MINISTERIO DE SALUD | GOBIERNO DE COSTA RICA

Política de Continuidad de las Operaciones soportadas por Tecnologías de Información y Comunicación

DEPARTAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

UNIDAD DE GESTIÓN DE SERVICIOS

febrero, 2024

Tabla de elaboración

Elaborado por: Fecha de elaboración:	Ing. Roberto Quirós García Inga. Florina Araya Bonilla Ing. Leonardo Brenes Guadamuz Octubre 2023
Revisado por: Fecha de revisión:	MCI. Petronila Mairena Traña, Ing Octubre 2023
Validado por: Fecha de validación:	Lic. Edgar Morales González Lic. Jonathan Gómez Benavides Lic. Shirley Espinoza Vindas Noviembre 2023

Tabla de control de versiones

Versión	Fecha	Actualizado por	Aprobado por
1.0	06 de febrero 2024		Consejo Tecnológico, Sesión Ordinaria MS-CT-002-2024. 6 de febrero de 2024

Contenido

1. Introducción

La política de continuidad de servicios de tecnologías de información y comunicación del Ministerio de Salud permite que los servicios críticos de tecnología de la información y comunicación se mantengan operando sin interrupción.

Esta política procura la continuidad y disponibilidad operativa de los servicios tecnológicos que menciona el Marco de Gestión TIC y propone las acciones necesarias para prevenir y mitigar interrupciones en los servicios de tecnologías de información y comunicación, ya sea debido a amenazas cibernéticas, desastres naturales u otras eventualidades.

El compromiso es garantizar que los funcionarios y los ciudadanos puedan acceder a la información y las herramientas necesarias en todo momento, lo que a su vez contribuye con una atención más eficiente y segura.

A través de esta política, el Ministerio de Salud reafirma su compromiso con la excelencia en la gestión de servicios de tecnologías de información y comunicación, y su determinación de proteger la integridad de los datos y la continuidad de las operaciones en beneficio de la salud pública.

2. Objetivo General

Promover la disponibilidad y continuidad de las operaciones soportadas por tecnologías de información y comunicación del Ministerio de Salud, mediante la planificación e implementación de acciones preventivas y correctivas en caso de eventos adversos que provoquen interrupciones.

2.1 Objetivos Específicos

- Minimizar la frecuencia de interrupciones en la operación de los procesos institucionales.
- Asegurar la oportunidad de las operaciones
- Validar el cumplimiento de la normativa referente a la continuidad de los servicios de tecnologías de información y comunicación.
- Garantizar que todos los procesos críticos operen adecuadamente, bajo los principios de seguridad, universalidad, continuidad, oportunidad, calidad y confiabilidad.

3. Alcance

Esta política es de acatamiento obligatorio para todos los funcionarios de las unidades organizativas en los tres niveles de gestión y terceros que estén involucrados directa o indirectamente con el uso de tecnologías de información y comunicación del Ministerio de Salud.

4. Política de Continuidad

Esta política es de competencia obligatoria para todos los niveles de gestión del Ministerio de Salud; por lo tanto, deben establecerse los mecanismos y medios que permitan comunicar la misma a todos los funcionarios con el fin de poder garantizar razonablemente la continuidad del servicio en caso de un evento que afecte su operación normal.

El Departamento de Tecnologías de Información y Comunicación (DTIC) es el responsable de mantener todos los procesos críticos de tecnologías de información y comunicación de la institución de forma activa.

Se establecen como elementos primordiales de esta política, la protección de los activos tecnológicos de la institución, y la continuidad de las operaciones.

La institución debe tomar las previsiones necesarias para garantizar la asignación de recursos humanos, financieros y materiales para asegurar el cumplimiento de la presente política, la ejecución del Plan de Contingencias y garantizar la continuidad de los servicios al ciudadano.

La Dirección de Desarrollo Humano debe velar y gestionar la asignación de recursos para que los funcionarios se capaciten y puedan dar continuidad a los servicios, con el compromiso de cumplir con la normativa vigente, y principalmente los requerimientos de oportunidad de los usuarios.

En resumen, la política de continuidad de los servicios soportados por tecnologías de información del Ministerio de Salud se alinea con el propósito institucional de garantizar la protección y mejoramiento de la salud física, mental y social de la población, mediante el ejercicio de la rectoría en salud, de tal forma que pueda evitarse o minimizarse el impacto y tiempo de respuesta al usuario, ante alguna interrupción o evento fortuito.

4.1. Gestión de riesgos TIC

El Departamento de Tecnologías de Información y Comunicación junto con las unidades organizativas correspondientes, debe mantener un registro actualizado de los activos tecnológicos (hardware, software, aplicaciones y comunicaciones), clasificados por nivel de gestión, según el nivel de criticidad, características, configuración, servicios; realizar el análisis de riesgos, plantear las medidas de mitigación y administrativas y definir un equipo de respuesta, conformado por los responsables del recurso crítico en cualquier nivel de gestión.

4.2 Elaboración de planes de contingencia

El Departamento de Tecnologías de Información y Comunicación y las unidades organizativas correspondientes, deben elaborar los planes de contingencias que considere todos los recursos críticos disponibles y establecer los puntos de control necesarios para maximizar la continuidad de todas las operaciones y servicios tecnológicos, los roles y responsables para su ejecución.

Cada unidad organizativa que conforma el Departamento de Tecnologías de Información y Comunicación debe elaborar el plan de contingencia de los servicios críticos que administra.

4.3 Implementación de los planes de contingencia

Cada unidad organizativa que conforma el Departamento de Tecnologías de Información y Comunicación y las unidades organizativas involucradas deben ejecutar sus planes de contingencia en el momento de ocurrencia o materialización de un riesgo.

4.4 Realización de Pruebas

Las unidades organizativas deben someter a pruebas periódicas los planes, para asegurar su correcto funcionamiento, así como la normativa que los sustenta, para identificar brechas en la planificación y comprobar su efectividad mediante simulacros.

Las pruebas pueden llevarse a cabo de varias maneras, según los recursos disponibles y el sistema o servicios a ser probados, para asegurar que cada aspecto definido en el plan de contingencia funcione como se espera y se recupere satisfactoriamente después de una interrupción.

Además, es importante establecer capacitaciones para preparar al personal responsable de la recuperación para la activación de los planes. Ambas actividades, las pruebas y la capacitación, mejoran la eficacia del plan y la preparación general de la institución.

4.5 Mantenimiento de los planes de contingencia

El mantenimiento de los planes de contingencias es un proceso de mejora continua que requiere una revisión y actualización regular para asegurar su relevancia, efectividad y calidad.

Cada unidad organizativa debe contemplar la revisión regular de las actividades, normativa, contactos de emergencia, entre otros aspectos, en el caso de producirse cambios de recursos humanos, infraestructura, sistemas de información y los servicios tecnológicos, así como realizar pruebas, capacitación constante al personal responsable y documentar estas revisiones, resultados de las pruebas y las actualizaciones y opciones de mejora de dichos planes.

La Política de Continuidad de las Operaciones soportadas por Tecnologías de Información y Comunicación debe ponerse en práctica constantemente y mantenerse actualizada.

5. Glosario

Amenaza: Una amenaza informática es toda circunstancia, evento o persona que tiene el potencial de causar daño a un sistema en forma de robo, destrucción, divulgación, modificación de datos o negación de servicio.

Disponibilidad: Esto significa que la información es accesible cuando los usuarios autorizados la necesitan.

Impacto: Conjunto de posibles efectos negativos que modifican el entorno normal como consecuencia de obras u otras actividades.

Interrupción: Una interrupción es una suspensión temporal de la ejecución de un proceso, para pasar a ejecutar una subrutina de servicio de interrupción, la cual, por lo general, no forma parte del programa, sino que pertenece al sistema operativo, u otra aplicación. Una vez finalizada dicha subrutina, se reanuda la ejecución del programa.

Plan de contingencia: Un plan de contingencia es un tipo de plan preventivo, predictivo y reactivo. Presenta una estructura estratégica y operativa que ayudará a controlar una situación de emergencia y a minimizar sus consecuencias negativas.

Riesgo: La probabilidad de que una amenaza se materialice, utilizando vulnerabilidades existentes de un activo o un grupo de activos, generándole perdidas o daños

Vulnerabilidad: En informática, una vulnerabilidad es una deficiencia en la programación. A este suceso también se lo denomina *bug* («bicho» en inglés), un error

o un fallo en un determinado programa de un ordenador que finaliza en un resultado no deseado.

6. Base Legal

- Decreto Ejecutivo Nº 40724-S Reglamento Orgánico del Ministerio de Salud, del 23 de setiembre de 2017 y sus reformas (febrero 2024).
- INTE G130:2022, Sistemas de Gestión de Continuidad de Servicios para organizaciones públicas y sin fines de lucro-Requisitos y orientación para su uso, 2022.
- Ley 8039, Ley de Procedimientos de Observancia de Derechos de Propiedad Intelectual y reformas.
- Ley 8220, Ley de Protección al Ciudadano del Exceso de Requisitos y Trámites, su reglamento y reformas de ambas normativas.
- Ley 8968, Ley de Protección Frente al Tratamiento de Datos Personales, su reglamento y reformas de ambas normativas.
- LTIC-CS-001. Lineamientos institucionales sobre ciberseguridad del Ministerio de Salud, 2022.
- Manual de Organización y Funciones, febrero 2024.
- Marco de Gestión de Tecnologías de Información y Comunicación del Ministerio de Salud, 2022 y sus actualizaciones.
- Norma en Seguridad de Información, 2017.
- Normas Técnicas para la Gestión y el Control de las Tecnologías de Información MICITT, 2022.
- Protocolo de Atención de Incidentes de Seguridad y Ciberseguridad del Ministerio de Salud, 2022.
- Estrategia de Transformación Digital, MICITT, 2023-2027
- Estrategia de Salud Digital MS, 2023-2030