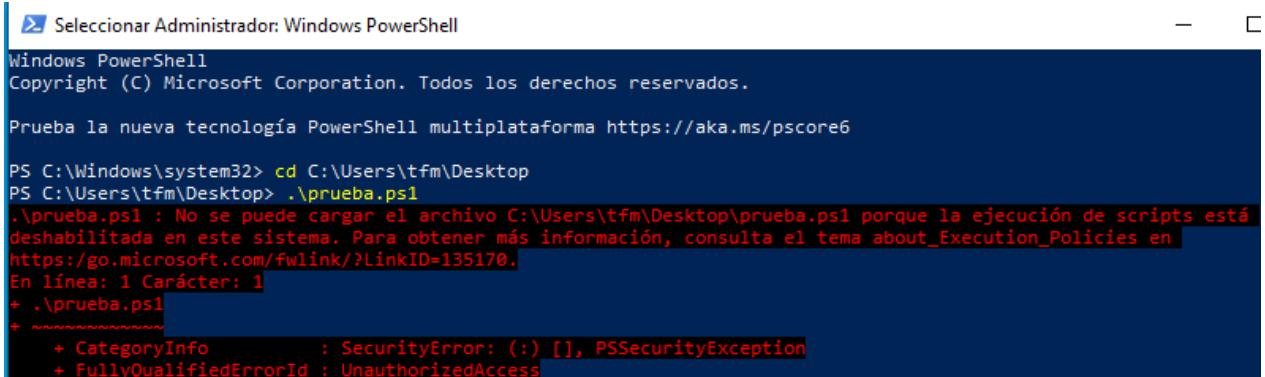


Figura 64 - 11.11 Powershell

Después accedemos a la ruta donde se encuentran los scripts y lo ejecutamos. Por defecto Windows tiene la ejecución de scripts deshabilitada por lo que posiblemente nos encontremos con un error.



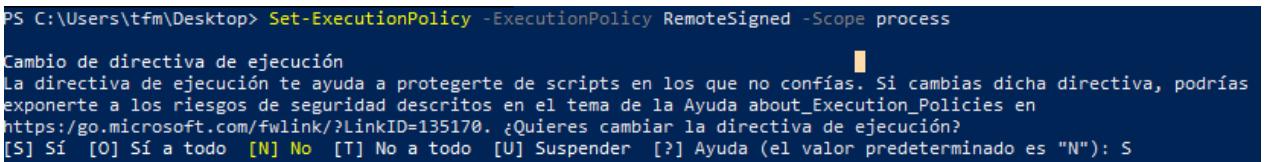
```
Seleccionar Administrador: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

Prueba la nueva tecnología PowerShell multiplataforma https://aka.ms/pscore6

PS C:\Windows\system32> cd C:\Users\tfm\Desktop
PS C:\Users\tfm\Desktop> .\prueba.ps1
.\prueba.ps1 : No se puede cargar el archivo C:\Users\tfm\Desktop\prueba.ps1 porque la ejecución de scripts está
deshabilitada en este sistema. Para obtener más información, consulta el tema about_Execution_Policies en
https://go.microsoft.com/fwlink/?LinkId=135170.
En línea: 1 Carácter: 1
+ .\prueba.ps1
+ ~~~~~
+ CategoryInfo          : SecurityError: () [], PSSecurityException
+ FullyQualifiedErrorId : UnauthorizedAccess
```

Figura 65 - 11.11 Ejecución fallido de script Powershell

Para poder evitar durante el desarrollo del demostrativo este problema deshabilitamos la protección para el proceso actual.



```
PS C:\Users\tfm\Desktop> Set-ExecutionPolicy -ExecutionPolicy RemoteSigned -Scope process
Cambio de directiva de ejecución
La directiva de ejecución te ayuda a protegerte de scripts en los que no confías. Si cambias dicha directiva, podrías
exponerte a los riesgos de seguridad descritos en el tema de la Ayuda about_Execution_Policies en
https://go.microsoft.com/fwlink/?LinkId=135170. ¿Quieres cambiar la directiva de ejecución?
[S] Sí [O] Sí a todo [N] No [T] No a todo [U] Suspender [?] Ayuda (el valor predeterminado es "N"): S
```

Figura 66 - 11.11 Modificación de política en Powershell

Después podremos ejecutar nuestro script.

```
PS C:\Users\tfm\Desktop> .\prueba.ps1
```

Figura 67 - 11.11 Ejecución de Script en Powershell

11.11.1 COPIAS DE SEGURIDAD

El script escrito en Powershell realiza copias de todos los ficheros y carpetas indicados en el script por sus rutas en una ruta “destino” donde se almacena la copia y se comprime en formato “zip”.

```
# Obtiene la fecha actual en el formato deseado (dd-MM-yyyy)
$fechaActual = Get-Date -Format "dd-MM-yyyy"

# Nombre del archivo ZIP resultante con la fecha actual
$nombreZip = "copia_de_seguridad_$fechaActual.zip"

# Rutas de los archivos y carpetas a comprimir
$archivosYCarpetas = @(
    "C:\Users\tfm\Desktop\Pruebas_scripts\datos_web.txt",
    "C:\Users\tfm\Desktop\Pruebas_scripts\datos_web2.txt",
    "C:\Users\tfm\Desktop\Pruebas_scripts\datos_web"
)

# Ruta donde se almacenará el archivo ZIP resultante
$rutaDestino = "C:\Users\tfm\Desktop\Copia_de_seguridad\$nombreZip"

# Verifica si la ruta de destino es válida
if (-not (Test-Path (Split-Path $RutaDestino))) {
    Write-Host "La ruta de destino no es válida."
    return
}

# Crea el archivo ZIP
try {
    # Crea el archivo ZIP
    #Get-ChildItem -Path "$RutaDestino" | Compress-Archive -DestinationPath "$RutaDestino"

    # Agrega cada archivo o carpeta al archivo ZIP
    foreach ($item in $ArchivosYCarpetas) {
        compress-archive -path "$item" -update -destinationpath "$RutaDestino"
    }
    Write-Host "Compresión completada con éxito."
} catch {
    Write-Host "Se produjo un error durante la compresión: $_"
}
```

Figura 68 - Código copias de seguridad

[Este script puede ser consultado en
https://github.com/TFMResiliencia/TFMResiliencia2023/blob/9bc4e16c6c9aa924e7da7276e865c9e9bf7Zef38/Script_crear_copia.ps1]

11.11.2 SUBIDA DE COPIAS DE SEGURIDAD A GOOGLE DRIVE

El script escrito en Powershell, utiliza Google Drive API para subir un archivo “zip” con un identificativo único formado por el nombre de la copia más la fecha de realización.

```
# Ruta donde se encuentra el archivo ZIP (sin conocer el nombre)
$rutaDirectorioZip = "C:\Users\tfm\Desktop\Copia_de_seguridad\"

# Obtiene el archivo ZIP en la ubicación dada
$archivoZip = Get-ChildItem -Path $rutaDirectorioZip -Filter "*.zip" | Select-Object -First 1

if ($archivoZip -eq $null) {
    Write-Host "No se encontró ningún archivo ZIP en la ubicación especificada."
    exit
}

New-GcsObject -Bucket "tfm_resiliencia_copias_de_seguridad" -File $archivoZip.FullName -Force

# Elimina el archivo Zip al terminar
Remove-Item -Path $archivoZip.FullName -Force
```

Figura 69 - Código subidas copias de seguridad

[Este script puede ser consultado en

[“https://github.com/TFMResiliencia/TFMResiliencia2023/blob/9bc4e16c6c9aa924e7da7276e865c9e9bf77ef38/Script_para_subir_las_copias.ps1”\]](https://github.com/TFMResiliencia/TFMResiliencia2023/blob/9bc4e16c6c9aa924e7da7276e865c9e9bf77ef38/Script_para_subir_las_copias.ps1)

11.11.3 ROTADO DE COPIAS DE SEGURIDAD EN GOOGLE DRIVE

El script escrito en Powershell, utiliza Google Drive API para comprobar la cantidad de copias de seguridad subidas. Una vez realizada la comprobación se compara dicha cantidad con el límite numérico indicado y en caso de coincidir o superar su valor, se borrará la copia más antigua.

```
#Cuenta las copias en el bucket
$contadorArchivos = (Get-GcsObject -Bucket "tfm_resiliencia_copias_de_seguridad").Length

#Si existen 3 o más copias se borra el más antiguo
if ($contadorArchivos -ge 3) {
    $file = Get-GcsObject -Bucket "tfm_resiliencia_copias_de_seguridad" | Select Name, TimeCreated | Sort-Object TimeCreated -Descending | Select-Object -First 1 |Select -ExpandProperty Name
    Remove-GcsObject -Bucket "tfm_resiliencia_copias_de_seguridad" -ObjectName $file
    Write-Host "Borrada la copia más antigua"
}
```

Figura 70 - Código rotado copias de seguridad

[Este script puede ser consultado en

https://github.com/TFMResiliencia/TFMResiliencia2023/blob/9bc4e16c6c9aa924e7da7276e865c9e9bf77ef38/Script_para_rotar_copias.ps1]

11.11.4 DESCARGA DE COPIAS DE SEGURIDAD EN GOOGLE DRIVE

El script escrito en Powershell, utiliza Google Drive API para descargar la copia de seguridad más reciente subida. El archivo se almacena en la ruta asignada.

```
#Ordena todos los archivos del bucket y selecciona el más reciente
$file = Get-GcsObject -Bucket "tfm_resiliencia_copias_de_seguridad" | Select Name, TimeCreated | Sort-Object TimeCreated -Descending | Select-Object -First 1 |Select -ExpandProperty Name

#Descarga el archivo mas reciente
Read-GcsObject -Bucket "tfm_resiliencia_copias_de_seguridad" -ObjectName $file -OutFile "C:\Users\tfm\Desktop\Copia_de_seguridad\$file" -Force
```

Figura 71 - Código descarga copias de seguridad

[Este script puede ser consultado en

https://github.com/TFMResiliencia/TFMResiliencia2023/blob/9bc4e16c6c9aa924e7da7276e865c9e9bf77ef38/Script_para_descargar_las_copias.ps1]

11.11.5 RESTAURAR LOS DATOS DE LA COPIA DE SEGURIDAD

El script escrito en Powershell, realiza la copia de los ficheros previamente descargados como copia de seguridad en sus respectivas rutas previamente indicadas.

```
# Ruta donde se encuentra el archivo ZIP (sin conocer el nombre)
$rutaDirectorioZip = "C:\Users\tfm\Desktop\Copia_de_seguridad\"

# Ruta de destino donde se descomprimirá el ZIP
$rutaDestino = "C:\Users\tfm\Desktop\Recuperacion_de_copias"

# Obtiene el archivo ZIP en la ubicación dada
$archivoZip = Get-ChildItem -Path $rutaDirectorioZip -Filter "*.zip" | Select-Object -First 1

if ($archivoZip -eq $null) {
    Write-Host "No se encontró ningún archivo ZIP en la ubicación especificada."
    exit
}

# Comando para descomprimir el archivo ZIP al destino
Expand-Archive -Path $archivoZip.FullName -DestinationPath $rutaDestino -Force

# Elimina el archivo Zip al terminar
Remove-Item -Path $archivoZip.FullName -Force

Write-Host "Extracción y movimiento de archivos completados con éxito."
```

Figura 72 - Código restauración copias de seguridad

[Este script puede ser consultado en

["https://github.com/TFMResiliencia/TFMResiliencia2023/blob/9bc4e16c6c9aa924e7da7276e865c9e9bf77ef38/Script_extraer_copia.ps1"\]](https://github.com/TFMResiliencia/TFMResiliencia2023/blob/9bc4e16c6c9aa924e7da7276e865c9e9bf77ef38/Script_extraer_copia.ps1)