Institución Universitaria

Diseño de una estrategia de racionalidad limitada para la implementación de un BCP para eventos de ciberseguridad.

Nelson Alejandro Palacios Galeano

Instituto Tecnológico Metropolitano

Facultad de ingenierías

Medellín, Colombia

2025

Diseño de una estrategia de racionalidad limitada para la implementación de un BCP para eventos de ciberseguridad.

Nelson Alejandro Palacios Galeano

Tesis o trabajo de investigación presentada(o) como requisito parcial para optar al título de:

Magister en Seguridad informática

Director (a):

MsC Fredy Humberto Gómez Orjuela

Codirector (a):

MsC Miguel Manosalva

Línea de Investigación:

Ciencias computacionales

Instituto Tecnológico Metropolitano

Facultad de ingenierías

Medellín, Colombia

2025

Dedicatoria:

A Dios, por entregarme salud, energía y sustento para alcanzar cada hito a lo largo de este camino.

A mi pequeña Ana Sofia, por todas las noches en que me besó y se fue a la cama tranquila comprendiendo que también era parte de este proceso de crecimiento académico, profesional, pero principalmente personal.

A mi esposa, quién con su cariño, palabras y acciones me ha brindado el soporte necesario para seguir adelante con mis propósitos.

A mi madre y hermana, que han sido desde mi niñez un ejemplo de constancia y perseverancia.

A mí mismo, para recordarme que puedo afrontar miedos, romper barreras y alimentar mi hambre constante de conocimiento.

"La verdadera sabiduría está en saber que no sabes nada".
Sócrates

Agradecimientos

Quiero expresar un agradecimiento al Magíster Fredy Humberto Gómez, quien asumió con alta disposición el reto de asesorarme. En su dedicación siempre estuvo dispuesto a compartir y debatir ideas conmigo, y con ello, construir conocimiento juntos.

Asimismo, deseo extender mi más sincero y especial agradecimiento al Magister Héctor Fernando Vargas, quién, con su conocimiento, cercanía y gestión diligente, me brindó, incluso quizá sin ser consciente de ello, nuevas perspectivas profesionales. Además, me invitó siempre a pensar por fuera de la caja, lo que me permitió ampliar mi visión y amor por esta profesión.

Por último, agradezco a los docentes y compañeros que hicieron parte de este camino que, indirectamente y sin percibirlo, enriquecieron mi aprendizaje y contribuyeron a que este viaje fuera mucho más ameno.

Resumen

El presente trabajo está orientado al diseño de una estrategia para la implementación de un plan de continuidad de negocio (BCP) para MiPymes del sector manufacturero en Colombia haciendo uso del modelo de racionalidad limitada. La metodología para la consecución de este objetivo fue estructurada en 4 fases, en las que, cada fase cubrió uno de los siguientes objetivos específicos: (1) Identificar los riesgos cibernéticos más relevantes que afectan la disponibilidad en el sector propuesto, para que puedan ser tenidos en cuenta en la definición de la estrategia; (2) Caracterizar los estándares de implementación de BCP en el contexto de ciberseguridad, identificando las prácticas que aporten a la reducción de riesgos en las MiPymes del sector seleccionado; (3) Integrar en una estrategia los componentes mínimos viables para un BCP según las necesidades y capacidades de las MiPymes, utilizando el modelo de racionalidad limitada; (4) Validar la estrategia en una prueba de escritorio con caso de estudio completo que permita la comprensión del resultado de la implementación un BCP. Como resultado del diseño, se realizó una prueba de escritorio a la estrategia de BCP por medio de un caso de estudio utilizando un instrumento en Excel, concluyendo en la implementación del 88.9% del BCP propuesto alrededor del alcance definido

Palabras clave: ciberseguridad, estándares, MiPymes, plan de continuidad de negocio, racionalidad limitada, riesgos cibernéticos.

Abstract

This work is aimed at designing a strategy for implementing a Business Continuity Plan (BCP) for MSMEs in Colombia's manufacturing sector, using the bounded rationality model. The methodology to achieve this objective was structured into four phases, each of which addressed one of the following specific objectives: (1) Identify the most relevant cyber risks that affect availability in the proposed sector, so they can be considered in defining the strategy; (2) Characterize BCP implementation standards in the cybersecurity context, identifying practices that contribute to risk reduction in MSMEs in the selected sector; (3) Integrate, into a single strategy, the minimum viable components for a BCP according to the needs and capabilities of MSMEs, using the bounded rationality model; and (4) Validate the strategy through a tabletop exercise supported by a complete case study, using an Excel-based instrument to facilitate understanding of the outcome of BCP implementation. As a result of the design, the BCP strategy was assessed through a tabletop exercise based on a case study using an Excel instrument, concluding in the implementation of 88.9% of the proposed BCP within the defined scope.

Keywords: cybersecurity, standards, MSMEs, business continuity plan, bounded rationality, cyber risks.

Contenido

Lista de figuras

Lista de tablas

Lista de Abreviaturas

Abreviatura	Término
ABCP	Associate Business Continuity Professional.
API	Application Programming Interface.
BCI	Business Continuity Institute.
BCM	Business continuity Management.
BCMS	Business continuity Managment System.
BCP	Business Continuity Plan.
BD	Base de datos.
BIA	Business Impact Analysis.
CBCP	Certified Business Continuity Professional.
CCTV	Closed Circuit Television.
CPU	Central Processing Unit.
DDoS	Distributed Denial of Service.
DMZ	Demilitarized Zone.
DoS	Denial of Service.
DRII	Disaster Recovery Institute International.
DRP	Disaster Recovery Plan.
EEUU	Estados Unidos.
ENTIC	Encuesta de Tecnologías de la Información y las Comunicaciones.
ESXi	Elastic Sky X Integrated.
GPG	Good Practice Guidelines.
GPU	Graphics processing unit.
HMI	Human-Machine Interface.
HTTP	Hypertext Transfer Protocol.
IACS	Industrial Automation and Control Systems.
IAM	Identity and Access Management.
IDS	Intrusion Detection System.
IIoT	Industrial Internet of Things.
IoT	Internet of Things.
IRBC	ICT Readiness for Business Continuity.
ISO	International Organization for Standardization.
LatAm	Latin America.
MINTIC	Ministerio de Tecnologías de la Información y las Comunicaciones.
MiPymes	Micro, pequeñas y medianas empresas.
MiTM	Man in the Middle.
MTPD	Maximum Tolerable Period of Disruption.
NAS	Network Attached Storage.
NFPA	National Fire Protection Association.

NIST	National Institute of Standards and Technology.
NVR	Network Video Recorder.
OWASP	Open Worldwide Application Security Project.
PAS	Publicly Available Specification.
PHVA	Planear - Hacer - Verificar – Actuar.
PLC	Programmable Logic Controller.
PYME	Pequeñas y medianas empresas.
RAT	Remote Access Trojan.
RDP	Remote Desktop Protocol.
RPO	Recovery Point Objective.
RTO	Recovery Time Objective.
SCADA	Supervisory Control and Data Acquisition.
SIEM	Security Information and Event Management.
SIM	Subscriber Identity Module.
SMB	Server Message Block.
SQL	Structured Query Language.
TI	Tecnologías de la Información.
TIC	Tecnologías de la Información y la Comunicación.
TO	Tecnologías de la operación.
USA	United States of America.
VM	Virtual Machine.
VPN	Virtual Private Network.
XSS	Cross Site Scripting.

Introducción

Implantar un Plan de Continuidad del Negocio (BCP) a nivel corporativo implica una inversión significativa de tiempo, recursos y compromiso organizacional. Este proceso debe seguir una metodología estructurada que integre activamente a las direcciones y niveles gerenciales, e incluya etapas criticas como la identificación y valoración de activos, la gestión de riesgos asociados, el análisis de impacto al negocio (BIA), el diseño de estrategias de recuperación, la socialización interna del plan y su mantenimiento continuo mediante pruebas y actualización periódica. En el contexto actual, donde los eventos de ciberseguridad son cada vez más frecuentes y disruptivos, implica que, para las micro, pequeñas y medianas empresas (MiPymes) también se vuelva esencial implementar acciones para garantizar la resiliencia organizacional. Sin embargo, para muchas MiPymes, los costos iniciales de implementación pueden representar una barrera significativa.

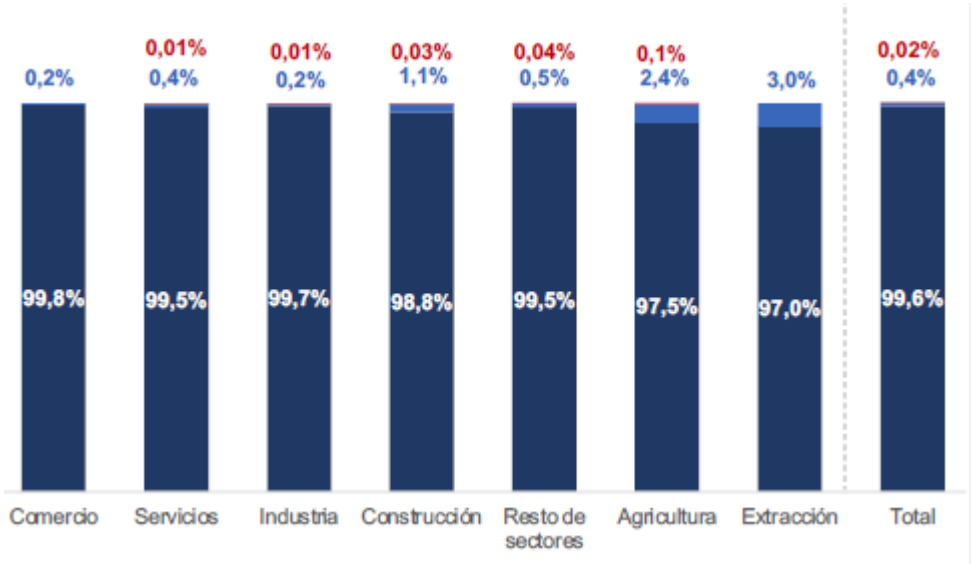
El problema surge cuando esta barrera económica lleva a no implementar ningún tipo de plan, lo que deja a las organizaciones altamente expuestas frente a eventos críticos. El riesgo de no implementar un BCP, ya sea por restricciones presupuestales u otras razones, expone a las organizaciones a una gestión inadecuada frente a situaciones de crisis, lo que puede traducirse en perdida de información crítica, daños reputacionales, impactos financieros y, en casos extremos, el cese indefinido de operaciones. La decisión de no actuar, motivada por limitaciones presupuestarias o falta de conciencia, se convierte así en un factor de vulnerabilidad estructural. Por lo tanto, para abordar esta problemática se propone tener una estrategia de desarrollo de planes de Continuidad del Negocio (BCP) más flexibles no tan estructurados como lo exigen las normas de certificación y adaptados a la realidad de las MiPymes.

Esta aproximación busca optimizar recursos y focalizar esfuerzos en los activos y procesos verdaderamente críticos para cada organización. Particularmente se plantea priorizar los riesgos asociados a la ciberseguridad, ya que representan una amenaza latente con alta probabilidad de ocurrencia. Amenazas como el phishing, ataques de fuerza bruta, malware, ransomware, entre otros, constituyen vectores comunes de interrupción, especialmente en sectores o regiones con limitada madurez cibernética. Esta orientación permitiría que las estrategias de continuidad estén alineadas con buenas prácticas de la industria y estándares internacionales sin exigir una implementación completa y onerosa desde el inicio.

Entonces, en consecuencia, definir un plan de continuidad de negocio incluso en versiones escalables y adaptadas, es una necesidad critica para organizaciones de cualquier tamaño. Cuantificar sus pérdidas puede ayudar a tomar decisiones sobre el impacto a corto, mediano y largo plazo ante un evento catastrófico que afecte a la compañía. En la Figura 1 se observa que, según la información reportada por la Dirección de Micro, Pequeña y Mediana Empresa del MINTIC y expuesta en la ponencia de [1] en "MiPymes: el pilar para la reactivación económica", las MiPymes representaban el 99.6% de las empresas en Colombia en 2021. A nivel internacional, las Naciones

Unidas reportan cifras similares, indicando que las MiPymes representan el 90% de las empresas, generando entre el 60 y el 70% del empleo y el 50% del PIB mundial [2].

Figura 1.
Unidades productivas por tamaño y sector. Tomado de [1].

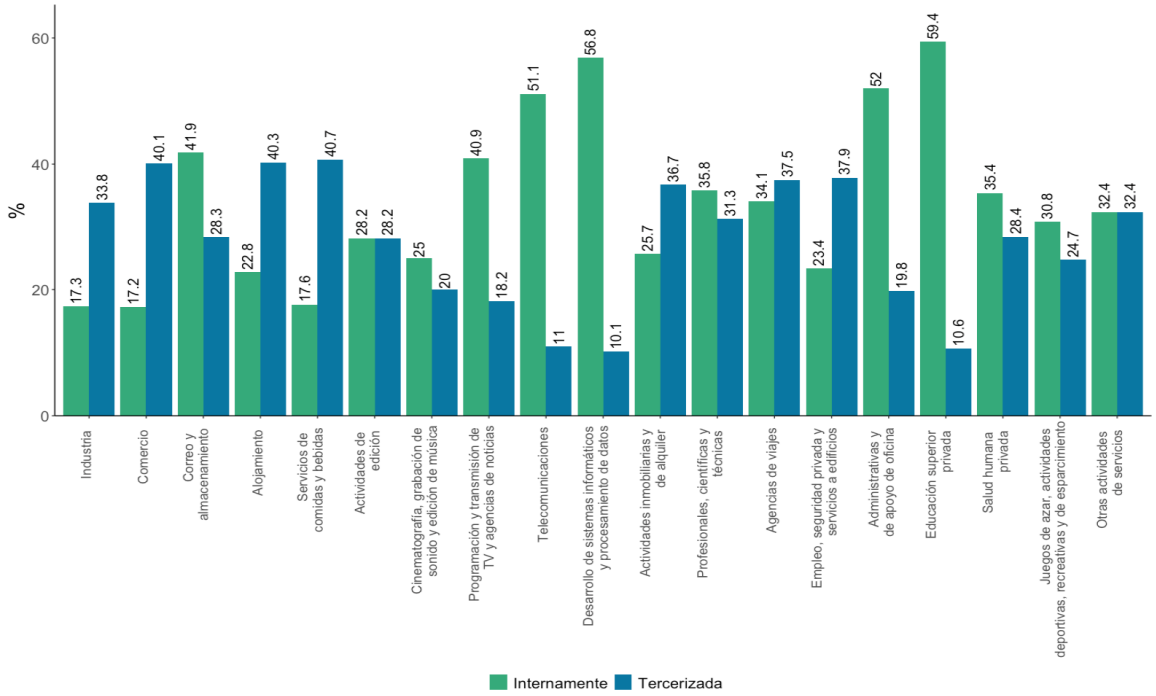


Nota: porcentaje representativo por cada tamaño relacionado por sector.

En el contexto colombiano, según [3], en su boletín técnico de la Encuesta de Tecnologías de la Información y las Comunicaciones en Empresas (ENTIC Empresas) 2020, reporta que solo el 17.2% de las empresas del sector comercio contaban con un área encargada de coordinar la implementación de las TIC internamente, y el 40.1% lo hacían de forma externa. Para las empresas de industria, los respectivos porcentajes fueron 17.3% y 33.8%, fíjese en la figura 2. Además, se indica que una de las principales causas de no tener personal contratado para ello está asociada al costo, lo que reduce la probabilidad de que estas empresas identifiquen los riesgos cibernéticos y cuenten con planes de continuidad de negocio.

Figura 2.

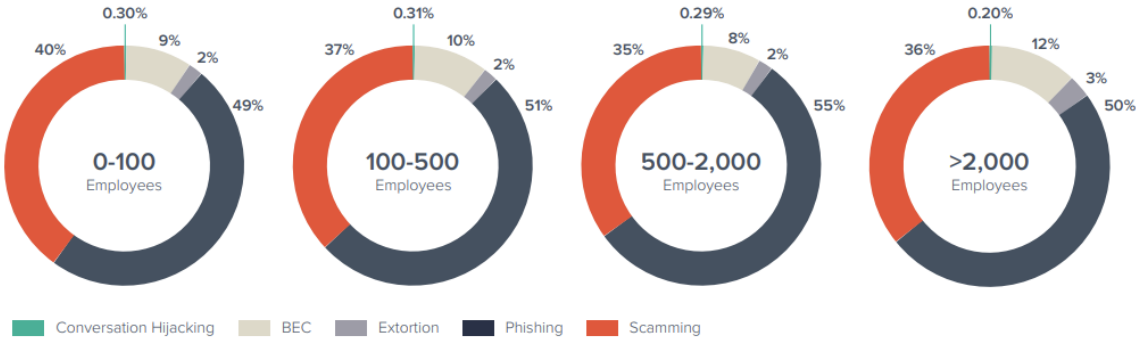
Porcentaje de empresas con áreas encargadas de coordinar TIC. Tomada de [3].



Nota: porcentaje de empresas que cuentan con un área o dependencia (diferente a la tradicional oficina de sistemas) encargada de coordinar la implementación de TIC (interna o externamente).

De acuerdo con lo anterior, es entonces necesario también hacer revisión de como las MiPymes se ven en el apartado de ataques, y, para dar un ejemplo de ello, [4] expone en la estadística presentada en la Figura 3, que en los tipos de ataques por email no hay gran diferencia en la distribución de los porcentajes de compromiso de acuerdo con el número de empleados, es decir, independientemente del tamaño, la tendencia se mantiene, y esto por ende nos permite inferir en que, al tener una estructura de seguridad menos definida, es probable que se genere una afectación mayor a la disponibilidad y, por ende, poner en jaque la operación.

Figura 3.
Tipo de ataques por email por tamaño de organización. Tomada de [4].



Nota: porcentaje de ataques discriminado por número de empleados.

Por lo tanto, teniendo en cuenta las estadísticas y la creciente cantidad de eventos de ciberseguridad a nivel mundial, es crucial contar con planes de continuidad que permitan mantener el negocio operativo. La información disponible puede ayudar a tomar decisiones sobre la aplicación de un BCP ante eventos de ciberseguridad que puedan afectar los sistemas informáticos y/u operativos según sea el objetivo de la compañía donde se pretenda implementar un estándar sin que ello conlleve a gastar altas sumas de dinero y tiempo productivo en hacer análisis profundos sobre soluciones implementables.

Pregunta de investigación

¿Qué estrategia podría ser utilizada en una MiPyme para desarrollar un BCP siguiendo el modelo de racionalidad limitada sin perder de vista las mejores prácticas propuestas por los estándares de seguridad de la información?

OBJETIVOS

OBJETIVO GENERAL

Diseñar una estrategia para la implementación de un BCP para eventos de ciberseguridad en las MiPymes del sector manufacturero de Colombia, utilizando el modelo de racionalidad limitada.

OBJETIVOS ESPECÍFICOS

- Identificar los riesgos cibernéticos más relevantes que afectan la disponibilidad en el sector propuesto, para que puedan ser tenidos en cuenta en la definición de la estrategia.

- Caracterizar los estándares de implementación de BCP en el contexto de ciberseguridad, identificando las prácticas que aporten a la reducción de riesgos en las MiPymes del sector seleccionado.
- Integrar en una estrategia los componentes mínimos viables para un BCP según las necesidades y capacidades de las MiPymes, utilizando el modelo de racionalidad limitada.
- Validar la estrategia en una prueba de escritorio con caso de estudio completo que permita la comprensión del resultado de la implementación un BCP.

1. Marco Teórico y Estado del Arte

1.1 Marco teórico

En la actualidad, hablar de ciberseguridad es común, sin embargo, los orígenes del término han pasado por múltiples revisiones a lo largo de la historia, adaptándose al contexto de cada época, lo que dificulta su definición. Para el presente trabajo, se usará la definición del Telecommunication Standardization expuesto por [5], que define en términos generales a la ciberseguridad como el conjunto de herramientas, políticas y conceptos de seguridad que establecen medidas para proteger un entorno cibernético, ya sea de un usuario o una organización. Esta definición es relevante dado que incluye conceptos administrativos que se añaden a la ciberseguridad y que no son visibles en otras definiciones.

Asimismo, debe considerarse que este trabajo se desarrolla en el contexto de las MiPymes; por ello, una definición con un nivel de tecnicismo excesivo podría generar una brecha entre quienes toman decisiones y quienes tienen a su cargo la protección de la información. En consecuencia, para efectos de esta investigación se adoptará una formulación más accesible, entendiendo la ciberseguridad como la manera en que organizaciones o individuos se preparan para reducir el riesgo de verse afectados por ciberdelincuentes [6]. Plantearla en estos términos no solo resalta su importancia, sino que también permite introducir el riesgo como un elemento central y diferenciador en la toma de decisiones.

No es sorprendente que el concepto de riesgos forme parte del lenguaje cotidiano en el ámbito corporativo, ya que está presente en prácticamente todos los procesos organizacionales. Cada actividad o función bajo responsabilidad de un área o persona conlleva un grado de exposición, lo que implica un impacto directo en la toma de decisión operativa y estratégicas por esta razón, se hace imprescindible comprender con mayor profundidad que es el riesgo, en que contexto se manifiesta y bajo qué criterios se deben establecer controles eficaces para su mitigación. Para ello, en [7] y [8] se indica como aquella probabilidad de que existan consecuencias económicas, sociales o ambientales en un sitio en particular, y que además, deberá existir en un periodo de tiempo específico, y, para que esto ocurra, deberá entonces existir una debilidad expuesta que pueda ser aprovechada por alguna amenaza, es decir, el riesgo en sí mismo evoca un conjunto de elementos probabilísticos que para cuantificarlos deberán ser identificados dentro del contexto al que pertenecen, de tal modo, que para evitar llegar a un punto de no retorno deberá ser gestionado correctamente pudiendo así ser mitigado de una forma que se evite llegar a un punto de no retorno.

En este sentido, [9]. describe la amenaza como una condición o evento adverso que podría presentarse y que, cuando ocurre, genera efectos negativos sobre los activos, tales como indisponibilidad, funcionamiento anómalo o pérdida de valor. Además, señala que estas

situaciones pueden originarse por causas naturales, accidentales o intencionadas y que, cuando coinciden con debilidades del sistema o se aprovechan de ellas, pueden desencadenar incidentes de seguridad. También por medio del marco de la gestión del riesgo de ISO 27005:2022 [10], se asegura que una amenaza, por sí sola, no constituye automáticamente un riesgo; más bien, actúa como un factor que puede materializarlo cuando existe una vulnerabilidad explotable y una probabilidad de ocurrencia suficiente, dando lugar a consecuencias concretas sobre los activos. En otras palabras, el riesgo se configura a partir de la interacción entre amenaza, vulnerabilidad e impacto, lo que resulta clave para priorizar decisiones y controles.

Ahora bien, de acuerdo con [9] la vulnerabilidad es una debilidad o fallo que puede ser aprovechado con fines maliciosos, y, además, podría estar presente en sistemas o entornos físicos o digitales, además estar asociada a la operación, componentes técnicos o incluso a los humanos. Cuando una vulnerabilidad se ve comprometida por una amenaza generará un impacto, y, por lo tanto, es necesario entenderla, para con este entendimiento poder hacer una gestión consiente y mesurada que permita a la organización definir en su caso particular la forma óptima que permita mitigar los impactos, y, que tal como se pretende abordar en este trabajo, las más críticas puedan contar con estrategias de continuidad de negocio en caso de un riesgo materializado.

En consecuencia, se podrá seguir metodologías ya establecidas que ayuden a las organizaciones en la gestión de los riesgos, y, para ello, normas como la ISO 27001:2022 [11] funcionan como marco general de la implementación de buenas prácticas de seguridad de la información, lo que llevará a la consecución de hitos de aseguramiento en entornos corporativos, que si bien una compañía pudiere no estar interesado en la certificación, bien se deberían adoptar los mejores marcos de trabajo, garantizando seguridad para sus clientes, proveedores y todos aquellos que pertenezcan a su línea de suministro. Por otro lado, la ISO 27005:2022 [12] funciona como guía en la gestión de riegos, enmarcando una metodología de identificar, evaluar y darle tratamiento a los riesgos identificados en estos marcos.

Además de lo anterior, en el marco de trabajo propuesto por la ISO 22301:2019 [13] se podrá hallar una herramienta de gestión central que aporte sustancialmente a la implementación de medidas para garantizar la continuidad de negocio de las compañías, ya que, si bien como se mencionó anteriormente aunque pudiere no existir la intensión de certificación, hacer uso de estrategias que garanticen la continuidad de negocio ayudará a sostener la operación diaria de la compañía y reducir el impacto asociado a la materialización de riesgos máxime cuando a hoy en pleno apogeo de la tecnología la probabilidad de impacto es alta en el contexto de ciberseguridad.

De acuerdo con lo anterior, es entonces de vital importancia ahondar en como un BCP es clave en la organización, y con este objetivo [14] y [15] concuerdan en que una buena forma de definir un BCP es como el proceso de identificación y posterior protección de los elementos críticos de una organización o negocio, y, con ello, se abre la posibilidad de gestionar correctamente la crisis,

manteniendo los procesos críticos en un nivel de operaciones aceptables, de tal modo, que se pueda mitigar el impacto del evento que causó dicha interrupción, y además quizá en algunos casos puntuales seguir conservando la ventaja competitiva, lo que, en un sentido organizacional es fundamental en un mundo donde el servicio, la reputación y la operación continua es vital.

En consecuencia, con todo lo anterior, se hace necesario entonces ahondar en este trabajo sobre conceptos que permitan comprender cómo se toman las decisiones a nivel organizacional. Para ello se introduce el término de racionalidad, mismo que ha sido acoplado para contextos de la economía y ha sido ampliamente explorado, pero que este trabajo de profundización basta con comprenderlo someramente con las definiciones aportadas por [16] y [17]. La racionalidad entonces podría explicarse como el modelo de toma de decisiones que se apoya en generar un contexto total del entorno, y para este fin deberá entonces, ahondar en todas las alternativas posibles, evaluar cada una de ellas, asociar un valor de resultado o utilidad, calcular las probabilidades y posteriormente optimizarlas por reglas de máximos y mínimos, reglas probabilísticas y reglas de certeza.

Este economista sostiene por medio de [16] y [18] que, en contextos reales, la toma de decisiones rara vez puede operar bajo un ideal de optimización completa, debido a limitaciones de información, tiempo disponible o incluso de capacidades propias para el procesamiento. Por ende, propone entonces, que los decisores tienden a seleccionar alternativas que resulten satisfactorias en función de un nivel de aspiración que define qué es aceptable para la organización en un momento dado. Esta lógica es especialmente útil cuando la decisión ocurre bajo escenarios de incertidumbre o presión operativa, dado que orienta el análisis hacia criterios mínimos verificables y reduce el costo asociado al tiempo invertido en evaluar todas las alternativas disponibles.

En esta misma línea, el autor explica en [18] que la racionalidad limitada opera mediante procesos de búsqueda limitada. De acuerdo con ello, el proceso consiste en explorar alternativas de manera incremental hasta encontrar una opción que cumpla el nivel de aspiración. Por su parte, [19] resalta que esta propuesta cobra sentido precisamente porque el decisor no dispone, ni tampoco necesita, disponer de información total para actuar de forma razonable en escenarios prácticos. Bajo este enfoque, decidir bien no equivale a agotar todas las opciones, sino a estructurar un proceso realista que permita elegir con evidencia suficiente y con un costo de análisis proporcional al contexto.

Luego, tanto [19] como [20] ahondan en cómo la racionalidad limitada se expresa en la organización a través de heurísticas y reglas de decisión simples, que permiten actuar con consistencia sin exigir cálculos complejos en cada evento. En términos de [18], estas reglas funcionan como mecanismos que reducen la carga cognitiva y estandarizan respuestas ante situaciones recurrentes, especialmente en entornos donde la urgencia y el riesgo obligan a actuar con rapidez. En consecuencia, documentar criterios mínimos, rutas de escalamiento y acciones prioritarias no debe entenderse como un reemplazo del análisis, sino como una forma de traducir

el análisis a operación. Es gracias a todas las bondades descritas por los autores alrededor de la racionalidad limitada y cómo puede ser aprovechada en las organizaciones que este trabajo se pretenda desarrollarlo con mayor profundidad.

1.2 Estado del arte

Múltiples autores han abordado la creación de BCP, siendo un tema bien explorado en contextos económicos. Actualmente, se busca implementar BCP en áreas individualizadas de una organización para integrarlo en las compañías independientemente de su tamaño. Dado que la era digital llegó para quedarse, es crucial revisar la literatura para identificar autores que han abordado la simplificación de la toma de decisiones para la implementación de un BCP ante eventos de ciberseguridad basados en el modelo de racionalidad limitada.

Un trabajo de maestría realizado en la Universidad de las Fuerzas Armadas de Ecuador por [21], titulado "Plan de Continuidad de Negocio BCP aplicado al Departamento de Tecnología de Laboratorios Bagó del Ecuador S.A.", aborda la metodología de implementación exhaustiva de un BCP, proporcionando un marco de referencia específico para TI, esta visión ayudará este trabajo a ahondar en las metodologías usadas en la industria, lo que significa que dará un punto de partida para entender en qué aspectos puede existir una simplificación, entendiendo que desde la norma de certificación los procedimientos son exhaustivos.

En el trabajo de maestría de [22], se expone un contexto importante de la aplicación de un BCP, además de contener una buena muestra teórica y técnica de los estándares actuales y buenas prácticas. Este desarrollo da muestras del despliegue de metodologías aplicables al alcance de seguridad informática que se pretende dar a este proyecto, de tal modo que, hay un acercamiento a implementaciones funcionales en el tamaño de industria que se quiere impactar, de modo que, servirá de base para identificar los aspectos esenciales que hoy funcionan en la industria siendo este un buen punto de partida.

Ahora bien, también se pueden encontrar propuestas con enfoques a los mínimos viables, es decir, se incluyen estrategias de racionalidad limitada que finalmente, conllevan a la consecución de hitos de simplificaciones, de tal modo que se vuelven adaptables a las empresas que tiene por objetivo impactar este trabajo. En [23] por ejemplo, se minimizan algunos de apartados sugeridos en los marcos metodológicos y se logra grosso modo entregar planes de continuidad llevando la mayor parte de esfuerzo hacia las actividades críticas, incluso aunque ello signifique sacrificar cierta operatividad de otros negocios importantes para la compañía de implementación.

Otra forma de simplificar los procesos es a través de la profundización de entendimiento de uno de los puntos vitales del BCP, y es que, es difícil pensar en un plan de continuidad que no esté

fundamentado en la cuantificación del impacto que puede generar una afectación del servicio al negocio mismo, por tanto, [24] habla sobre como establecer un BIA focalizado hacia las PYME y con ello, se aporta una visual de cómo podría simplificarse un análisis de impacto al negocio desde una perspectiva de compañías que tienen ciertas limitaciones al cumplimiento del alcance, o incluso se logran evidenciar mediante los ejemplos formas concretas de áreas que pueden ser impactadas de forma positiva y asertiva mediante este desarrollo.

Otro aporte importante para el alcance de este desarrollo lo hace [25], proponiendo estrategias basadas en la simplificación de los protocolos de ciberseguridad para PYMEs. Este trabajo ayuda a tener una vista clara de cómo se podría abordar de una manera simple pero coherente las necesidades de seguridad viables en una MIPYME, las cuales son útiles para la toma de decisiones en la implementación de BCP, es decir, se hace una revisión exhaustiva de las necesidades desde aspectos de ciberseguridad, de tal modo que ajusta el alcance de las implementaciones de BCP del mismo modo que este trabajo deberá hacerlo.

En general, los trabajos anteriormente expuestos han tenido un enfoque centrado en industrias del sector latinoamericano, entonces, para no sesgar la información y poder llegar a soluciones que sean aplicables a nivel global se hace necesario revisar trabajos como el propuesto por [26], en el cual se busca aprovechar el análisis de riesgos en TI de forma rápida para empresas del sector Pyme en Australia, quiere esto decir, que aportará entonces elementos que pueden ser diferenciadores a nivel de seguridad, dado que allí las amenazas y los riesgos pueden tener características diferentes y que quizá no estén muy caracterizadas en Latinoamérica lo que puede ayudar a marcar la diferencia en este trabajo. Además de lo anterior, este trabajo aportará la perspectiva de la importancia del conocimiento interno en la definición de riesgos, de tal modo que, sin definirlo, hace una exploración parecida a la que se desea con la implementación de modelo de racionalidad limitada.

Luego, si se pensara únicamente en TI, las prácticas abordadas por los trabajos anteriores apoyaran parámetros para la identificación de riesgos y la priorización basada en información, no obstante, el alcance del trabajo también requerirá de trabajos enfocados en aquellas industrias manufactureras en las cuales se integran las TO y sus elementos clave del día a día, y, por ello, [27] en sus capítulos 1 y 2 aportan y solidifican en este trabajo una vista de los riesgos de la manufactura y los aspectos de resiliencia. Este aporte además podría aportar ampliación del espectro en estrategias que permiten dar continuidad en entornos de manufactura, y, por lo tanto, el capítulo 4 propone una solución que podría ser aprovechada en el abordaje del diseño que se pretende plantear.

Ahora bien, con un enfoque hacia la ciberseguridad, en [27] se observa un rigor técnico suficiente para las TO, esto sin importar su tamaño, sin embargo, en [28] dedica un capítulo completo para analizar el impacto que generan los ataques cibernéticos sobre las MiPymes, que como bien se ha

ido hilando durante este documento será fundamental para comprender cómo implementar un BPC, podría incluso reducir el riesgo de las probables pérdidas ocasionadas por eventos de ciberseguridad, en otras palabras, tener un trabajo que haga revisión de los riesgos en un importante número de empresas MiPymes por un autor que opta por título de una maestría del ámbito de la economía fundamentará este trabajo bajo una viabilidad incluso desde lo monetario, buscando que al final para una compañía del tamaño mencionado puedan existir medidas basadas en buenas prácticas que busquen cubrir su continuidad de negocio.

Por último, también se evidenció en [29] una revisión cercana a la que se pretende hacer en este trabajo sobre las metodologías, guías y buenas prácticas planteadas por los entes que proponen las pautas para los sistemas de gestión hacia la continuidad de negocio, este aporte, es fundamental al proporcionar una recopilación de artículos basados en BCM y BCP y cuyo objetivo es dar una presentación clara de la evolución a través del tiempo, permitiendo comprender en gran medida como los sistemas actuales pueden mejorar problemas en tendencia, pero también como algunas prácticas se han mantenido en el tiempo gracias a su buena fundamentación hacia la industria. En resumen, los aportes presentados durante la exploración abarcan en gran medida aquellos enfoques que pretendan puedan enriquecer el resultado de este trabajo de profundización conllevando a entregar una herramienta que pueda aportar a la sociedad en la gestión de planes de continuidad en las MiPymes.

2. Metodología y resultados

El desarrollo de una estrategia que simplifique la implementación de un plan de continuidad de negocio en compañías donde generalmente no se implementan, requiere de una metodología que pueda ser lo suficientemente estructurada y alcanzable. Debido a que las metodologías pueden ser cualitativas, cuantitativas o mixtas, este trabajo se mantendrá en la metodología mixta, permitiendo valorar tanto parámetros estadísticos a partir del análisis de datos resultantes de la profundización, pero también adaptándola a resultados cualitativos, apalancando la adaptabilidad a un entorno que requiere ser simplificado, es decir, que aunque la estrategia misma busca ser simple, esto no necesariamente implica comprometer los estándares que a hoy han demostrado ser efectivos, más bien, se trata de adaptarlos a necesidades particulares. Para cumplir con este objetivo, este trabajo se compuso de 4 fases, y en ellas se abordaron consecutivamente aquellos hitos que en el proceso de desarrollo buscaron dar cumplimiento al objetivo general que se planteó.

Esta metodología se centró inicialmente en la identificación de riesgos de ciberseguridad, pasando posteriormente a la revisión de los estándares internacionales y conllevando luego al desarrollo de una estrategia que se apoya en un modelo de racionalidad limitada y que permite a las empresas MiPymes tener una herramienta adicional para la implementación de un BCP simplificado y,

finalmente, se contempló la validación de la estrategia propuesta a partir de la ejecución de un ejercicio que permitió poner a prueba su efectividad. A continuación, se describen las fases ejecutadas y las estrategias seguidas que soportan los resultados obtenidos en cada una de ellas, para que finalmente puedan ser tenidos en cuenta para quienes requieran de este enfoque en trabajos futuros.

2.1 Metodología y resultados fase 1

2.1.1 Metodología de la fase 1: identificar Riesgos relevantes en el sector manufacturero que afectan la disponibilidad.

La metodología implementada para alcanzar el objetivo específico 1 “Identificar los riesgos cibernéticos más relevantes que afectan la disponibilidad en el sector propuesto, para que puedan ser tenidos en cuenta en la definición de la estrategia.”, se estructuró en tres actividades que se describen a continuación:

2.1.1.1 Revisión de la literatura sobre amenazas y vulnerabilidades asociados a la disponibilidad.

Para lograr este objetivo se realizó una revisión en fuentes especializadas sobre las amenazas y vulnerabilidades que pueden ayudar a constituir un riesgo asociado a la disponibilidad, y, dado que este trabajo de profundización tiene como enfoque principal la industria manufacturera, entonces, se hizo esencial poder explorar los riesgos desde un contexto de las TI y TO. La búsqueda en las fuentes especializadas [9], [30], [12], [31], [32] y [33] permitieron abordar las metodologías y marcos de trabajo que han sido ampliamente aceptados y usados alrededor de ciberseguridad, por otra parte, también se tomó en consideración información relevante expuesta por [34], [35], [36], los cuales incluyeron papers de investigadores de estos proveedores de productos/servicios de ciberseguridad con la finalidad de obtener información sobre aquellos riesgos que tienen una mayor probabilidad de materialización y/o que generan mayor impacto al sector manufacturero. Como producto resultante de esta indagación se generó el listado de amenazas y vulnerabilidades con su respectiva definición dando un contexto acotado al alcance de estudio del presente trabajo, es decir, se presentan aquellos que generan afectación directa o parcial a la disponibilidad.

2.1.1.2 Identificación y clasificación de los riesgos relevantes en ciberseguridad con afectación a la disponibilidad.

A partir de la información obtenida en la actividad anterior, y, usando la metodología de riesgos de [10], se definieron los criterios para la evaluación cualitativa de riesgos en pro de calificar el impacto y la probabilidad de materialización de riesgos en escenarios, en los cuales las amenazas identificadas pudieran llegar a explotar las vulnerabilidades presentes en los activos identificados como comunes en el sector, y, de este modo, poder evaluar y ahondar en el impacto a la disponibilidad que las MiPymes manufactureras pueden llegar a tener en caso de que se materialicen dichos riesgos. El uso de esta metodología permitió tener el insumo principal para posteriormente trabajar en la proposición y definición de estrategias que permitieran mitigar estos riesgos identificados.

2.1.1.3 Exploración de casos de ciberseguridad perpetrados en el sector manufacturero.

Finalmente, para entender un poco mejor el impacto real que tiene la materialización de riesgos en la industria, es decir, fuera del contexto puramente teórico, y así permitiendo la observación directa del valor que agrega al marco corporativo la adopción de métodos de continuidad, se indagó en [28], [37], [38], [39], [40], [41], [42], es decir, que estas fuentes dieron como resultado información muy detallada para el contexto local y una fuente de información resumida para el contexto mundial sobre los efectos a los que se exponen las organizaciones, al no tomar medidas de mitigación, y, con ello, se aportó a una vista holística de las afectaciones reales. Esta metodología se usó además para hallar aquellos puntos relevantes que debían ser tenidos en cuenta en el planteamiento de la estrategia;

2.1.2 Resultados de la Fase 1: identificar Riesgos relevantes en el sector manufacturero que afectan la disponibilidad.

El proceso de identificación de riesgos en las organizaciones es una tarea fundamental para gestionar correctamente aquellos efectos adversos producto de factores implícitos en la operación diaria del negocio. Con este objetivo en mente es fundamental entonces poder apoyarse de una metodología que facilite el camino de identificación y clasificación de los riesgos, no obstante, este proceso es dispendioso y requiere de conocimiento base, por lo tanto, esta sección está centrada en facilitar la comprensión del método propuesto en [12], acotarlo al alcance de este trabajo de profundización y con ello poner sobre la mesa los riesgos cibernéticos asociados a la disponibilidad. Esta construcción fue además especialmente enfocada a aquellos riesgos que pueden afectar a las empresas MiPymes manufactureras, y, por lo tanto, puede ser incluso ajustado y replicado a los casos de uso de cada organización.

En consecuencia, en la tabla 1 se procedió a realizar la definición de activos, y, para ello, fueron seleccionados aquellos que comúnmente se encuentran presentes en las empresas del segmento elegido, además, se definió un tipo que clasifica a cada activo de información, y finalmente se ubicó en el grupo de tecnología donde es comúnmente usado, es decir, si pertenece a TI o TO o ambos, respectivamente. Luego en la tabla 2 se recopiló una versión simplificada de las amenazas frecuentemente asociadas a fallos que resultan en una afectación a la disponibilidad, bien sea directa o indirectamente. no obstante, dado que en materia de amenazas hay muchos componentes de valor a tener en cuenta, se deja la versión ampliada de la tabla 2 como anexo 1, y allí se pueden observar las familias de amenazas, la variante especifica que se seleccionó acompañada de una descripción ampliada según las fuentes de la literatura consultadas, además de un par de ejemplos de la variante, luego se proponen algunas de las tácticas y técnicas en donde se podrían enmarcar según [43] y finalmente columnas para especificar el tipo de tecnología donde pueden aparecer.

Tabla 1
Identificación de activos de información.

Clase (TI/TO)	Tipo	Entorno común
Correo / Suite en la nube	Servicio SaaS de comunicaciones/colaboración	TI
ERP / Contabilidad	Software/Aplicación de negocio	TI
Servidor de archivos / NAS	Infraestructura/Hardware de almacenamiento	TI
Endpoints	Hardware	TI
Red de datos	Redes/Comunicaciones	TI
Perímetro / VPN	Redes/Comunicaciones/Seguridad perimetral	TI
Conexión a Internet	Servicio externo de comunicaciones	TI
Sitio/Página web	Servicio / información publicada	TI
Servidores	Infraestructura/Hardware	TI
Backups / Copias	Servicio de respaldo/Datos respaldados	TI
PLC	Hardware	TO
HMI	Hardware	TO

SCADA/Historiador	Software	TO
Estación de ingeniería	Hardware	TO
Gateway IIoT/DMZ	Hardware	TO
CCTV / NVR	Hardware	TI
Administradores de sistemas	Personas	TI/TO

Tabla 2

Identificación de amenazas.

Familia	Variante	Descripción	Ejemplos	PRESENCIA EN TI	PRESENCIA EN TO
Malware	Ransomware	Ataque malicioso en el cual los atacantes cifran datos e información de una compañía [44].	**LockBit, BlackCat**	X	X
Malware	Downloader/Dropper	Archivo ejecutable que está diseñado para introducir malware habitualmente actúa como un instalador que descarga el malware desde servidores remotos a través de Internet [9].	**Emotet** como loader de TrickBot/IcedID, **SmokeLoader/Dofoil** (carga payloads adicionales)	X	X
Malware	Logic bomb	Fragmento de código malicioso que está oculto dentro de un programa legítimo. Permanece inactivo hasta que se cumple una o varias condiciones específicas definidas en su lógica y una vez activado, ejecuta una acción dañina [9].	**UBS PaineWebber 2002, Fannie Mae 2008–2009** – intento de "time/logic bomb" descubierto antes de activarse.	X	X

Malware	Rootkit	Herramientas o "kit" de programas electrónicos que permiten a un atacante tener acceso al root del sistema generalmente ocultando código, rutas y archivos [45].	**LoJax (UEFI), MoonBounce (UEFI)**.	X	X
Malware	RAT (Remote Access Trojan)	Es una herramienta o programa de administración remota que permite controlar un sistema a través de una red, esto es generalmente a través de una puerta trasera (backdoor) [9].	**PlugX/Korplug** –, **njRAT/Bladabindi** – RAT.	X	X
Malware	Malvertising	Es una técnica maliciosa que consiste en la utilización de anuncios digitales aparentemente legítimos como vehículo para distribuir malware o redirigir al usuario a sitios web maliciosos [9], [46].	**Campañas Zloader vía malvertising, BATLOADER/FakeBat vía anuncios maliciosos.**	X	

Ingeniería social / Compromiso de credenciales	SIM-swapping	El SIM swapping o en español suplantación de tarjeta SIM, es un ataque de ingeniería social en el cual un delincuente suplanta a la víctima ante el operador de telefonía móvil, logrando transferir el número de teléfono de la víctima hacia una tarjeta SIM en poder del atacante [47].	**LAPSUS$** empleó SIM-swapping para comprometer cuentas, **Caso Jack Dorsey (Twitter, 2019)** – secuestro de línea por SIM swap.	X	
Denegación de servicio	DoS/DDoS	Es un intento de interrumpir, bloquear o negar el flujo de información de un servicio, red o servidor mediante la creación de tráfico ilegitimo o malicioso que culmina en lentitud, falta de respuesta y/o no acceso para los usuarios finales [34], [48].	**Mirai botnet, Mēris**.	X	X

Denegación de servicio	Botnet	Las botnets son redes de dispositivos que han sido comprometidos, y que son usados de forma organizada, programada y autónoma para tareas de origen malicioso, algunas de las actividades comunes atraviesan desde la generación de tráfico en masa hasta la distribución de malware [49].	**Emotet botnet** (tras su reactivación, distribución masiva), **TrickBot botnet** (ecosistema de crimeware).	X	X
Ataques a aplicaciones web	SQL Injection	Ataque que consiste en insertar una sentencia de SQL en alguno de los métodos de entrada de datos a la aplicación a través del cliente, su finalidad es exponer, alterar o borrar información relevante de la base de datos [50].	**SQL reflection, SQL de boole**	X	

Ataques a aplicaciones web	Cross-Site Scripting (XSS)	Inyección de scripts maliciosos en sitios web que afecta a usuarios finales [42].	**Gusano "Samy" (MySpace, 2005)** – propagación masiva vía XSS, **TweetDeck**– XSS permitió ejecución automática de RTs.	X	
Amenaza interna (Insider)	Empleado/contratista malicioso	Se llama insider a una persona, bien sea empleado, exempleado o proveedor que tiene o tuvo acceso a la información de la compañía y que utiliza este privilegio de manera indebida, y de este modo pone en riesgo la seguridad de la organización [51], [52].	**Tesla 2020 – intento de soborno para introducir ransomware**, frustrado al denunciar el empleado (caso DOJ/FBI).	X	X
Minería ilícita	Criptojacking	Es un ataque en el cual un atacante hace uso de forma encubierta de los recursos de cómputo de una víctima para minar criptomonedas sin su consentimiento [53].	**TeamTNT** en contenedores/Kubernetes (Hildegard, Black-T). **Kinsing** explotando servicios cloud/containers para minar XMR.	X	
Movimiento lateral TI a TO	Propagación hacia IACS	Salto desde TI a **HMI/SCADA/PLC** por	**TRITON/TRISIS (HatMan)** contra controladores de seguridad Triconex, **INDUSTROYER2**		X

		DMZ/segmentación débil [54].	dirigido a subestaciones eléctricas (IEC-104).		

Posteriormente, en la tabla 3 se procedió con la definición de aquellas vulnerabilidades que pueden estar presentes para los activos elegidos en contextos de afectación a la disponibilidad y que posteriormente pudieran a ser aprovechados por alguna de las amenazas escogidas. Paso seguido se aprovecha la información para la construcción de los escenarios de riesgo, no obstante, primero se definieron en las tablas de la 4 a la 6 el alcance, el grado, la recuperabilidad y la criticidad del servicio como criterios de clasificación que apoyan la comprensión y calificación de impacto, es decir, la criticidad que representa para las compañías la materialización de un riesgo en el escenario dado.

Tabla 3

Identificación de vulnerabilidades.

Categoría	**Definición breve**
Zero-day	las vulnerabilidades de día cero son en su más simple expresión fallos en cualquier software, sistema o subsistema que no ha sido identificado con anterioridad, es decir, que no ha sido expuesto al público como una vulnerabilidad conocida, por lo tanto, no existe una cura, parche o metodología previa para la corrección, y por lo tanto, puede ser explotada hasta que su revisión de pie a la corrección por parte de los desarrolladores o de controles que conlleven a la reducción de probabilidad de explotación [55].
IoT/IIoT débil	Se refiere a la probabilidad de explotación de dispositivos IoT no protegidos en redes industriales o corporativas, abarca desde las violaciones a la autenticación básicas, obsolescencia de aplicaciones asociadas a dispositivos IoT, hasta las fallas de funcionamiento y disponibilidad en entornos de red o físicos [35].
Convergencia TI/TO insegura	Riegos asociados a la falta de protección en la red de convergencia entre las conexiones de redes administrativas TI y TO en industrias [54].

Seguridad móvil débil	En esta categoría no se simplifica a una definición, dado que la masificación del uso de dispositivos móviles en entornos personales y corporativos ha generado a su vez incremento de los riesgos de seguridad en el entorno móvil. Estos riesgos abarcan malware en dispositivos móviles como, por ejemplo, troyanos bancarios, spyware en apps de consumo, ataques de phishing dirigidos a SMS o aplicaciones de mensajería (smishing), filtraciones de datos bien sea por pérdida o robo del dispositivo o por apps maliciosas. La adopción de tecnología móvil, junto con políticas de BYOD expone a las organizaciones a amenazas como aplicaciones maliciosas descargadas fuera de tiendas oficiales, redes Wi-Fi inseguras utilizadas por empleados y vulnerabilidades en sistemas operativos móviles desactualizados [56].
Software no autorizado/pirata	La utilización de software sin licencia o no autorizado (pirata) conlleva importantes riesgos de ciberseguridad. En primer lugar, el software pirata suele provenir de fuentes poco confiables y es común que venga acompañado de malware insertado por los atacantes. Además, el uso de software no legítimo implica no recibir actualizaciones ni parches de seguridad del proveedor. Una herramienta pirata puede quedarse sin parches durante meses o años, exponiendo a los sistemas a vulnerabilidades ya conocidas y explotables. Asimismo, ejecutar software crackeado puede violar políticas corporativas y legales [57].
Parches tardíos/ausentes	No aplicar actualizaciones y parches de seguridad de forma oportuna es una de las causas primordiales de incidentes de ciberseguridad. Muchas brechas se producen explotando vulnerabilidades ya conocidas en sistemas desactualizados. Cuando un proveedor publica un parche para corregir una falla crítica (por ejemplo, una vulnerabilidad de día cero en un servidor web o en Windows), los atacantes a menudo invierten esfuerzos en crear exploits tan pronto como el parche se anuncia, aprovechando que muchas entidades tardan días o semanas en aplicarlo. Este retraso crea una ventana de riesgo. Adicionalmente, el ransomware ha sido uno de los ataques que más ha aprovechado esta brecha dado que generalmente usa vulnerabilidades que ya han sido parchadas a través de los años pero que no han sido correctamente gestionadas [58].

Configuraciones erróneas	Las configuraciones erróneas o débiles en sistemas y servicios constituyen otro vector frecuente de ataques. Las malas configuraciones provienen generalmente de descuidos humanos o falta de controles en los sistemas, ejemplos de esto son, dejar una base de datos en la nube sin contraseña de acceso, utilizar valores por defecto inseguros en un servidor, o no restringir puertos y servicios innecesarios en los perímetros. Estas brechas de configuración permiten a los atacantes explotar fácilmente el sistema sin necesidad de vulnerabilidades sofisticadas [59].
Segmentación de red inadecuada	La segmentación de red inadecuada está asociada a la inexistencia o mala configuración de los segmentos de una red. Segmentar la red es un ejercicio que consiste en dividir la red en segmentos o zonas de disponibilidad aisladas entre sí, esto es especialmente útil para evitar que una red sea penetrada de forma deliberada por algunas amenazas y/o atacantes, por lo tanto, una inadecuada segmentación de red permitirá a un intruso moverse lateralmente y llegar a los activos críticos. En conclusión, una segmentación deficiente se traduce en que todo está conectado con todo, hay pocas o incluso ninguna VLAN, o hay ausencia de firewalls que logren controlar de forma adecuada el tráfico interno entre departamentos, y cuentas con permisos en múltiples entornos. Esto amplifica enormemente el impacto de cualquier intrusión [60].
Wi-Fi insegura	Redes que soportan protocolos inalámbricos que han sido mal configurados, permitiendo ataques como Evil Twin/MiTM/de-auth, generalmente se da por presencia de PSK débiles/redes abiertas o protocolo 802.1X mal validado [61].

Virtualización / nube híbrida mal gestionada	a virtualización y la nube híbrida han aumentado la flexibilidad operativa, pero también han ampliado el panorama de riesgos de seguridad. En virtualización, uno de los escenarios más críticos es el **escape de máquina virtual**, donde un atacante compromete una VM y logra escalar hasta el hipervisor o el host, afectando potencialmente todas las máquinas alojadas. Este riesgo se vuelve especialmente grave cuando existen vulnerabilidades en plataformas como VMware ESXi o Hyper-V; de hecho, se han reportado casos recientes en los que fallas del hipervisor fueron aprovechadas por ransomware para obtener privilegios elevados y comprometer múltiples VM de forma simultánea [62]. En nube híbrida, la combinación de nube pública y privada incrementa la complejidad y, con ello, la superficie de ataque. A esto se suman debilidades frecuentes relacionadas con la adopción incompleta del modelo de responsabilidad compartida, problemas de cumplimiento y privacidad, y fallos técnicos como configuraciones inseguras de VPN o segmentación deficiente, que facilitan el movimiento de una afectación entre entornos. Finalmente, la gestión de identidades y permisos entre ambos dominios se mantiene como un punto de riesgo recurrente [63].

Escasez de Talento en Ciberseguridad	La escasez de profesionales de ciberseguridad es un riesgo a nivel corporativo y global, esto significa que las empresas no logran cubrir totalmente los cargos especializados en seguridad, lo que, de uno u otro modo, conlleva a dejar equipos de trabajo sobrecargados o funciones críticas sin cobertura. A hoy existe un déficit significativo de talento en ciberseguridad a nivel mundial, y se estima que para 2030 la cifra de escases sea de cerca de 85 millones de profesionales. La falta de talento implica a muchas organizaciones operar con equipos de seguridad reducidos, sin la capacidad suficiente de monitorear amenazas 24/7, responder en incidentes de forma eficaz o implementar todas las mejores prácticas de protección. Según [64], dos tercios de las organizaciones reconocen enfrentar riesgos adicionales debido a la falta de habilidades en sus plantillas de ciberseguridad. Por ejemplo, una empresa puede tener excelentes herramientas técnicas como firewalls, SIEM, sistemas de IDS, pero si carece de personal capacitado para administrarlas y analizar las alertas, esas inversiones no darán frutos y algún ataque crítico puede pasar inadvertido. Este problema se agrava con el rápido aumento y complejidad de las amenazas, mientras la formación de nuevos profesionales no crece al mismo ritmo.
Gestión Inadecuada de Identidades y Accesos (IAM)	Se da cuando no se administran de forma consiente los mecanismos para identificar usuarios/entidades, autenticar su acceso y autorizar sus privilegios. Esto suele reflejarse en cuentas huérfanas, privilegios excesivos, roles mal definidos, ausencia de segregación de funciones, uso de credenciales compartidas o métodos de autenticación débiles, y falta de revisión periódica de permisos [65].
Apis Inseguras	Deficiencias en las interfaces expuestas o consumidas por aplicaciones que, por fallas de diseño, configuración, desarrollo u operación, no controla adecuadamente quién accede, a qué puede acceder y bajo qué condiciones. Esto suele ocurrir cuando la API carece de controles consistentes en todo su ciclo de vida, por ejemplo: autorización deficiente, autenticación débil, validación insuficiente de entradas, falta de límites de consumo (rate limiting), inventario/versionado incompleto o exposición de endpoints no documentados. [66].

De acuerdo con el proceso de gestión de riesgos (figura 4) propuesto en la metodología de [10] se hizo necesario definir los criterios para la valoración del riesgo. De acuerdo con el rigor metodológico del estándar, es posible definir criterios de evaluación bien sea de una forma cuantitativa, es decir, a partir de datos provenientes de estadísticas públicas o incluso de las propias de la organización, o usar valores cualitativos, definiendo parámetros de cualidad que permitan dar una valoración tanto en probabilidad como en consecuencia de acuerdo con los escenarios en cuestión.

En consecuencia de ello, y en busca de abordar de una forma más general los criterios para la valoración del riesgo que posteriormente serán el insumo que se acotará y adaptará al análisis de riesgos propuesto dentro de la estrategia de BCP, se definen en la tabla 4 los criterios cualitativos para la valoración de la probabilidad y en la tabla 5 los criterios cualitativos para la valoración del impacto, incluyendo en su descripción parámetros que permitan encaminar la valoración de acuerdo al contexto que se esté abordando en materia de disponibilidad. Luego, en la tabla 6 se construyó la matriz cualitativa resultante de mezclar los criterios de probabilidad e impacto permitiendo dar completitud a los parámetros necesarios para realizar la evaluación.

Figura 4.
Proceso de gestión de riesgos para la seguridad de la información. Tomado de [10].

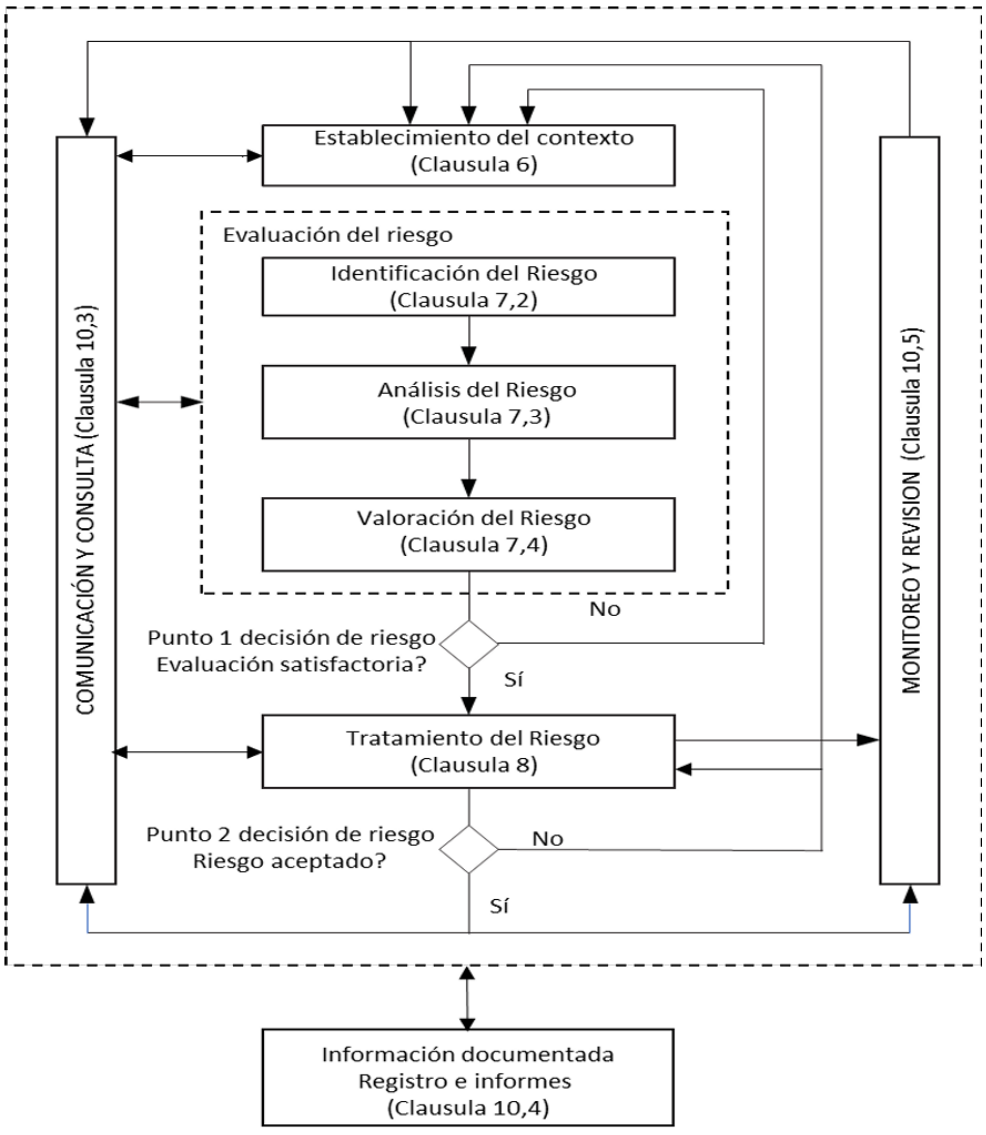


Tabla 4.
Criterio de selección para probabilidad. Adaptada de [12].

Nivel	Rangos	Descripción
1	Raro	La fuente de riesgo tiene muy pocas posibilidades de alcanzar su objetivo utilizando uno de los métodos de ataque considerados. La probabilidad del escenario de riesgo es muy baja.
2	Improbable	La fuente de riesgo tiene relativamente pocas posibilidades de alcanzar su objetivo utilizando uno de los métodos de ataque considerados. La probabilidad del escenario de riesgo es baja.
3	Posible	La fuente de riesgo es capaz de alcanzar su objetivo utilizando uno de los métodos de ataque considerados. La probabilidad del escenario de riesgo es significativa.
4	Probable	La fuente de riesgo probablemente alcanzará su objetivo utilizando uno de los métodos de ataque considerados. La probabilidad del escenario de riesgo es alta.
5	Casi seguro	La fuente de riesgo alcanzará con toda seguridad su objetivo utilizando uno de los métodos de ataque considerados. La probabilidad del escenario de riesgo es muy alta.

Tabla 5.
Criterio de selección impacto a la disponibilidad. Adaptada [12].

Nivel	Rangos	Descripción
1	Muy bajo	**Consecuencias insignificantes para la organización**: No hay consecuencias sobre las operaciones o el desempeño de la actividad, es decir, la organización superará la situación sin demasiada dificultad (se consumirán los márgenes).
2	Bajo	**Consecuencias significativas pero limitadas para la organización:** Degradación del rendimiento de la actividad sin consecuencias, es decir, la organización superará la situación a pesar de algunas dificultades (funcionamiento en modo degradado).
3	Moderado	**Consecuencias sustanciales para la organización:** Alta degradación en el desempeño de la actividad, es decir, la organización superará la situación con serias dificultades (funcionamiento en modo altamente degradado), sin impacto sectorial o estatal.
4	Alto	**Consecuencias desastrosas para la organización:** Incapacidad de la organización para garantizar toda su actividad, con

		posibles consecuencias graves. Lo más probable es que la organización no supere la situación.
5	Muy alto	**Consecuencias sectoriales o normativas más allá de la organización:** Dificultad para para asegurar una función reguladora o una de sus misiones de vital importancia.

Tabla 6.
Matriz cualitativa de criterios del riesgo. Adaptada de [12].

Probabilidad	**Consecuencia**				
	Muy bajo	**Bajo**	**Moderado**	**Alto**	**Muy alto**
Casi seguro	Tolerable	Inaceptable	Inadmisible	Inadmisible	Inadmisible
Probable	Tolerable	Inaceptable	Inaceptable	Inadmisible	Inadmisible
Posible	Aceptable	Tolerable	Tolerable	Inaceptable	Inadmisible
Improbable	Aceptable	Aceptable	Tolerable	Inaceptable	Inaceptable
Raro	Aceptable	Aceptable	Tolerable	Tolerable	Tolerable

Como resultado del proceso anterior y a partir de la selección de activos, amenazas y vulnerabilidades, en la tabla 7 se presentan los resultados de las evaluaciones de los escenarios de riesgo a los que están expuestas las organizaciones del sector en estudio. Además, también se incluyó una descripción de las posibles consecuencias en el contexto de la disponibilidad en caso de que dichos riesgos llegaren a materializarse, no obstante, esto siempre requerirá de profundidad, abarcando. De esta forma, las MiPymes obtienen la observabilidad necesaria para iniciar la gestión del riesgo conforme al tratamiento que se decida aplicar, es decir, pueden determinar cuáles riesgos serán tratados mediante controles definidos en un BCP. En conclusión, este proceso permite tomar acciones orientados a la reducción del impacto en el negocio, e incluso definir cuáles de ellos serán transferidos o asumidos.

Tabla 7.
Escenarios de riesgo.

ID	Activo	Amenaza	Vulnerabilidad	Escenario (evento)	Consecuencias a la disponibilidad	Probabilidad	Impacto a la disponibilidad	Valor cualitativo Impacto
R-001	Correo / Suite en la nube (SaaS)	SIM-swapping	Gestión Inadecuada de Identidades y Accesos (IAM)	Suplantación de SIM permite tomar cuentas y con ello se aplican bloqueos de las mismas	Buzones y calendarios de usuarios críticos sin acceso	Posible	Bajo	Tolerable
R-002	ERP / Contabilidad	Ransomware	Parches tardíos/ausentes	Cifrado de servidor/app/BD del ERP	Servicio ERP fuera de línea; procesos contables y transacciones detenidas	Probable	Muy alto	Inadmisible
R-003	ERP / Contabilidad	Criptojacking	APIs inseguras	Despliegue de minero en hosts del ERP vía API expuesta	Degradación notable del ERP; errores y caídas intermitentes	Posible	Moderado	Tolerable
R-004	Servidor de archivos / NAS	Ransomware	Configuraciones erróneas	Cifrado masivo en compartidos por permisos excesivos	Unidades compartidas indisponibles; procesos dependientes sin documentos	Probable	Muy alto	Inadmisible

R-005	Servidor de archivos / NAS	Logic bomb	Gestión Inadecuada de Identidades y Accesos (IAM)	Eliminación/cifrado programado por cuenta privilegiada	Repositorios perdidos; servicio de archivos fuera de línea hasta restauración	Improbable	Moderado	Tolerable
R-006	Endpoints	Malvertising	Seguridad móvil débil	Infecciones desde anuncios/tiendas no confiables obligan a aislar equipos	Estaciones puntuales fuera de servicio; usuarios operan en modo manual	Posible	Muy bajo	Aceptable
R-007	Endpoints	Ransomware	Parches tardíos/ausentes	Brote cifra perfiles locales y desconecta de red	Puestos inoperables; imposibilidad temporal de usar aplicaciones	Casi seguro	Moderado	Inadmisible
R-008	Red de datos	DoS/DDoS	Segmentación de red inadecuada	Tráfico malicioso se propaga sin contención	Conectividad interna caída o muy degradada; servicios dependientes interrumpidos	Probable	Moderado	Inaceptable
R-009	Red de datos	DoS/DDoS	Zero-day	Falla en equipo core provoca reinicios	Interrupciones de red; servicios intermitentes	Probable	Moderado	Inaceptable
R-010	Perímetro / VPN	DoS/DDoS	Configuraciones erróneas	Ausencia de rate-limit/mitigación	Acceso remoto degradado o	Probable	Moderado	Inaceptable

				adecuada en gateways	intermitente; teletrabajo afectado			
R-011	Perímetro / VPN	DoS/DDoS	Parches tardíos/ausentes	Explotación de vulnerabilidad conocida del gateway	Cortes recurrentes del servicio VPN hasta corrección	Probable	Moderado	Inaceptable
R-012	Conexión a Internet	DoS/DDoS	Configuraciones erróneas	Saturación del enlace sin blackholing/filtrado efectivo	Servicios públicos y salida a Internet indisponibles; impacto transversal	Probable	Alto	Inadmisible
R-013	Conexión a Internet	Empleado/contratista malicioso (Insider)	Escasez de Talento en Ciberseguridad	Cambios no autorizados en routing/ACL	Conectividad externa perdida; servicios expuestos no disponibles	Posible	Alto	Inaceptable
R-014	Sitio / Página web (pública)	DoS/DDoS	Configuraciones erróneas	Flood HTTP sin WAF/limitación adecuada	Sitio público degradado o con cortes intermitentes	Posible	Moderado	Tolerable
R-015	Sitio / Página web (pública)	SQL Injection	Parches tardíos/ausentes	Consultas abusivas bloquean/derriban la BD	Sitio con errores frecuentes o caídas intermitentes	Probable	Muy bajo	Tolerable
R-016	Servidores (infraestructura)	Ransomware	Virtualización / nube híbrida mal gestionada	Propagación a hosts/VMs y cifrado de datastores	Varios servicios fuera de línea de forma simultánea	Casi seguro	Muy alto	Inadmisible

R-017	Servidores (infraestructura)	Criptojacking	Parches tardíos/ausentes	Minero consume CPU/IO en hipervisores/VMs	Degradación general del rendimiento; caídas puntuales	Probable	Moderado	Inaceptable
R-018	Backups / Copias	Logic bomb	Gestión Inadecuada de Identidades y Accesos (IAM)	Borrado/alteración programada de repositorios de respaldo	Imposibilidad temporal de recuperar servicios; indisponibilidades prolongadas	Improbable	Moderado	Tolerable
R-019	Backups / Copias	Ransomware	Configuraciones erróneas	Repositorios de copia cifrados por exposiciones de red	Restauración no disponible; servicios dependientes permanecen caídos	Posible	Muy alto	Inadmisible
R-020	PLC (TO)	Movimiento lateral TI a TO	Convergencia TI/TO insegura	Acceso desde TI por DMZ débil	Paro de celdas/líneas; control automatizado interrumpido	Probable	Moderado	Inaceptable
R-021	PLC (TO)	Movimiento lateral TI a TO	IoT/IIoT débil	Autenticación básica/obsoleta permite acceso a PLC	Procesos automatizados interrumpidos; operación manual necesaria	Probable	Moderado	Inaceptable
R-022	HMI (TO)	Ransomware	Parches tardíos/ausentes	Estaciones HMI cifradas	Operación local indisponible; tareas de campo detenidas	Posible	Muy alto	Inadmisible

R-023	HMI (TO)	Movimiento lateral TI a TO	Convergencia TI/TO insegura	Malware de TI afecta HMIs operativas	Degradación o pérdida del control de planta	Posible	Moderado	Tolerable
R-024	SCADA / Historiador	DoS/DDoS	Segmentación de red inadecuada	Tráfico malicioso afecta colectores/servidores SCADA	Pérdida de telemetría/monitoreo; decisiones operativas a ciegas	Probable	Moderado	Inaceptable
R-025	SCADA / Historiador	Ransomware	Virtualización / nube híbrida mal gestionada	Cifrado de VMs de supervisión/registro	Monitoreo y registros indisponibles	Casi seguro	Muy alto	Inadmisible
R-026	Estación de ingeniería (TO)	Movimiento lateral TI a TO	Parches tardíos/ausentes	Toma de control de estaciones de ingeniería	Descarga de cambios bloqueada; paros por cargas no verificadas	Probable	Moderado	Inaceptable
R-027	Estación de ingeniería (TO)	Ransomware	Configuraciones erróneas	Proyectos cifrados; imposibilidad de compilar/descargar	Ajustes y mantenimiento detenidos	Probable	Moderado	Inaceptable
R-028	Gateway IIoT / DMZ	Movimiento lateral TI a TO	IoT/IIoT débil	Compromiso del gateway deja ruta a TO	Interrupciones en comunicaciones TO–TI; pérdida de telemetría	Probable	Bajo	Inaceptable
R-029	Gateway IIoT / DMZ	DoS/DDoS	Configuraciones erróneas	Saturación del gateway por falta de limitación	Enlaces TO–TI indisponibles; colas de mensajes	Probable	Moderado	Inaceptable

R-030	CCTV / NVR	Botnet	IoT/IIoT débil	Reclutamiento del NVR satura CPU/almacenamiento	Video en vivo y grabaciones indisponibles en zonas; cobertura reducida	Improbable	Bajo	Aceptable
R-031	CCTV / NVR	Ransomware	Parches tardíos/ausentes	Cifrado del NVR	Servicio de video degradado o con cortes; consulta de evidencias reciente afectada	Posible	Moderado	Tolerable
R-032	Administradores de sistemas (personas)	Empleado/contratista malicioso (Insider)	Gestión Inadecuada de Identidades y Accesos (IAM)	Baja intencional de servicios críticos	Varios servicios quedan fuera de línea hasta reversión autorizada	Posible	Muy alto	Inadmisible
R-033	Administradores de sistemas (personas)	Empleado/contratista malicioso (Insider)	Escasez de Talento en Ciberseguridad	Cambios urgentes mal ejecutados	Servicios afectados por errores de cambio; recuperación dependiente de expertos	Probable	Muy alto	Inadmisible

En este punto, una vez identificados y evaluados los escenarios de riesgo a partir de la metodología de riesgos escogida, surge la necesidad de avanzar, en tanto, se requiere pasar de tener una visión general del riesgo, hacia la comprensión del proceso decisional que conlleva a su tratamiento. En este sentido, la gestión del riesgo, más allá de la identificación y valoración, exige un ejercicio racional que considere no solo la magnitud del impacto, sino también las limitaciones y capacidades de la organización para responder ante cada escenario, esto quiere decir, que se debe limitar a tratar aquellos riesgos en los que se está en capacidad, preocupándose principalmente por los que puedan afectar la existencia misma, pero también preocupándose de que cuando se opte por tratarlo, la medida de tratamiento o control no sea mucho más costoso que el mismo impacto de materialización.

Entonces, de acuerdo con [18], no basta con que un proceso sea racional, pues dicha racionalidad no solo aporta mayor certeza en las decisiones, sino que también implica un costo adicional derivado del rigor de validación requerido al evaluar las opciones disponibles. Por ello, el sistema de toma de decisiones debe tender a seleccionar puntos de satisfacción, calibrando la necesidad que busca cubrirse al actuar. En este trabajo, resulta esencial priorizar los riesgos clave conforme al alcance de las compañías que se espera impactar, y así tomar las acciones necesarias para garantizar la continuidad del negocio incluso en momentos adversos. Este enfoque reconoce que, aunque la optimización absoluta es deseable, en la práctica los tomadores de decisiones, independientemente del tamaño de la empresa, enfrentan restricciones de tiempo, información y capacidad cognitiva.

Ahora bien, si se desea comprender cuales riesgos pudieren tener una criticidad mayor, entonces, se deberá tener una fuente de información mínima que pueda ayudar a asociar el riesgo en función de su impacto, y, por ende, es necesario también comprender el alcance que podría implicar la materialización de un riesgo. Para ello se ha explorado sobre aquellos casos de ciberseguridad que han sido perpetrados o que tienen relevancia al sector manufacturero, y como resultado de esta actividad, se presentan entonces el resumen y conclusiones de los casos más representativos en los últimos 10 años, y ello se abarca con especial cuidado de incluir el contexto latinoamericano, sin dejar de lado el ámbito global, ya que los eventos internacionales establecen las tendencias y marcos de referencia que pueden influir en la evolución de la ciberseguridad en la región. Al comprender los patrones y estrategias detrás de estos incidentes, se facilita la generación de mecanismos de prevención y respuesta, contribuyendo así a una gestión de riesgos más efectiva y alineada con las mejores prácticas del sector.

¿Qué se dice a nivel mundial acerca de los ciberataques en el contexto de la manufactura?

Según [38], la industria manufacturera fue el sector más atacado durante 2021 y 2022 siendo el ransomware el más destacado. Entre los argumentos más sólidos asociados a esta tendencia de ciberataques se encuentra el crecimiento de la digitalización, factor clave para la mejora en rentabilidad y eficiencia, lo que finalmente se traduce en el crecimiento corporativo. Además, la industria manufacturera también es un actor esencial en la economía circular, siendo consumidor

de industrias como la de bienes de consumo, energía, movilidad, alimentos, entre otras y a su vez también es proveedor para dichas industrias. Adicionalmente, este sector también ha ido creciendo en la adopción de tecnologías de la industria 4.0, lo que genera hiperconectividad al integrar en su operación automatización e IoT. En consecuencia, adopción de más elementos dependientes de las tecnologías de la información y las operaciones incrementan la superficie de ataque y la necesidad de más controles, lo que no necesariamente está 100% adoptado por todas las compañías. Por lo tanto, una afectación a este sector no solo tendrá impacto sobre él mismo sino también sobre su cadena de suministro y viceversa.

Casos relevantes de la industria Manufacturera

Grupo Nutresa - Colombia

En abril de 2023 la compañía confirmó un ataque a su infraestructura de TI, se indicó además que activó un protocolo para este tipo de ataque con la finalidad de poder evitar su propagación, como plan de acción se aislaron las plataformas de TI causando indisponibilidad del servicio [40], [41], [67]. Según información aportada por [40] el grupo que se adjudicó el ataque fue LockBit con la intención de negociar, y posterior a ello en [68] se informa acerca de exposición de datos producto del ataque publicados en la web de víctimas del grupo atacante.
Impactos: exposición de datos sensibles, indisponibilidad del servicio, pérdidas económicas.

IFX Networks - Colombia

En septiembre de 2023 la compañía con presencia en 17 países sufrió ataque de ransomware que afectó a 762 empresas y aunque no se informó específicamente el número de empresas por sector, algunas de las empresas reportaron perdidas por falta de registros por el ciberataque lo que generó millonarias pérdidas. La afectación se extendió por 7 días, no obstante, fueron paulatinamente haciendo la recuperación de sus clientes y para el día 21 informaron sobre una restauración del 90% de sus clientes [69], [39] [37].
Impactos: indisponibilidad del servicio, pérdidas económicas.

Casos relevantes en el contexto Internacional

Saliendo un poco del contexto latino en la tabla 8 se observa también una recopilación de los ataques perpetrados a nivel internacional en industrias manufactureras de múltiples sectores y tamaños en los últimos 15 años, esto es, con el objetivo de generar mayor observabilidad acerca de los impactos que puede generar la materialización de los riesgos en el mundo, ya que como se ha mencionado en múltiples momentos de este documento, si bien el foco son las compañías MiPymes manufactureras, los impactos no son ajenos a ninguna compañía ni región, es decir, las afectaciones no distinguen a sus víctimas, que incluso en muchos casos pueden llegar a ser afectados de forma colateral.

Tabla 8.

Ciberataques a empresas manufactureras.

Año	Organización / País	Ataque (vector)	Impacto en Operaciones
2010	Planta nuclear de Natanz (Irán)	Malware Stuxnet (gusano ICS vía USB)	Sabotaje de centrifugadoras (≈1000 dañadas), retraso producción
2014	Acería (Alemania)	Ataque dirigido ICS (phishing a red corporativa)	Daño físico severo: alto horno fuera de control, parada no planificada de la planta
2017	Renault-Nissan (Francia/Reino Unido/etc.)	Ransomware WannaCry (worm exploiting SMB vuln.)	Producción detenida en 5 plantas por 1-2 días; líneas reanudadas tras limpieza, pérdidas recuperables
2019	Norsk Hydro (Noruega, global)	Ransomware LockerGoga (credenciales AD)	Varias fábricas paradas, otras en modo manual; ≈$40M pérdidas en 1ª semana; recuperación total tomó semanas
2020	Honda (Japón, global)	Ransomware Ekans/Snake (phishing sospechado)	Producción detenida en plantas de EEUU, Europa, India, Brasil por cerca de 1 día; operaciones restauradas desde backups, impacto “mínimo” declarado
2021	JBS Foods (Brasil, global)	Ransomware REvil (acceso RDP/VPN)	Paralización de 47 plantas cárnicas en Australia y suspensión de faenas en EE.UU/Canadá por ~3 días; la empresa pagó USD $11M para resolver
2022	Bridgestone Americas (USA/LatAm)	Ransomware LockBit 2.0 (mov. lateral en red)	Redes de manufactura de neumáticos desconectadas; **producción detenida ~1 semana** en fábricas de EE.UU y Centroamérica. Datos corporativos comprometidos, investigación en curso.
2022	Proveedor de Toyota (Japón)	Ataque a cadena suministro (malware desconocido)	Fábricas Toyota en Japón (14 plantas) suspenden actividades por 1 día completo (13k vehículos no producidos); reanudación tras restaurar sistemas del proveedor.

Nota: se exponen algunos de los casos más renombrados del sector manufacturero en los últimos 15 años a nivel mundial. Fuente: elaboración propia.

Para concluir esta fase es importante indicar que los riesgos y escenarios de riesgo evidenciados a lo largo de esta construcción, son una forma de compartir una metodología replicable para enfocar esfuerzos que permitan posteriormente apostar por instaurar medidas que conlleven a la mitigación de aquellas afectaciones directas a la disponibilidad, incluso para próximos trabajos. Además de lo anterior también era importante conocer un poco de cómo el mundo ha sido

afectado cuando estos riesgos han sido materializados, lo que conlleva a ampliar la visión de consecuencias de no tener planes que conlleven a continuar operaciones en momentos de interrupción.

2.2 Metodología y resultados de la fase 2.

2.2.1 Metodología de la fase 2. Caracterizar los estándares.

Para la consecución del segundo objetivo específico "Caracterizar los estándares de implementación de BCP en el contexto de ciberseguridad, identificando las prácticas que aporten a la reducción de riesgos en las MiPymes del sector seleccionado." se estructuró la metodología en tres actividades, las cuales se describen a continuación.

2.2.1.1 Exploración de estándares internacionales de BCP.

De acuerdo con consultas realizadas en navegadores de búsqueda en internet, buscadores académicos, bases de datos bibliográficas y también con el uso de herramientas de inteligencia artificial, se identifican aquellos estándares que aportan al plan de continuidad de negocio. Las propuestas de [9], [52], [70], [71], [72], [73] permitieron abordar el análisis desde perspectivas de TI y TO, y además viabilizar su uso en contextos de racionalidad limitada. Esta metodología permitió conocer el alcance de cada propuesta, profundizar en conceptos de estándares vs guías de buenas prácticas y habilitar en conocimiento los parámetros necesarios para posteriormente caracterizarlos evitando el sesgo y la orientación por conocimiento previo.

2.2.1.2 Caracterización de los estándares de BCP seleccionados.

A partir de la información de las entidades que proponen marcos de trabajo, guías o estándares se identificaron cuáles eran compatibles, adaptables y coherentes con las necesidades de las empresas del sector manufacturero, especialmente en TI y TO, de tal modo que a partir del análisis de su estructura se identificaron los puntos clave que aportan para posteriormente usarlos con el objetivo de reducir los riesgos en las MiPymes. En consecuencia, el resultado obtenido fue la caracterización del estándar elegido, en el cual se detallan sus alcances, clausulas y características particulares que permiten abordar el alcance de este trabajo.

2.2.1.3 Análisis de las cláusulas del estándar y asociación de buenas prácticas aplicables al sector manufacturero para la reducción de riesgos.

Una vez caracterizado el estándar seleccionado y habiendo profundizado en su estructura, se relacionaron los aportes conceptuales que se relacionan a la reducción de los riesgos. Con esto, se identificó qué hacer, no obstante, aprovechando la investigación realizada en la actividad anterior, también se relacionaron las buenas prácticas que permiten ahondar en el cómo hacerlo, y, a partir de prácticas sugeridas en las guías se viabiliza la reducción de los riesgos asociados a las MiPymes identificados durante la fase 1 de este trabajo de profundización. Esta metodología propició la construcción de una tabla que permitió relacionar los escenarios de riesgo, las cláusulas de tratamiento pro-continuidad del estándar y las buenas prácticas sugeridas la implementación de controles que impactan directamente en la reducción del impacto a la continuidad, resultando en propuestas claras para la reducción de los riesgos que deben ser incluidos en el diseño de la estrategia implementación de BCP.

2.2.2 Resultados de la Fase 2: Caracterizar los estándares.

De acuerdo con la exploración realizada usando palabras clave como: continuidad, BCP, gestión de crisis, contingency planning, standard, guideline y framework. Se identifica que tanto ISO como NIST constituyen las entidades más relevantes en la formulación de estándares relacionados con la Continuidad del Negocio (BCP) para entornos de Tecnología de la Información (TI). Sin embargo, es importante señalar que no todas las buenas prácticas se encuentran contenidas explícitamente en estos estándares. De hecho, para las MiPymes en Colombia, la implementación estricta de dichos estándares puede resultar compleja y demandante. Por este motivo, existen entidades dedicadas específicamente a ofrecer guías prácticas de aplicación más sencillas y enfocadas. En este contexto destacan organizaciones como DRII, que proporciona guías basadas en prácticas profesionales orientadas al análisis, la estrategia, la implementación y la mejora continua del BCP. De manera similar, el BCI también propone guías de mejores prácticas caracterizadas por su flexibilidad, facilitando así una implementación más accesible y ajustada a las necesidades específicas del sector MiPyme. En este listado se resumen los estándares y guías de buenas prácticas que aportan hacia los BCP con la respectiva entidad que la propone:

ISO 22301:2019

La norma ISO 22301:2019 establece los requisitos para implementar y mantener un Sistema de Gestión de la Continuidad del Negocio (BCM), basado en el ciclo de mejora continua PHVA (Planificar-Hacer-Verificar-Actuar). Este estándar proporciona una estructura formal para identificar amenazas, evaluar impactos mediante un análisis de impacto al negocio (BIA), y establecer estrategias para asegurar la continuidad de las operaciones críticas ante disrupciones, incluyendo tanto entornos tecnológicos (TI) como físicos (TO). Su enfoque se centra en la resiliencia

organizacional, la recuperación y la planificación basada en riesgos, siendo aplicable a organizaciones de cualquier tamaño o sector [74], [72].

ISO/PAS 22399:2007

ISO/PAS 22399:2007 fue una especificación pública preliminar de la ISO que estableció las bases conceptuales para la gestión de la continuidad operativa y la preparación ante incidentes. Su propuesta se centra en la identificación de amenazas (naturales, tecnológicas o intencionales), la evaluación de su impacto en las operaciones, y el desarrollo de una cultura organizacional proactiva orientada a la preparación, respuesta y recuperación. Aunque no es certificable, fue fundamental en la transición hacia la ISO 22301, y se destaca por su aplicabilidad universal, tanto en el sector público como privado [71], [75].

NFPA 1600 (2016)

NFPA 1600 es una norma americana desarrollada por la National Fire Protection Association que proporciona criterios fundamentales para la gestión de emergencias, desastres y continuidad del negocio. Su estructura abarca planificación, mitigación, respuesta y recuperación, con énfasis en eventos físicos o naturales, pero también incluye aspectos tecnológicos. La edición 2016 consolida su enfoque integral incluyendo la gestión de crisis, continuidad operativa (COOP) y seguridad de la información, siendo ampliamente utilizada en sectores industriales donde las operaciones físicas y el entorno TO son predominantes [76].

NIST SP 800-34 Rev. 1

El NIST SP 800-34 Rev. 1 proporciona una guía detallada para la planificación de contingencias en sistemas de información, enfocándose en la preparación, respuesta y recuperación ante interrupciones tecnológicas. Desarrollado por el National Institute of Standards and Technology (NIST), este marco orienta la creación de planes de continuidad tecnológica (ITCP), recuperación ante desastres (DRP), y planes de operaciones alternas, integrando análisis de impacto (BIA), evaluación de riesgos, pruebas y mantenimiento continuo. Aunque no constituye un sistema de gestión completo como ISO 22301, es el marco más próximo en el ecosistema NIST a un BCMS, siendo especialmente útil para organizaciones con alta dependencia de sistemas TI, como ocurre en entornos industriales digitalizados o con componentes ciberfísicos [77].

ISO/IEC 27031:2025

La norma ISO/IEC 27031:2025 proporciona directrices actualizadas para establecer y mantener la preparación de las tecnologías de la información y comunicación (TIC) en apoyo a los sistemas de continuidad del negocio. Esta segunda edición reemplaza oficialmente a la versión de 2011, introduciendo una estructura más clara, enfoques ampliados en gestión de riesgos TIC, e integración con estrategias organizacionales modernas, incluyendo la respuesta a incidentes y la resiliencia basada en servicios en la nube. Es particularmente útil en entornos TI y TO interconectados como los de la industria manufacturera, donde la disponibilidad de sistemas y servicios digitales es esencial para la operación.

Su orientación modular permite aplicar desde soluciones básicas hasta estrategias avanzadas, facilitando la toma de decisiones racionales en entornos donde la información, los recursos o el tiempo son limitados, alineándose así con la teoría de la racionalidad limitada. Además, esta versión reconoce explícitamente la dependencia de proveedores externos y plataformas en la nube, lo que permite a las MiPymes planificar bajo criterios de viabilidad técnica y contractual sin necesidad de recursos sofisticados internos [78], [32].

Good Practice Guidelines (GPG) 7.0 edition – BCI

La versión 7.0 de las Good Practice Guidelines (GPG) del Business Continuity Institute introduce una actualización integral al enfoque del ciclo de vida de la gestión de la continuidad del negocio (BCM), alineado con ISO 22301:2019 y reforzado con principios de resiliencia organizacional. Esta edición mantiene sus seis fases fundamentales —Política y Programa, Análisis, Diseño, Implementación, Validación y Mejora— pero amplía su enfoque hacia un modelo más holístico que incorpora gestión del cambio, liderazgo organizacional y toma de decisiones bajo incertidumbre. También incluye guías sectoriales y un mayor énfasis en continuidad tecnológica, interdependencias críticas y comunicación efectiva. Su carácter no prescriptivo, junto con su estructura modular, la hace altamente adaptable a las capacidades operativas de MiPymes, permitiendo progresividad en su adopción y aplicación [73].

DRII Professional Practices

El marco de este documento estructura el proceso de continuidad en diez áreas clave, incluyendo evaluación de riesgos, análisis de impacto (BIA), desarrollo de estrategias, implementación de planes, pruebas y auditoría. Su enfoque técnico y sistemático está orientado a profesionales certificados en continuidad, y es altamente robusto en entornos tecnológicos críticos (TI), aunque también incorpora consideraciones para procesos físicos (TO) cuando estos tienen dependencia digital. Se utiliza como base para las certificaciones CBCP y ABCP de DRII [79].

Proceso de selección de estándares

Después de realizado el recorrido de documentación asociada a planes de continuidad de negocio, se hallaron materiales de gran valor, no obstante, el enfoque de este trabajo está orientado a poder trabajar con las mejores prácticas de los estándares, por lo tanto, en la tabla 9 se presenta la regla de elegibilidad que permite metodológicamente realizar la selección pro caracterización únicamente de aquellos documentos que representan rigurosamente un estándar, y, que adicionalmente, estaba en vigencia al momento de la ejecución de esta actividad. La razón de dirigir la decisión únicamente a estándares vigentes está orientada a aprovechar la robustez que ofrecen los estándares. No obstante, también se debe reconocer que en sí mismos, los estándares solo establecen en sus cláusulas la definición de los parámetros clave de una implementación, impulsando directamente el qué hacer, más no el cómo hacerlo, y, con ello, será posible para cada compañía elegir el cómo hacerlo. Esto quiere decir, que los estándares tienen un bajo nivel de sesgo desde una perspectiva sectorial y de tamaño, lo que a su vez permite que se aborden por medio de

otras metodologías el objetivo de especificidad, tanto al tamaño, sector y necesidades propias de cada compañía, por lo tanto, esta selección se hace fundamental para el alcance de este trabajo.

Tabla 9.
Regla de elegibilidad.

Criterio	Valores aceptados	Resultado
¿Es un estándar certificable?	SI	Aceptado (De lo contrario es rechazado)
¿Está vigente?	SI	Aceptado (De lo contrario es rechazado)

Después del análisis realizado de acuerdo con las reglas de elegibilidad (tabla 10), se definió que es la ISO 22301:2019 el único estándar que logra cumplir a cabalidad con todos los criterios de aceptación propuestos, y, gracias a que su alcance se adapta tanto a tecnologías de la información como a tecnologías de la operación y a que además se encontró dentro de su periodo de vigencia dentro del desarrollo de este documento se hizo necesario caracterizarlo brevemente permitiendo comprender sus aportes en materia de continuidad de negocio para las MiPymes. De acuerdo con ello, en la tabla 11 se procedió a estructurar la caracterización de los atributos que contiene el estándar. Esta caracterización permite aproximarse de forma específica a cada una de las cláusulas contenidas y asimilar porqué es ampliamente aceptada para posteriormente analizar cómo contribuye en la reducción del riesgo.

Tabla 10.
Resultado de elegibilidad.

Descripción	**¿Es un estándar certificable?**	**¿Está vigente?**	**Observación**	**Resultado**
ISO 22301:2019	SI	SI		Aceptado
ISO/PAS 22399:2007	SI	NO	Fue reemplazado por la ISO 22301	Rechazado
NFPA 1600 (2016)	SI	NO	Fue reemplazado por la NFPA 1660 (está enfocada en	Rechazado

			desastres naturales)	
NIST SP 800-34 Rev. 1	NO	SI	Es una guía técnica no un estándar	Rechazado
ISO/IEC 27031:2025	NO	SI	Aún está en proceso de estudio en Colombia, para calificar como estándar certificable	Rechazado
Good Practice Guidelines (GPG) 7.0 edition – BCI	NO	SI	Es una guía de buenas practicas	Rechazado
DRII Professional Practices	NO	SI	Es una guía de buenas practicas	Rechazado

Tabla 11.
Caracterización del estándar.

Atributo	Caracterización
Tipo y objetivo	Norma de requisitos para establecer, implementar, mantener y mejorar un BCMS. Cláusula 1 (Alcance) define el propósito; los requisitos aplicables están en Cláusulas 4–10.
Estructura y enfoque	Sigue la estructura armonizada y el ciclo PHVA. Requisitos por cláusula: Cl. 4 Contexto, Cl. 5 Liderazgo, Cl. 6 Planificación, Cl. 7 Soporte, Cl. 8 Operación, Cl. 9 Evaluación del desempeño, Cl. 10 Mejora.
Alcance / aplicabilidad	Aplica a organizaciones de cualquier tipo y tamaño. El alcance del BCMS se determina en Cl. 4.3, coherente con Cl. 4.1

	(Contexto) y Cl. 4.2 (Partes interesadas); el BCMS se establece en Cl. 4.4.
Elementos operativos clave	Cl. 8 Operación: 8.1 Planificación y control operacional → 8.2 BIA y evaluación de riesgos → 8.3 Estrategias y soluciones → 8.4 Planes y procedimientos (respuesta/recuperación) → 8.5 Ejercicios y pruebas → 8.6 Evaluación de documentación y capacidades.
Evaluación y mejora	Cl. 9: 9.1 Seguimiento/medición/análisis/evaluación; 9.2 Auditoría interna; 9.3 Revisión por la dirección. Cl. 10: No conformidades, acciones correctivas y mejora continua.
Documentos satélite	ISO 22313:2020 (guía para aplicar requisitos de Cl. 4–10 de 22301). ISO 22300 (vocabulario) — edición 2025 vigente.
Relación con ciberseguridad/IRBC	La preparación de TIC para sostener la continuidad (IRBC) se desarrolla en ISO/IEC 27031:2025, que complementa especialmente la Cl. 8 (operación/planes/estrategias)

Finalmente, tras analizar pausadamente las cláusulas de [72], [71] en el anexo 2 se detalló cómo cada uno de los riesgos puede ser mitigado si se adoptan las sub-cláusulas del estándar elegido. En este punto, se identifica que el componente más grande asociado a dar continuidad está con una gran medida en poder tener estrategias de retorno, definición de tiempos objetivo de restauración, en fortalecer el flujo de la comunicación y finalmente establecer procedimientos rápidos y claros para atender momentos de interrupción. En consecuencia, a partir de este resultado, también se usan las buenas prácticas sugeridas por [72], [32], [73]. Este insumo de información nutre el resultado presentado en la tabla 12, el cual, es en esencia, un resumen rápido y depurado de los resultados presentados en el anexo 2, y que permite conectar de una forma directa a los escenarios de riesgo obtenidos a partir de la investigación ejecutada en la fase 1 de este desarrollo, versus aquellas prácticas que deben plantearse como controles que aportan hacia la reducción del impacto a la disponibilidad, y que además, son clave en la definición de parámetros de continuidad incluidos posteriormente en el diseño de la estrategia.

Tabla 12.
Riesgos vs prácticas utilizables para reducción.

ID	Interpretación de la sugerencia del estándar	Resumen de buena práctica
R-001	Planes usables con pasos/recursos/dependencias	Procedimientos de operación/comunicación
R-002	Estrategias/soluciones alineadas a RTO/RPO	Aislamiento

R-002	Planes de continuidad operables	Procedimientos de operación/comunicación
R-003	Estrategias para recuperar funciones	Imagen original/verificar integridad
R-003	Planes operativos	Procedimientos de operación/comunicación
R-004	Estrategias/soluciones de recuperación	Back up
R-004	Plan de continuidad	Procedimientos de operación/comunicación
R-005	Estrategias de protección/rollback	back up
R-005	Plan de continuidad	Procedimientos de operación/comunicación
R-006	Estrategias para mantener operación	Equipos/servicios de respaldo en funciones criticas
R-006	Plan/procedimiento	Procedimientos de operación/comunicación
R-007	Estrategias de recuperación masiva	Imagen original/verificar integridad
R-007	Plan operativo	Procedimientos de operación/comunicación
R-008	Estrategias de resiliencia	AntiDDoS
R-008	Plan de respuesta	Procedimientos de operación/comunicación
R-009	Estrategias inmediatas	Equipos/servicios de respaldo en funciones criticas
R-010	Estrategias de disponibilidad	Equipos/servicios de respaldo en funciones criticas
R-010	Plan operativo	Procedimientos de operación/comunicación
R-011	Plan de reversión	Procedimientos de operación/comunicación
R-012	Estrategias de conectividad	Equipos/servicios de respaldo en funciones criticas
R-012	Plan operable	Procedimientos de operación/comunicación
R-013	Planes/procedimientos de continuidad	Procedimientos de operación/comunicación
R-013	Estrategias de segregación	Segmentación de roles
R-014	Estrategias/soluciones web	Equipos/servicios de respaldo en funciones criticas

R-014	Plan de cutover	Procedimientos de operación/comunicación
R-015	Plan de contención/restore	Procedimientos de operación/comunicación
R-016	Estrategias por servicio	Back up
R-016	Playbooks por servicio	Procedimientos de operación/comunicación
R-017	Estrategias de saneo	Imagen original/verificar integridad
R-017	Procedimiento operativo	Procedimientos de operación/comunicación
R-018	Estrategias de confianza	Back up
R-018	Plan de verificación/restore	Procedimientos de operación/comunicación
R-019	Estrategias de respaldo robustas	Back up
R-020	Estrategias TO seguras	Segmentación de redes
R-021	Estrategias de aislamiento/bypass	Aislamiento
R-021	Procedimiento Operativo Estándar de operación manual	Procedimientos de operación/comunicación
R-022	Estrategias de reinstalación	Imagen original/verificar integridad
R-022	Playbook en sitio	Procedimientos de operación/comunicación
R-023	Procedimiento Operativo Estándar de aislamiento	Procedimientos de operación/comunicación
R-024	Procedimiento Operativo Estándar de operación degradada	Procedimientos de operación/comunicación
R-025	Estrategias de respaldo/restore	Back up
R-025	Plan de reconstrucción	Procedimientos de operación/comunicación
R-026	Procedimiento Operativo Estándar de préstamo seguro	Procedimientos de operación/comunicación
R-027	Estrategias de reposición rápida	Back up
R-027	Playbook de reimagen	Procedimientos de operación/comunicación
R-028	Procedimiento Operativo Estándar de aislamiento	Procedimientos de operación/comunicación
R-029	Estrategias anti-DDoS en borde	AntiDDoS
R-029	Playbook con proveedor	Procedimientos de operación/comunicación
R-030	Estrategias de contención	Aislamiento

R-030	Procedimiento Operativo Estándar de limpieza/rotación	Procedimientos de operación/comunicación
R-031	Estrategias de reposición	Back up
R-031	Plan de reinstalación	Procedimientos de operación/comunicación
R-032	Estrategias de continuidad operativa	Establecimiento de turnos y accesos de contingencia
R-033	Estrategias de capacidad	Documentación viva
R-033	Garantizar competencia para funciones BCMS	Capacitación en roles críticos

2.3 Metodología y resultados de la fase 3.

2.3.1 Metodología de la Fase 3: diseño de la estrategia.

Para alcanzar el objetivo específico 3 “Integrar en una estrategia los componentes mínimos viables para un BCP según las necesidades y capacidades de las MiPymes, utilizando el modelo de racionalidad limitada”, se estructuraron dos actividades, las cuales son explicadas a continuación:

2.3.1.1 Definición de componentes mínimos viables de un BCP.

A partir de la comprensión de los riesgos, la caracterización de los estándares y las sugerencias de buenas prácticas para la reducción del riesgo asociado los escenarios tipo de las MiPymes manufactureras, se definieron los componentes mínimos viables, que permitieran dar sostenimiento a un BCP en el tiempo, buscando mantener alcances y viabilidad, es decir, que no solo se definieron componentes asociados a características técnicas sino también metodológicas, guiándose con el método PHVA. La metodología permitió la construcción de una tabla que permitió resumir los pasos deseados, el aporte que se cada uno pretendió cubrir de acuerdo con la racionalidad limitada y cómo se aplicaría a la estrategia, además se construyó un diagrama de flujo con la ruta de implementación.

2.3.1.2 Desarrollo de la estrategia utilizando el modelo de racionalidad limitada.

A partir del mínimo viable propuesto en la actividad anterior se realizó la estructuración final de la estrategia para la implementación del BCP que permite a partir de pasos específicos encaminar a las MiPymes en la ejecución, mejorando la comprensión no solo el qué (forma en que están construidos los estándares), sino también el cómo hacerlo (producto de las buenas prácticas), para

que por medio de información contundente y ejemplos se puedan lograr llegar a diversos públicos. Esta metodología permitió realizar el desarrollo de un documento escrito que contiene paso a paso la estrategia para la implementación de un BCP para las MiPymes, ejemplos y elementos clave, y, además, el planteamiento de instrumentos y formatos que permitieran asimilar lo descrito en ella.

2.3.2 Resultados de la Fase 3: diseño de la estrategia.

Para generar una estrategia que apoye la implementación de un plan de continuidad de negocio en las MiPymes y que además pueda aprovechar las características del modelo de racionalidad limitada, sin que ello conlleve a que sea una iniciativa que pueda perder vigencia rápidamente en el tiempo o incluso no tener la relevancia esperada dentro del contexto corporativo, primero es esencial comprender los resultados obtenidos en la fase anterior de este trabajo. La tabla 14 nos expresó de una forma contundente que a partir de las necesidades de mitigación de riesgo que presenta el sector la acción inmediata está dirigida hacia la implementación de controles que permitan reducir el impacto ante un evento catastrófico, sin embargo, también el alcance del objetivo anterior permitió explorar distintos documentos, especialmente estándares que dedican secciones fundamentalmente a la declaración de alcances, objetivos y mejora continua. Por ende, incluir estos elementos como parte de la estrategia, busca preservar en gran medida la estrategia en el tiempo y todo permitir que evolucione en la medida en que las compañías la implementan.

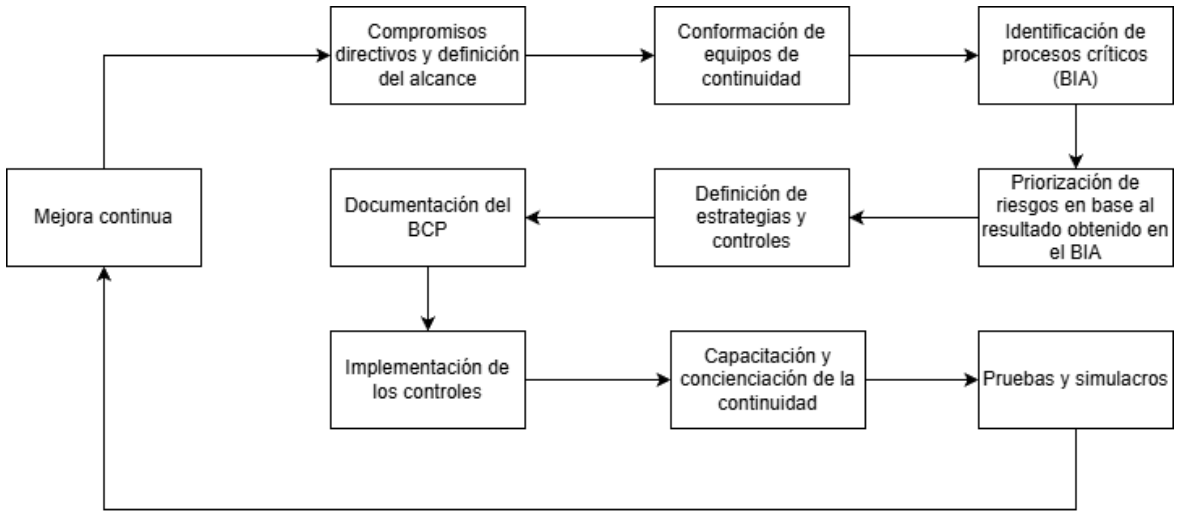
Como consecuencia de lo anterior, en la tabla 15 se observan los elementos propuestos como el producto mínimo viable en materia de BCP para las MiPymes del sector en estudio. La estrategia está basada en un proceso de 10 pasos, por ello, en la columna paso se determina el momento en que se deberá ejecutar una o varias acciones para garantizar que se cumple con la expectativa del plan de continuidad de negocio. Luego, en la columna resumen del objetivo se dio explicación simple de lo que contiene el paso en la construcción de la estrategia, luego, la columna aspecto de la racionalidad limitada a aplicar, menciona los elementos del modelo mencionado bien sea por Herbert Simón o como consecuencia de su trabajo y que haya sido ampliado en los estudios posteriores, y finalmente, en la columna de aplicación de racionalidad limitada se define aporta el modelo a la estrategia. Finalmente, dado que el BCP debiera ser un proceso susceptible a la evolución y mejora continua, se representa en la figura 5 su naturaleza cíclica, procurando que, por medio del proceso de refinamiento, cada compañía pueda madurar mejorando los alcances, coberturas y tiempos de recuperación esperados.

Tabla 15.
Elementos del BCP Mínimo viable.

Paso	Nombre	Resumen del objetivo del paso	Aspecto de la racionalidad limitada a aplicar	Aplicación de racionalidad limitada
1	Compromiso de la dirección y definición del alcance	Detallar cuales son los compromisos que adquieren las áreas que toman las decisiones en la organización, esto a su vez ayuda a la definición del alcance, lo que permite alinear las expectativas de la implementación del BCP	Satisfacción vs. Optimización	La definición basada en satisfacción permite a los ejecutores tomar decisiones más rápidas, es decir, no se busca perfeccionar sino cubrir aquellos elementos esenciales de la organización, por lo tanto, para que sea mínimo viable, debe estar muy bien acotada.
2	Formar el equipo de continuidad y asignar roles	Definir las personas de las distintas áreas que son claves para definir quién y cómo actuar ante la necesidad de activar el BCP.	Toma de decisiones bajo incertidumbre	Permitir tomar decisiones inmediatas a los participantes, usando su propia experiencia y no bajo procesos rigurosos de validación.
3	Identificar procesos críticos y recursos asociados (BIA simplificado)	Valorar los procesos/activos para identificar la criticidad que tienen para el negocio	Heurísticas organizacionales - toma de decisiones bajo incertidumbre	Seleccionar los procesos/activos críticos basados en formatos simples que permiten estimar rápidamente BIA basado en la experiencia de quién usa las heurísticas.
4	Identificar y priorizar riesgos de interrupción (amenazas y vulnerabilidades)	Tomar decisión informada para elegir la ruta de mitigación de riesgos basados en el BIA	Heurísticas organizacionales - toma de decisiones bajo incertidumbre	Definición de riesgos a BIA basados en heurísticas basadas en ISO 27005:2022

5	Definir estrategias de continuidad y controles mínimos	Concertar las medidas y controles para la continuidad de negocio en los procesos/activos críticos.	Heurísticas y rutinas organizacionales; estructuras formales como respuesta a la racionalidad limitada.	Tratamientos a los riesgos resultantes con heurísticas basadas en ISO 22301:2019
6	Documentar el Plan de Continuidad de forma sencilla	Levantar la base para garantizar la estandarización del proceso de continuidad de negocio.	Heurísticas y rutinas organizacionales; estructuras formales como respuesta a la racionalidad limitada.	Construcción de heurísticas propias y simples que permitan la satisfacción del proceso cuando se requiere del BCP
7	Implementar las medidas y controles planificados	Implementar y poner a punto los controles que han sido elegidos.	Satisfacción vs. Optimización	Velar por que los controles satisfagan la necesidad de reducción del impacto, de acuerdo, a las buenas prácticas propuestas por la estrategia.
8	Capacitación y concienciación general en continuidad	Capacitar transversalmente a toda la compañía para que el BCP pueda ser mantenido de acuerdo con el alcance esperado.	Mejora adaptativa y aprendizaje incremental.	Capacitación basada en el conocimiento interno adquirido durante el proceso de madurez.
9	Pruebas y simulacros del plan	Ejecutar acciones que permitan simular una pérdida de continuidad para prevenir puntos de fallo del proceso ante un evento real.	Mejora adaptativa y aprendizaje incremental.	Pruebas basadas en los conocimientos internos y el proceso de madurez adquirido.
10	Mejora continua	Aplicar las medidas necesarias que garanticen evolucionar, mantener o corregir el BCP.	Mejora adaptativa y aprendizaje incremental.	Evolución a partir de los conocimientos de causa adquiridos al interior.

Figura 5.
Flujo BCP Mínimo viable



Como resultado del proceso cíclico propuesto, se realizó el diseño de la estrategia para implementación de BCP para MiPymes del sector manufacturero, que, gracias a los resultados obtenidos en la ejecución de la completitud de los objetivos 1 y 2, permitió detallar en cada uno de los pasos cómo aprovechar el modelo de racionalidad limitada, incluyendo ejemplos que permiten crear un proceso adaptable y sostenible en el tiempo que, a su vez, está guiado por estándares internacionales certificables y que, además, se alimentan sustancialmente de las guías de buenas prácticas que apoyan a la reducción de riesgos, principalmente usando aquellos conceptos que viabilizan la disminución del impacto ante la materialización de eventos, que de acuerdo con el alcance del actual trabajo se enfoca principalmente a eventos de ciberseguridad, pero que, no obstante, cuenta la presencia de múltiples elementos que aportan a la mejora continua, haciendo que se logre tener una estrategia rápida, digerible y sobre todo sostenible en el tiempo que además invita a evolucionar constantemente, por lo tanto, en las figura 6 y 7 se observa la evidencia del contenido del documento final en cual puede ser consultado y extraído directamente del anexo C como un documento independiente.

Figura 6.
Evidencia 1 tabla de contenido estrategia BCP.

Contenido

Figura 7.
Evidencia 2 tabla de contenido estrategia BCP.

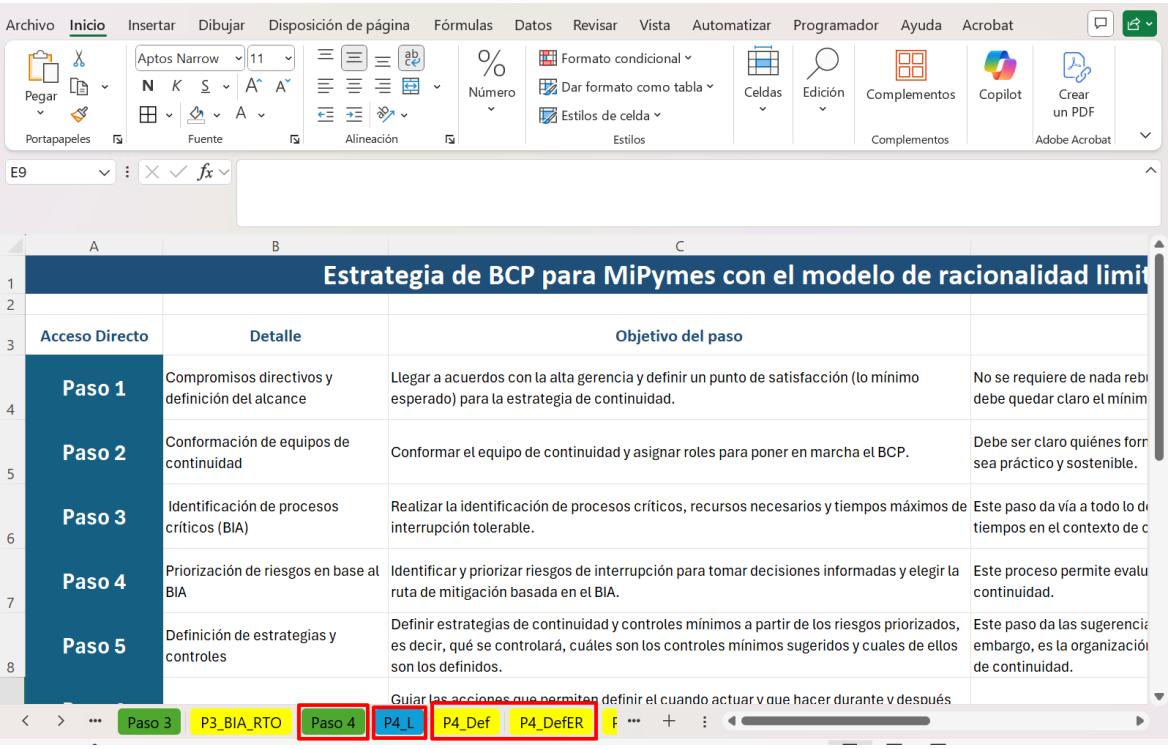
Como se mencionó anteriormente, los elementos claves del desarrollo están orientados al aprovechamiento de las características de racionalidad limitada, como lo son: la definición de los puntos de satisfacción esperados, de tal modo que no se trabaja con un punto de partida ideal sino más bien con un mínimo viable que se permite evolucionar en el tiempo. El aprovechamiento de heurísticas organizacionales, que permiten a partir de formatos y reglas definidas previamente por la organización tomar acciones rápidamente e incluso apoyar la toma de decisiones en escenarios no planificados, es decir, en escenarios bajo incertidumbre que finalmente conlleva siempre a la mejora continua de las estrategias inmersas dentro del plan de continuidad de negocio.

De acuerdo con lo anterior, y como parte del proceso que se sugirió dentro de la estrategia, en el cual se promueve el uso de formatos que aporten a las heurísticas organizacionales, se diseñó también una propuesta visual que incluyó algunas plantillas base y macros en Excel que permiten avanzar en cada paso propuesto dentro de la estrategia de BCP. Cabe aclarar, que cada organización deberá contar con su propio desarrollo, teniendo en cuenta que la propuesta de fondo de la estrategia está en el diseño mismo de los pasos, y que será este el que permita mantener la esencia, es decir, el valor mismo del BCP, y lo demás es resultado de las capacidades de cada organización para poner en marcha por medio de herramientas, bien sea tecnológicas fundamentales como Excel, otras más avanzadas o incluso llevar el BCP de forma manual.

Ahora bien, en la figura 8 se pueden observar las hojas que fueron utilizadas dentro del instrumento de Excel que fue desarrollado como parte de las heurísticas funcionales de racionalidad limitada. Las hojas en verde representan la materialización a alto nivel del paso propuesto en la estrategia. Las hojas amarillas son aquellos elementos necesarios para dar completitud a las necesidades del paso como por ejemplo definiciones, playbooks, matrices, entre otros, y finalmente, las hojas azules representan las listas que sirven de apoyo para estandarizar los registros que se usarán dentro de los pasos u hojas de completitud, de tal modo que, cuando se diligencie la información pueda sostenerse en el tiempo, y por lo tanto, posteriormente usarse para generar información

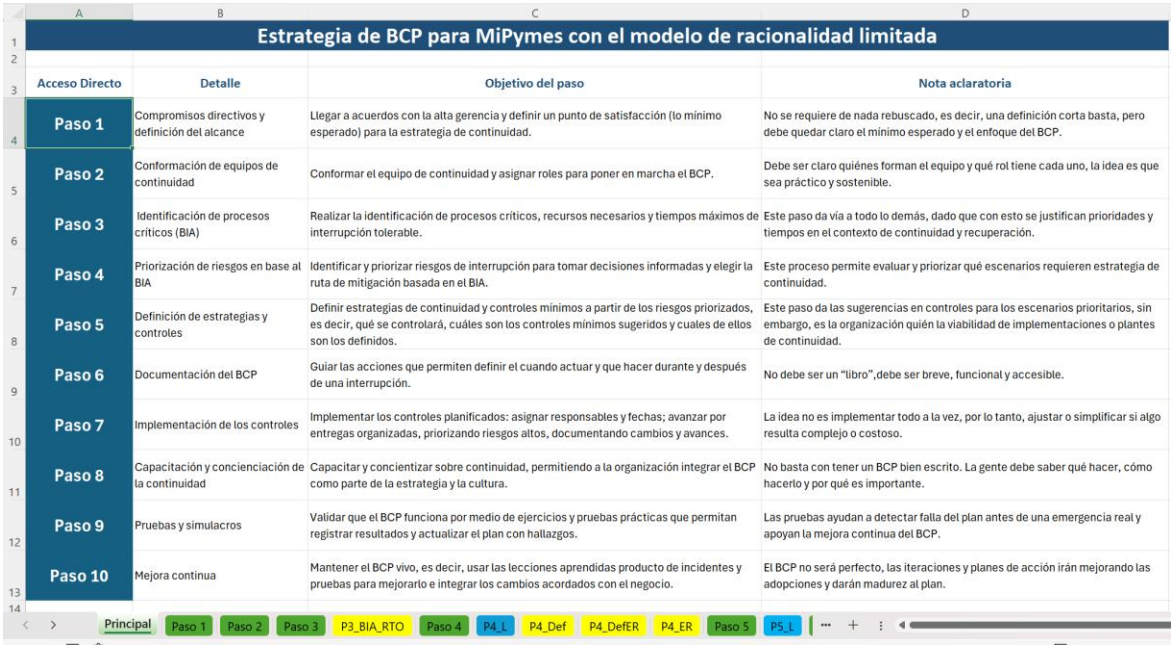
que sirva para extraer información de valor que permite alimentar la toma de decisiones dentro de cada uno de los pasos que se realizan.

Figura 8.
Estructura del instrumento excel (heuristica).



Luego, en la figura 9 se muestra una hoja nombrada como principal, que a nivel organizacional permite desde un desarrollo simple, resumir la estrategia en cada uno de sus pasos, además de ofrecer notas aclaratorias para el(los) individuo(s) encargado(s) de llevar el proceso, e incluye también algunos accesos directos que permiten ir avanzando según sea necesario. El objetivo principal de este formato es mantener el enfoque dentro del BCP conllevando a que siempre el documento original del diseño propuesto se mantenga al día y que lo que evolucione sea la madurez al interior de la organización.

Figura 9.
Pantalla guía de la estrategia.



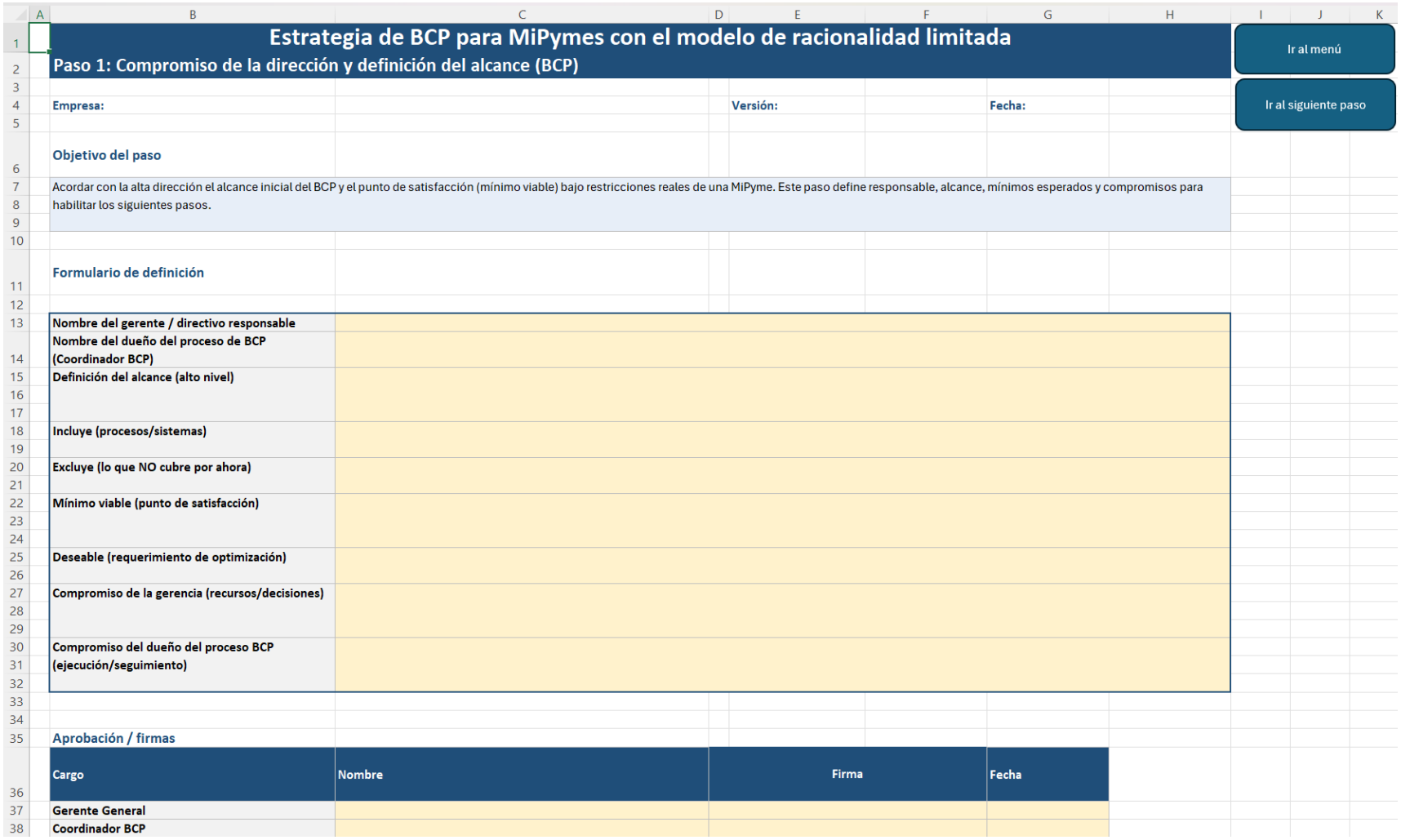
Estrategia de BCP para MiPymes con el modelo de racionalidad limitada

Acceso Directo	Detalle	Objetivo del paso	Nota aclaratoria
Paso 1	Compromisos directivos y definición del alcance	Llegar a acuerdos con la alta gerencia y definir un punto de satisfacción (lo mínimo esperado) para la estrategia de continuidad.	No se requiere de nada rebuscado, es decir, una definición corta basta, pero debe quedar claro el mínimo esperado y el enfoque del BCP.
Paso 2	Conformación de equipos de continuidad	Conformar el equipo de continuidad y asignar roles para poner en marcha el BCP.	Debe ser claro quiénes forman el equipo y qué rol tiene cada uno, la idea es que sea práctico y sostenible.
Paso 3	Identificación de procesos críticos (BIA)	Realizar la identificación de procesos críticos, recursos necesarios y tiempos máximos de interrupción tolerable.	Este paso da vía a todo lo demás, dado que con esto se justifican prioridades y tiempos en el contexto de continuidad y recuperación.
Paso 4	Priorización de riesgos en base al BIA	Identificar y priorizar riesgos de interrupción para tomar decisiones informadas y elegir la ruta de mitigación basada en el BIA.	Este proceso permite evaluar y priorizar qué escenarios requieren estrategia de continuidad.
Paso 5	Definición de estrategias y controles	Definir estrategias de continuidad y controles mínimos a partir de los riesgos priorizados, es decir, qué se controlará, cuáles son los controles mínimos sugeridos y cuales de ellos son los definidos.	Este paso da las sugerencias en controles para los escenarios prioritarios, sin embargo, es la organización quién la viabilidad de implementaciones o plantes de continuidad.
Paso 6	Documentación del BCP	Guiar las acciones que permiten definir el cuando actuar y que hacer durante y después de una interrupción.	No debe ser un "libro",debe ser breve, funcional y accesible.
Paso 7	Implementación de los controles	Implementar los controles planificados: asignar responsables y fechas; avanzar por entregas organizadas, priorizando riesgos altos, documentando cambios y avances.	La idea no es implementar todo a la vez, por lo tanto, ajustar o simplificar si algo resulta complejo o costoso.
Paso 8	Capacitación y concienciación de la continuidad	Capacitar y concientizar sobre continuidad, permitiendo a la organización integrar el BCP como parte de la estrategia y la cultura.	No basta con tener un BCP bien escrito. La gente debe saber qué hacer, cómo hacerlo y por qué es importante.
Paso 9	Pruebas y simulacros	Validar que el BCP funciona por medio de ejercicios y pruebas prácticas que permitan registrar resultados y actualizar el plan con hallazgos.	Las pruebas ayudan a detectar falla del plan antes de una emergencia real y apoyan la mejora continua del BCP.
Paso 10	Mejora continua	Mantener el BCP vivo, es decir, usar las lecciones aprendidas producto de incidentes y pruebas para mejorarlo e integrar los cambios acordados con el negocio.	El BCP no será perfecto, las iteraciones y planes de acción irán mejorando las adopciones y darán madurez al plan.

Posteriormente, de la figura 10 a la 21 se observan formatos base para que puedan ser replicados, lo que a su vez permite darle alcance a cada uno de los pasos de la estrategia, apalancando además de forma estratégica, la estandarización del proceso, no obstante, la adaptación de columnas y dinamismo por medio de formas, campos e hipervínculos entre los pasos, dependerá del conocimiento, capacidad y alcances de cada organización, y tal como se mencionó con anterioridad este pudiere ser un desarrollo en formatos 100% manuales, o bien mediado por herramientas tecnológicas, ya que aquí se trata de un tema de forma, es decir, lo importante es mantener los elementos propuestos en cada paso que finalmente son los que se encargan de propiciar la continuidad del negocio en momentos de crisis, teniendo preparadas con antelación respuestas a algunos de los escenarios más relevantes e incluso permitiendo aprovechar estas definiciones para actuar ante escenarios que aún no han sido previstos.

Figura 10.

Plantillas paso 1.



Estrategia de BCP para MiPymes con el modelo de racionalidad limitada

Paso 1: Compromiso de la dirección y definición del alcance (BCP)

Ir al menú

Ir al siguiente paso

Empresa: **Versión:** **Fecha:**

Objetivo del paso

Acordar con la alta dirección el alcance inicial del BCP y el punto de satisfacción (mínimo viable) bajo restricciones reales de una MiPyme. Este paso define responsable, alcance, mínimos esperados y compromisos para habilitar los siguientes pasos.

Formulario de definición

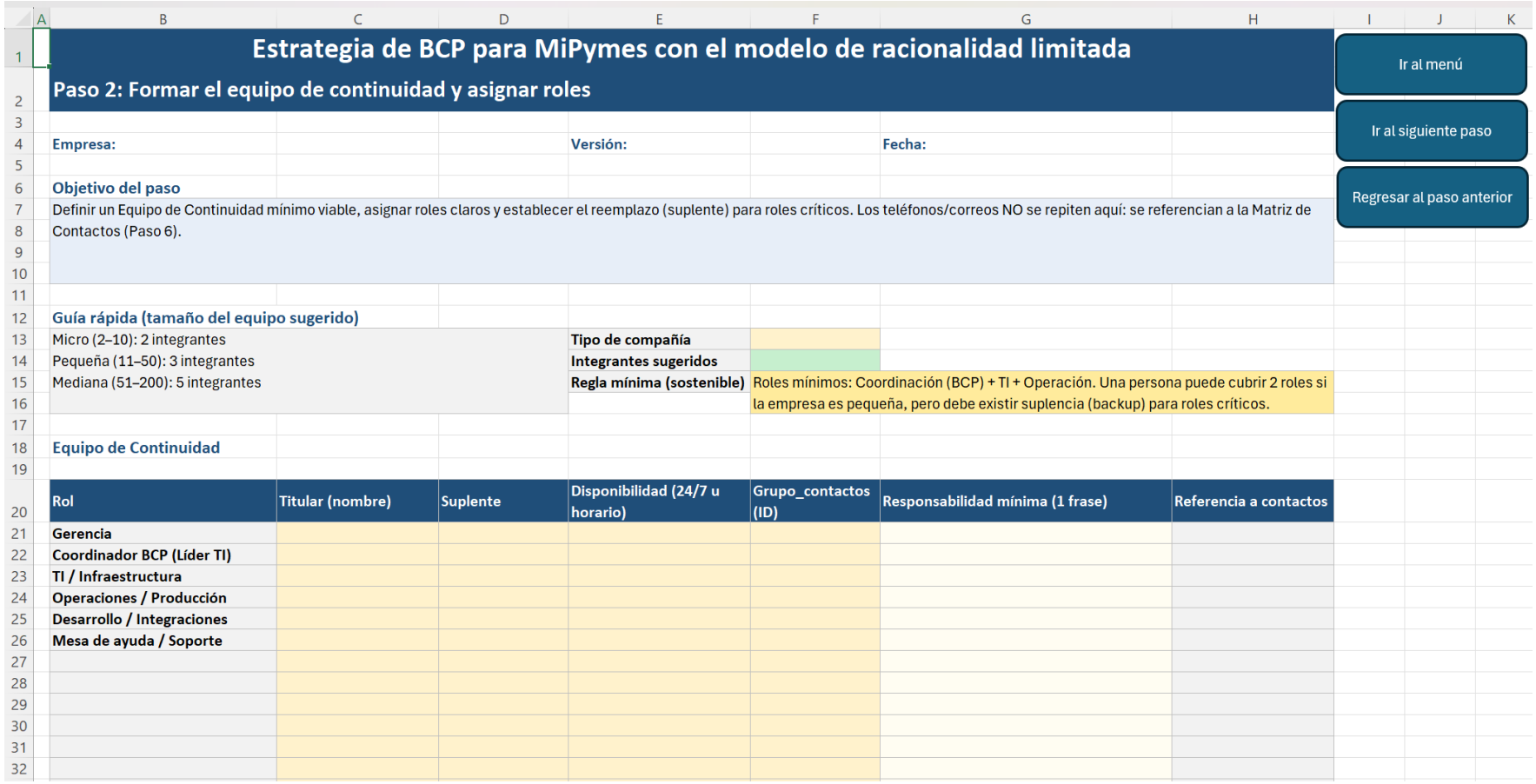
Nombre del gerente / directivo responsable	
Nombre del dueño del proceso de BCP (Coordinador BCP)	
Definición del alcance (alto nivel)	
Incluye (procesos/sistemas)	
Excluye (lo que NO cubre por ahora)	
Mínimo viable (punto de satisfacción)	
Deseable (requerimiento de optimización)	
Compromiso de la gerencia (recursos/decisiones)	
Compromiso del dueño del proceso BCP (ejecución/seguimiento)	

Aprobación / firmas

Cargo	Nombre	Firma	Fecha
Gerente General			
Coordinador BCP			

Figura 11.

Plantillas paso 2.



Estrategia de BCP para MiPymes con el modelo de racionalidad limitada

Paso 2: Formar el equipo de continuidad y asignar roles

Ir al menú

Ir al siguiente paso

Regresar al paso anterior

Empresa: **Versión:** **Fecha:**

Objetivo del paso

Definir un Equipo de Continuidad mínimo viable, asignar roles claros y establecer el reemplazo (suplente) para roles críticos. Los teléfonos/correos NO se repiten aquí: se referencian a la Matriz de Contactos (Paso 6).

Guía rápida (tamaño del equipo sugerido)

Micro (2–10): 2 integrantes
Pequeña (11–50): 3 integrantes
Mediana (51–200): 5 integrantes

Tipo de compañía	
Integrantes sugeridos	
Regla mínima (sostenible)	Roles mínimos: Coordinación (BCP) + TI + Operación. Una persona puede cubrir 2 roles si la empresa es pequeña, pero debe existir suplencia (backup) para roles críticos.

Equipo de Continuidad

Rol	Titular (nombre)	Suplente	Disponibilidad (24/7 u horario)	Grupo_contactos (ID)	Responsabilidad mínima (1 frase)	Referencia a contactos
Gerencia						
Coordinador BCP (Líder TI)						
TI / Infraestructura						
Operaciones / Producción						
Desarrollo / Integraciones						
Mesa de ayuda / Soporte						

Figura 12.
Plantillas paso 3.

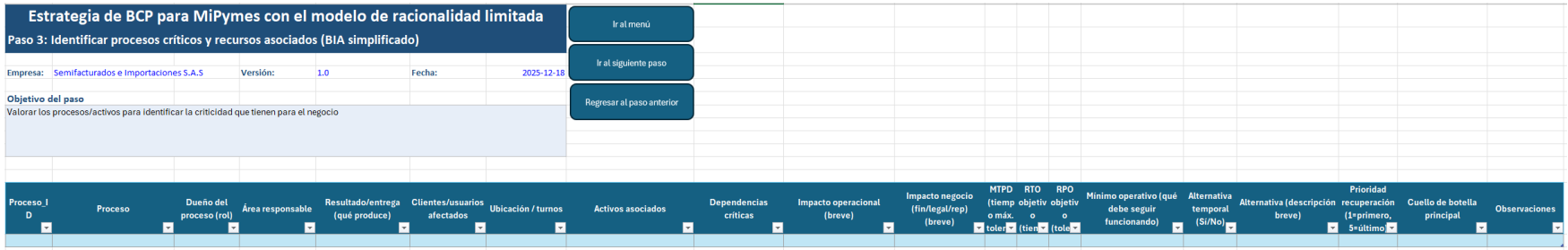


Figura 13.
Plantillas paso 3 (Resumen BIA).

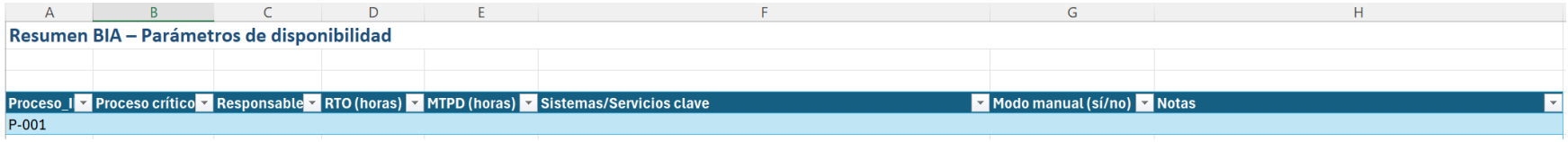


Figura 14.

Plantillas paso 4.

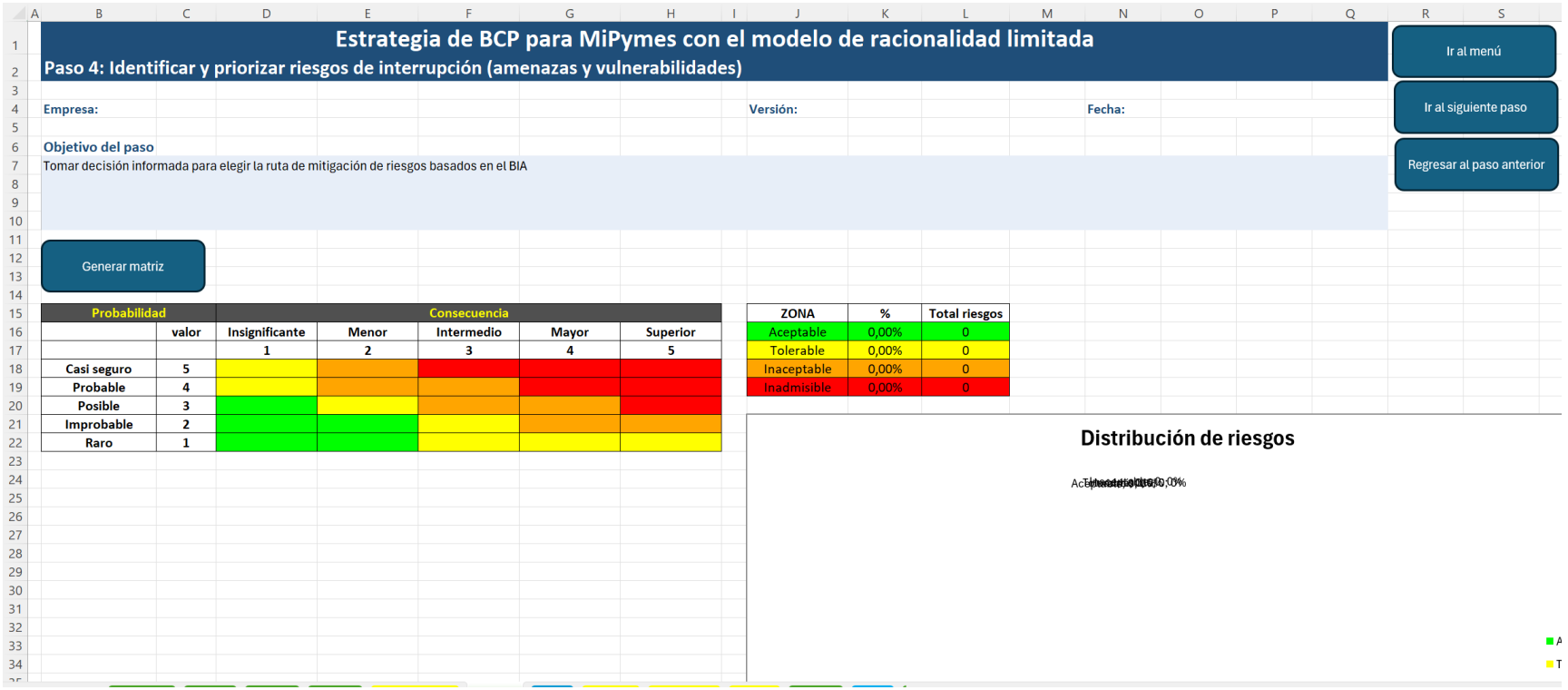


Figura 15.

Plantillas paso 4 (definiciones apoyo riesgos).

Tipo de activo	Catalogo de vulnerabilidades	Amenazas	Factor de riesgo
Datos / Información	Apis Inseguras	Botnet	Accidental
Documentación	Configuraciones erróneas	Criptojacking	Deliberada
Hardware	Convergencia TI/TO insegura	Cross-Site Scripting (XSS)	Física
Infraestructura	Escasez de Talento en Ciberseguridad	DoS/DDoS	Natural
Organización / Elementos institucionales	Gestión Inadecuada de Identidades y A	Downloader/Dropper	Organizacional
Personas	IoT/IIoT débil	Empleado/contratista malicioso	Tecnológica
Procesos	Parches tardíos/ausentes	Logic bomb	Terceros
Recursos externos / Proveedores	Segmentación de red inadecuada	Malvertising	
Servicios	Seguridad móvil débil	Propagación hacia IACS	
Software	Software no autorizado/pirata	Ransomware	
	Virtualización / nube híbrida mal gestic	RAT (Remote Access Trojan)	
	Wi-Fi insegura	Rootkit	
	Zero-day	SIM-swapping	
		SQL Injection	

TABLAS DE PROBABILIDAD/

Nivel	Rangos
1	Raro
2	Improbable
3	Posible
4	Probable
5	Casi seguro

TABLAS DE IMPACTO

Impacto en la OPERACIÓN /

Nivel	Rangos
1	Insignificante
2	Menor
3	Intermedio
4	Mayor
5	Superior

Figura 16.

Plantillas paso 5.

Figura 17.

Plantillas paso 6.

Figura 18.

Plantillas paso 7.

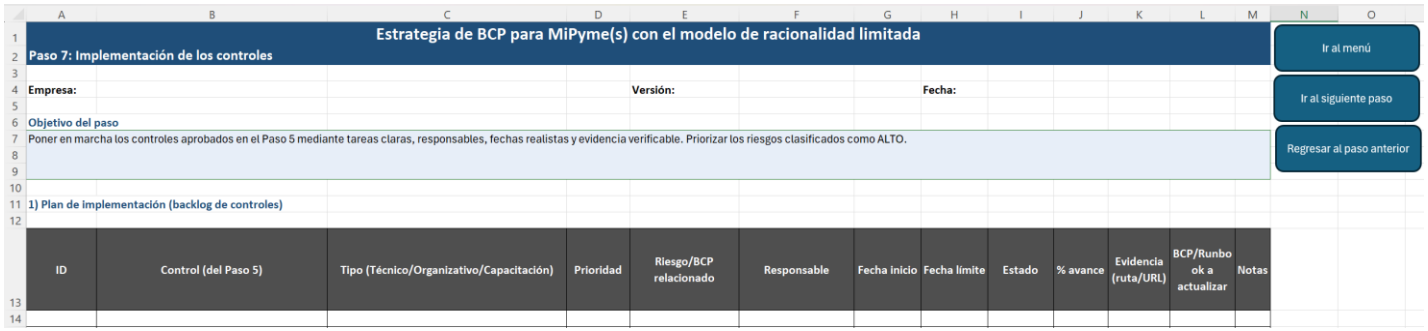


Figura 19.

Plantillas paso 8.

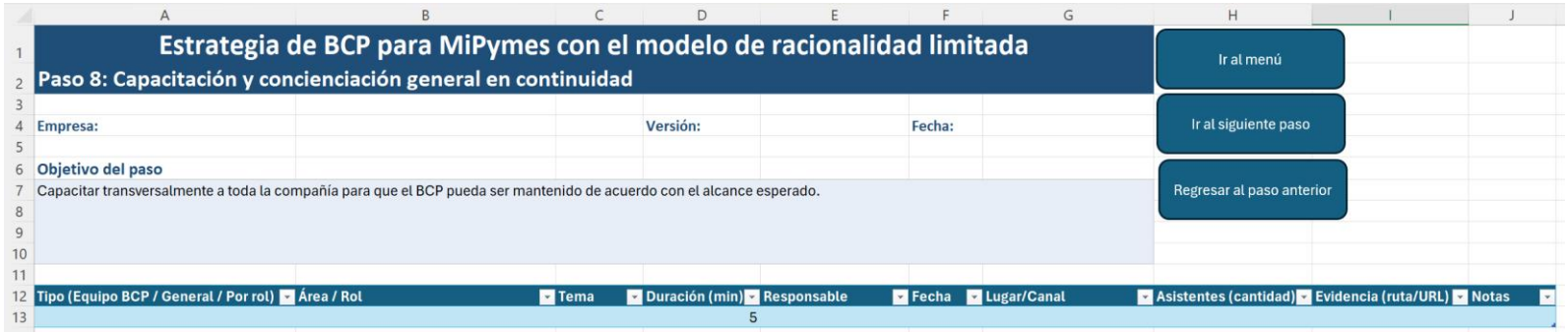


Figura 20.

Plantillas paso 9.

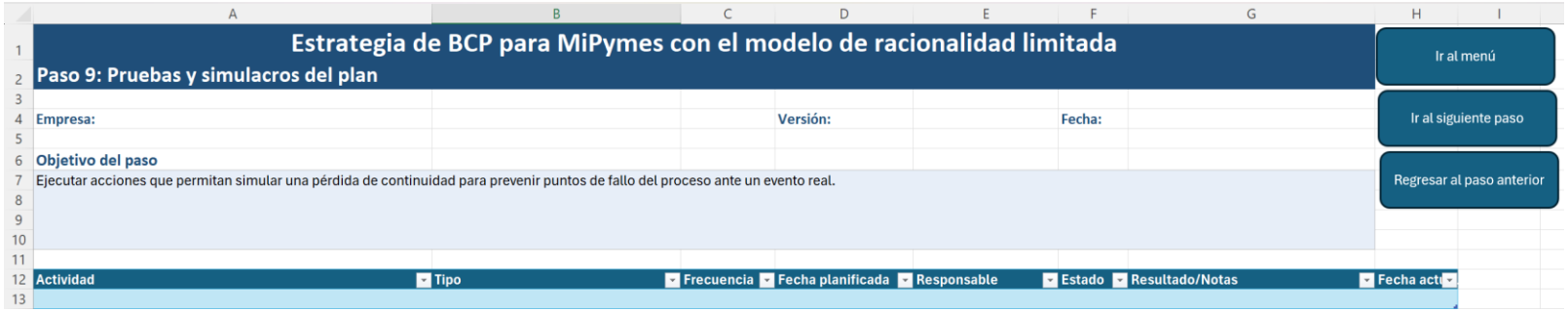


Figura 21.

Plantillas paso 10.

Estrategia de BCP para MiPymes con el modelo de racionalidad limitada

Paso 10: Mejora continua

Ir al menú

Regresar al paso anterior

Empresa: **Versión:** **Fecha:**

Objetivo del paso

Aplicar las medidas necesarias que garanticen evolucionar, mantener o corregir el BCP.

Incidente_ID	Fecha	Hora detección	ID_BCP	Descripción	Acciones tomadas (resumen)	Hora recuperación	Duración (hrs)	Impacto en producción	Lecciones aprendidas	Cerrado (SI/NO)
INC-001			BCP-001							NO

Finalmente, en el anexo D se deja detalle del proceso de replicación del instrumento de Excel diseñado a manera de ejemplo de adaptación de la estrategia, es decir, llevando de una forma dinámica y visual que permite aprovechar una herramienta cotidiana de muchas organizaciones como elemento de implementación de un BCP, propiciando así, que cualquier compañía manufacturera e incluso de otros sectores puedan aprovechar el diseño de la estrategia para tener un resultado final satisfactorio de acuerdo con las definiciones acotadas al alcance que definan dentro del BCP, en este caso definido para eventos de ciberseguridad, pero que al estar diseñado con las bases fundamentales de [71], está alineado con el ciclo PHVA, y por ende, bajo esta premisa permite a cada compañía reescalar y cubrir con el BCP aquellos elementos que dentro de su propia racionalidad limitada sean críticos o esenciales para mantener a flote su negocio.

2.4 Metodología y resultados de la fase 4.

2.4.1 Metodología de la fase 4: validación de la estrategia.

La metodología implementada para alcanzar el objetivo específico 4 “Validar la estrategia en una prueba de escritorio con caso de estudio completo que permita la comprensión del resultado de la implementación un BCP”, se estructuró con dos actividades esenciales que se describen a continuación:

2.4.1.1 Diseño del caso de estudio.

Se construyó un caso de estudio que permitiera poner en práctica la estrategia para implementación de BCP diseñada, y para ello, se redactó un texto que contiene implícitamente el contexto de una compañía ficticia del sector manufacturero, sus procesos e interacción de ellos en su cotidianidad, los recursos de los que dispone, sus activos tecnológicos, los controles actuales asociados y los problemas que requiere abordar. Esta construcción sería el punto de partida para poner a prueba un BCP fundamentado en la racionalidad limitado por lo que también se incluyeron restricciones con las cual se debía lidiar.

2.4.1.2 Ejecución de la prueba de escritorio.

A partir del caso de estudio se ejecutó una prueba de escritorio en la cual el principal insumo fueron los 10 pasos de la estrategia en los cuales se incluían ejemplos que permitían guiar la ejecución de acciones en pro de tener definiciones, avances y desarrollo de estrategias de continuidad, así como también sentar las bases necesarias para apalancar el proceso de evolución del BCP a partir de registros clave sugeridos en el diseño. Para dar completitud a esta prueba se debió usar el instrumento de Excel propuesto y se evaluó con el checklist para BCP incluido dentro de la estrategia. Esta metodología permitió validar si aplicando la estrategia de BCP propuesta la

organización contaba con elementos que permitieran tener estrategias en pro de la continuidad del negocio.

2.4.2 Resultados de la fase 4: validación de la estrategia.

Caso de estudio empresa semifacturados e importaciones S.A.S

Contexto

La compañía semifacturados e importaciones S.A.S es una empresa dedicada a la importación de equipos industriales. Su foco es principalmente emitir soluciones integrales para el corte en las industrias metálicas, madereras y de construcción, para ello, integra en su en su modelo de negocio, la importación y venta de equipos tanto manuales como automáticos que son integrados en líneas de producción de las industrias anteriormente descritas, también, se preocupa por la venta de químicos, herramientas, repuestos y software especializado para este tipo de maquinarias. Finalmente, para completar este catálogo, semifacturados e importaciones S.A.S cuenta con una línea especializada de producción en la cual transforman cintas vírgenes y las convierten finalmente en sierras de corte para diferentes soluciones de la industria de alimentos, además, cuenta con una línea de producción dedicada a la transformación y rectificado de discos de corte de diferentes materiales, entre los cuales se encuentran el tungsteno y diamante. En consecuencia de esto, y para poder efectuar sus operaciones en la planta de producción, cuenta con diferentes equipos de troquelado, corte tradicional y laser, rectificado, y como premisa de la venta de sus soluciones hace uso de muchas de las tecnologías en su propia planta.

Tecnología e interacciones entre sistemas.

Dentro de sus equipos productivos más importantes tienen una línea de corte de cinta automatizada, y tres equipos de rectificado de discos de diamante los cuales cuentan con un sistema de conteo de piezas que se encarga de entregar información de la producción (piezas cortadas/rectificadas, tiempo de trabajo, tiempo de paradas, fallos y alertas) a un computador con el cual tienen conexión bajo un segmento de red específicamente creado para comunicar los dispositivos de planta, y las estaciones de los ingenieros que hacen ingesta de la información para fines de generación de información de calidad y productividad.

Para el control de producción de las demás actividades en planta, cuenta con 5 estaciones de trabajo (computadores de mesa) que tienen acceso directo hacia un software desarrollado internamente llamado SEIM que se encarga del manejo de las ordenes de producción, y el cual se alimenta de los pedidos transmitidos por medio del CRM (Servicio SaaS). Por su parte el ERP atiende la gestión de inventarios, contabilidad, gestión humana y nómina, costos y presupuestos, y, por medio de su base de datos se centraliza la información que se genera tanto desde el CRM, SEIM e incluso desde las demás áreas que generan transacciones desde el mismo ERP. Por lo tanto, si la

base de datos falla, se genera entonces una falla total, debido a que tanto SEIM como el CRM se alimentan directamente de allí e intercambian la información general de la compañía.
La base de datos está instalada en un servidor de base de datos y su diseño original de tablas y relaciones pertenecen al ERP, sin embargo, para lograr la interacción entre todos los sistemas (ERP, CRM y SEIM) existen integraciones localizadas en un servidor de contenedores que tiene alcance a internet para conectar con el CRM y por medio de VLAN se conecta con un servidor de aplicaciones (donde están instalados el ERP y SEIM) y al servidor de bases de datos.

Infraestructura
En general para soportar la operación tecnológica cuenta con una infraestructura con los siguientes componentes:

- 1 CISCO Meraki que actúa como firewall y administrador de VLANS
- 1 Switch core y 5 más para atender las necesidades de puntos de red y accesos a VLANS, todos en L3.
- 1 servidor de directorio activo y DNS.
- 1 servidor de virtualización que contiene los siguientes servidores en su interior:
    - 1 servidor de bases de datos.
    - 1 servidor de archivos y aplicaciones.
    - 1 servidor de terminal server para los accesos remotos.
    - 1 servidor para servicios de contenedores (con dockerización: 1 servidor de certificados digitales, aplicaciones de integración del CRM/ERP)
    - 1 servidor de inventario digital.
    - 1 servidor de replica de directorio activo y DNS.
- 1 servidor de desarrollo.
- 1 servidor de respaldo del servidor de virtualización.
- 61 estaciones de trabajo entre los cuales se encuentran las 5 estaciones de ingeniería en producción, 40 estaciones de trabajo para personas con roles administrativos, 9 equipos para personal de ventas, 2 equipos del personal de diseño, y 5 equipos en inventario disponibles para fallas, mantenimientos y/o nuevos proyectos.
- 3 DVR
- 1 NVR
- 1 NAS

Cada servidor localizado en sede tiene activada la opción de copia completa (VSS) y se envía a una NAS la cual está conectada a la red por medio de la VLAN de servidores. Por su parte, la base de datos se respalda de forma local diariamente. Los documentos en contabilidad aún se imprimen, no obstante, de cada documento se deja una copia digital, la cual reposa el servidor de archivos. La herramienta de colaboración utilizada por todas las áreas es office 365, por lo tanto, se cuenta con licenciamiento asociado a un tenant a nombre de la compañía contratado

con un proveedor de servicios. En cuanto al servicio de internet se cuenta con un único canal con una velocidad de 300 Mb. Para la protección de las estaciones de trabajo se cuenta con licenciamiento de antivirus ESET Smart protection.

Recursos humanos de TI

La administración tecnológica es manejada desde la dirección administrativa, para ello, se tiene contratado a un ingeniero de sistemas quien se encarga de gestionar la administración general de los sistemas y seguridad dentro de la compañía, a su cargo tiene a dos desarrolladores, quienes son encargados de dar soporte principalmente a las soluciones de integración de los sistemas y dar mantenimiento a las bases de datos, también se tiene un contrato vía outsourcing con una compañía para el manejo de la mesa de ayuda, dicho contrato tiene incluido un analista de soporte inhouse, operación remota desde mesa de ayuda 5*8, un coordinador de mesa de ayuda y un experto en infraestructura.

Problema y resultados esperados

La gerencia se ha ido concientizando de la importancia de la ciberseguridad gracias a las múltiples sesiones de capacitación apalancadas por el ingeniero de sistemas a cargo, no obstante, no está dispuesta en invertir en más mano de obra para mejorar la postura de seguridad, pero ha solicitado especialmente mejorar la forma en que se pudiera responder ante indisponibilidad de los sistemas, esto incluye interrupciones ocasionados por eventos de ciberseguridad. Con la finalidad de poder estar mejor preparados ante estos eventos desafortunados que pueden poner en riesgo la continuidad del negocio, se le ha solicitado a la dirección la implementación de una propuesta que garantice operar al menos de forma esencial evitando efectos negativos que pudieran poner en riesgo el funcionamiento de la organización a largo plazo. La dirección ha encomendado esta tarea al ingeniero de sistemas a cargo y refuerza la idea de que debe garantizarse la continuidad bajo las condiciones actuales, es decir, con la utilización de los recursos disponibles (bajos recursos económicos, poco personal capacitado en ciberseguridad, y pocos procedimientos establecidos).

Finalmente, esta necesidad será una oportunidad para poner a prueba la estrategia para la implementación de BCP bajo la perspectiva de racionalidad limitada, es decir, se deberá tener una guía metodológica que permita no solo ahondar en el qué tal y como lo indican los estándares certificables sino que adicionalmente, dará una hoja de ruta con opciones claras que han sido tomadas de referencias de guías y buenas prácticas del mercado para la implementación del cómo, teniendo en cuenta las restricciones del caso de uso en tiempos y alcances.

Validación de la implementación de BCP basado en racionalidad limitada

Para validar los resultados de la estrategia, se tomó como punto de referencia el documento guía desarrollado en el objetivo 3, en el que se estructuran 10 pasos para la implementación de un Plan de Continuidad del Negocio para MiPymes. A partir de esta base, se diseñó una

herramienta en Excel con el propósito de ejecutar las sugerencias de dichos pasos en elementos operables y fácilmente verificables, de manera que fuese posible visualizar cómo se materializa la estrategia en un contexto organizacional real. Esta herramienta no se concibió únicamente como un soporte de registro, sino como un medio para facilitar la comprensión integral del proceso. En consecuencia, la validación buscó demostrar su aplicabilidad mediante una representación del "qué hacer" y, especialmente, del "cómo hacerlo" propuesto a partir de los elementos claves de racionalidad limitada, al priorizar decisiones simplificadas, criterios mínimos viables y una trazabilidad clara entre los pasos definidos y los resultados mostrados, procurando que la implementación sea realista y sostenible para organizaciones con capacidades restringidas.

Para poner en marcha la validación se tomó el checklist de los elementos clave propuestos en el caso de estudio definido con anterioridad (tabla 13), los cuales permitieron evaluar el estado inicial de implementación de BCP. Posteriormente, se dio inicio a la prueba de escritorio usando el instrumento de Excel, comenzando por la determinación del alcance y los resultados esperados para al final repetir la medición y que se permita concluir si la estrategia pudiese adoptarse a un entorno productivo manufacturero real. En la figura 22 se observa precisamente ejecución del paso 1, es decir, la definición del alcance, permitiendo delimitar lo que se incluye y lo que no, las responsabilidades y el punto de satisfacción esperado, en este caso poder tener estrategias de recuperación que permitan operar el top 3 de los procesos críticos seleccionados en el BIA. Luego, en la figura 23 se evidencia la ejecución asociada al paso 2 de la estrategia, es decir, la conformación del equipo a partir de las sugerencias, este paso es fundamental para definir los roles y las responsabilidades además de definir suplentes que, si bien pudieran no estar 100% con la construcción y la definición, si deben estar preparados y alineados para cuando deban ejecutar alguna acción asociada al BCP.

Tabla 13.
Validación de estado previo a la implementación de BCP.

Aspecto clave a verificar	¿Cumplido? (Sí/No)
La gerencia ha expresado su apoyo formal al BCP y existe un responsable asignado.	No
El alcance está definido: se conocen y documentan los procesos críticos y sus requerimientos.	No
La empresa cuenta con una lista actualizada de riesgos prioritarios (incluyendo ciberamenazas).	No
Los respaldos de datos críticos se realizan con frecuencia y **se ha probado su restauración**.	No
Existen redundancias básicas (equipo de respaldo, segundo enlace de Internet, proveedores alternos).	No
El BCP está escrito, vigente y accesible para quienes lo necesitan.	No

El personal ha recibido capacitación sobre su rol en el BCP.	No
Se ha realizado al menos una prueba o simulacro durante los últimos 12 meses.	No
El plan se revisa y actualiza periódicamente (contactos, cambios en procesos, nueva infraestructura, etc.).	No
Cumplimiento	(0/9) – 0%

Figura 22.
Ejecución paso 1.

Estrategia de BCP para MiPymes con el modelo de racionalidad limitada
Paso 1: Compromiso de la dirección y definición del alcance (BCP)

Ir al menú

Ir al siguiente paso

Empresa:	Semifacturados e Importaciones S.A.S	**Versión:**	1.0	**Fecha:**	2025-12-18

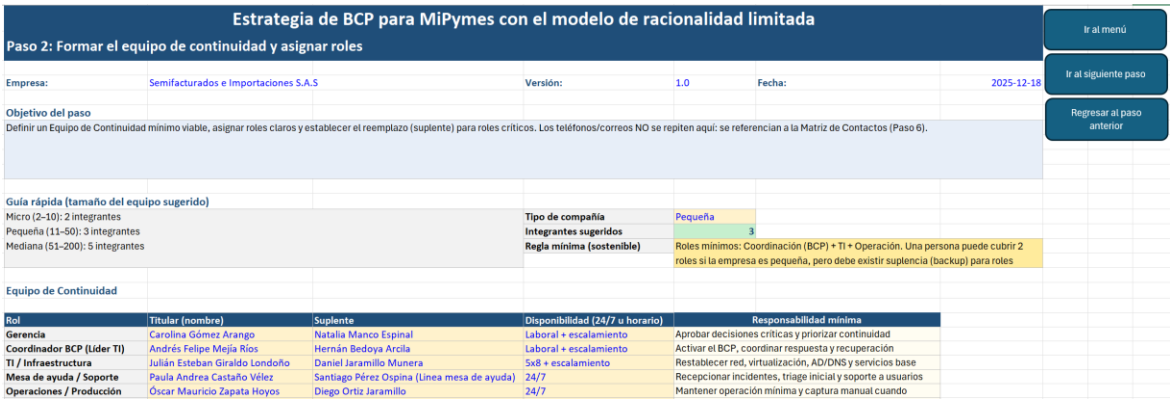
Objetivo del paso

Acordar con la alta dirección el alcance inicial del BCP y el punto de satisfacción (mínimo viable) bajo restricciones reales de una MiPyme. Este paso define responsable, alcance, mínimos esperados y compromisos para habilitar los siguientes pasos.

Formulario de definición

Nombre del gerente / directivo responsable	Carolina Gómez Arango / Gerencia
Nombre del dueño del proceso de BCP (Coordinador BCP)	Andrés Felipe Mejía Ríos / Líder TI
Definición del alcance (alto nivel)	BCP para interrupciones de disponibilidad originadas por eventos de ciberseguridad que afecten la operación esencial (ventas/pedidos, producción, despacho y gestión administrativa), priorizando ERP on premise, CRM SaaS, SEIM, virtualización, AD/DNS, red, respaldos y accesos.
Incluye (procesos)	Top 3 de procesos seleccionados en el BIA
Excluye (lo que NO cubre por ahora)	- Mejoras estructurales de ciberseguridad que requieran inversiones significativas (SOC, SIEM, EDR avanzado, duplicación de enlaces/infraestructura) - Proyectos de transformación tecnológica no relacionados con continuidad. - Alcance de confidencialidad/integridad más allá de lo requerido para restablecer disponibilidad.
Mínimo viable (punto de satisfacción)	Contar con elementos que permitan recuperar servicios críticos; habilitar alternativas manuales temporales para registro de pedidos y continuidad mínima de producción/despacho.
Deseable (requerimiento de optimización)	- Ejecutar pruebas periódicas de restauración y simulacros. - Mejorar progresivamente tiempos de recuperación y confiabilidad de respaldos. - Formalizar y mantener actualizado el BCP con ciclo de mejora continua.
Compromiso de la gerencia	1) Aprobar el alcance y priorización. 2) Garantizar disponibilidad del equipo mínimo para ejecutar el plan. 3) Autorizar paradas controladas para pruebas de recuperación. 4) Respaldar decisiones de continuidad.
Compromiso del dueño del proceso BCP	1) Coordinar entrevistas BIA. 2) Consolidar activos asociados y escenarios de indisponibilidad. 3) Mantener el BCP actualizado. 4) Liderar capacitaciones y pruebas. 5) Registrar lecciones aprendidas y mejoras.

Figura 23.
Ejecución paso 2.



Estrategia de BCP para MiPymes con el modelo de racionalidad limitada

Paso 2: Formar el equipo de continuidad y asignar roles

Ir al menú | Ir al siguiente paso | Regresar al paso anterior

Empresa:	Semifacturados e Importaciones S.A.S		**Versión:**	1.0	**Fecha:** 2025-12-18

Objetivo del paso

Definir un Equipo de Continuidad mínimo viable, asignar roles claros y establecer el reemplazo (suplente) para roles críticos. Los teléfonos/correos NO se repiten aquí: se referencian a la Matriz de Contactos (Paso 6).

Guía rápida (tamaño del equipo sugerido)

Micro (2–10): 2 integrantes
Pequeña (11–50): 3 integrantes
Mediana (51–200): 5 integrantes

Tipo de compañía	Pequeña
Integrantes sugeridos	3
Regla mínima (sostenible)	Roles mínimos: Coordinación (BCP) + TI + Operación. Una persona puede cubrir 2 roles si la empresa es pequeña, pero debe existir suplencia (backup) para roles

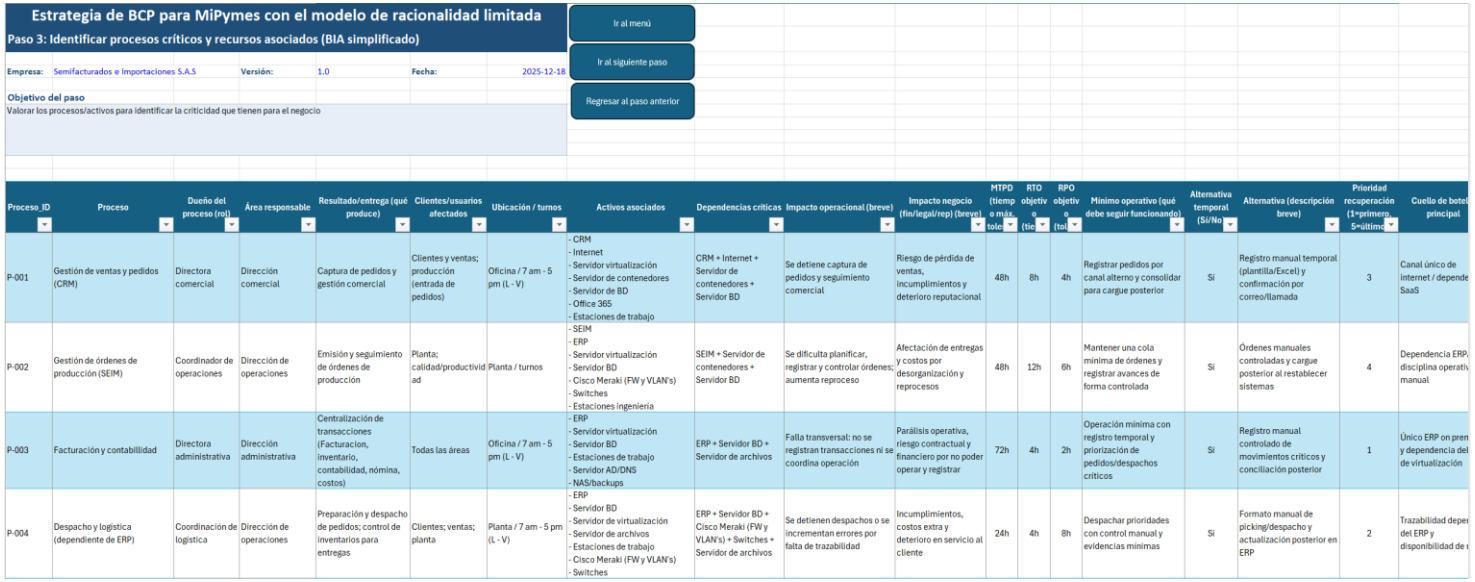
Equipo de Continuidad

Rol	Titular (nombre)	Suplente	Disponibilidad (24/7 u horario)	Responsabilidad mínima
Gerencia	Carolina Gómez Arango	Natalia Manco Espinal	Laboral + escalamiento	Aprobar decisiones críticas y priorizar continuidad
Coordinador BCP (Líder TI)	Andrés Felipe Mejía Ríos	Hernán Bedoya Arcila	Laboral + escalamiento	Activar el BCP, coordinar respuesta y recuperación
TI / Infraestructura	Julián Esteban Giraldo Londoño	Daniel Jaramillo Munera	5x8 + escalamiento	Restablecer red, virtualización, AD/DNS y servicios base
Mesa de ayuda / Soporte	Paula Andrea Castaño Vélez	Santiago Pérez Ospina (Línea mesa de ayuda)	24/7	Recepcionar incidentes, triage inicial y soporte a usuarios
Operaciones / Producción	Óscar Mauricio Zapata Hoyos	Diego Ortiz Jaramillo	24/7	Mantener operación mínima y captura manual cuando

Una vez fueron definidos los alcances y responsables, el paso siguiente era mapear los procesos críticos. Para ello, dentro del caso se encontraban algunas descripciones del funcionamiento de los sistemas de la compañía, y de este modo, se identificaron las relaciones clave entre los sistemas. En la estrategia la idea es hacer un BIA simple, es decir, que permitiera a partir del conocimiento interno y sin grandes cálculos definir tiempos objetivo. La completitud de este ejercicio se realizó simulando el proceso de llenado de información adicional que requiere el proceso, y al igual que en un ejercicio real se asignaron tiempos que desde una vista de negocio se entienden como cruciales, es decir, aunque no sean perfectos, permiten posteriormente ser ajustados en pasos posteriores, no obstante, estos tiempos no podían ser ni tan pequeños que no permitieran ejecutar estrategias ni tan grandes que pudieran en algunas condiciones poner en riesgo la operación del negocio, por lo tanto, este resultado será siempre diferente para cada organización. En la figura 24 se observa el resultado del ejercicio, y en la figura 25 se resume el BIA de los procesos que quedaron seleccionados como el top 3 de acuerdo con el alcance definido.

Figura 24.

Ejecución paso 3.



Estrategia de BCP para MiPymes con el modelo de racionalidad limitada

Paso 3: Identificar procesos críticos y recursos asociados (BIA simplificado)

Ir al menú | Ir al siguiente paso | Regresar al paso anterior

Empresa: Semifacturados e Importaciones S.A.S **Versión:** 1.0 **Fecha:** 2025-12-18

Objetivo del paso

Valorar los procesos/activos para identificar la criticidad que tienen para el negocio

Proceso_ID	Proceso	Dueño del proceso (rol)	Área responsable	Resultado/entrega (qué produce)	Clientes/usuarios afectados	Ubicación / turnos	Activos asociados	Dependencias críticas	Impacto operacional (breve)	Impacto negocio (fin/legal/rep) (breve)	MTPD (tiempo máx. tole	RTO objetiv e (tie	RPO objetiv e (tol	Mínimo operativo (qué debe seguir funcionando)	Alternativa temporal (Sí/No	Alternativa (descripción breve)	Prioridad recuperación (1=primero 5=último	Cuello de botel principal
P-001	Gestión de ventas y pedidos (CRM)	Directora comercial	Dirección comercial	Captura de pedidos y gestión comercial	Clientes y ventas; producción (entrada de pedidos)	Oficina / 7 am - 5 pm (L - V)	- CRM - Internet - Servidor virtualización - Servidor de contenedores - Servidor de BD - Office 365 - Estaciones de trabajo	CRM + Internet + Servidor de contenedores + Servidor BD	Se detiene captura de pedidos y seguimiento comercial	Riesgo de pérdida de ventas, incumplimientos y deterioro reputacional	48h	8h	4h	Registrar pedidos por canal alterno y consolidar para cargue posterior	Si	Registro manual temporal (plantilla/Excel) y confirmación por correo/llamada	3	Canal único de internet / depende SaaS
P-002	Gestión de órdenes de producción (SEIM)	Coordinador de operaciones	Dirección de operaciones	Emisión y seguimiento de órdenes de producción	Planta; calidad/productivid ad	Planta / turnos	- SEIM - ERP - Servidor virtualización - Servidor BD - Cisco Meraki (FW y VLAN's) - Switches - Estaciones ingeniería	SEIM + Servidor de contenedores + Servidor BD	Se dificulta planificar, registrar y controlar órdenes; aumenta reproceso	Afectación de entregas y costos por desorganización y reprocesos	48h	12h	6h	Mantener una cola mínima de órdenes y registrar avances de forma controlada	Si	Órdenes manuales controladas y cargue posterior al restablecer sistemas	4	Dependencia ERP, disciplina operativ manual
P-003	Facturación y contabilidad	Directora administrativa	Dirección administrativa	Centralización de transacciones (Facturacion, inventario, contabilidad, nómina, costos)	Todas las áreas	Oficina / 7 am - 5 pm (L - V)	- ERP - Servidor virtualización - Servidor BD - Estaciones de trabajo - Servidor AD/DNS - NAS/backups	ERP + Servidor BD + Servidor de archivos	Falla transversal: no se registran transacciones ni se coordina operación	Parálisis operativa, riesgo contractual y financiero por no poder operar y registrar	72h	4h	2h	Operación mínima con registro temporal y priorización de pedidos/despachos críticos	Si	Registro manual controlado de movimientos críticos y conciliación posterior	1	Único ERP on prem y dependencia del de virtualización
P-004	Despacho y logística (dependiente de ERP)	Coordinación de logística	Dirección de operaciones	Preparación y despacho de pedidos; control de inventarios para entregas	Clientes; ventas; planta	Planta / 7 am - 5 pm (L - V)	- ERP - Servidor BD - Servidor de virtualización - Servidor de archivos - Estaciones de trabajo - Cisco Meraki (FW y VLAN's) - Switches	ERP + Servidor BD + Cisco Meraki (FW y VLAN's) + Switches + Servidor de archivos	Se detienen despachos o se incrementan errores por falta de trazabilidad	Incumplimientos, costos extra y deterioro en servicio al cliente	24h	4h	8h	Despachar prioridades con control manual y evidencias mínimas	Si	Formato manual de picking/despacho y actualización posterior en ERP	2	Trazabilidad depe del ERP y disponibilidad de

Figura 25.

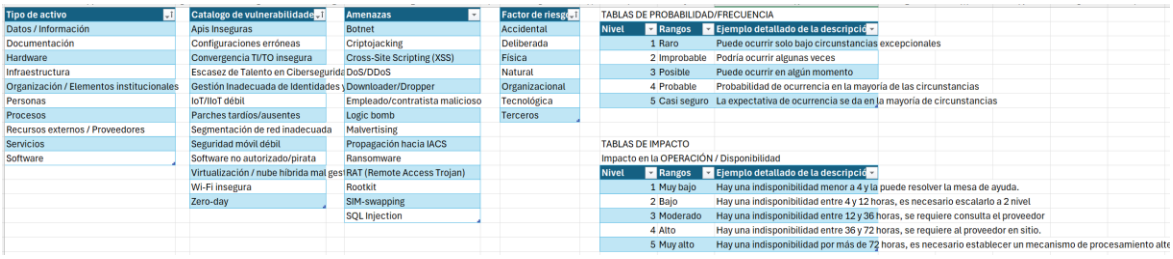
Resumen BIA Top 3 (definido en alcance).

Resumen BIA para BCP – Parámetros de disponibilidad

Proceso_ID	Proceso crítico	Responsable	RTO (hor	MTPD (hor	Sistemas/Servicios clave	Modo manual (sí/no)	Notas
P-001	Gestión de ventas y pedidos (CRM)	Directora comercial	8	48	CRM + Internet + Servidor de contenedores + Servidor BD	SI	Registrar pedidos por canal alterno y consolidar para cargue posterior
P-003	Facturación y contabilidad	Directora administrativa	24	72	ERP + Servidor BD + Servidor de archivos	SI	Operación mínima con registro temporal y priorización de pedidos/despachos críticos
P-004	Despacho y logística (dependiente de ERP)	Coordinación de logística	4	24	ERP + Servidor BD + Cisco Meraki (FW y VLAN's) + Switches + Servidor de archivos	SI	Despachar prioridades con control manual y evidencias mínimas

Para la ejecución del paso 4 de la estrategia, en la cual se requieren priorizar los riesgos con base en la selección del BIA, en la figura 26 se visualizan los listados creados para completar la información requerida posteriormente durante el proceso de evaluación de riesgos. Luego en la figura 27 se definen los catálogos de Activos, amenazas y vulnerabilidades. Los activos seleccionados fueron únicamente los asociados al alcance del top 3 del BIA, y que, a su vez, fueron seleccionados a partir del caso de estudio. El catálogo de amenazas y vulnerabilidades fueron creados a partir de la selección de los comunes para el sector identificados dentro del alcance de este trabajo de grado, y, posteriormente, como se observa en la figura 28 se definieron la selección de escenarios que son posibles de acuerdo con el alcance, tipo y contexto de la compañía.

Figura 26.
Definición parámetros y listas para paso 4.



Tipo de activo
Datos / Información
Documentación
Hardware
Infraestructura
Organización / Elementos institucionales
Personas
Procesos
Recursos externos / Proveedores
Servicios
Software

Catalogo de vulnerabilidades
Apis Inseguras
Configuraciones erróneas
Convergencia TI/TO insegura
Escasez de Talento en Ciberseguridad
Gestión Inadecuada de Identidades y
IoT/IIoT débil
Parches tardíos/ausentes
Segmentación de red inadecuada
Seguridad móvil débil
Software no autorizado/pirata
Virtualización / nube híbrida mal ges
Wi-Fi insegura
Zero-day

Amenazas
Botnet
Criptojacking
Cross-Site Scripting (XSS)
DoS/DDoS
Downloader/Dropper
Empleado/contratista malicioso
Logic bomb
Malvertising
Propagación hacia IACS
Ransomware
RAT (Remote Access Trojan)
Rootkit
SIM-swapping
SQL Injection

Factor de riesgo
Accidental
Deliberada
Física
Natural
Organizacional
Tecnológica
Terceros

TABLAS DE PROBABILIDAD/FRECUENCIA

Nivel	Rangos	Ejemplo detallado de la descripcio
1	Raro	Puede ocurrir solo bajo circunstancias excepcionales
2	Improbable	Podría ocurrir algunas veces
3	Posible	Puede ocurrir en algún momento
4	Probable	Probabilidad de ocurrencia en la mayoría de las circunstancias
5	Casi seguro	La expectativa de ocurrencia se da en la mayoría de circunstancias

TABLAS DE IMPACTO
Impacto en la OPERACIÓN / Disponibilidad

Nivel	Rangos	Ejemplo detallado de la descripcio
1	Muy bajo	Hay una indisponibilidad menor a 4 y la puede resolver la mesa de ayuda.
2	Bajo	Hay una indisponibilidad entre 4 y 12 horas, es necesario escalarlo a 2 nivel
3	Moderado	Hay una indisponibilidad entre 12 y 36 horas, se requiere consulta el proveedor
4	Alto	Hay una indisponibilidad entre 36 y 72 horas, se requiere al proveedor en sitio.
5	Muy alto	Hay una indisponibilidad por más de 72 horas, es necesario establecer un mecanismo de procesamiento alte

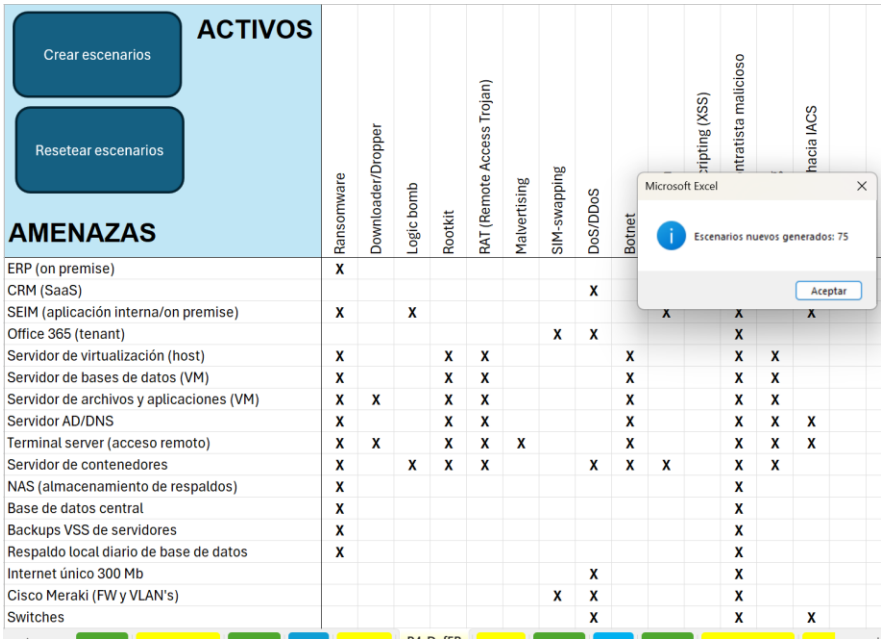
Figura 27.
Definición de catálogo de activos, amenazas y vulnerabilidades para paso 4.

Activos/Recursos	Tipo de activo
ERP (on premise)	Software
CRM (SaaS)	Software
SEIM (aplicación interna/on premise)	Software
Office 365 (tenant)	Servicios
Servidor de virtualización (host)	Hardware
Servidor de bases de datos (VM)	Hardware
Servidor de archivos y aplicaciones (VM)	Hardware
Servidor AD/DNS	Hardware
Terminal server (acceso remoto)	Hardware
Servidor de contenedores	Hardware
NAS (almacenamiento de respaldos)	Hardware
Base de datos central	Datos / Información
Backups VSS de servidores	Datos / Información
Respaldo local diario de base de datos	Datos / Información
Internet único 300 Mb	Recursos externos / Proveedores
Cisco Meraki (FW y VLAN's)	Infraestructura
Switches	Infraestructura

Vulnerabilidades	Control	%
Zero-day		
IoT/IIoT débil		
Convergencia TI/TO insegura		
Seguridad móvil débil		
Software no autorizado/pirata		
Parches tardíos/ausentes		
Configuraciones erróneas		
Segmentación de red inadecuada		
Wi-Fi insegura		
Virtualización / nube híbrida mal gestionada		
Escasez de Talento en Ciberseguridad		
Gestión Inadecuada de Identidades y Accesos (IAM)		
Apis Inseguras		

Amenazas	Factor de riesgo
Ransomware	
Downloader/Dropper	
Logic bomb	
Rootkit	
RAT (Remote Access Trojan)	
Malvertising	
SIM-swapping	
DoS/DDoS	
Botnet	
SQL Injection	
Cross-Site Scripting (XSS)	
Empleado/contratista malicioso	
Criptojacking	
Propagación hacia IACS	

Figura 28.
Cruce de escenarios de riesgo para paso 4.



ACTIVOS \ AMENAZAS	Ransomware	Downloader/Dropper	Logic bomb	Rootkit	RAT (Remote Access Trojan)	Malvertising	SIM-swapping	DoS/DDoS	Botnet						
ERP (on premise)	X														
CRM (SaaS)								X							
SEIM (aplicación interna/on premise)	X		X							X		X		X	
Office 365 (tenant)							X	X				X			
Servidor de virtualización (host)	X			X	X				X			X	X		
Servidor de bases de datos (VM)	X			X	X				X			X	X		
Servidor de archivos y aplicaciones (VM)	X	X		X	X				X			X	X		
Servidor AD/DNS	X			X	X				X			X	X	X	
Terminal server (acceso remoto)	X	X		X	X	X			X			X	X	X	
Servidor de contenedores	X		X	X	X			X	X	X		X	X		
NAS (almacenamiento de respaldos)	X											X			
Base de datos central	X											X			
Backups VSS de servidores	X											X			
Respaldo local diario de base de datos	X											X			
Internet único 300 Mb								X				X			
Cisco Meraki (FW y VLAN's)							X	X				X			
Switches								X				X		X	

La generación automática de los escenarios fue lograda gracias a las macros propuestas en el objetivo 3 y que fueron incluidos en el anexo 4, lo cual permitió optimizar el tiempo, centrando el esfuerzo en la calificación de los escenarios de riesgo. En las figuras 29 y 30 se puede observar dicha calificación para algunos de los escenarios de riesgo, la cual fue producto de valorar los impactos a la disponibilidad y la probabilidad de ocurrencia a partir de los controles actuales que el caso de estudio indicaba dentro de su narrativa. Finalmente, en la figura 31 se puede observar el resultado de ejecución de calificación de aceptabilidad de riesgo asociada a los escenarios, este resultado fue a su vez el insumo principal para que posteriormente, en el paso 5, se centren los esfuerzos en cubrir con estrategias de continuidad los riesgos inadmisibles e inaceptables (figura 32).

Figura 29.

Calificación de escenarios de riesgo para paso 4 (parte 1).

ID	Escenario de riesgo	Probabilidad	Descripción Probabilidad	Impacto a la disponibilidad	Descripción impacto	Riesgo de impacto a la operación	Controles actuales
R-001	La materialización de la amenaza 'Ransomware' sobre el activo 'ERP (on premise)' podría afectar la disponibilidad del servicio y la operación del negocio.	3	Posible	2	Bajo	6	- Antivirus Eset Smart Protection - Segmentación de red - Copia de seguridad diaria - Soporte de mesa de ayuda
R-002	La materialización de la amenaza 'SQL Injection' sobre el activo 'ERP (on premise)' podría afectar la disponibilidad del servicio y la operación del negocio.	3	Posible	2	Bajo	6	- Servidor de contenedores(integración controlada)
R-003	La materialización de la amenaza 'Empleado/contratista malicioso' sobre el activo 'ERP (on premise)' podría afectar la disponibilidad del servicio y la operación del negocio.	2	Improbable	2	Bajo	4	- AD - Copia de seguridad diaria - Soporte de mesa de ayuda
R-004	La materialización de la amenaza 'DoS/DDoS' sobre el activo 'CRM (SaaS)' podría afectar la disponibilidad del servicio y la operación del negocio.	3	Posible	5	Muy alto	15	
R-005	La materialización de la amenaza 'SQL Injection' sobre el activo 'CRM (SaaS)' podría afectar la disponibilidad del servicio y la operación del negocio.	3	Posible	5	Muy alto	15	
R-006	La materialización de la amenaza 'Cross-Site Scripting (XSS)' sobre el activo 'CRM (SaaS)' podría afectar la disponibilidad del servicio y la operación del negocio.	2	Improbable	5	Muy alto	10	
R-007	La materialización de la amenaza 'Empleado/contratista malicioso' sobre el activo 'CRM (SaaS)' podría afectar la disponibilidad del servicio y la operación del negocio.	3	Posible	3	Moderado	9	- Gestión de acceso mediante cuentas corporativas - Soporte de mesa de ayuda
R-008	La materialización de la amenaza 'Ransomware' sobre el activo 'SEIM (aplicación interna/on premise)' podría afectar la disponibilidad del servicio y la operación del negocio.	3	Posible	2	Bajo	6	- Antivirus Eset Smart Protection - Segmentación de red - Copia de seguridad diaria - Soporte de mesa de ayuda
R-009	La materialización de la amenaza 'Logic bomb' sobre el activo 'SEIM (aplicación interna/on premise)' podría afectar la disponibilidad del servicio y la operación del negocio.	3	Posible	3	Moderado	9	- Antivirus Eset Smart Protection - Segmentación de red - Copia de seguridad diaria - Soporte de mesa de ayuda
R-010	La materialización de la amenaza 'SQL Injection' sobre el activo 'SEIM (aplicación interna/on premise)' podría afectar la disponibilidad del servicio y la operación del negocio.	3	Posible	2	Bajo	6	- Servidor de contenedores(integración controlada)
R-011	La materialización de la amenaza 'Empleado/contratista malicioso' sobre el activo 'SEIM (aplicación interna/on premise)' podría afectar la disponibilidad del servicio y la operación del negocio.	2	Improbable	2	Bajo	4	- AD - Copia de seguridad diaria - Soporte de mesa de ayuda
R-012	La materialización de la amenaza 'Propagación hacia IACS' sobre el activo 'SEIM (aplicación interna/on premise)' podría afectar la disponibilidad del servicio y la operación del negocio.	2	Improbable	2	Bajo	4	- Segmentación de red
R-013	La materialización de la amenaza 'SIM-swapping' sobre el activo 'Office 365 (tenant)' podría afectar la disponibilidad del servicio y la operación del negocio.	1	Raro	4	Alto	4	- Soporte mesa de ayuda
R-014	La materialización de la amenaza 'DoS/DDoS' sobre el activo 'Office 365 (tenant)' podría afectar la disponibilidad del servicio y la operación del negocio.	3	Posible	2	Bajo	6	
R-015	La materialización de la amenaza 'Empleado/contratista malicioso' sobre el activo 'Office 365 (tenant)' podría afectar la disponibilidad del servicio y la operación del negocio.	2	Improbable	2	Bajo	4	- Gestión de acceso mediante cuentas corporativas - Soporte de mesa de ayuda
R-016	La materialización de la amenaza 'Ransomware' sobre el activo 'Servidor de virtualización	3	Posible	5	Muy alto	15	- Antivirus Eset Smart Protection - Segmentación de red

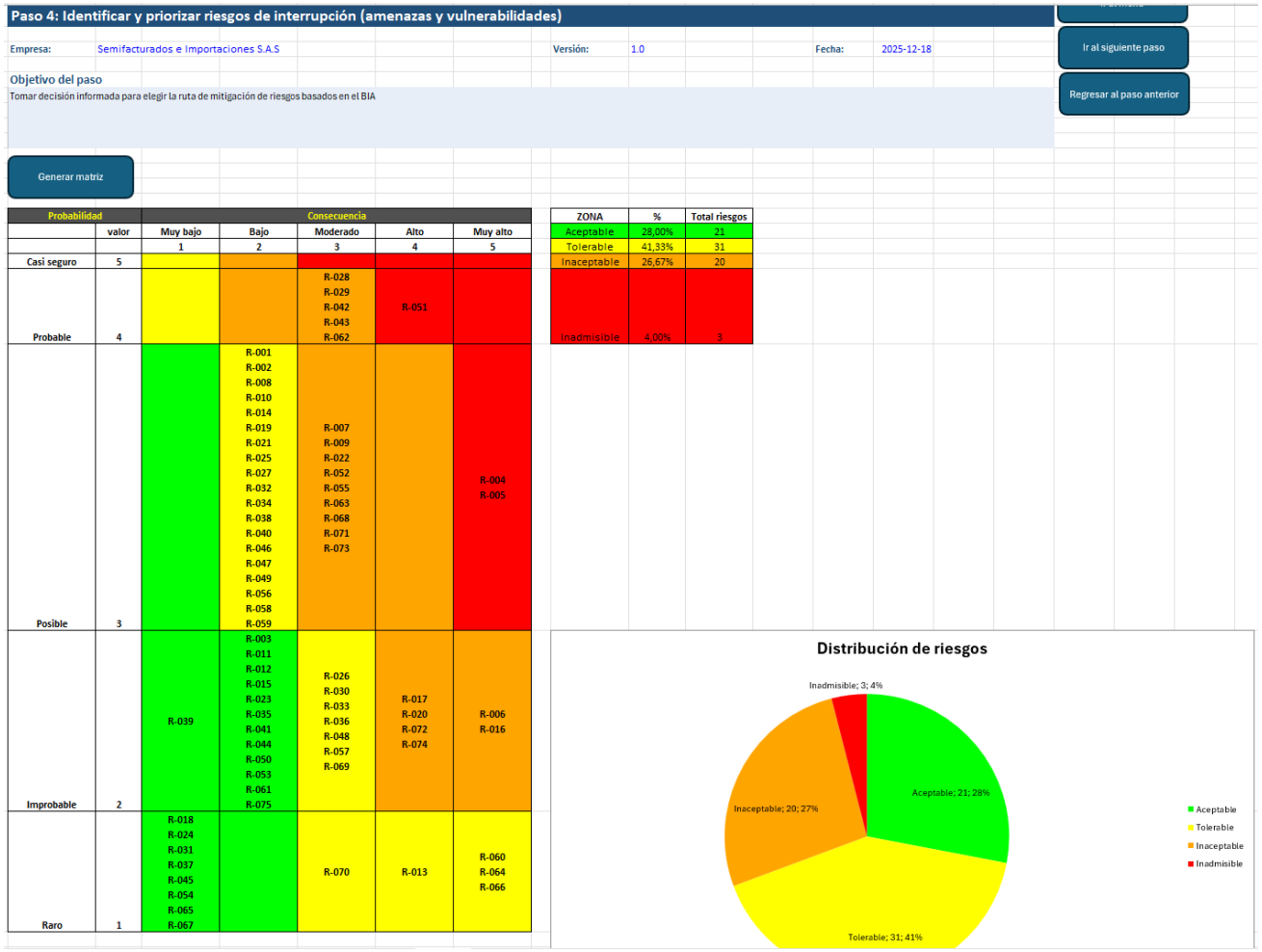
Figura 30.

Calificación de escenarios de riesgo para paso 4 (parte 2).

R-061	La materialización de la amenaza 'Empleado/contratista malicioso' sobre el activo 'NAS (almacenamiento de respaldos)' podría afectar la disponibilidad del servicio y la operación del negocio.	2	Improbable	2	Bajo	4	-Soporte de mesa de ayuda
R-062	La materialización de la amenaza 'Ransomware' sobre el activo 'Base de datos central' podría afectar la disponibilidad del servicio y la operación del negocio.	4	Probable	3	Moderado	12	- Antivirus Eset Smart Protection - Segmentación de red - Copia de seguridad diaria - Soporte de mesa de ayuda
R-063	La materialización de la amenaza 'Empleado/contratista malicioso' sobre el activo 'Base de datos central' podría afectar la disponibilidad del servicio y la operación del negocio.	3	Posible	3	Moderado	9	- AD - Copia de seguridad diaria - Soporte de mesa de ayuda
R-064	La materialización de la amenaza 'Ransomware' sobre el activo 'Backups VSS de servidores' podría afectar la disponibilidad del servicio y la operación del negocio.	1	Raro	5	Muy alto	5	- Antivirus Eset Smart Protection - Segmentación de red - Copia de seguridad diaria - Soporte de mesa de ayuda
R-065	La materialización de la amenaza 'Empleado/contratista malicioso' sobre el activo 'Backups VSS de servidores' podría afectar la disponibilidad del servicio y la operación del negocio.	1	Raro	1	Muy bajo	1	- AD - Copia de seguridad diaria - Soporte de mesa de ayuda
R-066	La materialización de la amenaza 'Ransomware' sobre el activo 'Respaldo local diario de base de datos' podría afectar la disponibilidad del servicio y la operación del negocio.	1	Raro	5	Muy alto	5	- Antivirus Eset Smart Protection - Segmentación de red - Copia de seguridad diaria - Soporte de mesa de ayuda
R-067	La materialización de la amenaza 'Empleado/contratista malicioso' sobre el activo 'Respaldo local diario de base de datos' podría afectar la disponibilidad del servicio y la operación del negocio.	1	Raro	1	Muy bajo	1	- AD - Copia de seguridad diaria - Soporte de mesa de ayuda
R-068	La materialización de la amenaza 'DoS/DDoS' sobre el activo 'Internet único 300 Mb' podría afectar la disponibilidad del servicio y la operación del negocio.	3	Posible	3	Moderado	9	
R-069	La materialización de la amenaza 'Empleado/contratista malicioso' sobre el activo 'Internet único 300 Mb' podría afectar la disponibilidad del servicio y la operación del negocio.	2	Improbable	3	Moderado	6	-Soporte de mesa de ayuda
R-070	La materialización de la amenaza 'SIM-swapping' sobre el activo 'Cisco Meraki (FW y VLAN's)' podría afectar la disponibilidad del servicio y la operación del negocio.	1	Raro	3	Moderado	3	- Soporte mesa de ayuda
R-071	La materialización de la amenaza 'DoS/DDoS' sobre el activo 'Cisco Meraki (FW y VLAN's)' podría afectar la disponibilidad del servicio y la operación del negocio.	3	Posible	3	Moderado	9	
R-072	La materialización de la amenaza 'Empleado/contratista malicioso' sobre el activo 'Cisco Meraki (FW y VLAN's)' podría afectar la disponibilidad del servicio y la operación del negocio.	2	Improbable	4	Alto	8	-Soporte de mesa de ayuda
R-073	La materialización de la amenaza 'DoS/DDoS' sobre el activo 'Switches' podría afectar la disponibilidad del servicio y la operación del negocio.	3	Posible	3	Moderado	9	
R-074	La materialización de la amenaza 'Empleado/contratista malicioso' sobre el activo 'Switches' podría afectar la disponibilidad del servicio y la operación del negocio.	2	Improbable	4	Alto	8	-Soporte de mesa de ayuda
R-075	La materialización de la amenaza 'Propagación hacia IACS' sobre el activo 'Switches' podría afectar la disponibilidad del servicio y la operación del negocio.	2	Improbable	2	Bajo	4	- Segmentación de red

Figura 31.

Clasificación escenarios de riesgos - resultado del paso 4.



Paso 4: Identificar y priorizar riesgos de interrupción (amenazas y vulnerabilidades)

Empresa: Semifacturados e Importaciones S.A.S | Versión: 1.0 | Fecha: 2025-12-18

Ir al siguiente paso

Regresar al paso anterior

Objetivo del paso

Tomar decisión informada para elegir la ruta de mitigación de riesgos basados en el BIA

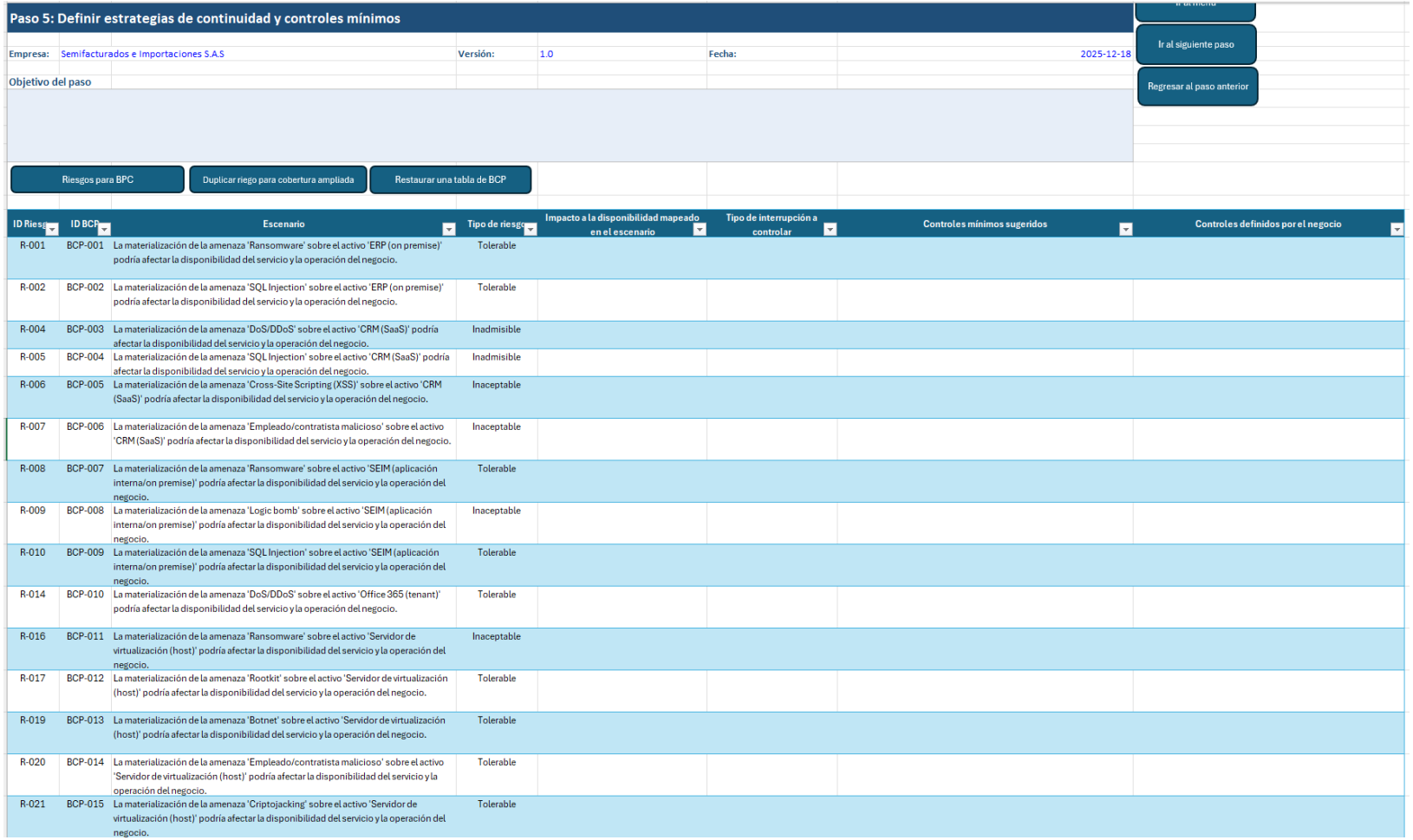
Generar matriz

Probabilidad	valor	Consecuencia: Muy bajo (1)	Bajo (2)	Moderado (3)	Alto (4)	Muy alto (5)
Casi seguro	5					
Probable	4			R-028 R-029 R-042 R-043 R-062	R-051	
Posible	3		R-001 R-002 R-008 R-010 R-014 R-019 R-021 R-025 R-027 R-032 R-034 R-038 R-040 R-046 R-047 R-049 R-056 R-058 R-059	R-007 R-009 R-022 R-052 R-055 R-063 R-068 R-071 R-073		R-004 R-005
Improbable	2	R-039	R-003 R-011 R-012 R-015 R-023 R-035 R-041 R-044 R-050 R-053 R-061 R-075	R-026 R-030 R-033 R-036 R-048 R-057 R-069	R-017 R-020 R-072 R-074	R-006 R-016
Raro	1	R-018 R-024 R-031 R-037 R-045 R-054 R-065 R-067		R-070	R-013	R-060 R-064 R-066

ZONA	%	Total riesgos
Aceptable	28,00%	21
Tolerable	41,33%	31
Inaceptable	26,67%	20
Inadmisible	4,00%	3

Figura 32.

Selección de escenarios para BCP (paso 5).



Paso 5: Definir estrategias de continuidad y controles mínimos

Empresa: Semifacturados e Importaciones S.A.S | Versión: 1.0 | Fecha: 2025-12-18

Objetivo del paso

Ir al siguiente paso

Regresar al paso anterior

Riesgos para BPC | Duplicar riego para cobertura ampliada | Restaurar una tabla de BCP

ID Riesg	ID BCP	Escenario	Tipo de riesgo	Impacto a la disponibilidad mapeado en el escenario	Tipo de interrupción a controlar	Controles mínimos sugeridos	Controles definidos por el negocio
R-001	BCP-001	La materialización de la amenaza 'Ransomware' sobre el activo 'ERP (on premise)' podría afectar la disponibilidad del servicio y la operación del negocio.	Tolerable				
R-002	BCP-002	La materialización de la amenaza 'SQL Injection' sobre el activo 'ERP (on premise)' podría afectar la disponibilidad del servicio y la operación del negocio.	Tolerable				
R-004	BCP-003	La materialización de la amenaza 'DoS/DDoS' sobre el activo 'CRM (SaaS)' podría afectar la disponibilidad del servicio y la operación del negocio.	Inadmisible				
R-005	BCP-004	La materialización de la amenaza 'SQL Injection' sobre el activo 'CRM (SaaS)' podría afectar la disponibilidad del servicio y la operación del negocio.	Inadmisible				
R-006	BCP-005	La materialización de la amenaza 'Cross-Site Scripting (XSS)' sobre el activo 'CRM (SaaS)' podría afectar la disponibilidad del servicio y la operación del negocio.	Inaceptable				
R-007	BCP-006	La materialización de la amenaza 'Empleado/contratista malicioso' sobre el activo 'CRM (SaaS)' podría afectar la disponibilidad del servicio y la operación del negocio.	Inaceptable				
R-008	BCP-007	La materialización de la amenaza 'Ransomware' sobre el activo 'SEIM (aplicación interna/on premise)' podría afectar la disponibilidad del servicio y la operación del negocio.	Tolerable				
R-009	BCP-008	La materialización de la amenaza 'Logic bomb' sobre el activo 'SEIM (aplicación interna/on premise)' podría afectar la disponibilidad del servicio y la operación del negocio.	Inaceptable				
R-010	BCP-009	La materialización de la amenaza 'SQL Injection' sobre el activo 'SEIM (aplicación interna/on premise)' podría afectar la disponibilidad del servicio y la operación del negocio.	Tolerable				
R-014	BCP-010	La materialización de la amenaza 'DoS/DDoS' sobre el activo 'Office 365 (tenant)' podría afectar la disponibilidad del servicio y la operación del negocio.	Tolerable				
R-016	BCP-011	La materialización de la amenaza 'Ransomware' sobre el activo 'Servidor de virtualización (host)' podría afectar la disponibilidad del servicio y la operación del negocio.	Inaceptable				
R-017	BCP-012	La materialización de la amenaza 'Rootkit' sobre el activo 'Servidor de virtualización (host)' podría afectar la disponibilidad del servicio y la operación del negocio.	Tolerable				
R-019	BCP-013	La materialización de la amenaza 'Botnet' sobre el activo 'Servidor de virtualización (host)' podría afectar la disponibilidad del servicio y la operación del negocio.	Tolerable				
R-020	BCP-014	La materialización de la amenaza 'Empleado/contratista malicioso' sobre el activo 'Servidor de virtualización (host)' podría afectar la disponibilidad del servicio y la operación del negocio.	Tolerable				
R-021	BCP-015	La materialización de la amenaza 'Criptojacking' sobre el activo 'Servidor de virtualización (host)' podría afectar la disponibilidad del servicio y la operación del negocio.	Tolerable				

Con el objetivo de definir algunos catálogos estandarizados que funcionen como heurísticas organizacionales que permitieran unificar estrategias de continuidad a partir de preguntas clave según la propuesta del instrumento del objetivo 3, en la figura 33 se parametrizaron algunos basados en los controles mínimos sugeridos para los tipos de riesgo de indisponibilidad que fueron identificados dentro del desarrollo de este trabajo, para que posteriormente, como se observa en la figura 34, se definiera en conjunto con el negocio aquellas que son aceptadas de acuerdo con el alcance actual del BCP.

Figura 33.

Catálogo de sugerencias para continuidad.

Codigo_Catalogo	Tipo_Interrupcion	Pregunta_Guia	Interpretacion_Estandar	Buena_Practica	Controles_Minimos	Clausula_ISO_22301
CAT-001	Indisponibilidad del ERP	¿Cómo operará la empresa si el ERP no responde?	Definir operación mínima y tiempos (RTO/RP	Registro manual y restaur	Backups; playbook; roles definidos; comunicación	8.4 / 8.4.4
CAT-002	Indisponibilidad del SEIM	¿Cómo operará la empresa si el SEIM no responde?	Definir operación mínima y tiempos (RTO/RP	Registro manual y restaur	Backups; playbook; roles definidos; comunicación	8.4 / 8.4.4
CAT-003	Indisponibilidad de servidores host virtualizació	¿Qué servicios se recuperan primero si cae el host?	Priorizar servicios por criticidad	Lista de servicios críticos :	Backups; pruebas de restauración; inventario	8.4.4
CAT-004	Indisponibilidad de servidores virtualizados	¿Qué hacer si un servidor virtualizado deja de operar o r	Definir operación mínima y tiempos (RTO/RP	Registro manual y restaur	Backups; playbook; roles definidos; comunicación	8.4 / 8.4.4
CAT-005	Indisponibilidad AD/DNS	¿Cómo accederán los usuarios si falla autenticación?	Asegurar acceso controlado y recuperación	Réplica/contingencia y ha	Cuentas de contingencia; procedimientos	8.4.4
CAT-006	Indisponibilidad del internet	¿Cómo comunicarse con clientes y realizar operacione:	Operación degradada para continuidad	Canales alternos de pedic	Procedimiento manual; contactos ISP	8.4.4
CAT-007	Indisponibilidad del CRM	¿Cómo se capturan pedidos sin CRM?	Operación degradada para continuidad	Canales alternos de pedic	Procedimiento manual; contactos SaaS	8.4.4
CAT-008	Backups no disponibles	¿Qué hacer si no se puede restaurar?	Proteger copias y alternativas	Separación y pruebas de (	Copia offline; control de acceso; pruebas	8.4.4
CAT-009	Indisponibilidad de red interna	¿Cómo restablecer conectividad rápidamente?	Control de cambios y recuperación de confi	Respaldos de configuraci	Backup config; checklist de red	8.4.4
CAT-010	Indisponibilidad integraciones	¿Cómo mantener flujo de pedidos si falla integración?	Procesos manuales temporales	Carga manual y validación	Procedimiento manual; rollback	8.4.4
CAT-011	Indisponibilidad en terminal server	¿Cómo asegurar operación remota?	Canales alternos y recuperación	Acceso alterno y comunic	Backups; playbook; roles definidos; comunicación	8.4 / 8.4.4

Figura 34.
Definición de estrategias de continuidad.

Estrategia de BCP para MiPymes con el modelo de racionalidad limitada

Paso 5: Definir estrategias de continuidad y controles mínimos

Ir al menú | Ir al siguiente paso | Regresar al paso anterior

Empresa: Semifacturados e Importaciones S.A.S | Versión: 1.0 | Fecha: 2025-12-18

Objetivo del paso

Definir estrategias de continuidad y controles mínimos a partir de los riesgos priorizados, es decir, qué se controlará, cuáles son los controles mínimos sugeridos y cuales de ellos son los definidos.

Riesgos para BPC | Duplicar riego para cobertura ampliada | Restaurar una tabla de BCP

ID Riesgo	ID BCP	Escenario	Tipo de riesgo	Impacto a la disponibilidad mapeado en el escenario	Tipo de interrupción a controlar	Controles mínimos sugeridos	Controles definidos por el negocio
R-004	BCP-003	La materialización de la amenaza 'DoS/DDoS' sobre el activo 'CRM (SaaS)' podría afectar la disponibilidad del servicio y la operación del negocio.	Inadmisible	Muy alto	Indisponibilidad del CRM	Procedimiento manual; contactos SaaS	Procedimiento manual; contactos SaaS
R-005	BCP-004	La materialización de la amenaza 'SQL Injection' sobre el activo 'CRM (SaaS)' podría afectar la disponibilidad del servicio y la operación del negocio.	Inadmisible	Muy alto	Indisponibilidad del CRM	Procedimiento manual; contactos SaaS	Procedimiento manual; contactos SaaS
R-006	BCP-005	La materialización de la amenaza 'Cross-Site Scripting (XSS)' sobre el activo 'CRM (SaaS)' podría afectar la disponibilidad del servicio y la operación del negocio.	Inaceptable	Muy alto	Indisponibilidad del CRM	Procedimiento manual; contactos SaaS	Procedimiento manual; contactos SaaS
R-007	BCP-006	La materialización de la amenaza 'Empleado/contratista malicioso' sobre el activo 'CRM (SaaS)' podría afectar la disponibilidad del servicio y la operación del negocio.	Inaceptable	Moderado	Indisponibilidad del CRM	Procedimiento manual; contactos SaaS	Procedimiento manual; contactos SaaS
R-009	BCP-008	La materialización de la amenaza 'Logic bomb' sobre el activo 'SEIM (aplicación interna/on premise)' podría afectar la disponibilidad del servicio y la operación del negocio.	Inaceptable	Moderado	Indisponibilidad del SEIM	Backups; playbook; roles definidos; comunicación	Backups; playbook; roles definidos; comunicación
R-016	BCP-011	La materialización de la amenaza 'Ransomware' sobre el activo 'Servidor de virtualización (host)' podría afectar la disponibilidad del servicio y la operación del negocio.	Inaceptable	Muy alto	Indisponibilidad de servidores host virtualización	Backups; pruebas de restauración; inventario	Backups; pruebas de restauración; inventario
R-022	BCP-016	La materialización de la amenaza 'Ransomware' sobre el activo 'Servidor de bases de datos (VM)' podría afectar la disponibilidad del servicio y la operación del negocio.	Inaceptable	Moderado	Indisponibilidad de servidores virtualizados	Backups; playbook; roles definidos; comunicación	Backups; playbook; roles definidos; comunicación
R-028	BCP-020	La materialización de la amenaza 'Ransomware' sobre el activo 'Servidor de archivos y aplicaciones (VM)' podría afectar la disponibilidad del servicio y la operación del negocio.	Inaceptable	Moderado	Indisponibilidad de servidores virtualizados	Backups; playbook; roles definidos; comunicación	Backups; playbook; roles definidos; comunicación
R-029	BCP-021	La materialización de la amenaza 'Downloader/Dropper' sobre el activo 'Servidor de archivos y aplicaciones (VM)' podría afectar la disponibilidad del servicio y la operación del negocio.	Inaceptable	Moderado	Indisponibilidad de servidores virtualizados	Backups; playbook; roles definidos; comunicación	Backups; playbook; roles definidos; comunicación
R-042	BCP-029	La materialización de la amenaza 'Ransomware' sobre el activo 'Terminal server (acceso remoto)' podría afectar la disponibilidad del servicio y la operación del negocio.	Inaceptable	Moderado	Indisponibilidad de servidores virtualizados	Backups; playbook; roles definidos; comunicación	Backups; playbook; roles definidos; comunicación
R-043	BCP-030	La materialización de la amenaza 'Downloader/Dropper' sobre el activo 'Terminal server (acceso remoto)' podría afectar la disponibilidad del servicio y la operación del negocio.	Inaceptable	Moderado	Indisponibilidad de servidores virtualizados	Backups; playbook; roles definidos; comunicación	Backups; playbook; roles definidos; comunicación
R-051	BCP-035	La materialización de la amenaza 'Ransomware' sobre el activo 'Servidor de contenedores' podría afectar la disponibilidad del servicio y la operación del negocio.	Inadmisible	Alto	Indisponibilidad de servidores virtualizados	Backups; playbook; roles definidos; comunicación	Backups; playbook; roles definidos; comunicación
R-052	BCP-036	La materialización de la amenaza 'Logic bomb' sobre el activo 'Servidor de contenedores' podría afectar la disponibilidad del servicio y la operación del negocio.	Inaceptable	Moderado	Indisponibilidad de servidores virtualizados	Backups; playbook; roles definidos; comunicación	Backups; playbook; roles definidos; comunicación
R-055	BCP-037	La materialización de la amenaza 'DoS/DDoS' sobre el activo 'Servidor de contenedores' podría afectar la disponibilidad del servicio y la operación del negocio.	Inaceptable	Moderado	Indisponibilidad integraciones	Procedimiento manual; rollback	Procedimiento manual; rollback
R-062	BCP-043	La materialización de la amenaza 'Ransomware' sobre el activo 'Base de datos central' podría afectar la disponibilidad del servicio y la operación del negocio.	Inaceptable	Moderado	Indisponibilidad integraciones	Procedimiento manual; rollback	Procedimiento manual; rollback
R-063	BCP-044	La materialización de la amenaza 'Empleado/contratista malicioso' sobre el activo 'Base de datos central' podría afectar la disponibilidad del servicio y la operación del negocio.	Inaceptable	Moderado	Indisponibilidad integraciones	Procedimiento manual; rollback	Procedimiento manual; rollback
R-068	BCP-047	La materialización de la amenaza 'DoS/DDoS' sobre el activo 'Internet único 300 Mb'	Inaceptable	Moderado	Indisponibilidad del internet	Procedimiento manual; contactos ISP	Procedimiento manual; contactos ISP

Con el resultado del paso 5, en el cual se obtuvo la definición general del negocio para las estrategias de continuidad, se realizaron las construcciones que permitieron darle solidez a las estrategias. Para lograrlo, se construyeron playbooks específicos para cada sistema o conjunto de ellos, tal como puede observarse en la figura 35. Luego, en la figura 36 se evidencia cómo se construyó un catálogo que está orientado a parámetros de disponibilidad, permitiendo que en momentos de atención a incidentes se pueda conectar de una forma rápida tanto los procesos críticos y los sistemas asociados a ellos, con los tiempos de RTO, y que además permita seleccionar el playbook a operar, además, también se construyó la matriz de contactos (figura 37) que es parte de los insumos sugeridos y usados al interior de los playbooks.

Finalmente, en este mismo paso se documentó el BCP de forma muy simple, con el propósito de priorizar su uso y comprensión en escenarios reales, y, como se visualiza en la figura 38, existe un paso a paso para operarlo de inicio a fin. En este sentido, el paso 6 fue el resultado conceptual de los esfuerzos realizados en los pasos anteriores, permitiendo que se llegara a estrategias claras de continuidad que habiliten la operación dentro de los procesos críticos objetivo del alcance del caso de estudio. Además, estableció los elementos necesarios para que en pasos posteriores pueda habilitar el proceso de mejora continua lo que conllevará a la evolución y madurez del BCP. En síntesis, aquí se logró validar el impacto de tomar decisiones informadas a partir de mapear los procesos críticos y los escenarios de riesgos de ciberseguridad asociados a ellos.

Figura 35.
Playbooks para paso 6.

Ir a matriz de contactos | Regresar al paso 6

PR_ID	Paso #	Acción	Responsable	Tiempo objetivo (min)	Entrada/Disparador	Salida/Evidencia	Notas
PR-ERP-01	1	Registrar incidente y confirmar indisponibilidad del ERP (prueba de acceso + transacción simple).	Analista soporte inhouse	10	Usuarios reportan "ERP no responde" / errores / lentitud severa	Ticket creado + captura de error	
PR-ERP-01	2	Determinar alcance: ¿es solo ERP o también BD, AD/DNS, red o virtualización?	Ingeniero de sistemas	15	Ticket abierto y falla confirmada	Matriz rápida de alcance (ERP/BD/AD/Red)	
PR-ERP-01	3	Activar operación esencial: captura manual de pedidos y despacho mínimo (formato/plantilla definida).	Coordinador BCP (con líder de ventas/producción)	30	ERP indisponible confirmado	Plantilla manual activada + responsables asignados	
PR-ERP-01	4	Contención si se sospecha ciberataque: aislar servidor ERP/BD de red y detener accesos remotos.	Ingeniero de sistemas	20	Indicadores de compromiso (ransomware/archivos cifrados/alertas Eset)	Evidencia de aislamiento (puertos/VLAN/ACL)	Proteger backups: evitar que se sigan montando recursos comprometidos.
PR-ERP-01	5	Recuperación rápida: revisar servicios ERP y BD, reinicio controlado de servicios.	Desarrollador + Ingeniero de sistemas	30	ERP cae pero host y red operativos	Servicios arriba + registro de acciones	Si reinicio no resuelve en 30 min, pasar a restauración (Paso 6 de PR-E 01).
PR-ERP-01	6	Restauración: recuperar ERP/BD desde backup aplicable (VSS a NAS + backup local BD) según runbook.	Ingeniero de sistemas + Desarrollador	240	Confirmación de falla persistente o corrupción	Bitácora de restauración + hora de restore + versión backup	
PR-ERP-01	7	Validación funcional: login, consulta, creación de transacción; verificar módulos críticos (inventario, facturación, nómina si aplica).	Usuario clave (área) + Desarrollador	45	ERP restaurado/arrancado	Registro de prueba OK + evidencia (pantallazo/log)	Validar también dependencias: SEIM y cualquier integración.
PR-ERP-01	8	Reconciliación: registrar en ERP lo capturado manualmente (pedidos/órdenes/despachos) y cerrar backlog.	Ventas/Producción + Desarrollador	60	ERP operativo y usuarios habilitados	Backlog cargado + control de duplicados	
PR-ERP-01	9	Cierre y mejora	Coordinador BCP	30	Operación estabilizada	Registro de cierre en ticket + formato de incidentes	
PR-CRM-01	1	Registrar incidente y validar si es problema del CRM o del internet local (prueba OOSE/otros sitios)	Analista soporte inhouse	10	Usuarios no acceden al CRM (SaaS)	Ticket creado + Evidencia de pruebas	Confirmar indisponibilidad del servicio en linea si es posible

Figura 36.

Catálogo de códigos BCP.

A	B	C	D	E	F	G
Catálogo de códigos BCP (orientado a disponibilidad)						
ID BCP	**Proceso_ID**	**Proceso**	**Servicio/Sistema**	**MTPD**	**RTO**	**PR_ID**
BCP-003	P-001	Gestión de ventas y pedidos (CRM)	CRM + Internet + Servidor de contenedores + Servidor BD	48	8	PR-CRM-01
BCP-004	P-001	Gestión de ventas y pedidos (CRM)	CRM + Internet + Servidor de contenedores + Servidor BD	48	8	PR-CRM-01
BCP-005	P-001	Gestión de ventas y pedidos (CRM)	CRM + Internet + Servidor de contenedores + Servidor BD	48	8	PR-CRM-01
BCP-006	P-001	Gestión de ventas y pedidos (CRM)	CRM + Internet + Servidor de contenedores + Servidor BD	48	8	PR-CRM-01
BCP-008	P-001	Gestión de ventas y pedidos (CRM)	CRM + Internet + Servidor de contenedores + Servidor BD	48	8	PR-SEIM-01
BCP-011	P-001 P-003 P-004	Todos	Servidor de virtualización (host)	12	4	PR-VIRT-HOST-01
BCP-016	P-001 P-003 P-004	Todos	Servidor de bases de datos (VM) + CRM + ERP + SEIM	12	4	PR-VMS-01
BCP-020	P-003 P-004	Todos	Servidor de archivos y aplicaciones (VM) + ERP + SEIM	12	4	PR-VMS-01
BCP-021	P-003 P-004	Todos	Servidor de archivos y aplicaciones (VM) + ERP + SEIM	12	4	PR-VMS-01
BCP-029	P-001 P-003 P-004	Todos	Terminal server (acceso remoto) + ERP + SEIM	12	4	PR-VMS-01
BCP-030	P-001 P-003 P-004	Todos	Terminal server (acceso remoto) + ERP + SEIM	12	4	PR-VMS-01
BCP-035	P-001 P-003 P-004	Todos	Servidor de contenedores + ERP + SEIM + CRM	12	4	PR-INTEG-01
BCP-036	P-001 P-003	Todos	Servidor de contenedores + ERP + SEIM + CRM	12	4	PR-INTEG-01

Figura 37.
Matriz de contactos.

Ir Playbooks | Ir a Catálogo de BCP | Regresar al paso 6

Matriz de contactos

Rol/Función	Nombre	Área	Teléfono	Alterno	Correo	Canal alterno	Horario	Prioridad	Escalar a (Rol)
Gerencia	Carolina Gómez Arango	Dirección Administrativa / Gerencia	+57 313 555 0182	+57 (604) 444 782	gerencia@seim-sas.com.co	Teléfono corporativo	Laboral	1	Coordinador BCP
Ingeniero de sistemas - Coordi	Andrés Felipe Mejía Ríos	TI	+57 300 821 4479	+57 301 700 2231	bcp@seim-sas.com.co	WhatsApp corporativo	Escalamiento	1	Gerencia
Infraestructura (outsourcing)	Julián Esteban Giraldo Londoño	TI	+57 310 668 9012	+57 (604) 448 910	infraestructura@soporteandino.com.c	Teléfono corporativo	5x8 + escalamien	1	Coordinador BCP
Soporte inhouse	Paula Andrea Castaño Vélez	Soporte	+57 320 412 7834	+57 311 558 4402	soporte.inhouse@seim-sas.com.co	WhatsApp corporativo	5x8	2	Coordinador BCP
Mesa de ayuda remota	Santiago Pérez Ospina	Soporte	+57 302 445 9901	+57 (604) 322 110	mesadeayuda@soporteandino.com.c	Teléfono corporativo	5x8	2	Soporte inhouse
Desarrollo	Laura Camila Toro Ramírez	Desarrollo	+57 315 904 6632	+57 300 820 1109	dev1@seim-sas.com.co	Teams/Correo	Laboral	2	Coordinador BCP
Integraciones	Juan David Restrepo Salazar	Desarrollo	+57 317 230 7788	+57 301 556 9090	dev2@seim-sas.com.co	Teams/Correo	Laboral	2	Coordinador BCP
Producción	Óscar Mauricio Zapata Hoyos	Producción	+57 319 610 2240	+57 304 515 7781	produccion@seim-sas.com.co	Teléfono corporativo	Turnos	2	Coordinador BCP
Planta	Martha Liliana Ceballos Vélez	Producción	+57 321 775 3046	+57 314 909 3322	supervisor.planta@seim-sas.com.co	Teléfono corporativo	Turnos	3	Producción
Ventas	Daniela Andrea Roldán Montoya	Ventas	+57 312 889 6507	+57 300 770 4411	ventas@seim-sas.com.co	Teléfono corporativo	Laboral	3	Coordinador BCP
Proveedor Internet	Soporte ISP	Tercero	01 8000 931 059	01 8000 910 909	cct.empresas.colombia@telefonica.cc	Línea soporte / Portal	24/7	1	Coordinador BCP
Proveedor CRM	Contact Center CRM	Tercero	00800 7253 3333	+353 14403500	N/A	Portal soporte	24/7	2	Ventas
Emergencias (Medellín)	Línea Única de Emergencias 123	Emergencias	123	N/A	N/A	Llamada directa	24/7	1	Coordinador BCP
Emergencias (Medellín)	DAGRD / Bomberos Medellín (mó	Emergencias	+57 (604) 444 414	01 8000 411 144	N/A	Llamada directa	24/7	1	Coordinador BCP
Emergencias (Colombia)	Bomberos	Emergencias	119	N/A	N/A	Llamada directa	24/7	1	Coordinador BCP
Emergencias (Colombia)	Ambulancias / Secretaría de Salu	Emergencias	125	N/A	N/A	Llamada directa	24/7	1	Coordinador BCP
Emergencias (Colombia)	Cruz Roja	Emergencias	132	N/A	N/A	Llamada directa	24/7	1	Coordinador BCP
Emergencias (Colombia)	Defensa Civil	Emergencias	144	N/A	N/A	Llamada directa	24/7	2	Coordinador BCP
Emergencias (Colombia)	GAULA (Antisecuestro)	Emergencias	165	N/A	N/A	Llamada directa	24/7	2	Gerencia
Emergencias (Colombia)	Línea 155 (Violencia contra la mu	Emergencias	155	N/A	N/A	Llamada directa	24/7	2	Gerencia
Emergencias (Colombia)	ICBF - Línea 141 (protección NNA	Emergencias	141	N/A	N/A	Llamada directa	24/7	2	Gerencia

Figura 38.

Paso 6.

Aunque en el paso 6 las estrategias de continuidad se formularon a partir de los recursos actualmente disponibles en el caso de estudio, también sirvió para identificar que es posible fortalecer la forma en que se ejecutan ciertos controles, con el fin de aumentar su consistencia y, en consecuencia, la fiabilidad del BCP durante una interrupción real. Con el objetivo de avanzar hacia la implementación, se definieron planeaciones orientadas a ejecutar acciones que, si bien hacen parte de las estrategias ya definidas, todavía no se encontraban listas para su ejecución. Ejemplos de estas necesidades se presentan en la figura 39, donde se propone, entre otras medidas, habilitar esquemas de respaldo para dispositivos que tienen la capacidad de respaldarse y que el caso de estudio no menciona, así como diseñar plantillas que soporten el registro manual de información en escenarios de interrupción. En las figuras 40, 41 y 42 se muestran la completitud del paso 7, plantando los formatos necesarios para registrar capacitaciones de cara al equipo de continuidad, formatos para registrar actualizaciones al plan y la comunicación de los hitos a la gerencia.

Figura 39.

Plan de implementación (paso 7).

Estrategia de BCP para MiPyme(s) con el modelo de racionalidad limitada

Paso 7: Implementación de las estrategias

Empresa: Semifacturados e Importaciones S.A.S **Versión:** 1.0 **Fecha:** 2026-01-05

Objetivo del paso

Poner en marcha los controles aprobados en el Paso 5 mediante tareas claras, responsables, fechas realistas y evidencia verificable. Priorizar los riesgos clasificados como ALTO.

1) Plan de implementación (backlog de controles)

ID	Estrategia	Tipo (Técnico/Organizativo/Capacitación)	Prioridad	Riesgo/BCP relacionado	Responsable	Fecha inicio	Fecha límite	Estado	% avance	Evidencia (ruta/URL)	BCP/Runbook a actualizar
IMP-001	Formalizar y publicar matriz de contactos (incluye proveedores ISP/CRM y emergencias).	Organizativo	1	R-016 / BCP-011; R-068 / BCP-047	Coordinador BCP	2025-12-18	2025-12-20	Completado	100%	O365/SharePoint/BCP/Contactos/matriz_contactos_v1.xlsx	PR-ERP-01; PR-INTERNET-01
IMP-002	Definir y socializar plantillas de operación manual: pedidos/ventas (CRM), despacho mínimo y control de backlog.	Organizativo	1	R-004 / BCP-003; R-068 / BCP-047	Líder de ventas + Coordinador BCP	2025-12-19	2025-12-27	En curso	60%	O365/SharePoint/BCP/Plantillas/operacion_manual_v1.xlsx	PR-CRM-01; PR-INTERNET-01
IMP-003	Crear checklist mínimo de verificación inicial (alcance) para incidentes: ERP/BD/AD/DNS/red/virtualización.	Técnico	1	R-016 / BCP-011; R-042 / BCP-029	Ingeniero de sistemas	2025-12-20	2025-12-28	En curso	40%	O365/SharePoint/BCP/Checklists/checklist_alcance_v1.docx	PR-ERP-01; PR-VIRT-HOST-01
IMP-004	Inventario mínimo de servicios críticos por VM (AD/DNS, BD, ERP, archivos, terminal, contenedores) y orden de arranque.	Técnico	1	R-016 / BCP-011; BCP-016; BCP-020; BCP-035	Ingeniero de sistemas + Experto infraestructura	2025-12-21	2026-01-05	En curso	30%	O365/SharePoint/BCP/Inventario/servicios_criticos_v1.xlsx	PR-VIRT-HOST-01; PR-VMS-01
IMP-005	Prueba de restauración controlada (ERP/BD) desde backup (VSS a NAS + backup local BD) y registro de evidencia.	Técnico	1	R-016 / BCP-011; R-062 / BCP-043	Experto infraestructura + Desarrollador	2026-01-06	2026-01-15	Planificado	0%	O365/SharePoint/BCP/Evidencias/Restauracion/	PR-ERP-01
IMP-006	Ajustar protección de backups: revisión de permisos NAS, cuentas de servicio y segregación básica (sin sobre-ingeniería).	Técnico	1	R-016 / BCP-011; R-028 / BCP-020	Ingeniero de sistemas	2026-01-08	2026-01-22	Planificado	0%	O365/SharePoint/BCP/Evidencias/Backups/	PR-ERP-01; PR-VMS-01
IMP-007	Definir procedimiento de rollback para contenedores e integraciones CRM↔ERP (última versión estable + ventana controlada).	Técnico	2	R-055 / BCP-037; R-063 / BCP-044	Desarrollador (Integraciones)	2026-01-10	2026-01-25	Planificado	0%	O365/SharePoint/BCP/Runbooks/rollback_integraciones_v1.docx	PR-INTEG-01
IMP-008	Guardar backup de configuración de Meraki y switches + checklist de recuperación de red interna.	Técnico	2	R-071 / BCP-049; R-073 / BCP-051	Experto infraestructura (outsourcing)	2026-01-12	2026-01-26	Planificado	0%	O365/SharePoint/BCP/Red/backup_config/	PR-NET-01
IMP-009	Ajustar ruta de escalamiento con ISP/CRM: tiempos objetivo, responsables y canales (teléfono/portal).	Organizativo	2	R-068 / BCP-047; BCP-003	Coordinador BCP	2026-01-13	2026-01-20	Planificado	0%	O365/SharePoint/BCP/Contactos/escalamiento_proveedores_v1.docx	PR-INTERNET-01; PR-CRM-01
IMP-010	Monitoreo mínimo: alertas de disponibilidad (ping/servicios) para ERP, host, internet y CRM (cuando aplique).	Técnico	2	BCP-011; BCP-047; BCP-003	Ingeniero de sistemas	2026-01-15	2026-01-31	Planificado	0%	O365/SharePoint/BCP/Evidencias/Monitoreo/	PR-ERP-01; PR-VIRT-HOST-01

Figura 40.

Registro de capacitaciones (paso 7)

2) Registro de capacitaciones

Fecha	Tema/Procedimiento	Área	Facilitador	Asistentes (nombres)	Evidencia (foto/lista)	Observaciones
2025-12-19	Inducción BCP: alcance, roles y activación (uso del Catálogo BCP).	Equipo BCP	Coordinador BCP	Carolina Gómez; Andrés Mejía; Paula Castaño; Julián Giraldo; Laura Toro; Juan Restrepo; Óscar Zapata; Daniela Roldán	O365/SharePoint/BCP/Evidencias/Capacitaciones/2025-12-19_lista.pdf	Sesión inicial, se acordó canal de comunicación y escalamiento.
2025-12-23	Ejecución guiada PR-ERP-01 (ERP/BD) y operación esencial (plantillas manuales).	TI + Ventas + Producción	Coordinador BCP	Andrés Mejía; Paula Castaño; Laura Toro; Juan Restrepo; Óscar Zapata; Daniela Roldán	O365/SharePoint/BCP/Evidencias/Capacitaciones/2025-12-23_evidencia.pdf	Enfocado a tiempos objetivo y evidencias mínimas.
2026-01-07	Ejecución guiada PR-CRM-01 (CRM SaaS) + pausa/reactivación de integraciones.	Ventas + Desarrollo	Desarrollador (Integraciones)	Daniela Roldán; Juan Restrepo; Laura Toro; Andrés Mejía	O365/SharePoint/BCP/Evidencias/Capacitaciones/2026-01-07_lista.pdf	Se definió punto de corte y conciliación posterior.
2026-01-16	Ejecución PR-INTERNET-01 (internet caído) y escalamiento a ISP.	TI + Ventas	Ingeniero de sistemas	Andrés Mejía; Paula Castaño; Daniela Roldán	O365/SharePoint/BCP/Evidencias/Capacitaciones/2026-01-16_lista.pdf	Se validó operación degradada y comunicación interna.
2026-01-24	Recuperación de red interna: backup config + checklist (Meraki/Switch).	TI + Infraestructura	Experto infraestructura (outsourcing)	Julián Giraldo; Andrés Mejía; Paula Castaño	O365/SharePoint/BCP/Evidencias/Capacitaciones/2026-01-24_lista.pdf	Se acordó mantener backup offline y registrar cambios.

Figura 41.

Registro de actualizaciones al BCP (paso 7).

3) Registro de actualización del BCP (qué se cambió cuando se implementó)

Fecha	Elemento BCP	Cambio realizado	Motivo	Actualizado por	Evidencia (ruta/URL)
2025-12-20	Matriz de contactos	Se completaron contactos internos, proveedores (ISP/CRM) y líneas de emergencia.	Implementación del Paso 1 y preparación para activación.	Coordinador BCP	O365/SharePoint/BCP/Contactos/matriz_contactos_v1.xlsx
2025-12-28	Checklists	Se agregó checklist de verificación inicial (alcance) y checklist de comunicación.	Reducir incertidumbre y acelerar decisiones.	Ingeniero de sistemas	O365/SharePoint/BCP/Checklists/checklist_alcance_v1.docx
2026-01-07	Playbook PR-CRM-01	Se ajustó procedimiento de pausa/reactivación de integraciones y conciliación de pedidos.	Lecciones de capacitación de integraciones.	Desarrollador (Integraciones)	O365/SharePoint/BCP/Playbooks/PR-CRM-01_v1.docx
2026-01-16	Plantillas manuales	Se consolidaron plantillas de operación manual (pedidos/despacho) y control de backlog.	Asegurar operación esencial sin CRM/internet.	Líder de ventas	O365/SharePoint/BCP/Plantillas/operacion_manual_v1.xlsx
2026-02-20	BIA (RTO/RPO)	Se revisaron RTO/RPO del ERP/BD tras ejercicio de mesa; ajustes puntuales.	Alinear tiempos objetivo con capacidad real de restauración.	Coordinador BCP	O365/SharePoint/BCP/BIA/ajustes_RTO_RPO_2026-02-20.docx

Figura 42.
Registro de comunicaciones de hitos a gerencia (paso 7).

4) Hitos comunicados a gerencia

Fecha	Hito	Impacto (disponibilidad)	Comunicado por	Canal	Confirmación/Respuesta
2025-12-18	Inicio del proyecto BCP y aprobación del alcance (enfoque disponibilidad por ciberincidentes).	Define priorización y límites del plan.	Coordinador BCP	Reunión + correo	Aprobado por Gerencia
2025-12-20	Matriz de contactos y escalamiento completada (incluye ISP/CRM y emergencias).	Reduce tiempo de reacción ante interrupciones.	Coordinador BCP	Correo	Recibido y validado
2025-12-23	Runbooks iniciales PR-ERP-01 y PR-CRM-01 listos y socializados.	Mejora capacidad de respuesta y recuperación.	Coordinador BCP	Reunión + Teams	Aprobado para uso operativo
2026-01-24	Checklist de recuperación de red y backups de configuración (Meraki/Switch) definidos.	Reduce indisponibilidad por fallas de red interna.	Ingeniero de sistemas	Correo	Recibido
2026-02-20	Ajustes al BIA (RTO/RPO) posteriores a simulacro de ransomware.	Mejora realismo del plan y su aplicabilidad.	Coordinador BCP	Correo	Aprobado

En la figura 43 se observa la ejecución del paso 8, el cual estaba dedicado a emitir las capacitaciones de continuidad al resto de la compañía del caso de estudio con datos simulados, este enfoque permitió plantear la perspectiva requerida de cultura, la cual es fundamental para la adopción general de los BCP al interior de la organización. Luego, de acuerdo con el paso 9, en la figura 44 se evidencian los registros de planeación y resultados de ejecución simulados de las pruebas requeridas dentro del plan de continuidad de negocio, y, finalmente en las figuras 45 y 46 se evidencian los registros también simulados de seguimiento a los incidentes, bien sea por ciberseguridad o interrupción, los cuales propician hallazgos y planes de acción, es decir, la mejora continua del BCP.

Figura 43.

Registro de capacitaciones en BCP.

Estrategia de BCP para MiPymes con el modelo de racionalidad limitada

Paso 8: Capacitación y concienciación general en continuidad

Empresa:	Semifacturados e Importaciones S.A.S	Versión:	1.0	Fecha:	2026-01-05

Objetivo del paso

Capacitar transversalmente a toda la compañía para que el BCP pueda ser mantenido de acuerdo con el alcance esperado.

Tipo (Equipo BCP / General / Por r	Área / Rol	Tema	Duración (mi	Responsable	Fecha	Lugar/Canal	Asistentes (cantid	Evidencia (ruta/URL)	Notas
Equipo BCP	Equipo BCP	Repaso del alcance del BCP y criterios de activación (disparadores por disponibilidad).	60	Coordinador BCP	2025-12-19	Sala juntas / Teams	9	O365/SharePoint/BCP/Evidencias/Capacitaciones/2025-12-19_lista.pdf	Enfoque: decisiones rápidas y evidencias mínimas.
Por rol	Ventas	Operación manual ante caída de CRM/internet: captura de pedidos y control de backlog.	45	Líder de ventas	2025-12-27	Sala ventas	10	O365/SharePoint/BCP/Evidencias/Capacitaciones/2025-12-27_lista.pdf	Incluye conciliación posterior con ERP.
Por rol	Producción / Planta	Operación manual ante caída de SEIM: registro mínimo de órdenes y trazabilidad básica.	45	Ingeniero de producción	2025-12-30	Planta	12	O365/SharePoint/BCP/Evidencias/Capacitaciones/2025-12-30_lista.pdf	Registrar punto de corte y responsables.
Por rol	TI / Soporte	Uso de playbooks PR-ERP-01, PR-VMS-01 y PR-VIRT-HOST-01 (restauración por fases).	90	Ingeniero de sistemas	2026-01-07	Sala TI	6	O365/SharePoint/BCP/Evidencias/Capacitaciones/2026-01-07_lista.pdf	Se revisa orden de arranque y validación mínima.
General	Administración	Qué hacer ante indisponibilidad: canales oficiales, comunicación y continuidad esencial.	30	Coordinador BCP	2026-01-10	Teams	25	O365/SharePoint/BCP/Evidencias/Capacitaciones/2026-01-10_lista.pdf	No técnico: foco en operación y reporte oportuno.
Por rol	Desarrollo / Integraciones	Rollback de integraciones y control de versiones (PR-INTEG-01).	60	Desarrollador (Integraciones)	2026-01-15	Teams	3	O365/SharePoint/BCP/Evidencias/Capacitaciones/2026-01-15_lista.pdf	Regla: pausar primero, conciliar después.
General	Toda la compañía	Concienciación: ransomware y buenas prácticas básicas (no abrir adjuntos sospechosos, reporte rápido).	30	Coordinador BCP	2026-01-20	Teams	45	O365/SharePoint/BCP/Evidencias/Capacitaciones/2026-01-20_lista.pdf	Alineado a disponibilidad: evitar interrupciones por ciber.
Equipo BCP	Equipo BCP	Cierre del ciclo: revisión de lecciones, actualización de contactos y preparación de simulacros.	45	Coordinador BCP	2026-02-05	Sala juntas	9	O365/SharePoint/BCP/Evidencias/Capacitaciones/2026-02-05_lista.pdf	Preparación para Paso 9 (pruebas).

Figura 44.

Planificación y ejecución de simulacros.

Estrategia de BCP para MiPymes con el modelo de racionalidad limitada

Paso 9: Pruebas y simulacros del plan

Empresa:	Semifacturados e Importaciones S.A.S	**Versión:**	1.0	**Fecha:**	2026-01-05

Objetivo del paso

Ejecutar acciones que permitan simular una pérdida de continuidad para prevenir puntos de fallo del proceso ante un evento real.

Actividad	Tipo	Frecuencia	Fecha planificada	Responsable	Estado	Resultado/Notas	Fecha actu
Ejercicio de mesa: ransomware ERP/BD (activación BCP-011 + PR-ERP-01).	Prueba de escritorio	Semestral	2026-02-14	Coordinador BCP	Ejecutado	Se identificó brecha en segregación de backups y tiempos de escalamiento; se ajustó BIA (RTO/RPO).	2026-02-20
Simulacro operativo: caída de internet (CRM SaaS no accesible) BCP-047 + PR-INTERNET-01.	Simulación	Semestral	2026-03-06	Ingeniero de sistemas	Ejecutado	Operación manual activada; se mejoró guion de comunicación y escalamiento a ISP/CRM.	2026-03-10
Prueba técnica: restauración controlada de ERP/BD desde backup (sin afectar producción).	Prueba técnica	Trimestral	2026-04-10	Experto infraestructura (outsourcing)	Planificado	Restaurar a entorno controlado; validar transacción y tiempos reales.	
Simulacro: caída de SEIM (operación manual de órdenes) BCP-008 + PR-SEIM-01.	Simulación	Anual	2026-05-15	Ingeniero de producción	Planificado	Se validará captura mínima y conciliación posterior.	
Prueba: rollback de integraciones (contenedores) PR-INTEG-01.	Prueba técnica	Semestral	2026-06-12	Desarrollador (Integraciones)	Planificado	Validar pausa/reactivación por fases y control de duplicados.	
Prueba: recuperación red interna (backup config Meraki/Switch + PR-NET-01).	Prueba técnica	Semestral	2026-07-18	Experto infraestructura (outsourcing)	Planificado	Cargar backup config en ventana controlada y validar conectividad priorizada.	
Ejercicio de comunicación: mensaje estándar a usuarios + gerencia ante indisponibilidad.	Ejercicio	Trimestral	2026-02-28	Coordinador BCP	Planificado	Ensayar comunicados breves y registro de evidencias.	
Revisión de escritorio (walkthrough): catálogo BCP y matriz de contactos (vigencia).	Revisión	Trimestral	2026-01-31	Coordinador BCP	Ejecutado	Se actualizó proveedor/horarios y se validaron canales alternos.	2026-02-01

Figura 45.

Registro de incidentes para mejora continua (paso 10).

Estrategia de BCP para MiPymes con el modelo de racionalidad limitada

Paso 10: Mejora continua

Empresa:	Semifacturados e Import	Versión:	1.0	Fecha:	2026-01-05

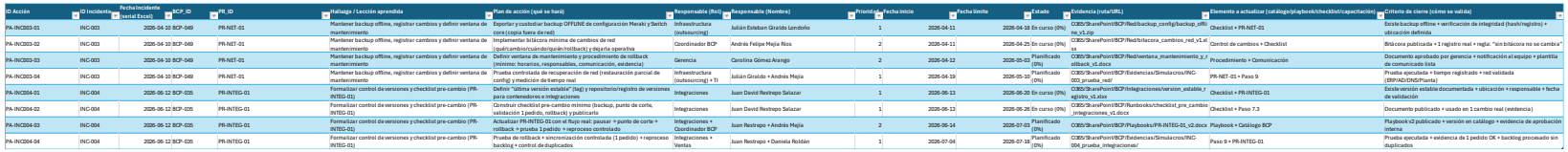
Objetivo del paso

Aplicar las medidas necesarias que garanticen evolucionar, mantener o corregir el BCP.

Incidente_ID	Fecha	Hora de	ID_BCP	Descripción	Acciones tomadas (resumen)	Hora recup	Duraci	Impactos	Lecciones aprendidas	Cerrado (SI/NO)
INC-003	2026-04-10	8:15	BCP-049	Simulación de indisponibilidad de red interna (Meraki/Switch)	Aplicación de checklist PR-NET-01; carga de backup config; validación por prioridades (servidores→usuarios→planta); comunicación	9:45	1.5	Paro parcial de accesos a ERP/archivos; impacto en planta por estaciones	Mantener backup offline, registrar cambios y definir ventana de mantenimiento	SI
INC-004	2026-06-12	11:00	BCP-035	Simulación de falla en integraciones CRM↔ERP (contenedores)	Pausa de integraciones; punto de corte; rollback a versión estable; prueba controlada 1 pedido; reproceso y conciliación	12:30	1.5	Retraso en reflejo de pedidos; necesidad de conciliación manual	Formalizar control de versiones y checklist pre-cambio (PR-INTEG-01)	SI

Figura 46.

Registro de seguimiento planes de acción (paso 10).



ID Acción	ID Incidente	Fecha Incidente (serial Excel)	BCP_ID	PR_ID	Hallazgo / Lección aprendida	Plan de acción (qué se hará)	Responsable (Rol)	Responsable (Nombre)	Prioridad	Fecha inicio	Fecha límite	Estado	Evidencia (ruta/URL)	Elemento a actualizar (catálogo/playbook/checklist/capacitación)	Criterio de cierre (cómo se valida)
PA-INC003-01	INC-003	2026-04-10	BCP-049	PR-NET-01	Mantener backup offline, registrar cambios y definir ventana de mantenimiento	Exportar y custodiar backup OFFLINE de configuración Meraki y Switch core (copia fuera de red)	Infraestructura (outsourcing)	Julián Esteban Giraldo Londoño	1	2026-04-11	2026-04-18	En curso (0%)	O365/SharePoint/BCP/Red/backup_config/backup_offline_v1.zip	Checklist + PR-NET-01	Existe backup offline + verificación de integridad (hash/registro) + ubicación definida
PA-INC003-02	INC-003	2026-04-10	BCP-049	PR-NET-01	Mantener backup offline, registrar cambios y definir ventana de mantenimiento	Implementar bitácora mínima de cambios de red (qué/cambio/cuándo/quién/rollback) y dejarla operativa	Coordinador BCP	Andrés Felipe Mejía Ríos	2	2026-04-11	2026-04-25	En curso (0%)	O365/SharePoint/BCP/Red/bitacora_cambios_red_v1.xlsx	Control de cambios + Checklist	Bitácora publicada + 1 registro real + regla: "sin bitácora no se cambia"
PA-INC003-03	INC-003	2026-04-10	BCP-049	PR-NET-01	Mantener backup offline, registrar cambios y definir ventana de mantenimiento	Definir ventana de mantenimiento y procedimiento de rollback (mínimo: horarios, responsables, comunicación, evidencia)	Gerencia	Carolina Gómez Arango	2	2026-04-12	2026-05-03	Planificado (0%)	O365/SharePoint/BCP/Red/ventana_mantenimiento_y_rollback_v1.docx	Procedimiento + Comunicación	Documento aprobado por gerencia + notificación al equipo + plantilla de comunicado lista
PA-INC003-04	INC-003	2026-04-10	BCP-049	PR-NET-01	Mantener backup offline, registrar cambios y definir ventana de mantenimiento	Prueba controlada de recuperación de red (restauración parcial de config) y medición de tiempo real	Infraestructura (outsourcing) + TI	Julián Giraldo + Andrés Mejía	1	2026-04-19	2026-05-10	Planificado (0%)	O365/SharePoint/BCP/Evidencias/Simulacros/INC-003_prueba_red/	PR-NET-01 + Paso 9	Prueba ejecutada + tiempo registrado + red validada (ERP/AD/DNS/Planta)
PA-INC004-01	INC-004	2026-06-12	BCP-035	PR-INTEG-01	Formalizar control de versiones y checklist pre-cambio (PR-INTEG-01)	Definir "última versión estable" (tag) y repositorio/registro de versiones para contenedores e integraciones	Integraciones	Juan David Restrepo Salazar	1	2026-06-13	2026-06-20	En curso (0%)	O365/SharePoint/BCP/Integraciones/version_estable_registro_v1.xlsx	Checklist + PR-INTEG-01	Existe versión estable documentada + ubicación + responsable + fecha de validación
PA-INC004-02	INC-004	2026-06-12	BCP-035	PR-INTEG-01	Formalizar control de versiones y checklist pre-cambio (PR-INTEG-01)	Construir checklist pre-cambio mínimo (backup, punto de corte, validación 1 pedido, rollback) y publicarlo	Integraciones	Juan David Restrepo Salazar	1	2026-06-13	2026-06-26	En curso (0%)	O365/SharePoint/BCP/Runbooks/checklist_pre_cambio_integraciones_v1.docx	Checklist + Paso 7.3	Documento publicado + usado en 1 cambio real (evidencia)
PA-INC004-03	INC-004	2026-06-12	BCP-035	PR-INTEG-01	Formalizar control de versiones y checklist pre-cambio (PR-INTEG-01)	Actualizar PR-INTEG-01 con el flujo real: pausar + punto de corte + rollback + prueba 1 pedido + reproceso controlado	Integraciones + Coordinador BCP	Juan Restrepo + Andrés Mejía	2	2026-06-14	2026-07-03	Planificado (0%)	O365/SharePoint/BCP/Playbooks/PR-INTEG-01_v2.docx	Playbook + Catálogo BCP	Playbook v2 publicado + versión en catálogo + evidencia de aprobación interna
PA-INC004-04	INC-004	2026-06-12	BCP-035	PR-INTEG-01	Formalizar control de versiones y checklist pre-cambio (PR-INTEG-01)	Prueba de rollback + sincronización controlada (1 pedido) + reproceso backlog + control de duplicados	Integraciones + Ventas	Juan Restrepo + Daniela Roldán	1	2026-07-04	2026-07-18	Planificado (0%)	O365/SharePoint/BCP/Evidencias/Simulacros/INC-004_prueba_integraciones/	Paso 9 + PR-INTEG-01	Prueba ejecutada + evidencia de 1 pedido OK + backlog procesado sin duplicados

Por último, se repite nuevamente la valoración realizada por medio del checklist propuesto en la estrategia (tabla 14), y se usa la guía de uso de resultados (figura 47) para la interpretación, obteniendo ocho de nueve puntos posibles (8/9), indicando que se cuenta con un BCP sólido para el tamaño y alcance definido dentro del caso de estudio. Cuantitativamente también podría expresarse el resultado como un 88.9% de cobertura de los parámetros evaluación clave propuestos dentro de la estrategia para implementación del BCP, que comparado contra el 0% proveniente de los cero puntos de nueve posibles (0/9) obtenidos en la valoración inicial.

El resultado obtenido permitió probar la adaptabilidad de la estrategia dentro de un modelo de negocio similar al de algunas MiPymes del sector manufacturero, esto a su vez quiere decir, que se contemplaron conocimientos, recursos e infraestructuras reducidas, además de escenarios de riesgos de ciberseguridad que pudieran conllevar a perdida o degradación de la disponibilidad, y, a partir de allí, identificar puntos de ajuste en los cuales la estrategia propuesta pudiere ser mejorada. En consecuencia, los resultados obtenidos permitieron sustentar el cumplimiento del alcance definido para el trabajo y, adicionalmente, formular recomendaciones para investigaciones futuras que amplíen el análisis hacia escenarios, variables o enfoques no contemplados en el alcance de este estudio.

Tabla 14.
Checklist validación BCP.

Aspecto clave a verificar	**¿Cumplido? (Sí/No)**
La gerencia ha expresado su apoyo formal al BCP y existe un responsable asignado.	Sí
El alcance está definido: se conocen y documentan los procesos críticos y sus requerimientos.	Sí
La empresa cuenta con una lista actualizada de riesgos prioritarios (incluyendo ciberamenazas).	Sí
Los respaldos de datos críticos se realizan con frecuencia y **se ha probado su restauración**.	Sí
Existen redundancias básicas (equipo de respaldo, segundo enlace de Internet, proveedores alternos).	No
El BCP está escrito, vigente y accesible para quienes lo necesitan.	Sí
El personal ha recibido capacitación sobre su rol en el BCP.	Sí
Se ha realizado al menos una prueba o simulacro durante los últimos 12 meses.	Sí
El plan se revisa y actualiza periódicamente (contactos, cambios en procesos, nueva infraestructura, etc.).	Sí
Cumplimiento	(8/9) – 88.9%

Figura 47.
Parámetros de evaluación del BCP.

Cómo usar los resultados

- Si la empresa cumple 8 o 9 puntos, tiene un BCP sólido para su tamaño.
- Si cumple 5 a 7 puntos, el BCP es funcional, pero necesita mejoras.
- Si cumple menos de 5, la continuidad está en riesgo y conviene reforzar áreas prioritarias.

3. Conclusiones y recomendaciones

3.1 Conclusiones

3.1.1 Conclusiones de la fase 1.

Aunque este trabajo centró el esfuerzo inicialmente en la exploración de riesgos asociados al sector manufacturero, industrial y más precisamente en búsqueda de aquellos que afectan directamente a las MiPymes, se pudo identificar que la realidad que abordan los riesgos no es una cuestión sectorial ni de tamaños, es decir, que aunque en efecto se logró el relacionamiento de los riesgos al sector en estudio dadas las particularidades mismas en la ejecución del negocio al que se dedican, esto no representa una diferencia muy significativa en el uso de los activos en contextos tecnológicos, estando la desviación más clara en entornos de TO, por lo tanto, los activos entre sectores pueden ser similares, al igual que las vulnerabilidades y amenazas en función de la disponibilidad.

En consecuencia, con la revisión de los riesgos y el posterior análisis de los casos que fueron perpetrados históricamente en las compañías se logra comprender que la verdadera diferencia entre cada compañía radica en cómo se interiorizan y gestionan los riesgos a los que se está expuesto. Ninguna organización está exenta de enfrentar eventos disruptivos, lo cual invita a un cambio de enfoque: la discusión no debería centrarse en si un incidente ocurrirá, sino en cuándo podría ocurrir y qué tan preparada se encuentra la organización para responder y recuperarse, y en esencia, esa no es una cuestión que esté relacionada ni al tamaño ni al sector, por lo tanto, también las MiPymes deben preocuparse por integrar metodologías que les permita conocer y gestionar sus riesgos para posteriormente instaurar controles de acuerdo con sus capacidades mismas. Por tanto, la gestión de riesgos y la instauración de controles es una cuestión estrategia corporativa necesaria para la supervivencia misma.

3.1.2 Conclusiones de la fase 2.

A partir de la exploración de estándares y guías de buenas prácticas, se concluyó que existen múltiples tipos de estrategias orientadas a preservar la continuidad del negocio. En consecuencia, cada organización enfrenta el reto de seleccionarlas y adaptarlas de acuerdo con sus características, capacidades y contexto de operación. En este sentido, la continuidad no se sustenta en recetas universales, sino más bien en metodologías que permiten prepararse de manera sistemática frente a interrupciones. Por ello, un enfoque que integre la comprensión de los riesgos a los que se está expuesto y los conecte con estrategias de continuidad facilita la priorización de

acciones, reduce el riesgo de impacto y disminuye los esfuerzos de adopción, al tiempo que aprovecha el uso de los recursos disponibles.

Asimismo, aunque la interpretación de los estándares puede ser un ejercicio dispendioso, su valor análisis permite la definición de la columna vertebral del proceso, aportando rigor metodológico y favoreciendo su sostenibilidad en el tiempo, así como la evolución gradual de las capacidades organizacionales. Ahora bien, descartar del análisis a las guías de buenas prácticas no significa que no sean importantes; por el contrario, puede complementar la base normativa al traducirla en acciones concretas orientadas a reducir el impacto y fortalecer la capacidad de respuesta y recuperación ante eventos de interrupción. De esta manera, las estrategias definidas pueden implementarse, someterse a prueba y ajustarse progresivamente mediante ciclos iterativos de mejora continua.

3.1.3 Conclusiones de la fase 3.

Al abordar el reto de construir una estrategia que permitiera a las MiPymes adoptar una implementación de BCP, era muy tentador crear otra guía de buenas prácticas, llevando acciones específicas para casos particulares, no obstante, de acuerdo con la exploración realizada en las fases anteriores se clarificó el camino de la estrategia, permitiendo concluir que la mejor manera de integrar en un mismo espacio toda la sustancia de un estándar con la adopción de buenas prácticas, sin caer en un espacio ampliamente explorado y documentado, era apalancar por medio de la explicación los conceptos clave de racionalidad limitada dentro de la narrativa de la estrategia, y, por medio de ejemplos, abordar en cada paso cómo usar esta teoría para que por sí misma, cada organización pueda encontrar su propio modo de implementación a su vez que evoluciona gracias al ciclo PHVA.

Entonces, de forma estratégica el documento guía las acciones al mismo tiempo que invita implícitamente a la organización a pensar en sus casos particulares, sin embargo, para tener éxito en la implementación, es importante que se sigan los pasos sin omisión alguna, dado que el diseño está pensado en que cada paso complemente de algún modo al paso siguiente, y que en cada iteración dentro del ciclo de mejora continua se vaya se va ajustando y mejorando. Para exponer este trasfondo sin poner en riesgo el resultado, se optó por incluir también propuesta de un modelo en Excel que clarificara como podría abordarse una implementación de BCP.

3.1.4 Conclusiones de la fase 4.

En la fase de validación de la estrategia fue necesario volver a la construcción original e incluir un checklist con elementos calificables que permitiera a partir del resultado de la implementación concluir si se cubrían parámetros para definir la cobertura de un BCP dentro del alcance definido por la organización, además fue de gran ayuda usar un instrumento en Excel que dinamizara la ejecución para poder conectar los pasos, por ello, se optó también por incluir en los anexos una

guía que permita a las MiPymes interesadas replicar al menos de forma parcial el instrumento propuesto.

La prueba de escritorio realizada a partir del diseño del caso de estudio permitió probar y concluir que, si se sigue la estrategia de implementación propuesta, se podrá disponer de un BCP perfectamente funcional que además se ajusta al alcance y necesidades de cada organización, hito logrado gracias al uso del modelo de racionalidad limitada. Además, este ejercicio permitió ahondar en la ejecución para comprender las dificultades en materia de implementación a las que pueden enfrentarse las organizaciones del sector, dando paso a nuevos retos que pueden ser abordado en trabajos futuros.

También es importante concluir que los resultados obtenidos sugieren que incluso en compañías con recursos limitados tanto en conocimiento especializado, talento humano, y capacidad financiera, es posible lograr aproximaciones viables y sostenibles a estándares sólidos y robustos, que, si bien en este trabajo se fundamentó en ISO 22301, un enfoque de racionalidad limitada podría permitir hacer ajustes que lleven a las organizaciones a tener resultados positivos en el estándar o guía de buenas prácticas de su elección con priorización y ajustes incrementales. Finalmente, se deberá considerar que el éxito de implementaciones bajo el modelo de racionalidad limitada, deberá contar con una base de información de buena calidad que permitan una buena toma de decisiones, porque si bien, no se espera algo óptimo, si se desea llegar un resultado satisfactorio, y esto solo es alcanzable si se parte de una base de información filtrada producto de la experiencia o conocimiento previo, es decir, que la incorporación de información de muy baja calidad podría desviar la priorización de esfuerzos y con ello, comprometer la efectividad y sostenibilidad en procesos de implementación.

3.2 Recomendaciones.

La ejecución del proceso de exploración, diseño y validación de la estrategia da pie a la emisión de recomendaciones sólidas orientadas a la implementación del BCP en MiPymes. En particular, los hallazgos que han sido obtenidos permiten pasar de una aproximación conceptual a una lectura más práctica sobre qué decisiones priorizar cuando existen limitaciones de tiempo, presupuesto, personal o incluso madurez organizacional. Estas recomendaciones se plantean como una guía para mejorar la sostenibilidad del BCP en el tiempo, facilitando su prueba, ajuste y maduración progresiva.

Existe una gran relevancia para las MiPymes en que las definiciones del RTO dentro del BIA sean producto de la concertación directa con la gerencia y las direcciones, permitiendo adaptar rápidamente los tiempos, este es un proceso que en sí mismo tiene una profundidad que podría dilatar ampliamente la implementación del BCP, no obstante, la manera de abordarlo deberá ser en inicio más simple y se deberá ir ajustando y profundizando en la medida en que se madure. Asimismo, desde la perspectiva de racionalidad limitada se trabaja con el conocimiento disponible

al momento de la implementación, sin embargo, es importante que mediante cada iteración también se pueda ahondar y capacitar en las metodologías de riesgos, permitiendo afianzar el conocimiento, reduciendo el sesgo cognitivo y agilizando el proceso de valoración de riesgos. Tanto el BIA como la valoración de riesgos son fundamentales para acotar el alcance del BCP, con una definición de los procesos críticos y la interacción entre los activos asociados a esos procesos se podrán posteriormente definir los riesgos específicos.

Hay que tener en cuenta que incluso en un alcance muy pequeño podrían generarse múltiples escenarios de riesgo que pudiera ser necesario controlar, no obstante, también se podrán unificar las estrategias de continuidad por tipos de activos, haciendo generales los playbooks y madurándolos progresivamente hacia runbooks más específicos. Simplificar, probar y posteriormente iterar, permitirá ir madurando las estrategias de continuidad sin fracasar en el intento. Incluso aunque se produzca alguna subjetividad durante el proceso de implementación, las iteraciones apalancadas por el ciclo PHVA permitirán ir mejorando las definiciones y la respuesta ante interrupciones.

3.3 Trabajos futuros.

En trabajos futuros podría profundizarse en las siguientes temáticas identificadas alrededor de este trabajo:

Desarrollar un software de bajo costo que permita aprovechar el diseño de la estrategia de implementación de BCP con el modelo de racionalidad limitada, reduciendo el esfuerzo en definiciones para procesos BIA, la estimación de riesgos de sistemas asociados a los procesos críticos, el mantenimiento y evolución de los playbooks y el seguimiento a los planes de acción que se produzcan dentro del proceso iterativo. Además, también dentro de este alcance se pudieran aprovechar los registros de hallazgos y planes de acción para correlacionar eventos e identificar brechas de ciberseguridad que quizá no sería fácil de identificar por métodos visuales o que requerirían de conocimiento y esfuerzos adicionales que quizá no está disponible al interior de las MiPymes.

Por último, desarrollar un modelo que permita a partir de la racionalidad limitada y parámetros clave, definir los tiempos de MTPD, RPO y RTO para las MiPymes. Este enfoque no solo facilitaría la definición del BIA de forma más transparente, sino que también impactaría directamente en la definición de estrategias de continuidad en las cuales se deben ajustar los tiempos de respuesta incluidos en los playbooks y runbooks.

Anexos

Anexo A. Ampliación tabla de amenazas + MITRE ATT&CK (fase 1).

Familia	Variante	Descripción	Ejemplos	MITRE ATT&CK (Táctica → Técnica [ID])	PRESENCIA EN TI	PRESENCIA EN TO
Malware	Ransomware	Ataque malicioso en el cual los atacantes cifran datos e información de una compañía y con ello solicitan el pago de una cifra económica generalmente en criptomonedas para restaurar el acceso. En algunos casos, el atacante suele no solo cifrar sino también robar la información exigiendo un pago adicional a cambio de no revelar la información a las autoridades, competidores comerciales o incluso al público en general [44].	**LockBit, BlackCat**	Impact → Data Encrypted for Impact (T1486); Impact → Inhibit System Recovery (T1490); opcional Defense Evasion → Impair Defenses (T1562/.001/.006).	X	X
Malware	Downloader/ Dropper	Tipo de archivo ejecutable que está diseñado para introducir malware en el sistema donde se ejecuta. En algunos casos el código malicioso puede estar integrado en el propio archivo, pero lo más habitual es que actúe como un instalador que descarga el malware desde servidores remotos a través de Internet [9].	**Emotet** como loader de TrickBot/IcedID, **SmokeLoader/Dofoil** (carga payloads adicionales)	Execution → User Execution (T1204.001/.002); Command & Control → Ingress Tool Transfer (T1105).	X	X
Malware	Logic bomb	Fragmento de código malicioso que está oculto dentro de un programa legítimo. Permanece inactivo hasta que se cumple una o varias condiciones específicas definidas en su lógica y una	**UBS PaineWebber 2002, Fannie Mae 2008–2009** – intento de "time/logic	Impact → Data Destruction (T1485) (borrado/alteración programada);	X	X

		vez activado, ejecuta una acción dañina. A diferencia de los virus, su ejecución no se da de forma inmediata, sino que depende de eventos específicos como por ejemplo una cantidad determinada de reinicios del sistema o el paso de cierto tiempo desde su instalación [9].	bomb" descubierto antes de activarse.	complementa con Impact → Inhibit System Recovery (T1490) si deshabilita recuperación.		
Malware	Rootkit	Herramientas o "kit" de programas electrónicos que permiten a un atacante tener acceso al root del sistema, esta amenaza es común que se mantenga indetectable dado que están diseñados para ocultarse del sistema, ocultando código, rutas y archivos, no obstante, muchos programas de carácter legal incluyen esta característica para garantizar el acceso al soporte remoto, por lo que, puede existir algunos casos en los que son cubiertos por la normativa de un estado [45].	**LoJax (UEFI)** – primer rootkit UEFI "in-the-wild", atribuido a Sednit, **MoonBounce (UEFI)** – implant persistente en SPI flash.	Defense Evasion → Rootkit (T1014); en casos de UEFI/firmware, Persistence/Priv. Esc. → Pre-OS Boot: System Firmware (T1542.001) (ejemplos de UEFI rootkit).	X	X
Malware	RAT (Remote Access Trojan)	Es una herramienta o programa de administración remota que permite controlar un sistema a través de una red. los atacantes utilizan RATs para tomar el control de equipos afectados sin el conocimiento ni consentimiento del usuario, esto es generalmente a través de una puerta trasera (backdoor) [9].	**PlugX/Korplug** – RAT modular usado por múltiples APTs, **njRAT/Bladabindi** – RAT observado desde 2012.	Command & Control → Remote Access Tools (T1219) (y sub-téc. .002 software de escritorio); C2 → Application Layer Protocol (T1071/.001/.003); Exfiltration → Exfiltration over C2 Channel (T1041).	X	X

Malware	Malvertising	Es una técnica maliciosa que consiste en la utilización de anuncios digitales aparentemente legítimos como vehículo para distribuir malware o redirigir al usuario a sitios web maliciosos, en esencia es una variación de Adware, es decir, a menudo se presenta en versiones gratuitas de aplicaciones o sitios web que integran publicidad como modelo de financiación. Aunque en sus formas menos agresivas puede limitarse a mostrar anuncios intrusivos, en los casos más críticos se emplea para ejecutar código malicioso sin intervención directa del usuario, comprometiendo la seguridad del dispositivo [9], [46].	**Campañas Zloader vía malvertising, BATLOADER/FakeBat vía anuncios maliciosos.**	Initial Access → Drive-by Compromise (T1189); (lado del actor) Resource Development → Acquire Infrastructure: Malvertising (T1583.008).	X	
Ingeniería social / Compromiso de credenciales	SIM-swapping	El SIM swapping o en español suplantación de tarjeta SIM, es un ataque de ingeniería social en el cual un delincuente suplanta a la víctima ante el operador de telefonía móvil, y para lograrlo es común que se indique al operador sobre la pérdida o daño del equipo móvil, de este modo se solicita que se le active un duplicado de SIM, logrando transferir el número de teléfono de la víctima hacia una tarjeta SIM en poder del atacante. Finalmente, el atacante se apropia de la línea telefónica de la víctima, y con ello, recibirá sus llamadas, mensajes de texto y podrá hacer uso de las aplicaciones que	**LAPSUS$** empleó SIM-swapping para comprometer cuentas, **Caso Jack Dorsey (Twitter, 2019)** – secuestro de línea por SIM swap.	Mobile ATT&CK → SIM Card Swap (T1451); normalmente habilita abuso de Valid Accounts (T1078/.004) en servicios que usan SMS/MFA.	X	

		usan el número celular como método de verificación de identidad, esto incluye los códigos de doble factor de autenticación, de este modo, el atacante podrá tener acceso a múltiples sitios e incluso cambiar las contraseñas de seguridad. Este tipo de ataques representa una gran amenaza para los métodos de verificación asociados al número telefónico [47].				
Denegación de servicio	DoS/DDoS	es un intento de interrumpir, bloquear o negar el flujo de información de un servicio, red o servidor mediante la creación de tráfico ilegitimo o malicioso que culmina en lentitud, falta de respuesta y/o no acceso para los usuarios finales, generalmente este tipo de ataques está dirigido a servicios críticos, suelen causar daños financieros, paralizar la operación en sitios web y afectar la reputación significativamente [34], [48].	**Mirai botnet** – IoT botnet usada para mega-DDoS, **Mēris** – picos récord de HTTP RPS usando pipelining.	Impact → Network Denial of Service (T1498) y sub-téc.: Direct Network Flood (T1498.001), Reflection/Amplification (T1498.002).	X	X
Denegación de servicio	Botnet	Las botnets son redes de dispositivos que han sido comprometidos, y que son usados de forma organizada, programada y autónoma para tareas de origen malicioso, algunas de las actividades comunes atraviesan desde la generación de tráfico en masa hasta la distribución de malware. El factor clave de este riesgo está asociado a las técnicas de comando y control que permite hacer manipulación de las actividades de los activos o recursos comprometidos haciendo participes a las	**Emotet botnet** (tras su reactivación, distribución masiva), **TrickBot botnet** (ecosistema de crimeware).	Resource Development → Acquire Infrastructure (T1583) (p. ej., Domains – T1583.001, VPS/Servers – T1583.003/.004, Botnet – T1583.005); ya en operación, C2 →	X	X

		víctimas de ataques masificados generalmente en contra de terceros [49].		Application Layer Protocol (T1071).		
Ataques a aplicaciones web	SQL Injection	Ataque que consiste en insertar una sentencia de SQL en alguno de los métodos de entrada de datos a la aplicación a través del cliente, su finalidad es exponer, alterar o borrar información relevante de la base de datos, sin embargo, su alcance puede llegar a afectar completamente el motor de la base de datos e incluso podría llegar al sistema operativo [50].	**TalkTalk (UK, 2015)** – brecha por SQLi (sanción ICO), **Yahoo Voices (2012)** – exfiltración vía SQLi (reportes).	Initial Access → Exploit Public-Facing Application (T1190) (expresamente incluye SQLi contra apps/bases expuestas).	X	
Ataques a aplicaciones web	Cross-Site Scripting (XSS)	Inyección de scripts maliciosos en sitios web que afecta a usuarios finales [42].	**Gusano "Samy" (MySpace, 2005)** – propagación masiva vía XSS, **TweetDeck (2014)** – XSS permitió ejecución automática de RTs.	Initial Access → Drive-by Compromise (T1189) (ejecución en cliente vía sitio comprometido); puede combinarse con Execution → User Execution: Malicious Link (T1204.001).	X	
Amenaza interna (Insider)	Empleado/contratista malicioso	Se llama insider a una persona, bien sea empleado, exempleado o proveedor que tiene o tuvo acceso a la información de la compañía y que utiliza este privilegio de manera indebida, y de este modo	**Tesla 2020 – intento de soborno para introducir ransomware**, frustrado al	Defense Evasion/Persistence/Initial Access/Priv. Esc. → Valid Accounts	X	X

		pone en riesgo la seguridad de la organización [51], [52].	denunciar el empleado (caso DOJ/FBI).	(T1078/.001/.002/.003 /.004); (según caso) Account Manipulation (T1098).		
Minería ilícita	Criptojacking	Es un ataque en el cual un atacante hace uso de forma encubierta de los recursos de cómputo de una víctima para minar criptomonedas sin su consentimiento [53]. Generalmente es ejecutado en segundo plano, esto puede darse, por ejemplo, mediante scripts en páginas web o infecciones en estaciones de trabajo, con ello lograr aprovecharse la potencia de procesamiento ajena. En consecuencia, los dispositivos afectados sufren sobrecarga (alto uso de CPU/GPU) e incluso sobrecalentamiento, y, por lo tanto, degradación del rendimiento.	**TeamTNT** en contenedores/Kubernetes (Hildegard, Black-T). **Kinsing** explotando servicios cloud/containers para minar XMR.	Impact → Resource Hijacking (T1496) (sub-téc.: Compute Hijacking – T1496.001, Bandwidth Hijacking – T1496.002, Cloud Service Hijacking – T1496.004).	X	
Movimiento lateral TI a TO	Propagación hacia IACS	Salto desde TI a **HMI/SCADA/PLC** por **DMZ/segmentación débil** [54].	**TRITON/TRISIS (HatMan)** contra controladores de seguridad Triconex, **INDUSTROYER2** dirigido a subestaciones eléctricas (IEC-104).	ICS – Lateral Movement → Exploitation of Remote Services (T0866) y/o Valid Accounts (T0859); en enterprise perimetral, Lateral Movement → Exploitation of Remote Services (T1210) / Remote		X

				Services (T1021) para cruzar hacia OT.		

Anexo B. Tabla ampliada de sugerencias para reducción de riesgos a partir de buenas prácticas de guías investigadas vs estándar ISO22301:2022.

ID	Riesgo	Clasificación del riesgo	Subcláusula	Interpretación de la sugerencia del estándar	Resumen buena práctica	Buena práctica recomendada	Explicación del efecto de aplicación de la buena práctica
R-001	Suplantación de SIM permite tomar cuentas y con ello se aplican bloqueos de las mismas	Tolerable	8.4.4 – Planes de continuidad del negocio	Planes usables con pasos/recursos/dependencias	Procedimientos de operación/comunicación	Diseño de runbook ante el evento / materialización	Acelera la conmutación y evita desorden
R-002	Cifrado de servidor/app/BD del ERP	Inadmisible	8.3.2 – Identificación y selección de estrategias y soluciones	Estrategias/soluciones alineadas a RTO/RPO	Back up	Backups inmutables 3-2-1 o DRaaS con aislamiento temprano	Asegura puntos limpios y retorno rápido
R-002	Cifrado de servidor/app/BD del ERP	Inadmisible	8.4.4 – Planes de continuidad del negocio	Planes de continuidad operables	Procedimientos de operación/comunicación	Diseño de runbook ante el evento / materialización	Disminuye tiempo fuera de servicio

R-003	Despliegue de minero en hosts del ERP vía API expuesta	Tolerable	8.4.4 – Planes de continuidad del negocio	Estrategias para recuperar funciones	Imagen original/verificar integridad	Reimagen dorada/ verificación de integridad	Recupera rendimiento nominal sin ensayo-error
R-003	Despliegue de minero en hosts del ERP vía API expuesta	Tolerable	8.4.4 – Planes de continuidad del negocio	Planes operativos	Procedimientos de operación/comunicación	Procedimiento de saneo con criterios de aceptación del servicio	Evita limpiezas fallidas que prolongan la caída
R-004	Cifrado masivo en compartidos por permisos excesivos	Inadmisible	8.4.4 – Planes de continuidad del negocio	Estrategias/soluciones de recuperación	Back up	Snapshots inmutables, back up offline, lista de prioridad por dataset	Evita pérdida y restaura primero lo crítico
R-004	Cifrado masivo en compartidos por permisos excesivos	Inadmisible	8.4.4 – Planes de continuidad del negocio	Plan de continuidad	Procedimientos de operación/comunicación	Diseño de runbook ante el evento / materialización	Reduce downtime operativo
R-005	Eliminación/cifrado programado por cuenta privilegiada	Tolerable	8.4.4 – Planes de continuidad del negocio	Estrategias de protección/rollback	back up	Versión conocida firmada	Evita activaciones maliciosas y facilita reversión

R-005	Eliminación/cifrado programado por cuenta privilegiada	Tolerable	8.4.4 – Planes de continuidad del negocio	Plan de continuidad	Procedimientos de operación/comunicación	Diseño de runbook ante el evento / materialización	Vuelta atrás rápida y segura
R-006	Infecciones desde anuncios/tiendas no confiables obligan a aislar equipos	Aceptable	8.4.4 – Planes de continuidad del negocio	Estrategias para mantener operación	Equipos/servicios de respaldo en funciones criticas	Modo degradado (VDI/apps remotas) y listas de bloqueo	Permite seguir trabajando mientras se contiene
R-006	Infecciones desde anuncios/tiendas no confiables obligan a aislar equipos	Aceptable	8.4.4 – Planes de continuidad del negocio	Plan/procedimiento	Procedimientos de operación/comunicación	Playbook de contención y comunicación al usuario	Baja tiempos muertos y propagación
R-007	Brote cifra perfiles locales y desconecta de red	Inadmisible	8.4.4 – Planes de continuidad del negocio	Estrategias de recuperación masiva	Imagen original/verificar integridad	Imágenes maestras y stock crítico para reimagen	Reinstala equipos en horas y corta expansión
R-007	Brote cifra perfiles locales y desconecta de red	Inadmisible	8.4.4 – Planes de continuidad del negocio	Plan operativo	Procedimientos de operación/comunicación	Diseño de runbook ante el evento / materialización	Proceso repetible y rápido

R-008	Tráfico malicioso se propaga sin contención	Inaceptable	8.4.4 – Planes de continuidad del negocio	Estrategias de resiliencia	AntiDDoS	Anti-DDoS, SD-WAN y rutas alternas endureciendo bordes	Preserva conectividad mínima y contiene alcance
R-008	Tráfico malicioso se propaga sin contención	Inaceptable	8.4.4 – Planes de continuidad del negocio	Plan de respuesta	Procedimientos de operación/comunicación	Playbook de mitigación y escalamiento con ISP	Mitiga más rápido y coordinado
R-009	Falla en equipo core provoca reinicios	Inaceptable	8.4.4 – Planes de continuidad del negocio	Estrategias inmediatas	Equipos/servicios de respaldo en funciones criticas	Circuit breaker (rate-limit/cutover) y políticas temporales	Evita colapso total de la red
R-010	Ausencia de rate-limit/mitigación adecuada en gateways	Inaceptable	8.4.4 – Planes de continuidad del negocio	Estrategias de disponibilidad	Equipos/servicios de respaldo en funciones criticas	HA/failover de concentradores y capacidad de teletrabajo alterno	Restituye acceso remoto en el RTO
R-010	Ausencia de rate-limit/mitigación adecuada en gateways	Inaceptable	8.4.4 – Planes de continuidad del negocio	Plan operativo	Procedimientos de operación/comunicación	Diseño de runbook ante el evento / materialización	Minimiza tiempo fuera de servicio

R-011	Explotación de vulnerabilidad conocida del gateway	Inaceptable	8.4.4 – Planes de continuidad del negocio	Plan de reversión	Procedimientos de operación/comunicación	Diseño de runbook ante el evento / materialización	Reversión rápida ante fallo
R-012	Saturación del enlace sin blackholing/filtrado efectivo	Inadmisible	8.4.4 – Planes de continuidad del negocio	Estrategias de conectividad	Equipos/servicios de respaldo en funciones criticas	Multi-ISP/4G/5G + SD-WAN y rutas alternativas	Mantiene salida por rutas alternas
R-012	Saturación del enlace sin blackholing/filtrado efectivo	Inadmisible	8.4.4 – Planes de continuidad del negocio	Plan operable	Procedimientos de operación/comunicación	Diseño de runbook ante el evento / materialización	Conmuta rápido y seguro
R-013	Cambios no autorizados en routing/ACL	Inaceptable	8.4.4 – Planes de continuidad del negocio	Planes/procedimientos de continuidad	Procedimientos de operación/comunicación	Plan de bloqueo y revocación masiva de accesos	Corta acceso indebido y evita escalamiento
R-013	Cambios no autorizados en routing/ACL	Inaceptable	8.4.4 – Planes de continuidad del negocio	Estrategias de segregación	Segmentación de roles	Reglas de segmentación/whitelisting por procesos críticos	Limita el alcance del daño

R-014	Flood HTTP sin WAF/limitación adecuada	Tolerable	8.4.4 – Planes de continuidad del negocio	Estrategias/soluciones web	Equipos/servicios de respaldo en funciones criticas	CDN/anti-DDoS/WAF y modo estático	Mantiene front disponible
R-014	Flood HTTP sin WAF/limitación adecuada	Tolerable	8.4.4 – Planes de continuidad del negocio	Plan de cutover	Procedimientos de operación/comunicación	Playbook a estático/edge y reversa	Baja downtime de cara al cliente
R-015	Consultas abusivas bloquean/derriban la BD	Tolerable	8.4.4 – Planes de continuidad del negocio	Plan de contención/restore	Procedimientos de operación/comunicación	Procedimiento de contención y restauración del servicio	Controla la indisponibilidad
R-016	Propagación a hosts/VMs y cifrado de datastores	Inadmisible	8.4.4 – Planes de continuidad del negocio	Estrategias por servicio	Back up	back up inmutables + DRP por servicio	Restores confiables y rápidos
R-016	Propagación a hosts/VMs y cifrado de datastores	Inadmisible	8.4.4 – Planes de continuidad del negocio	Runbooks por servicio	Procedimientos de operación/comunicación	Aislamiento/restore y criterios de retorno	Disminuye indisponibilidad

R-017	Minero consume CPU/IO en hipervisores/VMs	Inaceptable	8.4.4 – Planes de continuidad del negocio	Estrategias de saneo	Imagen original/verificar integridad	Reimage/CM estándar	Recupera desempeño nominal
R-017	Minero consume CPU/IO en hipervisores/VMs	Inaceptable	8.4.4 – Planes de continuidad del negocio	Procedimiento operativo	Procedimientos de operación/comunicación	Checklist de saneo y verificación	Evita recaídas
R-018	Borrado/alteración programada de repositorios de respaldo	Tolerable	8.4.4 – Planes de continuidad del negocio	Estrategias de confianza	Back up	back up offline/WORM y verificación previa a restore	Restore sin reinyectar malware
R-018	Borrado/alteración programada de repositorios de respaldo	Tolerable	8.4.4 – Planes de continuidad del negocio	Plan de verificación/restore	Procedimientos de operación/comunicación	Diseño de runbook ante el evento / materialización	Evita restores contaminados
R-019	Repositorios de copia cifrados por exposiciones de red	Inadmisible	8.4.4 – Planes de continuidad del negocio	Estrategias de respaldo robustas	Back up	Back up 3-2-1 con inmutabilidad y retención adecuada	Asegura puntos sanos

R-020	Acceso desde TI por DMZ débil	Inaceptable	8.4.4 – Planes de continuidad del negocio	Estrategias TO seguras	Segmentación de redes	Zonas/conductos, DMZ/diodo, whitelisting y estado seguro	Aísla y mantiene control seguro
R-021	Autenticación básica/obsoleta permite acceso a PLC	Inaceptable	8.4.4 – Planes de continuidad del negocio	Estrategias de aislamiento/bypass	Aislamiento	Aislamiento/bypass controlado; redundancia	Evita parada total
R-021	Autenticación básica/obsoleta permite acceso a PLC	Inaceptable	8.4.4 – Planes de continuidad del negocio	Procedimiento Operativo Estándar de operación manual	Procedimientos de operación/comunicación	Procedimiento de operación manual temporal	Mantiene producción mínima
R-022	Estaciones HMI cifradas	Inadmisible	8.4.4 – Planes de continuidad del negocio	Estrategias de reinstalación	Imagen original/verificar integridad	Imágenes golden y medios de arranque en campo	Reinstala rápido y retoma control
R-022	Estaciones HMI cifradas	Inadmisible	8.4.4 – Planes de continuidad del negocio	Runbook en sitio	Procedimientos de operación/comunicación	Pasos de reinstalación/validación en planta	Reduce corte de supervisión

R-023	Malware de TI afecta HMIs operativas	Tolerable	8.4.4 – Planes de continuidad del negocio	Procedimiento Operativo Estándar de aislamiento	Procedimientos de operación/comunicación	Procedimiento de aislamiento segmentado (RACI)	Evita expansión
R-024	Tráfico malicioso afecta colectores/servidores SCADA	Inaceptable	8.4.4 – Planes de continuidad del negocio	Procedimiento Operativo Estándar de operación degradada	Procedimientos de operación/comunicación	Procedimiento de operación mínima viable	Mantiene operación
R-025	Cifrado de VMs de supervisión/registro	Inadmisible	8.4.4 – Planes de continuidad del negocio	Estrategias de respaldo/restore	Back up	Backups offline y cadena de confianza	Reconstruye registros críticos
R-025	Cifrado de VMs de supervisión/registro	Inadmisible	8.4.4 – Planes de continuidad del negocio	Plan de reconstrucción	Procedimientos de operación/comunicación	Guía de reconstrucción priorizada de históricos	Normaliza operación
R-026	Toma de control de estaciones de ingeniería	Inaceptable	8.4.4 – Planes de continuidad del negocio	Procedimiento Operativo Estándar de préstamo seguro	Procedimientos de operación/comunicación	Procedimiento de préstamo y retiro controlado	Recupera mantenimiento sin abrir red

R-027	Proyectos cifrados; imposibilidad de compilar/descargar	Inaceptable	8.4.4 – Planes de continuidad del negocio	Estrategias de reposición rápida	Back up	Imágenes maestras y stock de equipos	Reposición en horas
R-027	Proyectos cifrados; imposibilidad de compilar/descargar	Inaceptable	8.4.4 – Planes de continuidad del negocio	Runbook de reimagen	Procedimientos de operación/comunicación	Procedimiento de reimagen y alta	Menos downtime
R-028	Compromiso del gateway deja ruta a TO	Inaceptable	8.4.4 – Planes de continuidad del negocio	Procedimiento Operativo Estándar de aislamiento	Procedimientos de operación/comunicación	Procedimiento de aislamiento del gateway	Mantiene servicios expuestos
R-029	Saturación del gateway por falta de limitación	Inaceptable	8.4.4 – Planes de continuidad del negocio	Estrategias anti-DDoS en borde	AntiDDoS	Scrubbing/anti-DDoS y coordinación con ISP	Filtra tráfico malicioso
R-029	Saturación del gateway por falta de limitación	Inaceptable	8.4.4 – Planes de continuidad del negocio	Runbook con proveedor	Procedimientos de operación/comunicación	Playbook coordinado con ISP/proveedor	Respuesta orquestada

R-030	Reclutamiento del NVR satura CPU/almacenamiento	Aceptable	8.4.4 – Planes de continuidad del negocio	Estrategias de contención	Aislamiento	Red segregada y grabación local	Impacto contenido y evidencia preservada
R-030	Reclutamiento del NVR satura CPU/almacenamiento	Aceptable	8.4.4 – Planes de continuidad del negocio	Procedimiento Operativo Estándar de limpieza/rotación	Procedimientos de operación/comunicación	Procedimiento de limpieza y rotación de equipos	Recupera servicio sin re-infectar
R-031	Cifrado del NVR	Tolerable	8.4.4 – Planes de continuidad del negocio	Estrategias de reposición	Back up	back up de configuración/firmware	Reposición acelerada
R-031	Cifrado del NVR	Tolerable	8.4.4 – Planes de continuidad del negocio	Plan de reinstalación	Procedimientos de operación/comunicación	Reinstalación/activación guiada	Menor corte de monitoreo
R-032	Baja intencional de servicios críticos	Inadmisible	8.3.2 – Identificación y selección de estrategias	Estrategias de continuidad operativa	Establecimiento de turnos y accesos de contingencia	Roles sombra/turnos y accesos contingentes	Reduce dependencia y tiempos de recuperación

			y soluciones				
R-033	Cambios urgentes mal ejecutados	Inadmisible	8.3.2 – Identificación y selección de estrategias y soluciones	Estrategias de capacidad	Documentación viva	Programa de sombra/rotación y documentación viva	Asegura continuidad del rol crítico
R-033	Cambios urgentes mal ejecutados	Inadmisible	7.2 – Competencia	Garantizar competencia para funciones BCMS	Capacitación en roles críticos	Formación mínima y certificación/entrenamiento del rol	Sostiene continuidad operativa

Anexo C. Documento completo de la estrategia de BCP para MiPymes manufactureras.

Estrategia de implementación de continuidad del negocio para MiPymes manufactureras basada en un modelo de racionalidad limitada

Nelson Alejandro Palacios Galeano

Instituto Tecnológico Metropolitano
Facultad de ingenierías
Medellín, Colombia
2025

Introducción

En el sector manufacturero colombiano, las micro, pequeñas y medianas empresas (MiPymes) se enfrentan cada vez más a interrupciones operativas causadas por problemas de ciberseguridad, como ataques de ransomware o fallas en la infraestructura de tecnologías de la información (TI) y tecnologías de la operación (TO). Cuando estos eventos ocurren, pueden detener procesos clave y poner en riesgo la continuidad del negocio. Por eso, contar con un Plan de Continuidad de Negocio (BCP) dejó de ser opcional: hoy es una herramienta esencial para mantener la operación diaria y reducir el impacto de incidentes, especialmente en un entorno donde la probabilidad de sufrir ataques es alta debido al avance tecnológico.

Un BCP bien diseñado ayuda a identificar y proteger los elementos más importantes de la organización, asegurando que los procesos esenciales sigan funcionando en un nivel aceptable durante una crisis. Incluso puede convertirse en una ventaja competitiva. Aun así, muchas MiPymes no cuentan con un BCP porque creen que es complicado, costoso o porque no tienen personal especializado.

La estrategia presentada aquí propone integrar poco a poco los componentes mínimos indispensables de un BCP en MiPymes manufactureras, tomando como base el modelo de racionalidad limitada de Herbert Simon. Esto implica enfocarse en decisiones "lo bastante buenas" en lugar de buscar soluciones perfectas que consuman demasiado tiempo o recursos. Se aprovechan heurísticas (en el contexto se refiere a formatos o fórmulas de carácter organizacional que permitan registrar rápidamente y posteriormente tomar decisiones) y simplificaciones que facilitan avanzar rápido sin perder rigor.

El enfoque se basa también en los estándares internacionales ISO 22301:2022 (Continuidad de Negocio) e ISO/IEC 27031:2025 (Preparación de TIC para la continuidad con énfasis en ciberseguridad), adaptándolos al contexto real de las MiPymes. Aunque estos estándares son robustos y técnicos, aquí se toman algunos de los elementos más relevante además de sugerir buenas prácticas de la industria y entidades como BCI y DRII a un formato amigable para quienes no son expertos, sin perder la estructura necesaria para que también resulten útiles a quienes sí lo son.

En las siguientes secciones se presenta una guía paso a paso para implementar un BCP mínimo viable, acompañada de tablas que resumen decisiones clave, priorización de riesgos, niveles de madurez y los componentes mínimos recomendados. Además, se incluyen materiales de apoyo como plantillas y listas de verificación. A lo largo del documento se destaca cómo los principios de la racionalidad limitada justifican la selección de prácticas: se elige la simplicidad que funciona por

encima de soluciones complejas difíciles de adoptar. Así, esta estrategia ofrece una continuidad operativa realista, científicamente sólida y alcanzable para MiPymes manufactureras en Colombia.

Enfoque y fundamentos de la estrategia

Esta estrategia se apoya en dos normas internacionales clave. La primera es ISO 22301:2022, que define los requisitos para implementar y mantener un Sistema de Gestión de Continuidad de Negocio. Esta norma sigue el ciclo PHVA (Planear–Hacer–Verificar–Actuar) y establece una ruta clara para identificar amenazas, realizar un Análisis de Impacto al Negocio (BIA) y diseñar estrategias que aseguren que los procesos críticos sigan funcionando pese a interrupciones. Su ventaja es que aplica a organizaciones de cualquier tamaño, lo que la hace muy adecuada para MiPymes.

La segunda es ISO/IEC 27031:2025, que ofrece lineamientos actualizados para preparar la infraestructura tecnológica (TIC) con el fin de asegurar la continuidad del negocio. Esta norma complementa específicamente la continuidad desde el ámbito técnico, con prácticas modernas de ciberseguridad, respuesta a incidentes y recuperación, incluso en ambientes con servicios en la nube. Su nueva versión incorpora un enfoque modular que facilita tomar decisiones informadas cuando los recursos son limitados, lo cual encaja perfectamente con la realidad de las MiPymes y con la teoría de la racionalidad limitada.
Dado que las empresas manufactureras dependen cada vez más de sistemas interconectados de TI y TO, ISO 27031:2025 resulta especialmente útil para garantizar la disponibilidad de estos entornos críticos.
En resumen:

- ISO 22301 indica qué se debe hacer para asegurar la continuidad.
- ISO 27031 indica cómo preparar la infraestructura tecnológica para lograrlo.

Ambas normas se complementan para dar una visión integral de continuidad y ciber-resiliencia.

Enfoque de racionalidad limitada

Tradicionalmente, diseñar un BCP implica intentar analizar todas las alternativas y riesgos de forma exhaustiva, algo que en MiPymes simplemente no es viable por falta de tiempo, personal o recursos. Aquí entra el enfoque de racionalidad limitada de Herbert Simon, que propone tomar decisiones “suficientemente buenas” con la información disponible, en lugar de perseguir soluciones perfectas que retrasan la acción.
En la práctica, este enfoque se refleja en:

1. Foco en lo crítico
Se concentran los esfuerzos en los procesos y activos que realmente sostienen al negocio. Por ejemplo, asegurar la continuidad de la línea principal de producción antes que procesos secundarios. Estudios previos demuestran que esta selección de “mínimos viables” es efectiva: si

es necesario sacrificar temporalmente actividades menos críticas para proteger las esenciales, se hace. El resultado es un BCP adaptable y de alto impacto.

2. Heurísticas y guías predefinidas
Para evitar que la empresa tenga que construir todo desde cero, se proporcionan listas, plantillas y catálogos de riesgos típicos del sector (basados en fuentes como NIST, INCIBE, OWASP, etc.). Así, la toma de decisiones es más rápida: se selecciona entre opciones probadas en lugar de diseñar controles desde cero.

3. Progresividad en la adopción
El modelo propone avanzar por niveles de madurez: primero un nivel básico, después uno intermedio y eventualmente uno avanzado si la empresa crece y puede invertir más. De esta forma no se abruma a la organización con exigencias desde el inicio. La idea es empezar con lo mínimo viable, aprender y fortalecer el plan en el tiempo.

4. Rigor conceptual con simplificación operativa
Aunque el enfoque es práctico, no sacrifica la calidad técnica. Los componentes del BCP están alineados con estándares internacionales, pero escritos y diseñados en un lenguaje fácil de entender para quienes no vienen del mundo TI. Se evita la terminología excesiva, pero se mantiene la esencia de una buena práctica profesional.

Componentes mínimos viables

A partir del análisis realizado, se identificaron ciertos componentes esenciales que cualquier BCP para MiPymes manufactureras debe incorporar, especialmente frente a incidentes de ciberseguridad. Estos elementos son básicos, pero altamente efectivos y viables.
Incluyen:

- Respaldos periódicos de datos críticos.
- Infraestructura redundante o equipos alternos para funciones clave.
- Procedimientos de respuesta y recuperación ante incidentes.
- Protocolos de comunicación interna y externa en crisis.
- Roles y responsabilidades claros.
- Pruebas periódicas del plan.

Cada componente se explica en detalle en las siguientes secciones con ejemplos prácticos y el razonamiento detrás de su selección. Lo importante es que todos fueron elegidos porque aportan valor real ante los riesgos más comunes del sector y pueden implementarse sin inversiones desmesuradas.

Guía paso a paso

Paso 1: Compromisos directivos y definición del alcance

El primer paso para construir un BCP funcional es lograr que la dirección de la empresa se comprometa con el proyecto. La alta gerencia debe entender por qué la continuidad del negocio es importante y estar dispuesta a brindar tiempo, recursos y respaldo visible. Esto no requiere documentos extensos: una breve política o declaración oficial donde la gerencia afirme su apoyo es suficiente para marcar el rumbo y legitimar el proceso.

Al mismo tiempo, es necesario definir el alcance inicial del BCP, es decir, qué áreas, procesos y sistemas cubrirá. Bajo el enfoque de racionalidad limitada, no se busca abarcar todo desde el principio. Es más práctico comenzar con lo esencial: aquellas partes del negocio cuya interrupción causaría pérdidas graves o detendría la operación principal.

Por ejemplo, la empresa puede decidir que el BCP inicial cubrirá:

- La planta de producción principal,
- El ERP que soporta manufactura e inventarios,
- La red y equipos de operación industrial,
- Servicios en la nube indispensables.
- Procesos menos críticos o áreas secundarias pueden integrarse más adelante.

Esta selección deliberada evita sobrecargar al equipo y facilita avanzar con un plan realista. La lógica es: primero asegurar la continuidad del corazón del negocio, después expandir. El documento de alcance debe incluir también el nombramiento del líder o coordinador del BCP, quien será responsable de dirigir y organizar todas las actividades relacionadas con el plan. Frecuentemente esta persona es alguien de TI o de operaciones. Con el compromiso directivo asegurado y el alcance bien delimitado, la empresa ya cuenta con las bases necesarias para avanzar hacia la conformación del equipo y el desarrollo técnico del plan.

Paso 2: Conformación de equipos de continuidad

Con el apoyo de la dirección ya formalizado, el siguiente paso es armar un Equipo de Continuidad del Negocio acorde al tamaño y capacidades de la MiPyme. No se trata de crear una estructura grande ni burocrática; bastan entre 3 y 5 personas clave que conozcan bien la operación y puedan asumir roles específicos durante una emergencia.

Un equipo básico puede formarse así:

- Coordinador del BCP: suele ser alguien de TI o de calidad; lidera todo el proceso y mantiene actualizado el plan.

- Representante de Operaciones o Producción: entiende los puntos críticos de la planta y cómo se verían afectados.
- Representante de TI / Seguridad de la Información: aporta el conocimiento técnico para respaldos, restauraciones, contención de incidentes y continuidad tecnológica.
- Miembro de Gerencia: funge como enlace con la dirección y facilita decisiones y recursos cuando la situación lo amerita.

Si la empresa es muy pequeña, incluso un equipo de dos personas (gerente + encargado de sistemas) puede funcionar como punto de partida. Cuando sea necesario, se puede pedir apoyo externo puntual. Cada integrante debe saber desde el principio qué papel le toca desempeñar si ocurre un incidente. Por ejemplo: quién activa el plan, quién decide detener operaciones, quién contacta proveedores, quién coordina la comunicación interna, etc. Lo ideal es dejar estos roles por escrito dentro del BCP para que no haya dudas en un momento crítico.

Un aspecto importante del enfoque de racionalidad limitada es no complicar la estructura. Menos, es más: un equipo pequeño, claro y bien coordinado suele funcionar mejor que muchos participantes con funciones difusas. En MiPymes es normal que una misma persona tenga varios roles, y eso es completamente válido siempre que las funciones esenciales queden cubiertas. Además, es buena práctica comenzar desde este punto a sensibilizar al personal sobre el proyecto de continuidad. No hace falta entrar en detalles técnicos; basta con informar que la empresa está desarrollando un plan formal para proteger la operación. Esto crea apertura y facilita futuras actividades como entrevistas, capacitaciones o simulacros.
Con el equipo formado y consciente de sus responsabilidades, la empresa está lista para iniciar el análisis de procesos críticos.

Paso 3: Identificación de procesos críticos (BIA)

Con el equipo de continuidad ya conformado, el siguiente paso es identificar qué partes del negocio no pueden detenerse sin causar daños serios. Para esto se realiza un Análisis de Impacto al Negocio (BIA), pero en una versión simplificada y adecuada para MiPymes, evitando procesos largos o demasiado técnicos.
La lógica aquí es práctica:
¿Qué actividades sostienen a la empresa y qué tan grave sería que se detuvieran?

1. Listar los procesos principales de la empresa
Incluye tanto procesos operativos como los de soporte indispensable. Algunos ejemplos habituales en manufactura serían:

- Fabricación del producto principal,

- Logística o despacho,
- Gestión de pedidos,
- Mantenimiento de maquinaria,
- Sistemas TI que apoyan la producción (como el ERP o software industrial),
- Procesos administrativos (Facturación, cartera, tesorería, entre otros).

Para cada proceso, el equipo debe preguntarse:

- "Si este proceso se detiene, ¿qué pasa en la empresa?"

Los procesos cuya interrupción frene la producción, afecte ingresos o cause pérdidas significativas se marcan como críticos.

2. Identificar los recursos esenciales de cada proceso crítico

Para cada proceso crítico se debe registrar qué necesita para operar, por ejemplo:

- Personal clave,
- Maquinaria específica,
- Sistemas o servidores,
- Insumos o proveedores indispensables.

Esto ayuda a saber exactamente qué proteger en el plan.

3. Estimar el tiempo máximo tolerable de interrupción (RTO) de forma sencilla

No se requieren cálculos financieros complejos; basta con clasificar el tiempo que la empresa puede tolerar sin operar ese proceso:

- Menos de 4 horas
- Hasta 24 horas
- Hasta 3 días
- Más de 3 días

Esta estimación sirve para decidir qué procesos deben recuperarse primero y qué medidas se necesitan.

4. Mantener el análisis simple y práctico

El BIA debe identificar entre 3 y 6 procesos críticos, no más. Esto evita dispersarse y ayuda a mantener el enfoque en lo verdaderamente importante.

Un ejemplo de tabla útil sería:

Proceso crítico	**Recursos clave**	**Tiempo máximo de interrupción**	**Impacto estimado**

Control de producción	Servidor ERP, 5 PCs de planta, personal de producción	1 día	Pérdidas altas y desperdicio

5. Identificar dependencias externas críticas

Muchos negocios dependen de servicios como:

- Plataformas en la nube,
- Correo electrónico,
- Proveedores únicos de maquinaria o insumos.

Si alguno de estos cae y afecta la operación, debe incluirse como elemento crítico.

Un BIA simple, pero suficiente

El objetivo no es obtener métricas exactas, sino entender qué es vital para el negocio y qué debe recuperarse con mayor urgencia.

Este BIA simplificado cumple su propósito sin consumir semanas de análisis y permite avanzar al siguiente paso: priorizar riesgos.

Paso 4: Priorización de riesgos en base al BIA

Una vez que la empresa tiene claro cuáles son sus procesos críticos y qué recursos necesita para mantenerlos, el siguiente paso es identificar qué podría interrumpirlos. Pero, siguiendo el enfoque práctico de la racionalidad limitada, no se trata de hacer una lluvia infinita de riesgos ni análisis complicados. El objetivo es enfocar la atención en los riesgos que realmente importan.

1. Usar un catálogo de amenazas típicas para manufactura

Para simplificar el trabajo, en lugar de inventar escenarios desde cero, el equipo revisa una lista predefinida de riesgos comunes en el sector manufacturero. Esta lista incluye eventos como:

- Ransomware que cifra servidores (por ejemplo, el ERP).
- Malware en equipos industriales o de oficina.
- Caídas de red por ataques DoS/DDoS.
- Fallas de hardware crítico (PLC, motores, servidores).
- Errores humanos que afectan datos o procesos.
- Cortes prolongados de energía.
- Incendios, inundaciones u otros eventos físicos relevantes.
- Sabotaje interno.

El equipo revisa cada riesgo y marca solo aquellos que realmente aplican al funcionamiento de la empresa.

2. Evaluar cada riesgo con un método sencillo: probabilidad e impacto

No es necesario asignar fórmulas ni porcentajes. Basta con clasificar cada riesgo como:

- Bajo,
- Medio-bajo,
- Medio-alto,
- Alto.

La probabilidad puede evaluarla el personal de TI, mientras que el impacto lo determina quien conoce los procesos operativos. Esta combinación permite priorizar rápidamente.

Por ejemplo:

ID Riesgo	Escenario	Nivel
R-002	Ransomware cifra servidor ERP, dejando producción y contabilidad inoperables	**INADMISIBLE**
R-010	Ataque DoS/DDoS afecta VPN o servidor perimetral	**INACEPTABLE**
R-006	Malware publicitario infecta una PC aislada	**ACEPTABLE**

3. Crear un ranking de riesgos de mayor a menor prioridad

Esto ayuda a decidir dónde invertir tiempo y recursos. Las reglas generales del enfoque son:

- Riesgos INADMISIBLES → deben tener medidas inmediatas.
- Riesgos INACEPTABLES → atender con soluciones factibles a corto plazo.
- Riesgos TOLERABLE → atender si la solución es factible o de bajo costo.
- Riesgos ACEPTABLE → se aceptan temporalmente y solo se monitorean.

Esta selección permite avanzar rápido sin intentar cubrir todo a la vez.

4. Aceptar que no todo puede mitigarse al 100% desde el inicio

Este es uno de los principios clave de la racionalidad limitada:

- Primero resolvemos lo que más duele, y lo demás lo mejoramos con el tiempo.

Así, el BCP se vuelve viable de implementar en una MiPyme.

5. Incluir también riesgos no intencionales

- Aunque el enfoque está orientado a ciberseguridad, también se consideran:
- Averías de maquinaria esencial,
- Fallos eléctricos,
- Degradación de equipos críticos.

Un riesgo físico puede afectar la continuidad tanto como un ataque cibernético, por lo que se integran en la evaluación.

6. Documentar la matriz y usarla como fundamento para las decisiones del plan

Esta tabla de riesgos priorizados será la base para definir las estrategias del siguiente paso: qué medidas se implementarán para cada riesgo.

Paso 5: Definición de estrategias y controles

Este paso es el corazón del BCP: aquí se define cómo la empresa enfrentará los riesgos priorizados y mantendrá la operación aun cuando ocurra un incidente. Desde la perspectiva de ISO 22301, esto corresponde a desarrollar estrategias de continuidad y soluciones de recuperación. Bajo nuestro enfoque práctico, se eligen únicamente las medidas mínimas viables, pero suficientes para proteger lo más crítico sin exigir grandes inversiones.
Las estrategias siguientes están organizadas como un "menú" de soluciones esenciales. Cada MiPyme debe seleccionar las que realmente necesita, basándose en los riesgos altos y medios identificados en el paso anterior.

Componentes mínimos viables del BCP
A continuación se explican, en lenguaje claro, los elementos esenciales que toda MiPyme manufacturera debería integrar en su plan de continuidad para enfrentar riesgos tecnológicos y cibernéticos.

1. Respaldos periódicos offline de datos críticos
Esta es la medida más importante contra ransomware y pérdida de información. Consiste en:

- Hacer copias de seguridad frecuentes del ERP, bases de datos y archivos clave.
- Guardar al menos una copia fuera de la red principal: en un disco externo, cinta o servicio seguro en la nube.
- Verificar periódicamente que las copias realmente se pueden restaurar.

El respaldo offline es barato, simple y puede salvar a la empresa de semanas de paro por cifrado de datos.

2. Equipos o servicios de respaldo para funciones críticas
Para evitar que un fallo físico detenga la producción, se recomiendan redundancias básicas:

- Un servidor de repuesto o virtualización en la nube para emergencias.
- Maquinaria o piezas clave duplicadas (por ejemplo, un PLC adicional).
- Un segundo enlace a Internet (un plan 4G suele ser suficiente).

La idea es tener un "plan B" tecnológico y operativo para los recursos que permiten producir.

3. Procedimientos operativos alternos (modo manual o degradado)
Cuando la tecnología falla, el negocio no debe detenerse por completo. Por ello se definen procesos alternos como:

- Registrar producción o pedidos en papel o en Excel si el ERP cae.
- Coordinar tareas por teléfono o radio si la red local falla.
- Procedimientos “a la vieja escuela” para continuar temporalmente la operación.

Estos métodos deben ser claros, fáciles y conocidos por el personal.

4. Plan de comunicaciones de emergencia

Incluye:

- Lista actualizada de contactos internos y externos (incluyendo proveedores críticos).
- Canales alternos de comunicación: teléfonos, WhatsApp, correos personales, etc.
- Mensajes predefinidos para comunicar la situación a clientes o proveedores.

La comunicación clara evita caos, rumores y decisiones tardías durante una crisis.

5. Planes de respuesta y recuperación ante incidentes (playbooks)

Estos documentos son instrucciones paso a paso para reaccionar ante incidentes específicos. Deben ser breves, por ejemplo:

- Guía de respuesta a ransomware: aislamiento del servidor, aviso inmediato a TI, restauración segura del backup, procedimientos temporales para operación manual.
- Guía ante caída de red: verificar equipos, activar enlace alterno, notificar a producción y gerencia.

Los playbooks ahorran tiempo y reducen errores cuando ocurre un incidente real.

6. Aislamiento y segmentación de redes críticas

Este control busca que un problema en una parte de la red no afecte toda la operación.

- Separar la red de oficinas de la red industrial mediante VLAN.
- Poder desconectar rápidamente una máquina comprometida sin apagar toda la planta.
- Reglas de firewall para bloquear tráfico sospechoso y limitar propagación de malware.

La segmentación es una defensa clave en entornos donde TI y TO conviven.

7. Control de accesos y cuentas de respaldo

Para reducir riesgos humanos y de abuso de privilegios:

- Limitar quién tiene permisos de administrador.
- Usar autenticación de dos factores en cuentas críticas.
- Mantener cuentas de emergencia guardadas de forma segura, por si un incidente bloquea accesos normales.

Si una sola persona tiene acceso total y no está disponible, la operación puede quedar detenida. Por eso este control es básico.

8. Plan de reversión y retorno a la normalidad

Después de contener una crisis, la empresa necesita volver a operar normalmente. El plan debe indicar:

- Cómo regresar del servidor de respaldo al servidor principal.

- Cómo reingresar datos capturados en papel.
- Cómo revertir cambios o actualizaciones fallidas.
- Cómo reconstruir sistemas desde imágenes limpias si fuera necesario.

Este paso asegura que la empresa no quede atrapada en "modo contingencia".

Cómo seleccionar las estrategias correctas

Cada componente debe vincularse directamente con los riesgos detectados. Por ejemplo:

- Si el riesgo principal es ransomware, se priorizan respaldos offline + playbook especializado.
- Si el riesgo es falla de red, se implementa un enlace alterno + segmentación.
- Si el riesgo es fallo de PLC, se adquiere una unidad de repuesto + procedimiento manual.

Un solo control puede cubrir varios riesgos, lo cual es ideal para MiPymes con recursos limitados.

Validación de viabilidad

Antes de avanzar a la documentación del plan:

- Verificar que cada medida es asequible,
- Fácil de implementar,
- Enteramente comprendida por el personal.

La regla clave del modelo de racionalidad limitada es:
"¿Cuál es la solución más simple que funciona, es decir, que satisface la necesidad?"
No se elige la solución perfecta, sino la que la empresa puede aplicar hoy mismo.

Paso 6: Documentación del BCP

Con las estrategias ya definidas, ahora toca poner todo por escrito de una manera clara, práctica y fácil de usar. El documento final del Plan de Continuidad de Negocio (BCP) será la guía oficial para actuar antes, durante y después de una interrupción. No debe ser un "libro" que nadie leerá en una emergencia; debe ser breve, funcional y accesible.

¿Cómo debe ser el documento BCP?

Debe ser:

- Corto y entendible, no técnico en exceso.
- Accionable, con pasos que el personal pueda ejecutar incluso bajo presión.
- De fácil acceso: disponible en digital, impreso y, si es posible, en ubicaciones clave.

A continuación, se describe la estructura recomendada, adaptada al estilo de una MiPyme:

1. Propósito y alcance

Una breve introducción donde se explique:

- Qué busca el plan (mantener los procesos esenciales funcionando durante interrupciones).

- Qué áreas, sistemas y procesos cubre, según lo definido en el Paso 1.
- Nada rebuscado: dos o tres párrafos son suficientes.

2. Equipo de Continuidad y contactos
Este apartado debe listar:

- Quiénes forman el equipo,
- Qué rol tiene cada uno,
- Cómo contactarlos 24/7 (números móviles, correos alternativos).

También se añaden:

- Contactos de proveedores críticos,
- Soportes técnicos externos,
- Autoridades relevantes si aplica (ej. bomberos, CERT, etc.).

Esta sección debe ser clarísima, pues en una crisis cada minuto vale.

3. Prioridades del negocio (resumen del BIA)
Aquí se integran de manera simple los resultados del Paso 3:

- Cuáles procesos son críticos,
- Qué recursos necesitan,
- Sus tiempos máximos de interrupción tolerable.
- Una tabla sencilla es suficiente.

4. Escenarios de riesgo y estrategias de continuidad
En este punto se conectan los riesgos identificados en el Paso 4 con las medidas del Paso 5.
Ejemplo de presentación:
Escenario: Ransomware en servidor ERP
Estrategia: Restaurar backup offline + uso de procedimiento manual temporal + comunicación interna.
Esta sección debe permitir a cualquier responsable “seguir el hilo” de qué hacer ante cada escenario importante.

5. Planes de respuesta y procedimientos (playbooks)
Aquí se incluyen:

- Los procedimientos detallados para actuar ante incidentes críticos (ransomware, caída de red, falla de PLC, etc.).
- El flujo para declarar emergencia, activar el plan y asignar tareas.
- Se recomienda un diagrama de flujo simple, por ejemplo:
- Se detecta el incidente.
- Se avisa al Coordinador.
- El Coordinador evalúa severidad.

- Si es crítico, se activa el playbook correspondiente.
- Se comunica al personal clave.

Estos procedimientos deben ser directos, de 1 a 3 páginas cada uno.

6. Recursos y logística de continuidad

Aquí se documenta todo lo que la empresa necesitará durante una contingencia:

- Ubicación de respaldos
- Equipo de respaldo
- Kits de emergencia
- Contraseñas o accesos de contingencia
- Información de sistemas esenciales

La organización debe poder encontrar estos recursos incluso sin sistemas digitales.

7. Cronograma de pruebas y revisiones

El BCP debe incluir un compromiso explícito de:

- Cuándo se probará (mínimo una vez al año),
- Cómo se actualizará después de cada prueba o incidente.

Esto mantiene vivo el plan y evita que se vuelva obsoleto.

8. Aprobación de la alta dirección

La firma de la gerencia asegura:

- Que el plan tiene respaldo institucional,
- Que se asignarán recursos cuando sea necesario.

No se necesita un lenguaje complicado: basta con una declaración breve.

Estilo de redacción recomendado

Debe ser:

- Sencillo
- Directo
- Lleno de instrucciones accionables
- Libre de jerga técnica innecesaria

Ejemplo de lenguaje adecuado:

- “Si el sistema ERP falla, active el procedimiento PR-ERP-01. Registre pedidos en el formato manual mientras TI restaura el servidor.”

El objetivo es que un encargado de planta pueda usar el plan incluso de madrugada durante un incidente real.

Distribución del BCP

El documento debe estar disponible:

- En digital (idealmente en la nube con acceso restringido),
- En formato impreso en sitios clave,
- En manos del equipo de continuidad.

También es útil preparar un resumen ejecutivo de 1 página con los primeros pasos ante emergencias.

Paso 7: Implementación de los controles

En este paso, el BCP deja de ser teoría y empieza a materializarse en acciones concretas. Aquí se ponen en marcha todas las decisiones tomadas en el Paso 5. Lo importante es avanzar de forma organizada, con tareas claras, responsables asignados y fechas realistas.
La idea no es implementar todo a la vez, sino ir completando pequeñas entregas que juntas fortalecen la continuidad del negocio.

1. Asignar responsables y fechas a cada control
Se toma la lista de medidas aprobadas (por ejemplo: "configurar backups diarios", "comprar servidor de respaldo", "crear playbook de ransomware") y se le asigna:

- Un responsable
- Una fecha límite razonable

Por ejemplo:
TI: configurar backup offline antes del 15 de noviembre.
Producción: completar procedimiento manual de empaque antes del 30 de noviembre.
La prioridad debe ir hacia los riesgos clasificados como ALTO.

2. Implementar los controles técnicos
Normalmente esta parte la asume el área de TI o un proveedor externo. Incluye acciones como:

- Activar scripts de backup y probar una restauración.
- Configurar el segundo enlace de internet.
- Implementar segmentación de red (VLAN).
- Actualizar software o sistemas críticos.
- Asegurar copias offline desconectadas.

Cada cambio debe documentarse de forma breve, pensando en que otro técnico pueda entender lo que se hizo en caso de emergencia.

3. Implementar las medidas organizativas
Aquí entran actividades que no son técnicas, pero sí cruciales:

- Comprar equipos de respaldo.
- Imprimir y distribuir listas de contactos de emergencia.
- Preparar kits o carpetas físicas con playbooks y materiales clave.
- Coordinar contratos con proveedores (por ejemplo, soporte especializado de maquinaria).

También es el momento de socializar con el personal los nuevos procedimientos.

4. Capacitar al personal en los nuevos procedimientos

No basta con escribir los protocolos: hay que asegurarse de que el personal los conozca y los pueda aplicar.

La capacitación puede incluir:

- Mostrar cómo llenar un formato manual cuando el ERP falla.
- Enseñar a los encargados de TI cómo restaurar un respaldo.
- Explicar quién debe avisar a quién en caso de interrupción.

Estas capacitaciones pueden combinarse con las pruebas del Paso 9.

5. Documentar avances y actualizar el plan

Cada vez que una tarea se complete:

- Se registra que ya fue implementada.
- Se actualiza el BCP si algún detalle cambió.

Por ejemplo:

Si se compra un servidor de respaldo, se agrega su ubicación y configuración al plan.

Si se crea un nuevo playbook, se incorpora a los anexos.

El BCP debe reflejar el estado real de la preparación, no lo que estaba planeado originalmente.

6. Ajustar conforme avance la implementación

Es normal que algunas medidas resulten más complejas o costosas de lo previsto. Bajo el modelo de racionalidad limitada:

- Se permite ajustar, simplificar o sustituir controles.
- Lo importante es que la solución elegida funcione y sea viable para la empresa.

Ejemplo:

- Si replicar datos a la nube es demasiado lento, se refuerza el proceso de backup local.
- Si un paso del procedimiento manual confunde al personal, se reescribe de manera más simple.

La flexibilidad es clave, sin embargo, dejar un registro que permita ver el cambio en el tiempo de las definiciones, habilita la reducción de esfuerzos futuros.

7. Mantener informada a la gerencia

No se requieren reportes formales, pero sí comunicar logros clave, como:

- “Ya funcionan los respaldos offline.”
- “El enlace de internet secundario quedó instalado.”
- “Playbook de ransomware listo y probado.”

Esto mantiene el apoyo institucional.

Paso 8: Capacitación y concienciación de la continuidad

Aunque en pasos anteriores ya se capacitó al personal directamente involucrado, este paso se enfoca en fortalecer la cultura de continuidad en toda la empresa. En pocas palabras: no basta con tener un BCP bien escrito; la gente debe saber qué hacer, cómo hacerlo y por qué es importante.
La capacitación y concienciación son clave para que el plan funcione cuando realmente se necesite.

1. Capacitación del equipo BCP
El equipo responsable del plan debe tener un entendimiento profundo del BCP. Se puede organizar un taller interno donde:

- Se repase cada sección del plan,
- Se simulen escenarios ("¿qué haríamos si el ERP se cae un lunes a las 8 am?"),
- Se clarifiquen roles y tiempos de respuesta,
- Se evalúe el uso de playbooks paso a paso.

Estos ejercicios ayudan a que el equipo gane seguridad y detecte posibles áreas confusas antes de una prueba formal.

2. Sensibilización del resto del personal
No es necesario que todos sean expertos en continuidad, pero sí deben:

- Saber que existe un plan,
- Conocer lo básico sobre qué hacer en una emergencia,
- Identificar a quién reportar incidentes,
- Entender que hay procedimientos alternos si los sistemas fallan.

Charlas breves en cada área, reuniones de turno o incluso pósters y folletos pueden ser suficientes.
Ejemplo de mensaje clave:
"Si notas algo extraño en tu equipo o en la maquinaria (ruidos, mensajes sospechosos, caídas), reporta de inmediato al coordinador o a tu supervisor."
Esto fomenta una cultura activa y alerta.

3. Entrenamiento por rol
Algunos roles requieren entrenamiento práctico, como:

- Personal de TI → restauración de backups, activar enlace alterno, ejecutar playbooks.
- Personal de planta → activar procedimientos manuales, cambiar a equipo de respaldo.
- Responsables de comunicación → preparar mensajes de crisis.
- Suplentes → deben saber cubrir funciones críticas si el titular no está disponible.

Esto evita que la continuidad dependa de una sola persona.

4. Mantener la concienciación viva
Una empresa suele olvidar rápidamente estos temas si no se recuerdan de forma periódica. Algunas buenas prácticas son:

- Enviar breves boletines internos sobre seguridad o continuidad.

- Hacer mini ejercicios de 5 minutos (“si esta máquina fallara, ¿qué harías?”).
- Incorporar continuidad en la inducción de nuevo personal.
- Reforzar aprendizajes después de simulacros o incidentes reales.

El objetivo es que el BCP deje de verse como un documento ajeno y se convierta en una práctica cotidiana.

Paso 9: Pruebas y simulacros

Aunque tengas el BCP documentado y las medidas implementadas, no puedes asumir que todo funcionará bien hasta que lo pruebes. Las pruebas y los simulacros permiten descubrir fallas, mejorar tiempos de respuesta y dar confianza al personal. Es mejor encontrar errores en un ejercicio controlado que durante una emergencia real.

El objetivo de este paso es validar que el plan funciona de verdad y que el equipo sabe cómo aplicarlo.

1. Iniciar con ejercicios de escritorio.

Este tipo de prueba no interrumpe la operación real. El equipo se reúne alrededor de una mesa y simula un escenario paso a paso, usando el plan.

Ejemplo:

Escenario: “Es lunes 8 a.m. El ERP muestra un mensaje de ransomware y toda la planta se detiene.”

El moderador guía la conversación:

- ¿Quién detecta el incidente?
- ¿A quién avisa primero?
- ¿Qué playbook se sigue?
- ¿Qué decisiones toman durante las primeras 2 horas?

Estas simulaciones ayudan a:

- Identificar pasos confusos,
- Aclarar roles,
- Detectar vacíos en la comunicación,
- Ajustar el plan antes de pruebas más complejas.

2. Realizar simulacros técnicos controlados

Una vez dominado el ejercicio de escritorio, se pueden realizar pruebas más reales, siempre con precaución para no causar interrupciones innecesarias.

Algunos ejemplos:

- **Prueba de restauración de respaldo**

En un servidor de pruebas:

1. Se simula un archivo corrupto o cifrado.
2. TI ejecuta el procedimiento real de restauración.

3. Se mide el tiempo que toma volver a tener el servicio funcional.
4. Esto frecuentemente revela si los respaldos sirven o no, algo que muchas empresas descubren demasiado tarde.

- **Prueba del enlace de Internet secundario**

En un momento de baja actividad:

1. Se desconecta temporalmente la red principal.
2. Se observa si el enlace 4G o alterno toma el control automáticamente.
3. Se confirma que el personal sabe qué hacer si esto falla.

- **Prueba de procedimientos manuales**

Sin afectar la operación real:

1. Por un par de horas, el área de producción registra información solo en los formatos alternos.
2. Se revisa si saben llenarlos, si falta información o si las instrucciones necesitan aclararse.

- **Simulacros por ausencia de personal clave**

1. Se plantea: “Hoy el encargado de TI no vino. ¿El suplente puede restaurar el servidor?”

Esto revela si existe dependencia excesiva en una sola persona.

3. Documentar resultados y lecciones aprendidas

Después de cada simulacro, el equipo debe reunirse para analizar:

- Qué funcionó bien,
- Qué no salió como se esperaba,
- Qué pasos fueron confusos o lentos,
- Qué se debe actualizar en el BCP,
- Qué capacidades faltan.
- Esto alimenta la mejora continua.

4. Frecuencia recomendada

Prueba inicial: 1–2 meses después de implementar el BCP mínimo viable.
Pruebas regulares: al menos una vez al año.
Pruebas adicionales: cuando haya cambios importantes, o tras un incidente real.
Si la empresa no tuvo emergencias durante el año, es vital generar una interrupción simulada para no “enfriar” el plan.

Paso 10: Mejora continua

La continuidad del negocio no es algo que se hace una vez y se olvida. Un BCP solo funciona si se mantiene actualizado, se revisa con frecuencia y evoluciona junto con la empresa. Este paso establece el ciclo de mejora continua, donde el plan se ajusta constantemente para seguir siendo útil y realista.

El enfoque de racionalidad limitada encaja perfectamente aquí: el primer BCP no será perfecto, pero será suficiente para empezar. Con el tiempo, se va afinando y fortaleciendo.

1. Revisar el plan periódicamente

Al menos una vez al año (o antes si hubo cambios importantes) el equipo debe reunirse para revisar:

- Procesos nuevos o modificados,
- Cambios en la infraestructura tecnológica,
- Personal que cambió de puesto o dejó la empresa,
- Nuevas amenazas o incidentes recientes,
- Resultados de simulacros o auditorías internas.

El BCP debe actualizarse para reflejar la realidad actual de la empresa, no la del año pasado.

2. Mantener y verificar los recursos críticos

Las medidas implementadas deben funcionar no solo cuando se instalan, sino siempre. Por eso es importante:

- Revisar que los respaldos se generen correctamente y sigan siendo restaurables.
- Encender equipos de respaldo para comprobar que sigan operativos.
- Verificar que las contraseñas de emergencia funcionen.
- Actualizar la lista de contactos cuando haya cambios.
- Encender generadores o equipos auxiliares periódicamente (si aplica).

Una pequeña rutina mensual o trimestral evita sorpresas desagradables durante una emergencia real.

3. Monitorear nuevas amenazas y el entorno

El riesgo cambia con el tiempo, especialmente en ciberseguridad. Algunas prácticas útiles son:

- Revisar boletines de alertas cibernéticas.
- Mantenerse al tanto de incidentes que afecten a empresas similares.
- Evaluar si las amenazas nuevas requieren agregar controles.
- Un riesgo que no existía hace un año puede ser crítico hoy.

4. Escalar el nivel de madurez del BCP de forma gradual

No todas las empresas necesitan llegar al nivel más avanzado, pero sí pueden mejorar progresivamente. La estrategia propone tres niveles:

Nivel Básico (mínimo viable)

Lo implementado durante esta guía: respaldos offline, playbooks esenciales, duplicidad básica, procedimientos manuales.

Nivel Intermedio

La empresa agrega más controles, más documentación y pruebas más frecuentes. Ya existe mayor formalidad y robustez.

Nivel Avanzado

Incluye capacidades como recuperación en sitio alterno, redundancia completa, métricas de tiempos de recuperación, auditorías internas y cumplimiento total de ISO 22301.

Lo importante es avanzar poco a poco, según los recursos, necesidades y crecimiento de la organización.

5. Usar lecciones aprendidas para reforzar el plan

Cada simulacro o incidente real es una oportunidad de aprendizaje. Tras cada evento se debe:

- Analizar qué funcionó,
- Qué falló,
- Qué pasos fueron confusos,
- Qué recursos faltaron,
- Qué decisiones tomaron demasiado tiempo.
- Con base en eso, se actualiza el plan.

6. Promover una cultura de resiliencia

La continuidad se integra en la cultura cuando:

- Los empleados reportan incidentes sin temor,
- Se toman medidas preventivas sin que lo pidan,
- Se realizan pruebas con naturalidad,
- El personal entiende que el BCP protege tanto a la empresa como a su propio trabajo.

Una cultura fuerte reduce riesgos, acelera respuestas y evita crisis.

Evaluación del Estado de Preparación del BCP

Para que la MiPyme tenga claridad sobre qué tan preparada está realmente en materia de continuidad del negocio, es útil contar con herramientas simples de autoevaluación. Esto permite identificar brechas, priorizar mejoras y asegurar que el BCP no se “enfríe” con el tiempo.

La idea es que la empresa pueda revisarse de forma rápida, objetiva y periódica.

Checklist de Preparación del BCP

A continuación, se presenta una lista de verificación fácil de usar. La empresa puede revisarla cada trimestre o antes de auditorías internas. Si algún punto se marca como “No”, significa que hay una brecha que debe atenderse.

Aspecto clave a verificar	¿Cumplido? (Sí/No)
La gerencia ha expresado su apoyo formal al BCP y existe un responsable asignado.	
El alcance está definido: se conocen y documentan los procesos críticos y sus requerimientos.	
La empresa cuenta con una lista actualizada de riesgos prioritarios (incluyendo ciberamenazas).	
Los respaldos de datos críticos se realizan con frecuencia y **se ha probado su restauración**.	
Existen redundancias básicas (equipo de respaldo, segundo enlace de Internet, proveedores alternos).	
El BCP está escrito, vigente y accesible para quienes lo necesitan.	
El personal ha recibido capacitación sobre su rol en el BCP.	
Se ha realizado al menos una prueba o simulacro durante los últimos 12 meses.	
El plan se revisa y actualiza periódicamente (contactos, cambios en procesos, nueva infraestructura, etc.).	

Este checklist resume los elementos mínimo-indispensables para que un plan de continuidad sea funcional en una MiPyme manufacturera.

Cómo usar los resultados

- Si la empresa cumple 8 o 9 puntos, tiene un BCP sólido para su tamaño.
- Si cumple 5 a 7 puntos, el BCP es funcional, pero necesita mejoras.
- Si cumple menos de 5, la continuidad está en riesgo y conviene reforzar áreas prioritarias.

También es útil registrar cada revisión con fecha para monitorear el progreso a lo largo del tiempo.

Modelo de madurez como herramienta de evaluación

Además del checklist, la empresa puede ubicarse dentro de un nivel de madurez (básico, intermedio o avanzado). Esto le permite visualizar su progreso y planear mejoras realistas.
Por ejemplo:

- Puede estar en Nivel Básico en estrategia,
- Pero Nivel Intermedio en respaldos,
- Y Nivel Avanzado en comunicación con proveedores.

Esta autoevaluación flexible ayuda a construir una ruta de crecimiento acorde a los recursos disponibles.

Materiales de Apoyo Propuestos

Para facilitar que una MiPyme implemente, mantenga y utilice su Plan de Continuidad del Negocio (BCP), es útil contar con herramientas prácticas y listas para usar. Estos materiales no solo simplifican el trabajo del equipo, sino que también reducen errores y aceleran la respuesta durante una crisis.
A continuación, se presentan los materiales de apoyo recomendados, descritos en un lenguaje claro y cercano:

1. Plantilla de Plan de Continuidad del Negocio (BCP)
Un documento base con la estructura ya preparada para que la empresa solo tenga que llenar su propia información.
Incluye secciones como:

- Objetivo y alcance
- Procesos críticos
- Riesgos priorizados
- Estrategias de continuidad
- Contactos y roles
- Playbooks o procedimientos
- Cronograma de pruebas

Esto evita que la empresa parta desde cero o improvise una estructura.

2. Lista de verificación de respuesta inicial a incidentes
Diseñada para los primeros minutos de una crisis, cuando el estrés es alto y la mente tiende a fallar.
Ejemplo de pasos:

- Asegurar la integridad de las personas.
- Identificar el tipo de incidente.
- Notificar al Coordinador del BCP.
- Aislar los sistemas afectados (si es incidente cibernético).
- Registrar hora y síntomas.

Esta lista puede colocarse en lugares visibles o junto a teléfonos importantes.

3. Formato de registro de incidentes
Una ficha para anotar claramente qué pasó, cuándo, quién actuó y qué efectos tuvo.
Incluye:

- Hora de detección
- Descripción del evento
- Acciones tomadas
- Tiempos de recuperación
- Impactos en producción

- Lecciones aprendidas

Este registro es valioso para mejorar el BCP.

4. Guía rápida para evaluar daños y activar el BCP

Un cuadro de decisión que ayuda al personal a determinar si un incidente es menor o si amerita activar formalmente el plan.

Ejemplo de criterios:

- ¿Afecta un proceso crítico?
- ¿La interrupción durará más de X horas?
- ¿Existe riesgo para la seguridad?

Si la respuesta es sí a ciertos puntos, se activa el plan.

5. Matriz de decisiones de recuperación de sistemas

Tabla clara que indica qué hacer ante fallas específicas:

Sistema	Escenario	Acción de recuperación
ERP	Cifrado por ransomware	Restaurar backup offline + procedimiento manual
Red local	Caída total	Activar enlace alterno + aislar segmentos
PLC	Falla abrupta	Cambiar por unidad de repuesto

Esto acelera decisiones y evita improvisaciones.

6. Lista de contactos y escalamiento

Incluye:

- Soporte técnico de proveedores
- Mantenimientos industriales
- Contactos de emergencia
- Líneas directas con responsables
- Escalamiento interno (a quién llamar si el responsable principal no responde)

Tener esta lista impresa accesible es vital cuando los sistemas están caídos.

7. Calendario anual de actividades del BCP

Un cronograma que marque:

- Pruebas planificadas
- Revisiones del BCP
- Rotación de respaldos

- Verificación de equipos de contingencia
- Capacitaciones

Sirve para evitar que las tareas rutinarias queden al olvido.

8. Catálogo de riesgos sectoriales con medidas sugeridas

Documento que presenta:

- Una lista de amenazas comunes en manufactura
- Los controles típicos que las mitigan

Esto ayuda a actualizar el plan y capacitar nuevos miembros del equipo.

Anexo D. Macros del instrumento de Excel propuesto en fase 3.

Con el objetivo de complementar la visión del cómo se puede ejecutar el diseño de la estrategia propuesta, también se diseñó un instrumento que facilita por medio de macros de Excel la ejecución de algunas de las tareas mas dispendiosas al momento de:

- Cruzar amenazas y activos para la construcción de escenarios de riesgo,
- Calificar los escenarios de riesgo,
- Visualizar la criticidad actual del negocio en cuestión de riesgos,
- Trasladar los riesgos para crear estrategias de continuidad.

Sin embargo, cada organización puede plantear sus propias macros, aportando en gran medida al proceso de generar heurísticas organizacionales y agilizar el proceso de actualización y análisis de acciones para las estrategias, y, por lo tanto, impulsar la evolución del BCP. De acuerdo con lo anterior, se comparten aquí las macros usadas para que sirva como material de apoyo, y para replicarlas, basta con: nombrar las hojas del libro de Excel tal como se hizo en las imágenes de evidencia, replicar la estructura, usar el gestor de nombre de Excel para nombrar los rangos de listas, y posteriormente, adaptarlo en las variables asociadas a nombres de hojas y listas de las macros compartidas. Después de realizar lo anterior, se podrán crear módulos en el gestor de macros de Excel y pegar código VB compartido y posteriormente asociar la funcionalidad a botones o formas creadas al interior de las hojas.

Modulo 1:

```
Option Explicit

'=========================================================
' 1) GENERAR ESCENARIOS EN P4_ER (desde P4_DefER)
'    - evita duplicados por Descripción (col B)
'    - asegura encabezados
'    - al final: formatea tabla + valida listas + pone descripciones
'=========================================================
Sub GenerarEscenariosISO27005()

    Const HOJA_MATRIZ As String = "P4_DefER"
    Const HOJA_ESCENARIOS As String = "P4_ER"
    Const HOJA_PARAM As String = "P4_Def"         ' (opcional: si no existe, no falla)
    Const MAX_ESCENARIOS As Long = 10000

    Dim wsMatriz As Worksheet
    Dim wsEsc As Worksheet
    Dim wsPar As Worksheet

    Dim lastRow As Long, lastCol As Long
    Dim r As Long, c As Long

    Dim amenaza As String         ' En P4_DefER: Col A (filas)
    Dim activo As String          ' En P4_DefER: Fila 1 (columnas)
    Dim descEscenario As String
    Dim posCoinc As Variant

    Dim lastRowEsc As Long
    Dim nextId As Long
    Dim numNuevos As Long

    Dim tablaParam As Range
    Dim vProb As Variant, vImp As Variant

    On Error GoTo ErrHandler

    Set wsMatriz = ThisWorkbook.Worksheets(HOJA_MATRIZ)
    Set wsEsc = ThisWorkbook.Worksheets(HOJA_ESCENARIOS)
```

```
' Hoja P4_Def es opcional (si no está, igual genera)
On Error Resume Next
Set wsPar = ThisWorkbook.Worksheets(HOJA_PARAM)
On Error GoTo 0
If Not wsPar Is Nothing Then
   Set tablaParam = wsPar.Range("A2").CurrentRegion
End If

Application.ScreenUpdating = False
Application.Calculation = xlCalculationManual

'--------------------------------
' Asegurar encabezados en P4_ER
'--------------------------------
With wsEsc
   If Application.WorksheetFunction.CountA(.Rows(1)) = 0 Then
      .Range("A1").Value = "ID"
      .Range("B1").Value = "Escenario de riesgo"
      .Range("C1").Value = "Probabilidad"
      .Range("D1").Value = "Descripción Probabilidad"
      .Range("E1").Value = "Impacto a la disponibilidad"
      .Range("F1").Value = "Descripción impacto"
      .Range("G1").Value = "Riesgo de impacto a la operación"
      .Range("H1").Value = "Controles actuales"
   End If
End With

'--------------------------------
' Calcular siguiente ID (R-###)
'--------------------------------
lastRowEsc = wsEsc.Cells(wsEsc.Rows.Count, "A").End(xlUp).Row
If lastRowEsc < 2 Then
   nextId = 1
Else
   nextId = ExtraerSiguienteConsecutivo(wsEsc.Cells(lastRowEsc, "A").Value)
   If nextId <= 0 Then nextId = (lastRowEsc) ' fallback
End If

'--------------------------------
```

```
    ' Recorrer matriz P4_DefER
    ' Formato esperado:
    '   - Amenazas en columna A (desde fila 2)
    '   - Activos en fila 1 (desde columna B)
    '   - Cruces con "X"
    '--------------------------------
    lastRow = wsMatriz.Cells(wsMatriz.Rows.Count, "A").End(xlUp).Row
    lastCol = wsMatriz.Cells(1, wsMatriz.Columns.Count).End(xlToLeft).Column
    numNuevos = 0

    For r = 2 To lastRow
        amenaza = Trim(CStr(wsMatriz.Cells(r, "A").Value))
        If amenaza <> "" Then

            For c = 2 To lastCol
                activo = Trim(CStr(wsMatriz.Cells(1, c).Value))

                If activo <> "" Then
                    If UCase$(Trim$(CStr(wsMatriz.Cells(r, c).Value))) = "X" Then

                        descEscenario = "La materialización de la amenaza '" & amenaza & _
                                        "' sobre el activo '" & activo & _
                                        "' podría afectar la disponibilidad del servicio y la operación del negocio."

                        ' Evitar duplicados comparando la descripción
                        posCoinc = Application.Match(descEscenario, wsEsc.Columns("B"), 0)

                        If IsError(posCoinc) Then
                            numNuevos = numNuevos + 1
                            If numNuevos > MAX_ESCENARIOS Then
                                MsgBox "Se alcanzó el límite de " & MAX_ESCENARIOS & " escenarios.",
vbExclamation
                                GoTo Salir
                            End If

                            ' Valores iniciales desde P4_Def (si existe)
                            vProb = ""
                            vImp = ""
                            If Not tablaParam Is Nothing Then
                                On Error Resume Next
                                vProb = Application.VLookup(amenaza, tablaParam, 2, False)
```

```
                    vImp = Application.VLookup(amenaza, tablaParam, 3, False)
                    On Error GoTo 0
                    If IsError(vProb) Then vProb = ""
                    If IsError(vImp) Then vImp = ""
                End If

                lastRowEsc = wsEsc.Cells(wsEsc.Rows.Count, "A").End(xlUp).Row + 1

                wsEsc.Cells(lastRowEsc, "A").Value = "R-" & Format(nextId, "000")
                nextId = nextId + 1

                wsEsc.Cells(lastRowEsc, "B").Value = descEscenario

                ' IMPORTANTE:
                ' Probabilidad/Impacto deben ser NUMÉRICOS (1..5),
                ' para que riesgo = C*E funcione.
                If IsNumeric(vProb) Then wsEsc.Cells(lastRowEsc, "C").Value = CLng(vProb)
                If IsNumeric(vImp) Then wsEsc.Cells(lastRowEsc, "E").Value = CLng(vImp)

              End If
            End If
          End If
        Next c
      End If
    Next r

    '--------------------------------
    ' Formato tabla + validaciones
    '--------------------------------
    Call FormatoTablaEscenarios(wsEsc)
    Call ConfigurarProbabilidadImpacto(wsEsc)

Salir:
    Application.ScreenUpdating = True
    Application.Calculation = xlCalculationAutomatic

    MsgBox "Escenarios nuevos generados: " & numNuevos, vbInformation
    Exit Sub
```

```
ErrHandler:
    Application.ScreenUpdating = True
    Application.Calculation = xlCalculationAutomatic
    MsgBox "Error en GenerarEscenariosISO27005: " & Err.Description, vbCritical

End Sub

'=========================================================
' Función: Extrae siguiente consecutivo desde "R-001"
'=========================================================
Private Function ExtraerSiguienteConsecutivo(ByVal idTexto As String) As Long
    On Error GoTo fin
    idTexto = Replace$(idTexto, "R-", "")
    idTexto = Replace$(idTexto, "r-", "")
    ExtraerSiguienteConsecutivo = CLng(Val(idTexto)) + 1
    Exit Function
fin:
    ExtraerSiguienteConsecutivo = 1
End Function

'=========================================================
' 2) FORMATO DE TABLA EN P4_ER
'    - Compatible (sin argumentos nombrados)
'    - Crea/rehace ListObject "TablaEscenarios"
'=========================================================
Sub FormatoTablaEscenarios(ws As Worksheet)

    Dim lastRow As Long
    Dim lastCol As Long
    Dim lo As ListObject
    Dim tblRng As Range

    lastRow = ws.Cells(ws.Rows.Count, "A").End(xlUp).Row
    lastCol = ws.Cells(1, ws.Columns.Count).End(xlToLeft).Column
    If lastCol < 8 Then lastCol = 8
    If lastRow < 1 Then Exit Sub

    Set tblRng = ws.Range(ws.Cells(1, 1), ws.Cells(lastRow, lastCol))

    ' Quitar tablas existentes (si hay)
    On Error Resume Next
```

```
    For Each lo In ws.ListObjects
        lo.Unlist
    Next lo
    On Error GoTo 0

    Set lo = ws.ListObjects.add(xlSrcRange, tblRng, , xlYes)
    lo.Name = "TablaEscenarios"
    lo.TableStyle = "TableStyleMedium2"

    With ws.Range(ws.Cells(1, 1), ws.Cells(1, 8))
        .Font.Bold = True
        .Interior.Color = RGB(200, 220, 255)
        .HorizontalAlignment = xlCenter
        .VerticalAlignment = xlCenter
    End With

    ws.Columns("A:H").AutoFit
    ws.Columns("B").ColumnWidth = 80
    ws.Columns("B").WrapText = True
    ws.Columns("D").ColumnWidth = 35
    ws.Columns("F").ColumnWidth = 35

End Sub

'============================================================
' 3) LISTAS + DESCRIPCIONES (P4_L)
'    - Validación usa Nivel (col 1) para guardar números
'    - Descripción muestra RANGOS (col 2)
'============================================================
Sub ConfigurarProbabilidadImpacto(ws As Worksheet)

    Dim lastRow As Long
    Dim rngProb As Range, rngImp As Range
    Dim rngDescProb As Range, rngDescImp As Range
    Dim rngRiesgo As Range

    lastRow = ws.Cells(ws.Rows.Count, "A").End(xlUp).Row
    If lastRow < 2 Then Exit Sub
```

```
    Set rngProb = ws.Range("C2:C" & lastRow)
    Set rngDescProb = ws.Range("D2:D" & lastRow)
    Set rngImp = ws.Range("E2:E" & lastRow)
    Set rngDescImp = ws.Range("F2:F" & lastRow)
    Set rngRiesgo = ws.Range("G2:G" & lastRow)

    '--------------------------------
    ' Validación: lista de NIVELES (números)
    ' Usamos la tabla nombrada:
    '   T_Probabilidad[...]
    '   T_ImpactoDisponibilidad[...]
    ' y si no existe, caemos a L_NivelProbabilidad/L_NivelImpacto
    '--------------------------------
    On Error Resume Next

    With rngProb.Validation
        .Delete
        .add xlValidateList, xlValidAlertStop, xlBetween, "=T_Probabilidad[Nivel]"
        If Err.Number <> 0 Then
            Err.Clear
            ' fallback: nombre existente del libro
            .add xlValidateList, xlValidAlertStop, xlBetween,
"=OFFSET(L_NivelProbabilidad,1,0,ROWS(L_NivelProbabilidad)-1,1)"
        End If
        .IgnoreBlank = True
        .InCellDropdown = True
    End With
    With rngImp.Validation
        .Delete
        .add xlValidateList, xlValidAlertStop, xlBetween, "=T_ImpactoDisponibilidad[Nivel]"
        If Err.Number <> 0 Then
            Err.Clear
            .add xlValidateList, xlValidAlertStop, xlBetween,
"=OFFSET(L_NivelImpacto,1,0,ROWS(L_NivelImpacto)-1,1)"
        End If
        .IgnoreBlank = True
        .InCellDropdown = True
    End With
    On Error GoTo 0
    '--------------------------------
    ' Descripción = columna RANGOS (2)
```

```
    ' usando L_NivelProbabilidad/L_NivelImpacto
    '-------------------------------
    rngDescProb.Formula = "=IF(C2="""","""",VLOOKUP(C2,L_NivelProbabilidad,2,FALSE))"
    rngDescImp.Formula = "=IF(E2="""","""",VLOOKUP(E2,L_NivelImpacto,2,FALSE))"
    ' Riesgo = P x I
    rngRiesgo.Formula = "=IF(OR(C2="""",E2="""")),"""",C2*E2)"
End Sub
```

Modulo 2:

```
Option Explicit

' ========================================================
' PASO 4 - Generar Matriz + Distribución + Gráfica
' Matriz: B15:H22
' Columna I: espacio
' Distribución: J15:L19
' Gráfica: J21 (a la derecha)
' Datos: hoja P4_ER (A=ID, C=Prob, E=Impacto)
' Listas (para textos): Nombres L_NivelProbabilidad y L_NivelImpacto
' ========================================================
Public Sub Paso4_GenerarMatrizDistribucion()

    Const HOJA_DATOS As String = "P4_ER"
    Const HOJA_PASO As String = "Paso 4"

    Const ROW_TITULO As Long = 15
    Const ROW_IMP_TEXTO As Long = 16
    Const ROW_IMP_VAL As Long = 17
    Const ROW_PROB_5 As Long = 18

    Const COL_PROB_TEXTO As Long = 2 'B
    Const COL_PROB_VALOR As Long = 3 'C
    Const COL_IMP_1 As Long = 4      'D

    Dim wsData As Worksheet, wsPaso As Worksheet
    Dim rngProb As Range, rngImp As Range
    Dim lastRow As Long, r As Long
    Dim probVal As Variant, impVal As Variant
    Dim prob As Long, impacto As Long
    Dim filaM As Long, colM As Long
    Dim txtID As String, txtActual As String
    Dim cntA As Long, cntT As Long, cntI As Long, cntInadm As Long
    Dim zona As Long

    On Error Resume Next
    Set wsData = ThisWorkbook.Worksheets(HOJA_DATOS)
    Set wsPaso = ThisWorkbook.Worksheets(HOJA_PASO)
    On Error GoTo 0
```

```
    If wsData Is Nothing Or wsPaso Is Nothing Then
        MsgBox "No encuentro las hojas '" & HOJA_DATOS & "' o '" & HOJA_PASO & "'.", vbCritical
        Exit Sub
    End If

    Application.ScreenUpdating = False

    ' 1) Limpiar zona (NUEVA)
    Paso4_LimpiarZona wsPaso

    ' 2) Obtener rangos por nombre (si existen)
    Set rngProb = Nothing: Set rngImp = Nothing
    On Error Resume Next
    Set rngProb = ThisWorkbook.Names("L_NivelProbabilidad").RefersToRange
    Set rngImp = ThisWorkbook.Names("L_NivelImpacto").RefersToRange
    On Error GoTo 0

    ' 3) Encabezados (igual texto)
    With wsPaso.Range(wsPaso.Cells(ROW_TITULO, COL_IMP_1), wsPaso.Cells(ROW_TITULO,
COL_IMP_1 + 4))
        .Merge
        .Value = "Consecuencia"
        .HorizontalAlignment = xlCenter
        .VerticalAlignment = xlCenter
        .Font.Bold = True
        .Interior.Color = RGB(80, 80, 80)
        .Font.Color = RGB(255, 255, 0)
    End With

    With wsPaso.Range(wsPaso.Cells(ROW_TITULO, COL_PROB_TEXTO),
wsPaso.Cells(ROW_TITULO, COL_PROB_VALOR))
        .Merge
        .Value = "Probabilidad"
        .HorizontalAlignment = xlCenter
        .VerticalAlignment = xlCenter
        .Font.Bold = True
        .Interior.Color = RGB(80, 80, 80)
        .Font.Color = RGB(255, 255, 0)
```

```
    End With

    wsPaso.Cells(ROW_IMP_TEXTO, COL_PROB_VALOR).Value = "valor"
    wsPaso.Cells(ROW_IMP_TEXTO, COL_PROB_VALOR).HorizontalAlignment = xlCenter
    wsPaso.Cells(ROW_IMP_TEXTO, COL_PROB_VALOR).Font.Bold = True

    ' 4) Impacto (texto + número)
    For impacto = 1 To 5
        wsPaso.Cells(ROW_IMP_VAL, COL_IMP_1 + impacto - 1).Value = impacto
        wsPaso.Cells(ROW_IMP_VAL, COL_IMP_1 + impacto - 1).HorizontalAlignment = xlCenter
        wsPaso.Cells(ROW_IMP_VAL, COL_IMP_1 + impacto - 1).Font.Bold = True

        wsPaso.Cells(ROW_IMP_TEXTO, COL_IMP_1 + impacto - 1).HorizontalAlignment = xlCenter
        wsPaso.Cells(ROW_IMP_TEXTO, COL_IMP_1 + impacto - 1).Font.Bold = True

        If Not rngImp Is Nothing Then
            wsPaso.Cells(ROW_IMP_TEXTO, COL_IMP_1 + impacto - 1).Value =
Paso4_VLookupSafe(impacto, rngImp, 2)
        Else
            wsPaso.Cells(ROW_IMP_TEXTO, COL_IMP_1 + impacto - 1).Value = Choose(impacto,
"Insignificante", "Menor", "Intermedio", "Mayor", "Superior")
        End If
    Next impacto

    ' 5) Probabilidad (texto + valor) 5..1
    Dim probLoop As Long
    For probLoop = 5 To 1 Step -1
        filaM = ROW_PROB_5 + (5 - probLoop)

        wsPaso.Cells(filaM, COL_PROB_VALOR).Value = probLoop
        wsPaso.Cells(filaM, COL_PROB_VALOR).HorizontalAlignment = xlCenter
        wsPaso.Cells(filaM, COL_PROB_VALOR).Font.Bold = True

        wsPaso.Cells(filaM, COL_PROB_TEXTO).HorizontalAlignment = xlCenter
        wsPaso.Cells(filaM, COL_PROB_TEXTO).Font.Bold = True

        If Not rngProb Is Nothing Then
            wsPaso.Cells(filaM, COL_PROB_TEXTO).Value = Paso4_VLookupSafe(probLoop, rngProb, 2)
        Else
            wsPaso.Cells(filaM, COL_PROB_TEXTO).Value = Choose(probLoop, "Raro", "Improbable",
"Posible", "Probable", "Casi seguro")
```

```
    End If
Next probLoop

' 6) Pintar colores base
Dim i As Long, j As Long
For i = 1 To 5          ' prob
    For j = 1 To 5      ' impacto
        filaM = ROW_PROB_5 + (5 - i)
        colM = COL_IMP_1 + (j - 1)

        zona = Paso4_ZonaSegunMatriz(i, j)

        With wsPaso.Cells(filaM, colM)
            .Interior.Color = Paso4_ColorZona(zona)
            .HorizontalAlignment = xlCenter
            .VerticalAlignment = xlCenter
            .WrapText = True
            .Font.Bold = True
        End With
    Next j
Next i

' 7) Ubicar riesgos desde P4_ER (A=ID, C=Prob, E=Impacto)
lastRow = wsData.Cells(wsData.Rows.Count, "A").End(xlUp).Row

For r = 2 To lastRow
    probVal = wsData.Cells(r, "C").Value
    impVal = wsData.Cells(r, "E").Value

    If IsNumeric(probVal) And IsNumeric(impVal) Then
        prob = CLng(probVal)
        impacto = CLng(impVal)

        If prob >= 1 And prob <= 5 And impacto >= 1 And impacto <= 5 Then

            filaM = ROW_PROB_5 + (5 - prob)
            colM = COL_IMP_1 + (impacto - 1)

            txtID = CStr(wsData.Cells(r, "A").Value)
```

```
            txtActual = CStr(wsPaso.Cells(filaM, colM).Value)
            If txtActual = "" Then
               wsPaso.Cells(filaM, colM).Value = txtID
            Else
               wsPaso.Cells(filaM, colM).Value = txtActual & Chr(10) & txtID
            End If

            zona = Paso4_ZonaSegunMatriz(prob, impacto)
            Select Case zona
               Case 1: cntA = cntA + 1
               Case 2: cntT = cntT + 1
               Case 3: cntI = cntI + 1
               Case Else: cntInadm = cntInadm + 1
            End Select

         End If
      End If
   Next r

   ' 8) Bordes y tamaños
   Paso4_FormatearBordes wsPaso

   ' 9) Distribución + gráfico
   Paso4_DistribucionYGrafico_ConEspacio wsPaso, cntA, cntT, cntI, cntInadm

   Application.ScreenUpdating = True

End Sub

' ------------------------------------------------------------
' LIMPIAR ZONA (matriz + distribución + gráficos)
' ------------------------------------------------------------
Private Sub Paso4_LimpiarZona(ByVal ws As Worksheet)

   On Error Resume Next
   ws.Range("B15:H22").UnMerge
   ws.Range("J15:L19").UnMerge
   On Error GoTo 0

   ws.Range("B15:H22").Clear
```

```
    ws.Range("B15:H22").Interior.ColorIndex = xlNone

    ws.Range("J15:L19").Clear
    ws.Range("J15:L19").Interior.ColorIndex = xlNone

    Dim ch As ChartObject
    For Each ch In ws.ChartObjects
        ch.Delete
    Next ch

End Sub

' ------------------------------------------------------------
' FORMATO BORDES / ANCHOS
' ------------------------------------------------------------
Private Sub Paso4_FormatearBordes(ByVal ws As Worksheet)

    With ws.Range("B15:H22")
        .Borders.LineStyle = xlContinuous
        .Borders.Weight = xlThin
        .Borders.Color = RGB(0, 0, 0)
        .Font.Name = "Calibri"
        .Font.Size = 11
    End With

    ws.Columns("B").ColumnWidth = 16
    ws.Columns("C").ColumnWidth = 8
    ws.Columns("D").ColumnWidth = 14
    ws.Columns("E").ColumnWidth = 14
    ws.Columns("F").ColumnWidth = 14
    ws.Columns("G").ColumnWidth = 14
    ws.Columns("H").ColumnWidth = 14

    ws.Columns("I").ColumnWidth = 3 'espacio

    ws.Columns("J").ColumnWidth = 14
    ws.Columns("K").ColumnWidth = 10
    ws.Columns("L").ColumnWidth = 12
```

```
    With ws.Range("J15:L19")
        .Borders.LineStyle = xlContinuous
        .Borders.Weight = xlThin
        .Borders.Color = RGB(0, 0, 0)
        .Font.Name = "Calibri"
        .Font.Size = 11
    End With

End Sub

' ------------------------------------------------------------
' VLOOKUP SEGURO
' ------------------------------------------------------------
Private Function Paso4_VLookupSafe(ByVal key As Long, ByVal rng As Range, ByVal colIndex As
Long) As String
    On Error GoTo Fallback
    Paso4_VLookupSafe = CStr(Application.WorksheetFunction.VLookup(key, rng, colIndex, False))
    Exit Function
Fallback:
    Paso4_VLookupSafe = ""
End Function

' ------------------------------------------------------------
' 1=Aceptable(verde) 2=Tolerable(amarillo) 3=Inaceptable(naranja) 4=Inadmisible(rojo)
' ------------------------------------------------------------
Private Function Paso4_ZonaSegunMatriz(ByVal prob As Long, ByVal impacto As Long) As Long

    Select Case prob
        Case 5
            Select Case impacto
                Case 1: Paso4_ZonaSegunMatriz = 2
                Case 2: Paso4_ZonaSegunMatriz = 3
                Case Else: Paso4_ZonaSegunMatriz = 4
            End Select

        Case 4
            Select Case impacto
                Case 1: Paso4_ZonaSegunMatriz = 2
                Case 2, 3: Paso4_ZonaSegunMatriz = 3
                Case Else: Paso4_ZonaSegunMatriz = 4
            End Select
```

```
    Case 3
      Select Case impacto
        Case 1: Paso4_ZonaSegunMatriz = 1
        Case 2: Paso4_ZonaSegunMatriz = 2
        Case 3, 4: Paso4_ZonaSegunMatriz = 3
        Case Else: Paso4_ZonaSegunMatriz = 4
      End Select

    Case 2
      Select Case impacto
        Case 1, 2: Paso4_ZonaSegunMatriz = 1
        Case 3: Paso4_ZonaSegunMatriz = 2
        Case Else: Paso4_ZonaSegunMatriz = 3
      End Select

    Case 1
      Select Case impacto
        Case 1, 2: Paso4_ZonaSegunMatriz = 1
        Case Else: Paso4_ZonaSegunMatriz = 2
      End Select

    Case Else
      Paso4_ZonaSegunMatriz = 2
  End Select

End Function

Private Function Paso4_ColorZona(ByVal zona As Long) As Long
  Select Case zona
    Case 1: Paso4_ColorZona = RGB(0, 255, 0)       ' Verde
    Case 2: Paso4_ColorZona = RGB(255, 255, 0)     ' Amarillo
    Case 3: Paso4_ColorZona = RGB(255, 165, 0)     ' Naranja
    Case Else: Paso4_ColorZona = RGB(255, 0, 0)    ' Rojo
  End Select
End Function

' ------------------------------------------------------
' DISTRIBUCIÓN + GRÁFICO (J15:L19) + COLORES
```

```
' ------------------------------------------------------------
Private Sub Paso4_DistribucionYGrafico_ConEspacio(ByVal ws As Worksheet, ByVal cntA As Long,
ByVal cntT As Long, ByVal cntI As Long, ByVal cntInadm As Long)

    Dim total As Long
    total = cntA + cntT + cntI + cntInadm

    ws.Range("J15").Value = "ZONA"
    ws.Range("K15").Value = "%"
    ws.Range("L15").Value = "Total riesgos"

    ws.Range("J15:L15").Font.Bold = True
    ws.Range("J15:L15").HorizontalAlignment = xlCenter

    ws.Range("J16").Value = "Aceptable"
    ws.Range("J17").Value = "Tolerable"
    ws.Range("J18").Value = "Inaceptable"
    ws.Range("J19").Value = "Inadmisible"

    ws.Range("L16").Value = cntA
    ws.Range("L17").Value = cntT
    ws.Range("L18").Value = cntI
    ws.Range("L19").Value = cntInadm

    If total = 0 Then
        ws.Range("K16:K19").Value = 0
    Else
        ws.Range("K16").Value = cntA / total
        ws.Range("K17").Value = cntT / total
        ws.Range("K18").Value = cntI / total
        ws.Range("K19").Value = cntInadm / total
    End If

    ws.Range("K16:K19").NumberFormat = "0.00%"

    ' Colores consistentes con matriz
    ws.Range("J16:L16").Interior.Color = RGB(0, 255, 0)
    ws.Range("J17:L17").Interior.Color = RGB(255, 255, 0)
    ws.Range("J18:L18").Interior.Color = RGB(255, 165, 0)
    ws.Range("J19:L19").Interior.Color = RGB(255, 0, 0)
```

```
  ws.Range("J15:L19").HorizontalAlignment = xlCenter
  ws.Range("J15:L19").Borders.LineStyle = xlContinuous

  ' Crear gráfico
  Dim ch As ChartObject
  Set ch = ws.ChartObjects.add(ws.Range("J21").Left, ws.Range("J21").Top, 700, 380)
  ch.Name = "Grafica_Distribucion_Riesgos"

  With ch.Chart
     .ChartType = xlPie
     .HasTitle = True
     .ChartTitle.Text = "Distribución de riesgos"

     .SeriesCollection.NewSeries
     .SeriesCollection(1).Values = ws.Range("L16:L19")
     .SeriesCollection(1).XValues = ws.Range("J16:J19")
     .SeriesCollection(1).ApplyDataLabels
     .SeriesCollection(1).DataLabels.ShowPercentage = True
     .SeriesCollection(1).DataLabels.ShowCategoryName = True

     ' Fuerza colores iguales a la tabla (y por ende a la matriz)
     With .SeriesCollection(1)
        If .Points.Count >= 4 Then
           .Points(1).Format.Fill.ForeColor.RGB = RGB(0, 255, 0)     'Aceptable
           .Points(2).Format.Fill.ForeColor.RGB = RGB(255, 255, 0)   'Tolerable
           .Points(3).Format.Fill.ForeColor.RGB = RGB(255, 165, 0)   'Inaceptable
           .Points(4).Format.Fill.ForeColor.RGB = RGB(255, 0, 0)     'Inadmisible
        End If
     End With

  End With

End Sub
```

Modulo 3:

```
Option Explicit

Sub ResetearEscenarios_P4_ER()

   Const HOJA_ESCENARIOS As String = "P4_ER"
   Const HOJA_MATRIZ As String = "P4_DefER"   ' amenazas y activos

   Dim wsEsc As Worksheet
   Dim wsBackup As Worksheet
   Dim wsRetorno As Worksheet
   Dim resp As VbMsgBoxResult
   Dim nombreBackup As String
   Dim lo As ListObject

   Set wsEsc = ThisWorkbook.Worksheets(HOJA_ESCENARIOS)
   Set wsRetorno = ThisWorkbook.Worksheets(HOJA_MATRIZ)

   '---------------------------------
   ' Validar si la hoja está vacía
   '---------------------------------
   If Application.WorksheetFunction.CountA(wsEsc.Cells) = 0 Then
      MsgBox _
         "La hoja '" & HOJA_ESCENARIOS & "' ya está vacía." & vbCrLf & _
         "No se realizó ningún borrado ni se creó respaldo.", _
         vbInformation, _
         "Sin acción requerida"

      wsRetorno.Activate
      wsRetorno.Range("A1").Select
      Exit Sub
   End If

   '---------------------------------
   ' Confirmación 1
   '---------------------------------
   resp = MsgBox( _
      "Se va a borrar TODO el contenido de la hoja '" & HOJA_ESCENARIOS & "'." & vbCrLf & _
      "¿Desea continuar?", _
      vbExclamation + vbYesNo, _
```

```
    "Confirmación")

If resp <> vbYes Then Exit Sub

'----------------------------------
' Confirmación 2
'----------------------------------
resp = MsgBox( _
    "Se creará un respaldo antes de borrar la información." & vbCrLf & _
    "¿Confirma que desea continuar?", _
    vbCritical + vbYesNo, _
    "Confirmación final")

If resp <> vbYes Then Exit Sub

Application.ScreenUpdating = False
Application.DisplayAlerts = False

'----------------------------------
' Crear respaldo
'----------------------------------
nombreBackup = "P4_ER_Backup_" & Format(Now, "yyyymmdd_hhmmss")
wsEsc.Copy After:=Sheets(Sheets.Count)
Set wsBackup = ActiveSheet
wsBackup.Name = nombreBackup
wsBackup.Visible = xlSheetHidden

'----------------------------------
' Limpiar hoja P4_ER
'----------------------------------
For Each lo In wsEsc.ListObjects
    lo.Unlist
Next lo
wsEsc.Cells.Clear

Application.DisplayAlerts = True
Application.ScreenUpdating = True

'----------------------------------
```

```
    ' Volver a la hoja de trabajo
    '---------------------------------
    wsRetorno.Activate
    wsRetorno.Range("A1").Select

    MsgBox _
        "Escenarios eliminados correctamente." & vbCrLf & _
        "Respaldo creado: " & nombreBackup, _
        vbInformation

End Sub
```

Modulo 4:

```
Option Explicit

'=========================
' Configuración
'=========================
Private Const HOJA_P4 As String = "P4_ER"
Private Const HOJA_P5 As String = "Paso 5"
Private Const HOJA_CAT As String = "P5_L"

Private Const TABLA_P4 As String = "TablaEscenarios"
Private Const TABLA_P5 As String = "PlanContinuidad"
Private Const TABLA_CAT As String = "L_Catalogo_Sugerencias"

' Encabezados Paso 5 (BCP)
Private Const H_ID As String = "ID Riesgo"
Private Const H_ID_BCP As String = "ID BCP"
Private Const H_ESC As String = "Escenario"
Private Const H_TIPO_RIESGO As String = "Tipo de riesgo"
Private Const H_IMP_MAP As String = "Impacto a la disponibilidad mapeado en el escenario"
Private Const H_TIPO_INT As String = "Tipo de interrupción a controlar"
Private Const H_CTRL_SUG As String = "Controles mínimos sugeridos"
Private Const H_CTRL_NEG As String = "Controles definidos por el negocio"

' Encabezados Paso 4 (TablaEscenarios)
Private Const H4_ID As String = "ID"
Private Const H4_ESC As String = "Escenario de riesgo"
Private Const H4_RIESGO As String = "Riesgo de impacto a la operación"
Private Const H4_IMP_MAP As String = "Impacto a la disponibilidad mapeado por el negocio" '
opcional

' Catálogo (P5_L)
Private Const HC_TIPO As String = "Tipo_Interrupcion"
Private Const HC_CTRL As String = "Controles_Minimos"

' Nombre dinámico para validación (Administrador de nombres)
Private Const NM_TIPO As String = "NM_P5_TipoInterrupcion"
```

```
Public Const P5_HEADER_ROW As Long = 8
Public Const P5_START_COL As Long = 2

'============================================================
' MACRO PRINCIPAL (botón: Riesgos para BPC / Generar Paso 5)
'============================================================
Public Sub P5_GenerarDesdePaso4()

    Dim ws4 As Worksheet, ws5 As Worksheet, wsCat As Worksheet
    Dim lo4 As ListObject, lo5 As ListObject, loCat As ListObject

    On Error GoTo ErrHandler

    Set ws4 = ThisWorkbook.Worksheets(HOJA_P4)
    Set ws5 = ThisWorkbook.Worksheets(HOJA_P5)
    Set wsCat = ThisWorkbook.Worksheets(HOJA_CAT)

    Application.ScreenUpdating = False
    Application.Calculation = xlCalculationManual
    Application.EnableEvents = False

    EnsurePlanContinuidad ws5
    Set lo5 = ws5.ListObjects(TABLA_P5)

    Set lo4 = ws4.ListObjects(TABLA_P4)

    Set loCat = wsCat.ListObjects(TABLA_CAT)

    AsegurarNombreCatalogo loCat

    If Not BackupSiTieneDatos(ws5, lo5) Then GoTo Salir

    LimpiarTabla lo5
    PoblarPaso5 lo4, lo5

    AsegurarValidacionTipo ws5
    AplicarEstetica lo5
    P5_RestaurarAvisosMasivo

Salir:
    Application.EnableEvents = True
```

```
    Application.Calculation = xlCalculationAutomatic
    Application.ScreenUpdating = True

    ws5.Activate
    If ws5.ListObjects(TABLA_P5).ListRows.Count > 0 Then
        ws5.ListObjects(TABLA_P5).DataBodyRange.Cells(1, 1).Select
    End If
    Exit Sub

ErrHandler:
    Application.EnableEvents = True
    Application.Calculation = xlCalculationAutomatic
    Application.ScreenUpdating = True
    ws5.Activate
    MsgBox "Error al generar Paso 5: " & Err.Description, vbCritical
End Sub

'============================================================
' Duplicar fila (para varios tipos de interrupción)
'============================================================
Public Sub P5_DuplicarFila()
    Dim ws As Worksheet, lo As ListObject
    Dim cell As Range, rowIndex As Long

    Set ws = ThisWorkbook.Worksheets(HOJA_P5)
    Set lo = ws.ListObjects(TABLA_P5)

    If lo Is Nothing Or lo.DataBodyRange Is Nothing Then
        MsgBox "No hay filas para duplicar.", vbInformation
        ws.Activate
        Exit Sub
    End If

    Set cell = ActiveCell
    If cell Is Nothing Then Exit Sub
    If Intersect(cell, lo.DataBodyRange) Is Nothing Then
        MsgBox "Ubícate dentro de una fila de la tabla para duplicarla.", vbExclamation
        ws.Activate
        Exit Sub
```

```
    End If

    rowIndex = cell.Row - lo.DataBodyRange.Row + 1
    If rowIndex < 1 Or rowIndex > lo.ListRows.Count Then Exit Sub

    Application.ScreenUpdating = False
    Application.EnableEvents = False

    lo.ListRows.add Position:=rowIndex + 1
    lo.ListRows(rowIndex).Range.Copy
    lo.ListRows(rowIndex + 1).Range.PasteSpecial xlPasteValues
    Application.CutCopyMode = False

    lo.ListRows(rowIndex + 1).Range.Cells(1, lo.ListColumns(H_ID_BCP).Index).Value = "BCP-" &
Format$(P5_SiguienteBCP(lo), "000")

    ' limpiar solo campos dependientes
    lo.ListRows(rowIndex + 1).Range.Cells(1, lo.ListColumns(H_TIPO_INT).Index).Value =
vbNullString
    lo.ListRows(rowIndex + 1).Range.Cells(1, lo.ListColumns(H_CTRL_SUG).Index).Value =
vbNullString

    AsegurarValidacionTipo ws
    P5_RestaurarAvisosMasivo

    Application.EnableEvents = True
    Application.ScreenUpdating = True

    ws.Activate
    lo.ListRows(rowIndex + 1).Range.Cells(1, lo.ListColumns(H_TIPO_INT).Index).Select
End Sub

'============================================================
' Restaurar desde backup (sin cambiar nombre de tabla)
'============================================================
Public Sub P5_RestaurarDesdeBackup()
    Dim ws5 As Worksheet, lo5 As ListObject, sh As Worksheet
    Dim backups() As String, n As Long, i As Long
    Dim lista As String, sel As Variant
    Dim src As Range, arr As Variant
    Dim rowsData As Long, colsData As Long
```

```
Set ws5 = ThisWorkbook.Worksheets(HOJA_P5)
EnsurePlanContinuidad ws5
Set lo5 = ws5.ListObjects(TABLA_P5)

n = 0
For Each sh In ThisWorkbook.Worksheets
   If LCase$(Left$(sh.Name, Len("Paso5_Backup_"))) = LCase$("Paso5_Backup_") Then
      n = n + 1
      ReDim Preserve backups(1 To n)
      backups(n) = sh.Name
   End If
Next sh

If n = 0 Then
   MsgBox "No hay backups de tablas del BCP disponibles.", vbInformation
   ws5.Activate
   Exit Sub
End If

lista = "Backups disponibles:" & vbCrLf & vbCrLf
For i = 1 To n
   lista = lista & i & ") " & backups(i) & vbCrLf
Next i

sel = InputBox(lista & vbCrLf & "Digite el número a restaurar:", "Restaurar tabla BCP anterior")
If sel = "" Then Exit Sub
If Not IsNumeric(sel) Then
   MsgBox "Selección inválida.", vbCritical
   Exit Sub
End If

i = CLng(sel)
If i < 1 Or i > n Then
   MsgBox "Selección fuera de rango.", vbCritical
   Exit Sub
End If

Set sh = ThisWorkbook.Worksheets(backups(i))
```

```
Set src = sh.Range("A1").CurrentRegion
If src.Rows.Count < 2 Then
   MsgBox "El backup seleccionado no tiene datos válidos.", vbExclamation
   Exit Sub
End If

arr = src.Value
colsData = src.Columns.Count
rowsData = src.Rows.Count - 1

Application.ScreenUpdating = False
Application.EnableEvents = False

LimpiarTabla lo5

If rowsData > 0 Then
   Dim k As Long
   For k = 1 To rowsData
      lo5.ListRows.add
   Next k

   Dim outArr() As Variant, r As Long, c As Long
   If colsData = 7 And lo5.ListColumns.Count = 8 Then
      ReDim outArr(1 To rowsData, 1 To 8)
      For r = 1 To rowsData
         outArr(r, 1) = arr(r + 1, 1)
         outArr(r, 2) = vbNullString
         For c = 2 To 7
            outArr(r, c + 1) = arr(r + 1, c)
         Next c
      Next r
      lo5.DataBodyRange.Cells(1, 1).Resize(rowsData, 8).Value = outArr
   Else
      ReDim outArr(1 To rowsData, 1 To colsData)
      For r = 1 To rowsData
         For c = 1 To colsData
            outArr(r, c) = arr(r + 1, c)
         Next c
      Next r
      lo5.DataBodyRange.Cells(1, 1).Resize(rowsData, colsData).Value = outArr
   End If
```

```
    End If

    AsegurarValidacionTipo ws5
    AplicarEstetica lo5
    P5_RestaurarAvisosMasivo

    Application.EnableEvents = True
    Application.ScreenUpdating = True

    ws5.Activate
    If lo5.ListRows.Count > 0 Then lo5.DataBodyRange.Cells(1, 1).Select

    MsgBox "Paso 5 restaurado desde: " & sh.Name, vbInformation
End Sub

'============================================================
' BUSCAR: Tipo Interrupción -> Controles sugeridos
'============================================================
Public Function P5_BuscarControlSugerido(ByVal tipo As String) As String
    Dim wsCat As Worksheet, loCat As ListObject
    Dim idxTipo As Long, idxCtrl As Long
    Dim i As Long, vTipo As String

    tipo = Trim$(tipo)
    If tipo = vbNullString Then
        P5_BuscarControlSugerido = vbNullString
        Exit Function
    End If

    Set wsCat = ThisWorkbook.Worksheets(HOJA_CAT)
    Set loCat = wsCat.ListObjects(TABLA_CAT)

    idxTipo = loCat.ListColumns(HC_TIPO).Index
    idxCtrl = loCat.ListColumns(HC_CTRL).Index

    For i = 1 To loCat.ListRows.Count
        vTipo = Trim$(CStr(loCat.DataBodyRange(i, idxTipo).Value))
        If StrComp(vTipo, tipo, vbTextCompare) = 0 Then
            P5_BuscarControlSugerido = Trim$(CStr(loCat.DataBodyRange(i, idxCtrl).Value))
```

```
        Exit Function
      End If
    Next i

    P5_BuscarControlSugerido = vbNullString
End Function

'============================================================
' Tabla Paso 5: crear/asegurar
'============================================================
Private Sub EnsurePlanContinuidad(ws5 As Worksheet)
    Dim lo As ListObject

    On Error Resume Next
    Set lo = ws5.ListObjects(TABLA_P5)
    On Error GoTo 0

    If Not lo Is Nothing Then
      If Not ColExiste(lo, H_ID_BCP) Then
        lo.ListColumns.add Position:=lo.ListColumns(H_ID).Index + 1
      End If
      EscribirEncabezados ws5, lo.HeaderRowRange.Row, lo.HeaderRowRange.Column
      CentrarEncabezados lo
      Exit Sub
    End If

    Dim headerRow As Long, startCol As Long
    Dim rng As Range

    headerRow = P5_HEADER_ROW
    startCol = P5_START_COL

    Set rng = ws5.Range(ws5.Cells(headerRow, startCol), ws5.Cells(headerRow + 1, startCol + 7))

    Do While RangoSeSuperponeConAlgunaTabla(ws5, rng)
      headerRow = headerRow + 1
      Set rng = ws5.Range(ws5.Cells(headerRow, startCol), ws5.Cells(headerRow + 1, startCol + 7))
    Loop

    EscribirEncabezados ws5, headerRow, startCol
```

```
    Set lo = ws5.ListObjects.add(xlSrcRange, rng, , xlYes)
    lo.Name = TABLA_P5
    lo.TableStyle = "TableStyleMedium2"
    CentrarEncabezados lo
End Sub

Private Sub EscribirEncabezados(ws As Worksheet, ByVal r As Long, ByVal c As Long)
    ws.Cells(r, c + 0).Value = H_ID
    ws.Cells(r, c + 1).Value = H_ID_BCP
    ws.Cells(r, c + 2).Value = H_ESC
    ws.Cells(r, c + 3).Value = H_TIPO_RIESGO
    ws.Cells(r, c + 4).Value = H_IMP_MAP
    ws.Cells(r, c + 5).Value = H_TIPO_INT
    ws.Cells(r, c + 6).Value = H_CTRL_SUG
    ws.Cells(r, c + 7).Value = H_CTRL_NEG
End Sub

Private Sub CentrarEncabezados(lo As ListObject)
    With lo.HeaderRowRange
        .HorizontalAlignment = xlCenter
        .VerticalAlignment = xlCenter
        .WrapText = True
    End With
End Sub

Private Function P5_SiguienteBCP(lo As ListObject) As Long
    Dim idx As Long, i As Long
    Dim v As String, p As Long, n As Long, mx As Long

    mx = 0
    idx = lo.ListColumns(H_ID_BCP).Index

    If lo.DataBodyRange Is Nothing Then
        P5_SiguienteBCP = 1
        Exit Function
    End If

    For i = 1 To lo.ListRows.Count
        v = Trim$(CStr(lo.DataBodyRange(i, idx).Value))
```

```
        If v <> vbNullString Then
            p = InStrRev(v, "-")
            If p > 0 And p < Len(v) Then
                On Error Resume Next
                n = CLng(Mid$(v, p + 1))
                If Err.Number <> 0 Then
                    Err.Clear
                    n = 0
                End If
                On Error GoTo 0
                If n > mx Then mx = n
            End If
        End If
    Next i

    P5_SiguienteBCP = mx + 1
End Function

'============================================================
' Poblar Paso 5 desde Paso 4
'============================================================
Private Sub PoblarPaso5(lo4 As ListObject, lo5 As ListObject)
    Dim i As Long, tr As String
    Dim idxID As Long, idxEsc As Long, idxRiesgo As Long
    Dim tieneImpMap As Boolean, idxImpMap As Long
    Dim nextBCP As Long

    idxID = lo4.ListColumns(H4_ID).Index
    idxEsc = lo4.ListColumns(H4_ESC).Index
    idxRiesgo = lo4.ListColumns(H4_RIESGO).Index

    tieneImpMap = ColExiste(lo4, H4_IMP_MAP)
    If tieneImpMap Then idxImpMap = lo4.ListColumns(H4_IMP_MAP).Index

    nextBCP = 0

    For i = 1 To lo4.ListRows.Count
        tr = TipoRiesgoTexto(lo4.DataBodyRange(i, idxRiesgo).Value)
        If LCase$(tr) <> "aceptable" And tr <> vbNullString Then
            nextBCP = nextBCP + 1
            lo5.ListRows.add
```

```
        With lo5.ListRows(lo5.ListRows.Count).Range
          .Cells(1, lo5.ListColumns(H_ID).Index).Value = lo4.DataBodyRange(i, idxID).Value
          .Cells(1, lo5.ListColumns(H_ID_BCP).Index).Value = "BCP-" & Format$(nextBCP, "000")
          .Cells(1, lo5.ListColumns(H_ESC).Index).Value = lo4.DataBodyRange(i, idxEsc).Value
          .Cells(1, lo5.ListColumns(H_TIPO_RIESGO).Index).Value = tr

          If tieneImpMap Then
            .Cells(1, lo5.ListColumns(H_IMP_MAP).Index).Value = lo4.DataBodyRange(i,
idxImpMap).Value
          Else
            .Cells(1, lo5.ListColumns(H_IMP_MAP).Index).Value = vbNullString
          End If

          .Cells(1, lo5.ListColumns(H_CTRL_SUG).Index).Value = vbNullString
          .Cells(1, lo5.ListColumns(H_CTRL_NEG).Index).Value = vbNullString
        End With
      End If
    Next i
End Sub

Private Function TipoRiesgoTexto(ByVal v As Variant) As String
    If Not IsNumeric(v) Then
      TipoRiesgoTexto = vbNullString
      Exit Function
    End If
    Select Case CLng(v)
      Case 1 To 4: TipoRiesgoTexto = "Aceptable"
      Case 5 To 8: TipoRiesgoTexto = "Tolerable"
      Case 9 To 14: TipoRiesgoTexto = "Inaceptable"
      Case Else: TipoRiesgoTexto = "Inadmisible"
    End Select
End Function

'=========================================================
' Validación: lista de Tipo de interrupción (nombre dinámico)
'=========================================================
Private Sub AsegurarValidacionTipo(ws5 As Worksheet)
    Dim lo5 As ListObject, rngTipo As Range
```

```
    Set lo5 = ws5.ListObjects(TABLA_P5)
    If lo5 Is Nothing Or lo5.DataBodyRange Is Nothing Then Exit Sub

    Set rngTipo = lo5.ListColumns(H_TIPO_INT).DataBodyRange

    With rngTipo.Validation
        .Delete
        .add xlValidateList, xlValidAlertStop, xlBetween, "=" & NM_TIPO
        .IgnoreBlank = True
        .InCellDropdown = True
    End With
End Sub

Private Sub AsegurarNombreCatalogo(loCat As ListObject)
    If Not ColExiste(loCat, HC_TIPO) Then Err.Raise vbObjectError + 201, , "Falta '" & HC_TIPO & "'
en catálogo."
    CreateOrUpdateName NM_TIPO, "=" & loCat.Name & "[" & HC_TIPO & "]"
End Sub

Private Sub CreateOrUpdateName(ByVal nm As String, ByVal ref As String)
    On Error Resume Next
    ThisWorkbook.Names(nm).RefersTo = ref
    If Err.Number <> 0 Then
        Err.Clear
        ThisWorkbook.Names.add Name:=nm, RefersTo:=ref
    End If
    On Error GoTo 0
End Sub

'============================================================
' Limpieza masiva de avisos
'============================================================
Public Sub P5_RestaurarAvisosMasivo()
    Dim ws As Worksheet, lo As ListObject, rng As Range

    Set ws = ThisWorkbook.Worksheets(HOJA_P5)
    Set lo = ws.ListObjects(TABLA_P5)
    If lo Is Nothing Or lo.DataBodyRange Is Nothing Then Exit Sub

    Set rng = lo.ListColumns(H_CTRL_SUG).DataBodyRange
    If rng Is Nothing Then Exit Sub
```

```
    On Error Resume Next
    rng.Errors(xlInconsistentFormula).Ignore = True
    rng.Errors(xlInconsistentListFormula).Ignore = True
    On Error GoTo 0
End Sub

'============================================================
' Backup SOLO de la tabla (valores)
'============================================================
Private Function BackupSiTieneDatos(ws5 As Worksheet, lo5 As ListObject) As Boolean
    BackupSiTieneDatos = False

    If lo5.DataBodyRange Is Nothing Then
        BackupSiTieneDatos = True
        Exit Function
    End If
    If Application.WorksheetFunction.CountA(lo5.DataBodyRange) = 0 Then
        BackupSiTieneDatos = True
        Exit Function
    End If

    If MsgBox("Se regenerará la tabla y se borrará el contenido actual." & vbCrLf & _
            "¿Desea continuar?", vbExclamation + vbYesNo, "Confirmación 1 de 2") <> vbYes Then
Exit Function

    If MsgBox("Confirmación final: se creará un BACKUP de la tabla y luego se regenerará." &
vbCrLf & _
            "¿Confirma continuar?", vbCritical + vbYesNo, "Confirmación 2 de 2") <> vbYes Then Exit
Function

    Dim shBkp As Worksheet, nombreBackup As String, rngTabla As Range

    nombreBackup = "Paso5_Backup_" & Format(Now, "yyyymmdd_hhmmss")

    Application.DisplayAlerts = False
    Set shBkp =
ThisWorkbook.Worksheets.add(After:=ThisWorkbook.Sheets(ThisWorkbook.Sheets.Count))
    shBkp.Name = nombreBackup
```

```
    shBkp.Visible = xlSheetHidden
    Application.DisplayAlerts = True

    Set rngTabla = lo5.Range
    shBkp.Range("A1").Resize(rngTabla.Rows.Count, rngTabla.Columns.Count).Value =
rngTabla.Value

    BackupSiTieneDatos = True
End Function

Private Sub LimpiarTabla(lo As ListObject)
    On Error Resume Next
    If Not lo.DataBodyRange Is Nothing Then lo.DataBodyRange.Delete
    On Error GoTo 0
End Sub

'============================================================
' Estética estable
'============================================================
Private Sub AplicarEstetica(lo5 As ListObject)
    lo5.Range.WrapText = True
    lo5.Range.VerticalAlignment = xlTop

    lo5.ListColumns(H_ID).Range.ColumnWidth = 10
    lo5.ListColumns(H_ID_BCP).Range.ColumnWidth = 10
    lo5.ListColumns(H_ESC).Range.ColumnWidth = 70
    lo5.ListColumns(H_TIPO_RIESGO).Range.ColumnWidth = 16
    lo5.ListColumns(H_IMP_MAP).Range.ColumnWidth = 34
    lo5.ListColumns(H_TIPO_INT).Range.ColumnWidth = 26
    lo5.ListColumns(H_CTRL_SUG).Range.ColumnWidth = 60
    lo5.ListColumns(H_CTRL_NEG).Range.ColumnWidth = 55

    CentrarEncabezados lo5
End Sub

'============================================================
' Utilidades
'============================================================
Private Function UltimaFilaUsada(ws As Worksheet) As Long
    Dim c As Range
```

```
  Set c = ws.Cells.Find(What:="*", LookIn:=xlFormulas, SearchOrder:=xlByRows,
SearchDirection:=xlPrevious)
  If c Is Nothing Then UltimaFilaUsada = 0 Else UltimaFilaUsada = c.Row
End Function

Private Function RangoSeSuperponeConAlgunaTabla(ws As Worksheet, rng As Range) As Boolean
  Dim lo As ListObject
  For Each lo In ws.ListObjects
    If Not Intersect(lo.Range, rng) Is Nothing Then
      RangoSeSuperponeConAlgunaTabla = True
      Exit Function
    End If
  Next lo
  RangoSeSuperponeConAlgunaTabla = False
End Function

Private Function ColExiste(lo As ListObject, headerName As String) As Boolean
  On Error Resume Next
  ColExiste = (lo.ListColumns(headerName).Index > 0)
  On Error GoTo 0
End Function
```

Bibliografía

[1] C. F. PRADA L., «MiPymes: el pilar para la reactivación económica,» de *MiPymes: el pilar para la reactivación económica*, Bogotá, 2021.

[2] N. Unidas, «www.un.org,» Naciones Unidas, 16 03 2024. [En línea]. Available: https://www.un.org/es/observances/micro-small-medium-businesses-day#:~:text=Las%20microempresas%20y%20las%20peque%C3%B1as%20y%20medianas%20empresas%20(MIPYME)%20representan,el%2050%25%20del%20PIB%20mundial.. [Último acceso: 16 03 024].

[3] DANE, «ENCUESTA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES EN EMPRESAS (ENTIC EMPRESAS) 2020,» DANE, BOGOTÁ, 2020.

[4] I. Barracuda Networks, «Key findings on the latest social engineering,» *Spear Phishing: Top Threats and Trends,* vol. 7, 2022.

[5] I. T. Union, «Overview of cybersecurity,» ITU-T, 2009.

[6] J. H. K. B. C. H. Lorenzo Neil, «Cybersecurity Definitions for Non-Experts,» de *Symposium on Usable Privacy and Security*, Anaheim, CA, US, 2023.

[7] A. Lavell, «Sobre la gestión del riesgo: apuntes hacia una definición,» *Biblioteca Virtual en Salud de Desastres-OPS,* nº 4, pp. 1-22, 2001.

[8] ISO, ISO/IEC Guide 51:2014 Safety aspects – Guidelines for their inclusion in standards, Ginebra: ISO, 2014.

[9] INCIBE, «Instituto Nacional de Ciberseguridad,» [En línea]. Available: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf. [Último acceso: 16 04 2025].

[10] International Organization for Standarization, ISO/IEC 27005:2022 - Information security, cybersecurity and privacy protection — Guidance on managing information security risks, Geneva, 2022.

[11] ISO, ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection — Information security management systems — Requirements, Ginebra: ISO, 2022.

[12] ISO, ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks, Ginebra: ISO, 2022.

[13] ICONTEC, «https://www.icontec.org/,» ICONTEC, 2019. [En línea]. Available: https://www.icontec.org/eval_conformidad/certificacion-iso-223012019-sistemas-de-gestion-de-continuidad-de-negocio/. [Último acceso: 27 08 2024].

[14] L. S. P. Leni Sagita Riantini Supriadi, «Business Continuity Management (BCM),» de *Business Continuity Management in Construction*, Springer, Singapore, Management in the Built Environment, 2017, pp. 41-73.

[15] T. L. O. D. E. L. E. G. J. C. Shannon Tracey, «Promoting Resilience Using an Asset-Based Approach to Business,» *Sage Open,* vol. 7, nº 2, 2017.

[16] H. A. Simon, «A Behavioral Model of Rational Choice,» *The Quarterly Journal of Economics,* vol. 69, nº 1, pp. 99-118, 1955.

[17] S. O. S. Agil, «Rationality in economic theory: A critical appraisal,» *International Journal of Economics, Management and Accounting,* vol. 2, nº 2, pp. 79-94, 1989.

[18] H. A. Simon, «Bounded Rationality,» de *Utility and Probability*, Londres, Palgrave Macmillan, 1990, pp. 15-18.

[19] A. H. T. Oviedo, «El principio de racionalidad limitada de H.A. Simon y el premio novel de economia,» *El basilisco,* nº 4, pp. 68-79, 1978.

[20] D. Kahneman, Thinking, Fast and Slow, Nueva York: Farrar, Straus and Giroux, 2011.

[21] C. F. Z. Vásquez, «Plan de Continuidad del Negocio BCP aplicado al Departamento de Tecnología de Laboratorios Bagó del Ecuador SA,» Ecuador, 2020.

[22] A. J. G. Mendoza, «Diseño del plan de continuidad de negocio aplicado a seguridad de información en PYME Intervisión de Guayaquil,» Ecuador, 2022.

[23] A. M. O. Montoya, Artist, *PLAN DE CONTINUIDAD DEL NEGOCIO UNA PERSPECTIVA PREVENTIVA PARA EVITAR IMPACTOS POTENCIALES CASO PREBEL, S. A..* [Art]. Universidad EAFIT, 2011.

[24] C. F. O. MOLINA, Artist, *GUÍA PARA LA IMPLEMENTACIÓN BIA – BUSINESS IMPACT ANALYSIS – EN PYMES.* [Art]. UNIVERSIDAD CATÓLICA DE COLOMBIA, 2024.

[25] J. R. S. Olda Bustillos Ortega, «PROTOCOLO BÁSICO DE CIBERSEGURIDAD PARA PYMES,» Costa rica, 2022.

[26] C. A. D. E.-L. Damien Hutchinson, «The application of an agile approach to it security risk,» de *12th Australian Information Security Management Conference*, Australia, 2014.

[27] C. O. Espinoza Zelaya, Artist, *ENHANCING THE OPERATIONAL RESILIENCE OF CYBERMANUFACTURING SY TURING SYSTEMS (CMS) A STEMS (CMS) AGAINST CYBER-A GAINST CYBER-ATTACKS.* [Art]. Syracuse University, 2023.

[28] S. V. Mesa, Artist, *IMPACTO DEL RIESGO CIBERNÉTICO EN EL SEGMENTO MIPYME..* [Art]. Universidad EAFIT, 2018.

[29] J. R. B. M. H. C. C. C. J. O. Rocío Becerra Acevedo, «Evolución y modelos de implementación de sistemas de gestión de continuidad del negocio,» *Signos,* vol. 13, nº 2, 2021.

[30] INCIBE, «Taxonomia,» [En línea]. Available: https://www.incibe.es/incibe-cert/incidentes/taxonomia. [Último acceso: 15 08 2025].

[31] INCIBE-CERT, «Github,» INCIBE, [En línea]. Available: https://github.com/enisaeu/Reference-Security-Incident-Taxonomy-Task-Force/blob/master/working_copy/humanv1.md. [Último acceso: 15 08 2025].

[32] International Organization for Standardization, ISO/IEC 27031:2025 Cybersecurity - Information and communication technology readiness for business continuity, 2025.

[33] OWASP Foundation, «OWASP Top Ten: The Ten Most Critical Web Application Security Risks,» OWASP, 09 2024. [En línea]. Available: https://owasp.org/www-project-top-ten/. [Último acceso: 15 04 2025].

[34] P. networks, «Paloaltonetworks.com,» Paloalto networks, [En línea]. Available: https://www.paloaltonetworks.com/cyberpedia/what-is-a-ddos-attack. [Último acceso: 15 02 2025].

[35] «www.trendmicro.com,» Trend Micro, [En línea]. Available: https://www.trendmicro.com/vinfo/us/security/definition/industrial-internet-of-things-iiot.

[36] SentinelOne, «www.sentinelone.com,» SentinelOne, 14 10 2024. [En línea]. Available: https://www.sentinelone.com/cybersecurity-101/threat-

intelligence/cyber-espionage/#:~:text=Cyber%20espionage%20is%20the%20unauthorized,organizations%2C%20corporations%2C%20or%20research%20institutions. [Último acceso: 15 03 2025].

[37] IFX, «ifxnetworks.com,» [En línea]. Available: https://ifxnetworks.com/updates.

[38] D. C. F. B. G. M. Mansur Abilkasimov, «es.weforum.org,» World Economic Forum, 25 04 2023. [En línea]. Available: https://es.weforum.org/stories/2023/04/la-industria-manufacturera-es-el-sector-mas-atacado-por-los-ciberataques-por-que-es-importante-aumentar-la-seguridad/. [Último acceso: 02 04 2025].

[39] RCN, «www.rcn.com,» RCN, [En línea]. Available: https://www.noticiasrcn.com/colombia/fiscalia-identifica-a-ransomhouse-como-presuntos-responsables-del-ciberataque-454108.

[40] hyperconectado, «muchohacker.lol,» 24 04 2023. [En línea]. Available: https://muchohacker.lol/2023/04/ransomware-lockbit-se-adjudica-ataque-a-grupo-nutresa-y-le-da-cuatro-dias-para-negociar-extorsion/. [Último acceso: 15 03 2025].

[41] L. L. Díaz, «www.eltiempo.com,» El tiempo, 21 04 2023. [En línea]. Available: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/nutresa-sufrio-ciberataque-pero-no-perdio-informacion-761698. [Último acceso: 15 03 2025].

[42] J. Báez, «www.welivesecurity.com,» Eset, 28 09 2021. [En línea]. Available: https://www.welivesecurity.com/la-es/2021/09/28/que-es-ataque-xss-cross-site-scripting/. [Último acceso: 18 01 2025].

[43] Mitre, «cwe.mitre.org,» [En línea]. Available: https://cwe.mitre.org/data/definitions/502.html. [Último acceso: 20 03 2025].

[44] B. ,. S. M. ,. B. W. y. S. K. Pescador, «Ransomware Risk Management: A Cybersecurity Framework Profile,» Pubs NIST, Gaithersburg, 2022.

[45] G. &. B. J. Hoglund, de *Rootkits: subverting the Windows kernel*, Addison-Wesley Professional, 2006, p. 4.

[46] National Initiative for Cybersecurity Careers and Studies, «NICCS-CISA,» CISA, [En línea]. Available: https://niccs.cisa.gov/cybersecurity-career-resources/vocabulary. [Último acceso: 16 04 2025].

[47] J. S. H. K. Myounghoon Kim, «A Study of the Emerging Trends in SIM Swapping Crime and Effective Countermeasures,» de *International Conference on Big Data, Cloud Computing, and Data Science*, Danang, Vietnam, 2022.

[48] P. Networks, «paloaltonetworks.com,» Paloalto Networks, [En línea]. Available: https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos. [Último acceso: 15 02 2025].

[49] J. X. Y. G. K. D. H. &. Z. J. Liu, «Botnet: classification, attacks, detection, tracing, and preventive measures,» *EURASIP journal on wireless communications and networking,* vol. 2009, pp. 1-11, 2009.

[50] z. kingthorin, «owasp.org,» OWASP, [En línea]. Available: https://owasp.org/www-community/attacks/SQL_Injection. [Último acceso: 10 02 2025].

[51] INCIBE, «www.incibe.es,» INCIBE, 18 07 2023. [En línea]. Available: https://www.incibe.es/empresas/blog/insiders-como-atacan-desde-dentro. [Último acceso: 31 01 2025].

[52] L. Institute, «www.lisainstitute.com,» LISA Institute, [En línea]. Available: https://www.lisainstitute.com/blogs/blog/insiders-amenaza-interna. [Último acceso: 31 1 2025].

[53] Z. M. P. M. C. L. J. M. A. M. N. B. M. A. M. B. Amin Kharraz, «Outguard: Detecting In-Browser Covert Cryptocurrency Mining in the Wild,» de *WWW '19: The World Wide Web Conference*, 2019.

[54] C. K. M. D. G. Thomas Kampa, «Interlocking IT/OT security for edge cloud-enabled manufacturing,» *Ad Hoc Networks,* vol. 154, 2024.

[55] M. Fidler, Artist, *Anarchy or regulation: controlling the global trade in zero-day vulnerabilities.* [Art]. Stanford University, 2014.

[56] L. L. Pawel Weichbroth, «Mobile Security: Threats and Best Practices,» *Mobile Information Systems,* pp. 1-15, 2020.

[57] R. Peacock, «www.atlanticcouncil.org,» Atlantic council, 01 07 2024. [En línea]. Available: https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/the-impact-of-corruption-on-cybersecurity-rethinking-national-strategies-across-the-global-south/#:~:text=the%20case,costly. [Último acceso: 15 03 2025].

[58] M. Kreisa, «www.pdq.com,» 26 03 2024. [En línea]. Available: https://www.pdq.com/blog/risks-of-unpatched-software-vulnerabilities/. [Último acceso: 22 02 2025].

[59] C. Nobles, «Investigating cloud computing misconfiguration errors using the human factors analysis and classification system,» *Scientific Bulletin,* vol. 27, nº 1, pp. 59-66, 2022.

[60] C. Daniel, «Building a More Secure Network: A Comprehensive Guide to Network Segmentation Strategies and Best Practices.,» *REVISTA DE INTELIGENCIA ARTIFICIAL EN MEDICINA,* vol. 15, nº 1, 2024.

[61] NIST, «NIST Special Publication 800-153: guidelines for Securing Wireless Local Area Networks (WLANs),» National Institute of Standards and Technology , Gaithersburg, 2012.

[62] E. Z. M. P. C.-E. B. V. D. Danielle Kuznets Nohi, «www.microsoft.com/,» Microsoft Threat Intelligence Community, 29 07 2024. [En línea]. Available: https://www.microsoft.com/en-us/security/blog/2024/07/29/ransomware-operators-exploit-esxi-hypervisor-vulnerability-for-mass-encryption/#:~:text=Microsoft%20researchers%20have%20uncovered%20a,to%20access%20hosted%20VMs%20and. [Último acceso: 10 03 2025].

[63] S. Anja, «VMware Cloud Foundation (VCF) Blog,» VMware Cloud Foundation, 08 08 2023. [En línea]. Available: https://blogs.vmware.com/cloud-foundation/2023/08/08/why-should-you-rethink-your-hybrid-cloud-security-strategy/#:~:text=The%20adoption%20of%20hybrid%20cloud,security%20architecture%20across%20heterogeneous%20environments. [Último acceso: 12 03 2025].

[64] M. Meineke, «www.weforum.org,» 28 04 2024. [En línea]. Available: https://www.weforum.org/stories/2024/04/cybersecurity-industry-talent-shortage-new-report/#:~:text=The%20global%20cybersecurity%20industry%20is,Image%3A%C2%A0Unsplash%2FJefferson%20Santos. [Último acceso: 16 03 2025].

[65] National Institute of Standards and Technology, NIST 800-53 Rev.5 Security and Privacy Controls for Information Systems and Organizations, 2020.

[66] B. Z. Chandramouli R, «NIST SP 800-228: guidelines for API Protection for cloud-Native Systems,» National Institute of Standards and Technology, Gaithersburg, 2025.

[67] M. Figueroa, «https://www.infobae.com/colombia/2023/04/21,» Infobae, 21 04 2023. [En línea]. Available: https://www.infobae.com/colombia/2023/04/21/nutresa-fue-objeto-de-un-ataque-cibernetico-la-compania-confirmo-que-es-victima-de-un-ransomware/. [Último acceso: 15 03 2025].

[68] hyperconectado, «muchohacker.lol,» 28 04 2023. [En línea]. Available: https://muchohacker.lol/2023/04/lockbit-publica-10-pruebas-de-documentos-robados-al-grupo-nutresa/. [Último acceso: 15 03 2025].

[69] Incibe, «INCIBE-Cert,» INCIBE, [En línea]. Available: https://www.incibe.es/incibe-cert/publicaciones/bitacora-de-seguridad/ciberataque-ransomware-contra-ifx-networks.

[70] NIST, «https://www.nist.gov/,» NIST, 16 01 2020. [En línea]. Available: https://www.nist.gov/privacy-framework/nist-sp-800-34. [Último acceso: 27 08 2024].

[71] International Organization for Standardization, «www.iso.org,» International Organization for Standardization, [En línea]. Available: https://www.iso.org/standard/50295.html. [Último acceso: 04 05 2025].

[72] British Standars Institution, «www.bsigroup.com,» bsigroup, [En línea]. Available: https://www.bsigroup.com/en-GB/products-and-services/standards/iso-22301-business-continuity-management/. [Último acceso: 04 05 2025].

[73] Business Continuity Institute, Good Practice Guidelines 2023 Edition (v7.0): The Professional Practices for Business Continuity Management, Reading, United kindom, 2023.

[74] International Organization for Standarization, «www.iso.org,» International Organization for Standarization, [En línea]. Available: https://www.iso.org/standard/75106.html. [Último acceso: 04 05 2025].

[75] H. Hamidovic, «An Introduction to Incident Preparedness and Operational Continuity Management Based on ISO/PAS 22399:2007,» *ISACA,* vol. III, 2011.

[76] D. R. L. O. P. H. Brian J. O'Connor, «NFPA 1600 Handbook,» NFPA, 2016.

[77] National Institute of Standards and Technology (NIST), «NIST Special Publication 800-34 Revision 1: Contingency Planning Guide for Federal Information Systems,» National Institute of Standards and Technology, Gaithersburg, 2010.

[78] Secure Step Forward Ltd, «marketing.securestepforward.com,» Secure Step Forward Ltd, 22 05 2025. [En línea]. Available: https://marketing.securestepforward.com/blog/digitalresilience. [Último acceso: 25 05 2025].

[79] DRI International, «Professional Practices (Business Continuity Management),» DRI International, Dearborn, 2023.

[80] A. P. S. Silmie Vidiya Fani, «Business Continuity Plan: Examining of Multi-Usable Framework,» *Procedia Computer Science,* vol. 161, pp. 275-282, 2019.

[81] S. Panda, Artist, *Optimal Strategies for Cyber Security.* [Art]. University of surrey, 2022.

[82] Mitre, «cwe.mitre,» Mitre, [En línea]. Available: https://cwe.mitre.org/data/definitions/89.html. [Último acceso: 20 03 2025].

[83] NIST, Managing Information Security Risk, Gaithersbburg: NIST, 2011.

[84] J. C. B. Simon Kramer, «A general definition of malware,» *Journal in Computer Virology ,* vol. 6, pp. 105-114, 2009.

[85] S. &. C. T. Chanti, «A literature review on classification of phishing attacks,» *International Journal of Advanced Technology and Engineering Exploration,* vol. 9, nº 89, pp. 446-476, 2022.

[86] K. K. T. S. a. O. I. Huseyn Huseynov, Artist, *Virtual Machine Introspection for Anomaly-Based Keylogger Detection.* [Art]. City University of New York, Kyushu Institute of Technology, 2020.

[87] H. Z. P. L. L. S. Zuoguang Wang, «Social engineering in cybersecurity: a domain ontology and knowledge graph application examples,» *Cybersecur,* vol. 4, nº 31, 2021.

[88] G. Wright, «www.techtarget.com,» Informa TechTarget Editorial Network, [En línea]. Available: https://www.techtarget.com/searchsecurity/definition/dictionary-attack#:~:text=Brute. [Último acceso: 18 03 2025].

[89] G. A. a. S. Z. Mark Elsner, «Global Risks Report 2025,» World Economic Forum, Cologny, Geneva, Switzerland, 2025.

[90] World Economic Forum, Accenture, «Global Cybersecurity Outlook 2025,» World Economic Forum, Geneva, Switzerland, 2025.

[91] KPMG Advisory, Tax & Legal S.A.S., «Benchmark de Ciber Riesgo Cuantificado por industria en Colombia 2024: Resumen Ejecutivo.,» KPMG Colombia, Bogotá D.C, Colombia, 2024.

[92] National Institute of Standards and Technology, «Security and Privacy Controls for Information Systems and Organizations,» U.S. Department of Commerce, Gaithersburg, MD, 2020.

[93] National Institute of Standards and Technology, «Cybersecurity Framework Profile for Ransomware Risk Management,» U.S. Department of Commerce, Gaithersburg, MD, 2022.

[94] National Institute of Standards and Technology, «Digital Identity Guidelines: Authentication and Lifecycle Management,» U.S. Department of Commerce, Gaithersburg, MD, 2020.

[95] International Organization for Standardization, «ISO/IEC 27002:2022 — Information security, cybersecurity and privacy protection — Information security controls,» ISO/IEC, Geneva, 2022.

[96] International Organization for Standardization, «ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements,» ISO/IEC, Geneva, 2022.

[97] National Institute of Standards and Technology, «Technical Guide to Information Security Testing and Assessment,» U.S. Department of Commerce, Gaithersburg, MD, 2008.

[98] International Electrotechnical Commission; International Society of Automation, «ISA/IEC 62443 — Industrial communication networks – Network and system security for industrial-process measurement and control,» IEC / ISA, Geneva, 2018.

[99] International Organization for Standardization, 31000:2018 – Risk management — Guidelines, Geneva, Suiza, 2018.

[100] International Society of Automation, ISA/IEC 62443 Series – Security for Industrial Automation and Control Systems.

[101] Fortinet, «www.fortinet.com,» [En línea]. Available: https://www.fortinet.com/resources/cyberglossary/iec-62443. [Último acceso: 03 05 2025].

[102] International Organization for Standardization, ISO 22316:2017 – Security and resilience – Organizational resilience – Principles and attributes, Geneva, Suiza, 2017.

[103] INCIBE, «Guía nacional de notificación y gestión de ciberincidentes,» 2020. [En línea]. Available: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_nacional_notificacion_gestion_ciberincidentes.pdf. [Último acceso: 15 08 2025].

[104] P. C. B. OCHOA, Artist, *IDENTIFICACIÓN DE ACTIVOS DE INFORMACIÓN, RIESGOS Y CONTROLES ASOCIADOS PARA LA EMPRESA ESTRATEGIAS EMPRESARIALES DE COLOMBIA BAJO LA NORMA ISO 27001 E ISO 31000.* [Art]. UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD, 2019.

[105] V. B. M. B. FRANTISEK KORCEK, «SECURITY OF INFORMATION ASSETS IN SMALL AND MEDIUM-SIZED ENTERPRISES,» *EKONOMICKÉ ROZHLADY,* vol. 45, nº 1, 2016.