MINISTERIO DE ECONOMÍA, INDUSTRIA Y COMERCIO | GOBIERNO DE COSTA RICA

Ministerio de Economía, Industria y Comercio (MEIC)

Plan de Acción Institucional para la Continuidad del Servicio (PAICS)

Versión 1

Diciembre, 2024

Dirección: Oficentro ASEBANACIO, Llorente de Tibás, Avenida 45
Teléfono: 2549-1400 ext. 299 / 276 / 222 / 269
Correo electrónico: planificacioninstitucional@meic.go.cr web: www.meic.go.cr
Apartado Postal: 10216-1000 San José, Costa Rica

CONTROL DE VERSIONES

Fecha	Versión	Elaboración /Revisión Cambio/ Aprobación	Autor	Puesto	Dependencia
22/10/2024 al 15/11/2024	V1	Diseño y elaboración	Wendy María Fallas Garro	Jefe y Contralora de Servicios a.i	Unidad de Planificación Institucional y Contraloría de Servicios
14/11 /2024 al 29/11/2024	V1	Revisión	Fabián David Quirós Álvarez	Director Administrativo Financiero y Oficial Mayor	Dirección Administrativa Financiera y Oficialía Mayor
			Marilyn Rodríguez Arias	Asesora	
			Gerardo Rojas Cubero	Jefe Despacho	Despacho del Ministro
			Joselyn Corrales Solís	Asesora	
			Samuel González De la Cruz	Asesor	
			Luis Guillermo Rojas Solano	Jefe	Departamento de Tecnología de Información y Comunicación
			Andrea Gutiérrez Ruíz	Asesora	Unidad de Planificación Institucional
11/12/2024	V1	Aprobación	Fabián David Quirós Álvarez	Director Administrativo Financiero y Oficial Mayor	Dirección Administrativa Financiera y Oficialía Mayor

APROBACIONES

Acción	Nombre	Puesto	Dependencia	Firma
Aprobación V1 – Sesión Ordinaria N° 005-2024 – Comité para la Continuidad del Negocio	Fabián David Quirós Álvarez	Director Administrativo Financiero y Oficial Mayor	Dirección Administrativa Financiera y Oficialía Mayor	FABIAN DAVID QUIROS ALVAREZ (FIRMA) Firmado digitalmente por FABIAN DAVID QUIROS ALVAREZ (FIRMA) Fecha: 2024.12.18 15:18:56 -06'00'

SIGLAS

Sigla	Significado
BIA	Análisis de Impacto del Servicio
CCS	Comité para la Continuidad del Servicio
DAC	Dirección de Apoyo al Consumidor del MEIC
DAI	Departamento de Apoyo Institucional de la Dirección de Mejora Regulatoria del MEIC
DAR	Departamento de Análisis Regulatorio de la Dirección de Mejora Regulatoria del MEIC
DCAL	Dirección de Calidad del MEIC
DECVP	Departamento de Educación al Consumidor y Ventas a Plazo de la DAC
DEPA	Departamento de Procedimientos Administrativos de la DAC
DIAF	Dirección Administrativa Financiera y Oficialía Mayor
Digepyme	Dirección General de Apoyo a la Pequeña y Mediana Empresa
DMR	Dirección de Mejora Regulatoria
DRTC	Departamento de Reglamentación Técnica y Codex de la DCAL
DTIC	Departamento de Tecnologías de Información y Comunicación del MEIC
MEIC	Ministerio de Economía, Industria y Comercio
MH	Ministerio de Hacienda
MICITT	Ministerio de Ciencia, Tecnología y Telecomunicaciones
MTPD	Maximum Tolerable Period of Disruption – Tiempo de máximo de inactividad tolerable
PACO	Departamento Plataforma de Atención al Consumidor de la DAC
PACS–Dependencias	Planes de Acción para la Continuidad del Servicio de cada dependencia del MEIC
PAICS	Plan de Acción Institucional para la Continuidad del Servicio del MEIC

Sigla	Significado
PCS	Política de Continuidad del Servicio del MEIC
Racsa	Radiográfica Costarricense S.A
RPO	RPO (Recovery Point Objective – Punto de Recuperación Objetivo):
RTO	Recovery Time Objective – Objetivo de Tiempo de Recuperación
SIEC	Sistema de Información Empresarial Costarricense
TIC	Tecnología de Información y Comunicación
UPI	Unidad de Planificación Institucional
WRT	Work Time Recovery – Tiempo de trabajo de recuperación

DEFINICIONES

a. **Crisis:** estado de pérdida de control de las actividades o procesos de la institución en un período determinado.

b. **Expertos de recuperación:** funcionarios de la institución que tienen el conocimiento o las capacidades técnicas para atender la plataforma tecnológica que soporta los procesos vitales.

c. **Incidente:** interrupción no planificada del servicio o reducción de la calidad del servicio brindado.

d. **Pérdida:** recursos no recuperables como consecuencia de un incidente.

e. **Plan de Acción Institucional para la Continuidad del Servicio:** es la hoja de ruta diseñada para responder a los objetivos y resultados ante un evento disruptivo y reanudar, recuperar y restaurar la prestación de los servicios de acuerdo con sus objetivos de la continuidad del servicio.

f. **Plataforma tecnológica:** son todos aquellos elementos de "hardware" y "software" que en conjunto soportan las aplicaciones y servicios tecnológicos.

g. **Procesos críticos:** son todos aquellos procesos de la institución esenciales para la operación de esta.

h. **Protocolo:** conjunto de actividades definidas de forma anticipada que describen las pautas necesarias para recuperar la infraestructura tecnológica del MEIC.

i. **Pruebas de continuidad:** actividad en la que el plan de acción para la continuidad del servicio o los procedimientos de recuperación se ensayan de forma individual o en conjunto para procurar que tengan la información apropiada y que produzcan el resultado deseado cuando se lleven a ejecución.

j. **Reanudación:** operaciones que se ejecutan después de la ocurrencia de un desastre con el objetivo de reanudar las operaciones de la organización.

k. **RPO (Recovery Point Objective – Punto de Recuperación Objetivo):** El RPO establece el punto en el tiempo hasta el cual los datos deben ser restaurados después de un desastre. Este indicador determina la ventana temporal en la cual la pérdida de datos no impactaría significativamente en las operaciones comerciales. Medido en horas o minutos, un RPO efectivo asegura la integridad de la información crucial para el funcionamiento continuo del negocio.

l. **RTO (Recovery Time Objective – Objetivo de Tiempo de Recuperación**): El RTO se erige como un elemento vital en la planificación de la recuperación de desastres, enfocándose en el tiempo máximo permitido para restaurar los servicios de TI después de un incidente. Este plazo crítico se mide en unidades temporales, generalmente horas o días. Un RTO eficiente es esencial para minimizar la interrupción del negocio y garantizar una respuesta rápida y efectiva ante eventos adversos.

m. **WTR (Work Time Recovery – Tiempo de trabajo de recuperación):** El WTR se centra en el tiempo necesario para restaurar completamente los servicios de TI durante las horas laborables normales. Este indicador abarca todas las tareas esenciales, desde la verificación de datos hasta pruebas de recuperación y pruebas de estrés. Un WTR eficiente asegura que la recuperación se realice de manera efectiva y sin comprometer la calidad de las operaciones. Es el tiempo disponible para recuperar datos perdidos, incluyendo la carga y prueba de verificación.

n. **MTPD (Maximum Tolerable Period of Disruption – Tiempo de máximo de inactividad tolerable):** El MTPD representa el período máximo de tiempo que una organización puede tolerar estar sin sus servicios de TI antes de que se produzca un impacto significativo en el negocio. Este indicador va más allá de la mera recuperación técnica, considerando las ramificaciones financieras y de reputación. Es crucial determinar un MTPD realista para evitar consecuencias graves en términos de pérdidas económicas o daño a la reputación empresarial.

ÍNDICE DE CONTENIDOS

ÍNDICE DE CUADROS

ÍNDICE DE IMÁGENES

1. INTRODUCCIÓN

La Ley Orgánica N° 6054 crea el Ministerio de Economía, Industria y Comercio (MEIC), el cual debe desempeñar una serie de funciones en materia de fomento a la iniciativa privada, desarrollo empresarial, cultura empresarial, la generación de políticas y acciones necesarias para la tutela de los intereses legítimos y la defensa efectiva de los derechos del consumidor.

Además, de la realización de investigaciones de mercado, promoción de un marco regulatorio que brinde seguridad jurídica al administrado y propicie servicios del Estado eficientes, y reglamentos claros que se basen en las normas técnicas, internacionales, regionales o nacionales para evitar obstáculos técnicos al comercio, la coordinación y ejecución de la verificación de mercados y la evaluación de la conformidad de los Reglamentos Técnicos.

Lo anterior evidencia la importancia de las actividades que realiza el MEIC para el cumplimiento de estas funciones que generan un bienestar a la población costarricense e impactan el desarrollo socioeconómico del país. Por lo que es indispensable que el MEIC cuente con las herramientas necesarias y tenga claridad de las acciones que debe ejecutar antes, durante y después de un incidente, con el propósito de minimizar los efectos que este puede ocasionar de cara a la prestación de los servicios a los ciudadanos.

Actualmente, el MEIC cuenta con la Política de Continuidad del Servicio, y el Análisis de Impacto del Servicio (BIA)[1], mediante el cual se han identificado los procesos y recursos críticos que se deben de considerar y los riesgos asociados a estos. Sin embargo, adicional a dichas herramientas surge la necesidad de elaborar el Plan Institucional de Acción para la Continuidad del Servicio, con el fin de garantizar que estos procesos críticos continúen funcionando o sean restablecidos en el menor tiempo posible ante un incidente. Es así como en el presente plan se describirán las acciones para la gestión de la continuidad del servicio, y la estrategia de recuperación y operación junto con sus responsables en función de los procesos críticos identificados.

[1] https://www.meic.go.cr/web/63_cicap/red-transparencia/planes-institucionales.php

2. Objetivos

2.1 Objetivo General

Garantizar la continuidad y disponibilidad de los servicios esenciales que brinda el Ministerio de Economía, Industria y Comercio, así como minimizar el impacto de los eventos disruptivos que se puedan presentar.

2.2 Objetivos Específicos

- Establecer el procedimiento para la atención de un evento disruptivo o incidente que tiene afectación en los procesos críticos vinculados a los servicios que brinda el MEIC.
- Determinar los roles, acciones y responsabilidades para la atención de un evento disruptivo que afecte la continuidad de los servicios.
- Establecer las funciones de los equipos de recuperación y operación, así como su interacción para el establecimiento de estrategias de continuidad de los servicios críticos.

3. Alcance

Este plan de acción aplica para las direcciones responsables de los procesos críticos que fueron identificados mediante el Análisis de Impacto del Servicio (BIA)[2], así mismo a aquellas cuya operación se vea afectada por la manifestación de un evento disruptivo.

4. Documentos relacionados

- Política de Continuidad del Servicio, Versión 2.0. [3]
- Análisis de Impacto del Servicio (BIA) [4], Versión 1
- Metodología para la elaboración de los Planes de Acción para la Continuidad del Servicio, Versión 2.0. [5]

[2] http://reventazon.meic.go.cr/informacion/reddetransparencia/planesinstitucionales/bia_meic_v1_2024.pdf

[3] http://reventazon.meic.go.cr/informacion/reddetransparencia/planesinstitucionales/PoliticaContinuidadServicioMEICv2.pdf

[4] http://reventazon.meic.go.cr/informacion/reddetransparencia/planesinstitucionales/bia_meic_v1_2024.pdf

[5] http://reventazon.meic.go.cr/informacion/reddetransparencia/planesinstitucionales/MetodologiaPlanAccionv2.pdf

5. Descripción del Plan de Acción Institucional para la Continuidad del Servicio

El Plan de Acción Institucional de Continuidad del Servicio del MEIC, se centra en estrategias de optimización de recursos ya existentes, pretende asegurar la continuidad de los servicios esenciales de la institución, minimizando el impacto de posibles interrupciones y garantizando la capacidad de recuperación.

Es una estrategia integral que asegura que los servicios críticos continúen operativos, se restablezcan rápidamente o en el menor tiempo posible; en caso de interrupciones. Este plan se orienta a minimizar el impacto de desastres, fallas de infraestructura, u otros eventos disruptivos que puedan comprometer el funcionamiento de los procesos críticos identificados que afectan la prestación de los servicios de la institución.

Este es un plan de acción marco que establece los lineamientos y acciones macro para que las respectivas dependencias del MEIC establezcan sus planes de acción dependiendo de las particularidades de cada trámite o servicio y el sistema de información que lo soporta, en coordinación con el personal involucrado que se describe en este documento de manera detallada.

6. Planes de Acción para la Continuidad del Servicio de las dependencias y listas de tareas

El MEIC ha venido trabajando y tomando como base para la gestión de la continuidad de los servicios, elementos y mejores prácticas que el MH ya ha implementado, con el acompañamiento de la Contraloría General de la República.

Por ende, también en apego a la norma ISO 22301:2020; se detallan los factores a analizar a la hora de seguir los pasos del PAICS (lo indicado no debe visualizarse secuencialmente, sino que dependerá del evento disruptivo), estos factores son:

- **Activación del PAICS:** Se realizará conforme la definición de responsabilidades establecida para cada equipo y rol específico, destacando que, una vez activado el plan, se debe

comunicar al gestor de continuidad a cargo del proceso crítico para que se inicien las acciones correspondientes.

- **Acciones por parte de los gestores de continuidad:** Cada dependencia responsable en coordinación con el DTIC tendrán sus estrategias de recuperación y procedimientos de continuidad, en los cuales se definirá la secuencia de pasos a seguir para activar la continuidad de la operativa para cada proceso crítico ante un evento de interrupción. Esto deberá ser integrado en el PACS que desarrolle el DTIC. Así mismo cada dependencia podrá desarrollar un PACS en caso de que se deban establecer acciones que no sean abordadas en conjunto con el DTIC.

- **Lugar de movilización:** En caso de un evento que implique la evacuación de las instalaciones, en primera instancia se debe garantizar la salvaguarda de la vida.

- **Disponibilidad de recursos en crisis:** Se debe coordinar previamente con la Dirección Administrativa Financiera y Oficialía Mayor para que en un caso de activación que implique la necesidad de adquirir insumos necesarios para mantener la operativa, ésta pueda darse de manera ágil. A la vez, cada área responsable de los procesos críticos debe planificar y presupuestar los recursos necesarios.

- El DTIC deberá formular su PACS para los sistemas de información que soporten los trámites y servicios, y las dependencias deberán establecer las estrategias para continuar brindando el servicio en caso de que este sea interrumpido (las acciones a seguir en una interrupción, los responsables en la atención y gestión de incidentes y crisis).

- La Valoración de Riesgos debe realizarse por cada dependencia.

7. Sistemas de Información Críticos

La identificación de sistemas que soportan trámites o servicios críticos es trascendental en la gestión de la continuidad del negocio.

Para el caso del MEIC, la identificación de los sistemas de información que soportan servicios o trámites críticos es fundamental, dado a que debemos garantizar la resiliencia, disponibilidad y recuperación rápida de estos ante incidentes que puedan interrumpir la prestación normal de los servicios y trámites por parte de la organización.

Tal cual lo indica el MH, el ejercicio de verificar cuales son los sistemas críticos permite *definir una priorización de los recursos y las inversiones en la continuidad del negocio, al enfocarse en la protección y recuperación de los sistemas más críticos, la organización puede minimizar el impacto de una interrupción en la continuidad del negocio y acelerar la recuperación. Además, promueve que a nivel de la contingencia tecnológica se definan planes de recuperación específicos para cada sistema.*

La importancia de identificar el RPO en los sistemas críticos rescinde en la capacidad institucional para establecer objetivos claros para la recuperación de datos y tomar medidas para minimizar la cantidad de datos perdidos en caso de un desastre o interrupción. Esto implica la implementación de estrategias y soluciones de respaldo y recuperación que permitan al ministerio recuperar rápidamente los datos hasta el punto en que se produjo el fallo, minimizando así el impacto en la continuidad del negocio y en la satisfacción del cliente.

El RPO, RTO, WRT y MTPD de cada gestión crítica y el detalle de los sistemas de información que los soportan se puede ver en el BIA Versión V1[6] del MEIC.

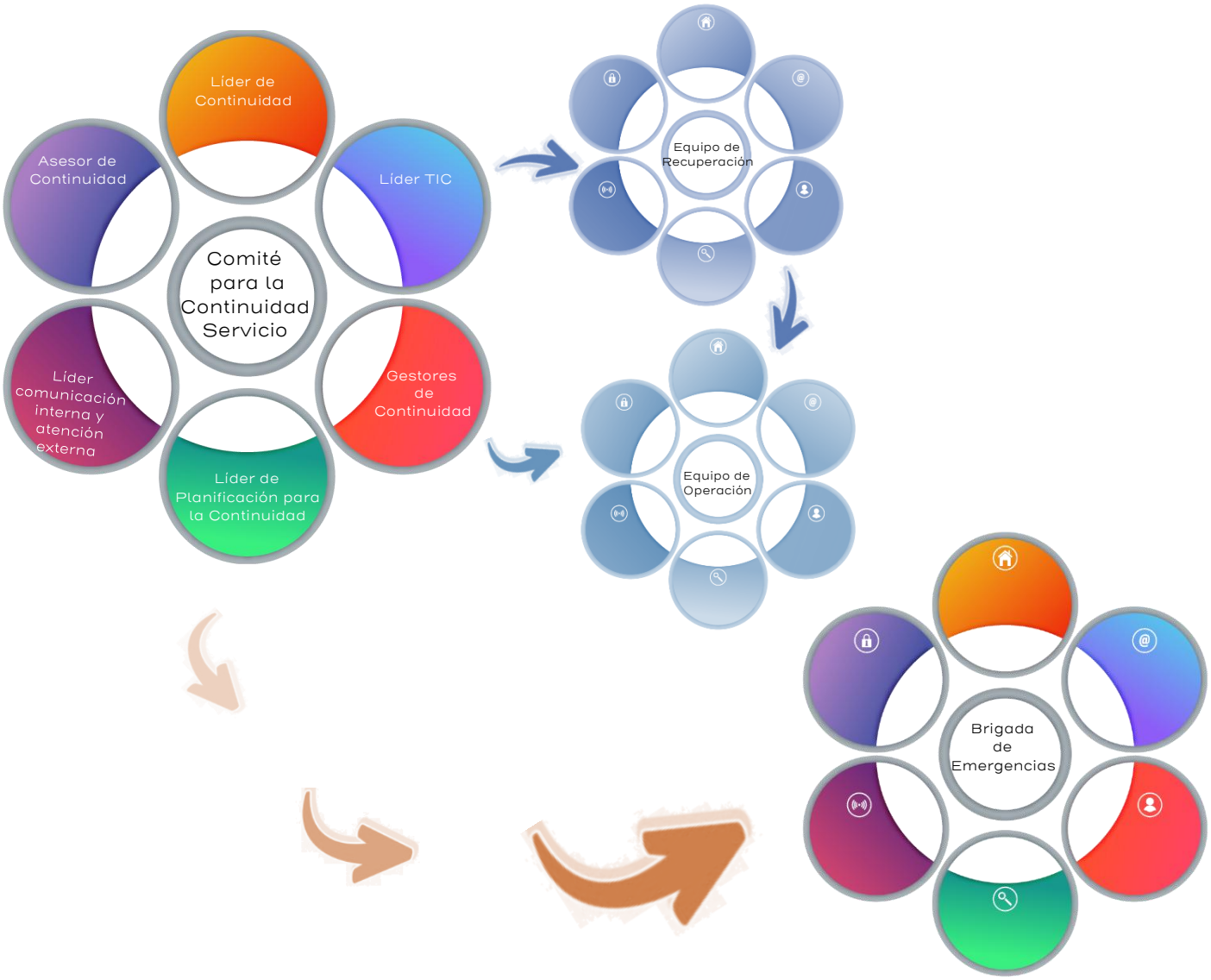
8. Roles, acciones y responsabilidades del personal involucrado

Para el funcionamiento y aplicación de este plan, es necesario el involucramiento del personal que posea la autoridad para tomar decisiones en lo relativo a la autorización de acciones y de gastos (en caso sea necesario y se cuenten con los recursos).

Por lo anterior, se contará con el siguiente personal involucrado en las gestiones de continuidad del servicio:

[6] http://reventazon.meic.go.cr/informacion/reddetransparencia/planesinstitucionales/bia_meic_v1_2024.pdf

Figura N°1: Comité para la Continuidad del Servicio y los Equipos de Apoyo.



Fuente: UPI, PCS, MEIC

8.1 Comité para la Continuidad del Servicio:

Será el responsable de elaborar, implementar, revisar y actualizar este plan de acción para la continuidad del servicio. Los miembros del Comité son:

Cuadro N°1: Comité para la continuidad del servicio, roles, acciones y responsabilidades

Puesto	Oficina	Correo electrónico	Teléfono	Rol	Acciones y responsabilidades
Oficial Mayor y Director(a)	DIAF	diradministrativofinanciero@meic.go.cr	2549-1400 Ext: 260, 286.	Líder de Continuidad	• Gestionar el presupuesto y recursos para la continuidad del negocio. • Supervisar y optimizar el flujo del proceso durante la interrupción para asegurar la continuidad de los servicios. • Informar al Comité de Continuidad sobre el progreso de las acciones y los problemas encontrados. • Coordinar con la Brigada de Emergencias lo que corresponda en el caso de que se presente un fallo ambiental. • Analizar el evento ocurrido para activar el PAICS.
Asesor(a)	Despacho Ministerial especialista en TIC	despachoministro@meic.go.cr	2549-1400 Ext: 279.	Asesor de Continuidad	• Actuar como el principal punto de contacto en caso de crisis, dirigiendo las acciones de respuesta en coordinación con el Jefe de DTIC. • Coadyuvar al Líder TIC para que se establezcan los PACS de las dependencias correspondientes.

Puesto	Oficina	Correo electrónico	Teléfono	Rol	Acciones y responsabilidades
					• Coordinar las acciones que se requieren de los Despachos Ministeriales para asegurar la continuidad de los servicios. • Informar a los jerarcas del evento disruptivo de primera mano. • Coordinar las comunicaciones a lo externo de la institución según indicaciones de los jerarcas. • Asistir en la realización de pruebas y la mejora continua del plan.
Jefatura	UPI	planificacioninstitucional@meic.go.cr	2549-1400 Ext: 299, 222, 276, 269.	Líder de Planificación para la Continuidad	• Liderar la elaboración y actualización del PAICS, asegurando que esté alineado con la PCS y el BIA. • Coordinar la gestión de los riesgos que podrían afectar la continuidad del negocio. • Velar en conjunto con el Comité para la Continuidad del Servicio para que se establezcan los PACS de las dependencias del MEIC.
Contralor (a) de Servicios	Contraloría de Servicios	contraloria@meic.go.cr	2549-1400 Ext: 274.	Líder de Comunicación Interna y Atención Externa	• Generar la comunicación interna (alertas) para las crisis, asegurando mensajes claros y consistentes, tanto en el caso de que la interrupción se detecte por medio de los usuarios externos, como por medio de usuarios internos; que le contacten. • Informar al personal involucrado sobre la situación y las acciones de respuesta necesarias.

Puesto	Oficina	Correo electrónico	Teléfono	Rol	Acciones y responsabilidades
Jefatura	DTIC	deptotecnologiasinformacioncomunicacion@meic.go.cr	2549-1400 Ext: 253, 284, 219, 280, 207, 213, 214, 223.	Líder TIC	• Planificar y supervisar simulacros y pruebas del PACS de las dependencias para verificar su eficacia. • Identificar, evaluar y gestionar los riesgos que podrían afectar la continuidad del negocio. • Garantizar la protección de la infraestructura tecnológica y la disponibilidad de los sistemas críticos. • Implementar sistemas de respaldo y recuperación de datos, incluyendo redundancias. • Mantener activas las infraestructuras de comunicación y acceso remoto. • Realizar simulacros de recuperación de sistemas ante desastres para asegurar la rapidez de respuesta. • Activar y aplicar las medidas de contingencia previstas en el PACS de las dependencias en caso de interrupciones. • Trabajar en la rápida restauración de las operaciones críticas. • Conformar el "Equipo de Recuperación" y coordinar las estrategias, acciones y los procedimientos para el análisis, diagnóstico y recuperación de los sistemas que constan en el PACS de las dependencias. • Liderar las acciones para establecer en conjunto con las dependencias los PACS.

Puesto	Oficina	Correo electrónico	Teléfono	Rol	Acciones y responsabilidades
					• Coordinar en conjunto con los Gestores de Continuidad para que el "Equipo de Recuperación" y el "Equipo de Operación" trabajen en las acciones y los procedimientos para el restablecimiento de los sistemas, incluyendo las pruebas correspondientes.
Directores	DAC Digepyme DMR Dependencias	Correos personales de los directores y jefaturas activos y grupales	Celulares asignados, extensiones fijas	Gestores de Continuidad	• Conformar el "Equipo de Operación" de su dependencia. • Actuar como enlace entre el comité y sus respectivas Direcciones, implementando las acciones correspondientes en plan para cada área. • Asegurar que el personal de su dirección esté informado y capacitado en el PAICS. • Supervisar y ejecutar las políticas de continuidad en sus áreas de trabajo. • Mantener informado al equipo de recuperación sobre el estado de su área durante la crisis. • Dar prioridad al llamado del Comité de Continuidad y el Líder de TIC para las acciones que se requieran en caso de la detección de interrupción de los servicios. • Establecer el PACS de su dependencia en coordinación con el DTIC, el Líder de TIC y el Asesor de Continuidad.

Fuente: UPI, PCS, MEIC.

8.2 Equipos de apoyo:

Para este caso, los equipos de apoyo están concebidos para atender de manera específica los eventos disruptivos que afecten los sistemas de información que soportan los trámites y servicios críticos priorizados en el BIA Versión V1[7].

- **Equipo de Recuperación:**

Las funciones de un equipo de recuperación en la gestión de la continuidad del servicio son esenciales para garantizar que una organización pueda afrontar y superar incidentes que amenacen sus operaciones. El equipo de recuperación es especialista en TIC, dado a que deben desarrollar su PACS en relación con sus procesos y los sistemas que soportan los trámites y servicios críticos identificados y priorizados. Las siguientes corresponden a sus principales acciones, pero se debe desarrollar estrategias específicas dependiendo de cada sistema de información y del evento disruptivo que se pueda presentar:

- Evaluación inicial y análisis de daños:
  - Coordinación de recursos humanos y técnicos.
  - Acceso a instalaciones alternativas.
  - Activación e implementación estrategias de recuperación.
  - Restauración de sistemas y servicios críticos.
  - Reactivación de servicios esenciales.

- Validación de operatividad:
  - Comunicación con el equipo de operación.
  - Documentación exhaustiva del proceso.
  - Registro de eventos y acciones.
  - Generación de informes post-acción.

- Evaluación posterior y mejora continua:
  - Análisis de desempeño.
  - Propuestas de optimización.
  - Pruebas y simulaciones.

[7] http://reventazon.meic.go.cr/informacion/reddetransparencia/planesinstitucionales/bia_meic_v1_2024.pdf

- **Equipo de Operación:**

Son expertos en la operación del servicio, cuyo objetivo es ejecutar las acciones para emprender la operación (pruebas, comunicación con DTIC), este debe involucrar a las personas funcionarias claves del proceso, incluyendo las jefaturas y directores de las dependencias afectadas, y todas las personas responsables de aplicar las medidas tanto preventivas como de recuperación ante un evento disruptivo, en el servicio o trámite. Entre las acciones importantes están:

- Seguimiento continuo y monitoreo del funcionamiento de los sistemas de información.
- Comunicación ante la detección de una interrupción o anomalía en el funcionamiento del sistema de información.
- Levantamiento y documentación de fallas.
- Apoyo en las pruebas de recuperación y operación.

8.3 Brigada de Emergencias:

Su conformación y funciones corresponden a las que se definan en el marco institucional y en las funciones del experto de Salud Ocupacional y Dirección Administrativa Financiera y Oficialía Mayor, y que en materia de continuidad les corresponde velar por el adecuado funcionamiento del Plan de Emergencias, así como aquellas funciones establecidas.

9. Acciones institucionales para la Continuidad del Servicio

Para implementar un plan de continuidad del servicio, es fundamental establecer lineamientos claros y estructurados que guíen a la organización desde la activación del plan hasta la completa recuperación y normalización de las operaciones. A continuación, detallamos las acciones principales de cada fase:

Figura N°2: Fases del Plan de Acción Institucional para la Continuidad del Servicio (PAICS)

Fuente: UPI, MEIC.

9.1 Fase 1: Gestión de riesgos

Se realizó un exhaustivo análisis de riesgos en la aplicación de la herramienta SEVRI y en el BIA Versión V1[8].

9.2 Fase 2: Activación del PAICS

La activación del plan debe de realizarse una vez se tenga claridad de si se está ante un evento o una crisis, analizando y evaluando el panorama y el impacto.

Tener claridad si se está ante un incidente o una crisis es vital a efecto de no entorpecer el actuar institucional; un **incidente se refiere a cualquier evento que pueda interrumpir o afectar negativamente un proceso o servicio,** como una interrupción del suministro eléctrico o un error humano que causa un fallo en el sistema. Una **crisis se refiere a una situación más grave que amenaza la continuidad del negocio en su totalidad,** como un desastre natural, un ciberataque masivo o un brote de enfermedades. La diferencia principal radica en su nivel de impacto. Un incidente puede ser manejado por los enlaces de dependencia con la finalidad de mitigar su impacto y restaurar los servicios afectados. Una crisis puede requerir la activación del PAICS, que involucra los diversos actores y equipos definidos para tal fin.

Asimismo, se debe considerar la naturaleza del evento para su debida activación, es decir, cuando se trata de interrupciones por una causa de desastre que afecte alguna de las instalaciones del MEIC, los protocolos de activación recaerán sobre Salud Ocupacional del ministerio y la brigada de emergencia. Es importante indicar que esta sección es tomada del MH, en su Plan de Continuidad. (Anexo 1: "Ficha Criterios para Activación del PAICS")

[8] http://reventazon.meic.go.cr/informacion/reddetransparencia/planesinstitucionales/bia_meic_v1_2024.pdf

Cuadro N°2: Situaciones y responsables de la activación del PAICS

Situación	Comité para la Continuidad del Servicio Roles					Brigada de Emergencias	DIAF
	Gestores de Continuidad Procesos Críticos	Líder TIC	Asesor Continuidad	Líder Continuidad	Líder de Comunicación Interna y Atención Externa		
Amenazas contra la vida de las personas	■	■	■	■	■	■	■
Incidentes causados por el personal -Fraude -Hurto -Robo -Error Humano	■						
Problemas con Instalaciones Clave -Problemas de acceso al Edificio -Deterioro o daño total o parcial				■		■	■
Toma de instalaciones				■		■	■
Problemas con la Tecnología -Problemas con Sistemas o infraestructura que soportan los procesos críticos del negocio-	■	■	■	■	■		
Problemas con Proveedores				■			■
Afectación de la Imagen Institucional	■		■	■	■		
Emergencia Nacional	■	■	■	■		■	■
Ciberseguridad		■	■	■			
Cambios regulatorios o legales	■	■	■	■	■		

Fuente: UPI, MEIC y MH.

9.3 Fase 3: Identificación de fallas

Es importante identificar los tipos de fallas, para así establecer las acciones pertinentes y los procedimientos de continuidad, en este caso podemos enlistar (podrían presentarse otras, por lo que podría requerirse actualizar este listado en cualquier momento):

Cuadro N°3: Fallas que podrían afectar la continuidad del servicio

Técnicas	Administrativas	Ambientales
1. Fallas en el hardware – Problemas con los servidores. – Redes y routers defectuosos. – Pérdida de energía eléctrica. 2. Fallas en el software – Errores de Código. – Actualizaciones fallidas. – Incompatibilidades entre sistemas. 3. Problemas de bases de datos – Corrupción de datos. – Fallas de replicación o sincronización. 4. Fallas en la infraestructura de red – Cortes de Internet o baja conectividad. – Congestión en la red. 5. Problemas de seguridad – Ataques de denegación de servicio (DDoS). – Malware o ransomware. 6. Errores de configuración – Configuraciones incorrectas del sistema. – Errores en permisos o accesos.	1. Falta de planificación de continuidad y gestión de riesgos – Ausencia de un plan de continuidad. – Análisis de riesgos incompleto o deficiente. – No priorizar servicios críticos. 2. Falta de políticas y procedimientos documentados – Procedimientos poco claros o inexistentes. – Inconsistencias en la documentación. – Falta de control de cambios. 3. Deficiencias en la gestión de personal – Escasez de personal capacitado. – Alta rotación de personal. – Roles y responsabilidades poco definidos. 4. Falta de comunicación eficaz – Canales de comunicación inadecuados. – Falta de plan de comunicación para emergencias. – Desconexión entre departamentos. 5. Carencia de capacitación y simulacros – Falta de entrenamiento en manejo de crisis.	1. Desastres naturales – Terremotos. – Inundaciones. – Huracanes y tormentas. – Incendio. 2. Condiciones climáticas extremas – Altas temperaturas. – Bajas temperaturas. – Tormentas de lluvias ventosas y con granizo. 3. Cortes de energía – Interrupciones en el suministro eléctrico. – Fluctuaciones de voltaje. – Fallas en sistemas de respaldo de energía. 4. Problemas de infraestructura física – Fallas en sistemas de climatización. – Problemas en la estructura del edificio. – Humedad y corrosion. 5. Contaminación y polución – Contaminación del aire. – Contaminación acústica – Contaminación electromagnética. 6. Plagas y fauna – Invasión de roedores. – Insectos. – Aves y otros animales. 7. Fallas en el suministro de agua

Técnicas	Administrativas	Ambientales
	– No realizar simulacros regulares. – Ausencia de revisión post-incidente. 6. Fallas en la gestión de recursos financieros y presupuestarios – Inversión insuficiente en infraestructura de respaldo. – Presupuesto limitado para seguridad. – Recortes en programas de capacitación. 7. Procesos de toma de decisiones ineficientes – Proceso de decisión lento o burocrático. – Falta de un líder de continuidad. – Delegación inadecuada de autoridad. 8. Deficiencias en la gestión de proveedores y terceros – Dependencia excesiva de proveedores únicos. – Contratos y acuerdos de nivel de servicio (SLA) deficientes. – No realizar evaluaciones de riesgos en proveedores. 9. Falta de evaluación y mejora continua – No realizar revisiones periódicas. – Falta de un plan de mejora continua. – Ignorar lecciones de incidentes anteriores.	– Interrupción del suministro de agua. – Contaminación del agua. – Inundaciones internas. 8. Problemas en la infraestructura de telecomunicaciones – Interrupciones en la conectividad. – Fallas en el proveedor de servicios de internet. – Torres de telecomunicaciones dañadas. 9. Problemas de salud pública y crisis sanitarias – Pandemias. – Brotes de enfermedades en el personal. – Condiciones de trabajo inseguras.

Fuente: UPI, MEIC.

9.4 Fase 4: Implementación – Recuperación

A continuación, se muestra el procedimiento de recuperación:

Cuadro N°4: Procedimiento institucional para la recuperación ante un evento disruptivo.

MINISTERIO DE ECONOMÍA, INDUSTRIA Y COMERCIO | GOBIERNO DE COSTA RICA	**Proceso:**	Continuidad del Servicio	**Versión:**	1.2024
	Subproceso:	Gestión Institucional de la Continuidad de los Servicios	**Código:**	MEIC-CCS-PAICS-PIRED-2024
	Procedimiento:	Procedimiento institucional para la recuperación ante un evento disruptivo.	**Fecha de actualización:**	14/11/2024
	Unidad responsable:	Comité para la Continuidad del Servicio	**Elaborado por:**	Wendy María Fallas Garro, Jefatura UPI y Contralora de Servicios a.i

Código	Actividad	Observaciones	Responsable	Entradas	Salidas
PIRED-01	Analizar el evento para determinar la activación del Plan de Acción Institucional de Continuidad del Servicio (PAICS).	Se presentan un evento disruptivo que afecta la prestación de los trámites y servicios priorizados. En este caso el Líder de Continuidad analiza el evento mediante los criterios correspondientes que constan en la "Ficha Criterios para Activación del PAICS". Si es un incidente causado por el personal: fraude, hurto, robo, error humano, quien activa el plan es el "Gestor de Continuidad" correspondiente. Ver Cuadro N°2: Situaciones.	Líder de Continuidad o Gestor de Continuidad	Evento disruptivo	PAICS activado
PIRED-02	Identificar el tipo de falla que desencadenó el evento disruptivo.	El tipo de falla puede ser: técnica, administrativa o ambiental. Dependiendo de las mismas, se deben iniciar las acciones establecidas por cada responsable para la recuperación y continuidad. Ver Cuadro N°3: Fallas que podrían afectar la continuidad del servicio.	Líder de Continuidad	PAICS activado	Tipo de falla identificada

MINISTERIO DE ECONOMÍA, INDUSTRIA Y COMERCIO | GOBIERNO DE COSTA RICA

Proceso:	Continuidad del Servicio	**Versión:**	1.2024
Subproceso:	Gestión Institucional de la Continuidad de los Servicios	**Código:**	MEIC-CCS-PAICS-PIRED-2024
Procedimiento:	Procedimiento institucional para la recuperación ante un evento disruptivo.	**Fecha de actualización:**	14/11/2024
Unidad responsable:	Comité para la Continuidad del Servicio	**Elaborado por:**	Wendy María Fallas Garro, Jefatura UPI y Contralora de Servicios a.i

Código	Actividad	Observaciones	Responsable	Entradas	Salidas
PIRED-03	¿Es una falla técnica?	**Si:** Continuar con PIRED-06, en este caso, los Equipo de Apoyo, tanto el equipo de recuperación como el equipo de operación realizan las acciones necesarias para que se continúe con la prestación de los trámites y servicios en el menor tiempo posible. El Líder de Continuidad debe alertar de inmediato para que se inicien los procesos de recuperación y operación. **No:** continúa a actividad PIRED-04	Líder TIC, Gestores de Continuidad, Equipo de Recuperación, Equipo de Operación	Tipo de falla identificada	Alerta generada e inicio de recuperación
PIRED-04	¿Es una falla administrativa?	**Si:** Continuar con PIRED-06, en este caso, el Líder de Continuidad o los Gestores de Continuidad realizan las acciones correspondientes para reestablecer la operación. El Líder de Continuidad debe alertar de inmediato para que se inicien los procesos de recuperación y operación. **No:** continúa a actividad PIRED-05	Líder de Continuidad o Gestor de Continuidad	Tipo de falla identificada	Alerta generada e inicio de recuperación
PIRED-05	¿Es una falla ambiental?	**Si:** Continuar con PIRED-06, en este caso, el Líder de Continuidad y la Brigada de Emergencias o los Gestores de Continuidad realizan las acciones correspondientes para reestablecer la operación. El Líder de Continuidad debe alertar de inmediato para que se inicien los procesos de recuperación y operación. **No:** Ir a PIRED-01 para analizar el evento.	Líder de Continuidad y Brigada de Emergencias o Gestor de Continuidad	Tipo de falla identificada	Alerta generada e inicio de recuperación

MINISTERIO DE ECONOMÍA, INDUSTRIA Y COMERCIO | GOBIERNO DE COSTA RICA

Proceso:	Continuidad del Servicio	**Versión:**	1.2024
Subproceso:	Gestión Institucional de la Continuidad de los Servicios	**Código:**	MEIC-CCS-PAICS-PIRED-2024
Procedimiento:	Procedimiento institucional para la recuperación ante un evento disruptivo.	**Fecha de actualización:**	14/11/2024
Unidad responsable:	Comité para la Continuidad del Servicio	**Elaborado por:**	Wendy María Fallas Garro, Jefatura UPI y Contralora de Servicios a.i

Código	Actividad	Observaciones	Responsable	Entradas	Salidas
PIRED-06	Atender el evento disruptivo según los planes, acciones y estrategias establecidas por cada responsable.	En este caso, el evento debe ser atendido por los **responsables de atención del evento**, dependiendo del tipo de falla pueden ser: Líder de Continuidad, Brigada de Emergencias, Gestores de Continuidad, Líder TIC y Equipos de Apoyo (equipo de recuperación y equipo de operación), quienes deben poner en práctica las acciones y estrategias plasmadas en sus planes de acción.	Responsables de la atención del evento	Comunicaciones notificadas	Evento disruptivo atendido
PIRED-07	Informar al Comité para la Continuidad del Servicio y a los involucrados correspondientes.	El Líder de Comunicación Interna y de Atención Externa, coordina las acciones necesarias con los responsables para generar los comunicados correspondientes, en aras de que todos los interesados estén informados del estado de las acciones y de los procesos de recuperación y operación.	Líder de Comunicación Interna y Atención Externa	Inicio de recuperación	Comunicaciones notificadas
PIRED-08	Informar al Comité para la Continuidad del Servicio.	Los responsables de la atención del evento deben notificar al Comité para la Continuidad del Servicio sobre el estado del proceso de recuperación y operación.	Responsables de la atención del evento	Evento disruptivo atendido	Comunicación generada
PIRED-09	Registrar el evento ocurrido.	El líder de Continuidad debe registrar el evento ocurrido para documentar el proceso, esto en la ficha: "Registro de evento disruptivo en la continuidad de los servicios"	Líder de Continuidad	Comunicación generada	Ficha generada y evento documentado

Fuente: UPI, MEIC

Figura N°3: Flujograma del procedimiento institucional para la recuperación ante un evento disruptivo.

DIAGRAMA DE ACTIVIDADES

Proceso:	Continuidad del Servicio	**Fecha de actualización:**	14/11/2024
Subproceso:	Gestión Institucional de la Continuidad del Servicio	**Elaborado por:**	Wendy María Fallas Garro, Jefatura UPI y Contralora de Servicios a.i
Procedimiento:	Procedimiento institucional para la recuperación ante un evento disruptivo. Cod: MEIC-CCS-PAICS-PIRED-2024	**Revisado por:**	Comité para la Continuidad del Servicio

Código	Actividad	Responsables								Observaciones
		LC	GC	LTIC	ER	EA	BE	LCIAE	RAED	
PIRED-01	Analizar el evento para determinar la activación del Plan de Acción Institucional de Continuidad del Servicio (PAICS).									Se presentan un evento disruptivo que afecta la prestación de los trámites y servicios priorizados. En este caso el Líder de Continuidad analiza el evento y mediante los criterios correspondientes que constan en la "Ficha Criterios para Activación del PAICS". Si es un incidentes causado por el personal: fraude, hurto, robo, error humano, quien activa el plan en el "Gestor de Continuidad" correspondiente. Ver Cuadro N°2: Situaciones
PIRED-02	Identificar el tipo de falla que desencadenó el evento disruptivo.									El tipo de falla puede ser: técnica, administrativa o ambiental. Dependiendo de las mismas, se deben iniciar las acciones establecidas por cada responsable para la recuperación y continuidad. Ver Cuadro N°3: Fallas que podrían afectar la continuidad del servicio.
PIRED-03	¿Es una falla técnica?									**Si:** Continuar con PIRED-06, en este caso, los Equipo de Apoyo, tanto el equipo de recuperación como el equipo de operación realizan las acciones necesarias para se continúe con la prestación de los trámites y servicios en el menor tiempo posible. El Líder de Continuidad debe alertar de inmediato para que se inicien los procesos de recuperación y operación. **No:** continúa a actividad PIRED-04
PIRED-04	¿Es una falla administrativa?									**Si:** Continuar con PIRED-06, en este caso, el Líder de Continuidad o los Gestores de Continuidad realizan las acciones correspondientes para reestablecer la operación. El Líder de Continuidad debe alertar de inmediato para que se inicien los procesos de recuperación y operación. **No:** continúa a actividad PIRED-05
PIRED-05	¿Es una falla ambiental?									**Si:** Continuar con PIRED-06, en este caso, el Líder de Continuidad y la Brigada de Emergencias o los Gestores de Continuidad realizan las acciones correspondientes para reestablecer la operación. El Líder de Continuidad debe alertar de inmediato para que se inicien los procesos de recuperación y operación. **No:** Ir a PIRED-01 para analizar el evento.
PIRED-06	Atender el evento disruptivo según los planes, acciones y estrategias establecidas por cada responsable.									En este caso, el evento debe ser atendido por los responsables de atención del evento, dependiendo del tipo de falla pueden ser: Líder de Continuidad, Brigada de Emergencias, Gestores de Continuidad, Líder TIC y Equipos de Apoyo (equipo de recuperación y equipo de operación), quienes deben poner en práctica las acciones y estrategias plasmadas en sus planes de acción.
PIRED-07	Informar al Comité para la Continuidad del Servicio y a los involucrados correspondientes.									El Líder de Comunicación Interna y de Atención Externa, coordina las acciones necesarias con los responsables para generar los comunicados correspondientes, en aras de que todos los interesados estén informados del estado de las acciones y de los procesos de recuperación y operación.
PIRED-08	Informar al Comité para la Continuidad del Servicio.									Los responsables de la atención del evento deben notificar al Comité para la Continuidad del Servicio sobre el estado del proceso de recuperación y operación.
PIRED-09	Registrar el evento ocurrido.									
TOTAL:										

Responsables

LC	Líder de Continuidad
GC	Gestores de Continuidad
LTIC	Líder de TIC
ER	Equipo de Recuperación
EA	Equipo de Operación
BE	Brigada de Emergencia
LCIAE	Líder de Comunicación Interna y Atención
RAED	Responsables de la atención del evento disruptivo

1 de 1

Fuente: UPI, MEIC

9.5 Fase 5: Ciclo de pruebas de continuidad

Algunos modelos de pruebas propuestos por el MH, también se considera de importante adopción para el MEIC. La realización de pruebas permite:

- Identificar debilidades o puntos de falla en el plan.
- Asegurar que el personal esté preparado para actuar en situaciones de emergencia y de interrupción de la prestación de trámite y servicios.
- Garantizar que los sistemas y procesos críticos puedan ser restaurados.
- Validar y actualizar el plan periódicamente.

Es fundamental realizar las pruebas de forma regular y actualizar el plan con base en los hallazgos para mejorar la resiliencia de la organización.

Existen diferentes tipos de pruebas que se pretenden realizar como parte del ciclo de pruebas de continuidad del negocio. Los tipos para aplicar son:

• **Pruebas de escritorio o tabletop:** Se realizarán cuando sea requerido, considerando que este tipo de prueba implica una revisión detallada del plan de continuidad del negocio por parte de los responsables y otros miembros del equipo para verificar su completitud, relevancia y necesidad de actualización.

• **Simulación de un evento de interrupción del negocio o Pruebas de simulacro funcional:** Esta prueba consiste en simular un evento de interrupción del negocio, como un corte de energía o una inundación, y ver cómo se activa el plan de continuidad. Implican la ejecución de ciertos elementos del plan en condiciones controladas. Se busca activar algunos procedimientos, como comunicación de emergencia o reubicación de operaciones críticas, sin afectar la operatividad normal. Esta prueba se realizará de acuerdo con el cronograma que defina el Comité de Continuidad del Negocio y que será coordinado con las áreas responsables.

· **Pruebas de recuperación de datos y sistemas (Disaster Recovery Testing):** Se enfocan en evaluar los procedimientos para restaurar datos, servidores, sistemas de TI y servicios. Puede incluir la recuperación de servidores en un sitio secundario o la restauración desde respaldos. Esta prueba se realizará en coordinación con el Departamento de Tecnologías de Información y el Comité de Continuidad del Negocio, cuando se refiera a sistemas informáticos.

9.6 Fase 6: Mejora Continua

La Fase Mejora Continua en este PAICS, busca asegurar que el plan esté siempre actualizado, sea efectivo y responda de manera óptima ante incidentes. La mejora continua implica un ciclo de revisión, ajuste y optimización del plan basándose en experiencias, pruebas y cambios en el entorno interno o externo de la institución.

El objetivo de esta fase es garantizar la constante actualización y optimización del plan mediante la evaluación y retroalimentación periódicas, con el fin de mantener su relevancia, eficacia y eficiencia en respuesta a incidentes o interrupciones. Esta fase comprende:

- Revisión periódica del PAICS:
  - Frecuencia de revisión: El PAICS debe revisarse al menos una vez al año o cada vez que ocurran cambios significativos en el entorno institucional, como cambios de liderazgo, normativas, estructura operativa, tecnologías o ubicaciones físicas.
  - Responsable de la revisión: El Comité de Continuidad del Servicio, en coordinación con el Líder de Planificación para la Continuidad, liderará las revisiones, involucrando a los responsables de las áreas críticas de la institución.

- Análisis post-incidente y retroalimentación:
  - Análisis post-incidente: Después de un evento que active el PAICS, se debe llevar a cabo una revisión exhaustiva para analizar la efectividad de la respuesta.
  - Análisis de lecciones aprendidas: Identificar éxitos y fallos en la ejecución del plan.

- Informe de incidentes: Documentar el incidente, la respuesta, el tiempo de recuperación y los resultados obtenidos.
- Acciones correctivas: Incorporar ajustes o modificaciones al plan con base en las lecciones aprendidas.

- Monitoreo de cambios en el entorno:
  - Cambios normativos o legales: Estar atentos a las modificaciones en leyes, regulaciones y políticas gubernamentales que puedan afectar la continuidad de la institución.
  - Avances tecnológicos: Evaluar e incorporar nuevas tecnologías que puedan mejorar la capacidad de respuesta o comunicación durante incidentes.
  - Cambios internos: Cualquier reestructuración, cambio en los procesos o incorporación de nuevas áreas debe reflejarse en el PAICS.

- Actualización documental
  - Gestión de versiones: Mantener un registro detallado de todas las modificaciones del PAICS, indicando la fecha de revisión, los cambios realizados y los responsables.
  - Distribución de actualizaciones: Asegurar que la última versión del plan esté disponible y sea accesible para todos los actores clave, evitando confusiones durante una emergencia.

10. ANEXOS

10.1: Anexo 1: Ficha: Criterios de activación del PAICS

Tipo de problema	Situación	
Problemas con el personal	Ausencia o pérdida del personal necesario para la ejecución de los procesos críticos (enfermedad, licencias, movimientos de personal, secuestro, muerte, accidente o violencia)	☐
	Declaratoria de emergencia nacional por pandemia	☐
	Imposibilidad de acceso a las instalaciones del MEIC (por huelgas, bloqueos o inundación)	☐
Problemas de infraestructura	Deterioro o daño de la infraestructura física de edificios luego de un evento natural (tormenta, sismo, incendio, erupción volcánica, etc.) o provocado por el hombre de forma accidental o intencionalmente	☐
Problemas con la tecnología	Caída nacional de los servicios de telecomunicaciones donde su recuperación por parte del proveedor sea mayor al RTO mínimo de los procesos críticos afectados	☐
	Caída de los sistemas críticos que supere los RTO´s establecidos para las aplicaciones que soportan los procesos críticos y la atención a usuarios	☐
	Faltante del fluido eléctrico superior al tiempo de operación estándar de las fuentes alternas (plantas eléctricas y UPS) de manera permanente, causado por agentes externos o internos	☐
	Ciberataque a un nivel de afectación de los sistemas críticos	☐
Problemas con los proveedores	No disponibilidad de los recursos (tecnológicos o de personal) adquiridos por parte del ministerio que sean necesarios para el soporte y la ejecución de los procesos críticos	☐
Problemas con la operativa institucional	No disponibilidad, entrega tardía o inconsistencias en la información que sirve como insumo para la operación de los procesos críticos	☐
	Materialización de los riesgos identificados en el Análisis de Riesgos de Continuidad de Negocio que detengan los procesos críticos.	☐
	Cambios en la normativa de los procesos críticos	☐

10.2: Anexo 2: Ficha: Registro de evento disruptivo en la continuidad de los servicios.

Información General	
Fecha de incidente:	Hora de incidente:
Área o persona que reporta el incidente:	
Proceso crítico afectado:	
Ubicación del incidente (Edificio, piso o área donde ocurre el incidente):	
Breve descripción del incidente:	
Respuesta	
1. Tipo de falla, relacionado con: ☐ Técnica ☐ Administrativa ☐ Ambiental Detalle la falla:	
2. ¿Cuáles áreas o departamentos se vieron afectados como consecuencia de esta interrupción?	
3. ¿En cuánto tiempo se controló la situación antes de activar la continuidad? ☐ De 0 hora a 4 horas ☐ De 4 horas a 1 día ☐ De 1 día a 2 días ☐ De 2 días y hasta 4 días	
4. ¿Se activó el Plan de Acción Institucional para la Continuidad del Negocio? ☐ Si ☐ No	
Recuperación	
5. ¿Estaban habilitados los sistemas de información que soportan el proceso crítico? ☐ Si ☐ No Si su pregunta es "No", indique cuáles sistemas no estaban habilitados:	
6. ¿Se coordinó con equipos de apoyo para la realización de trabajos? ☐ Si ☐ No	
Reactivación de Operaciones	
7. ¿Cómo se resolvió el incidente?	
8. ¿Cuántas horas tomó volver al funcionamiento normal del negocio? (desde el momento en que se controló la situación hasta el regreso a la operación normal):	
9. ¿Cuáles otros procesos fueron afectados por dicha interrupción?	
Recuperación de desastres	
10. ¿Es necesario realizar trabajos a la infraestructura del edificio? ☐ Si ☐ No	
Realizado por:	Aprobado por: