Lima, 25 de Octubre del 2024

RESOLUCION DIRECCION EJECUTIVA N° D000111-2024-MIDIS/PNPAIS-DE

VISTOS:

El Informe N° D000439-2024-MIDIS/PNPAIS-UTI-MCP y el Memorando N° D000580-2024-MIDIS/PNPAIS-UTI de la Unidad de Tecnologías de la Información, el Informe N° D000488-2024-MIDIS/PNPAIS-UPP de la Unidad de Planeamiento y Presupuesto y el Informe Nº D000532-2024-MIDIS/PNPAIS-UAJ de la Unidad de Asesoría Jurídica; y,

CONSIDERANDO:

Que, mediante Decreto Supremo N° 013-2017-MIDIS, publicado el 07 de setiembre de 2017, se constituye el Programa Nacional “Plataformas de Acción para la Inclusión Social – PAIS”;

Que, mediante el Artículo 30 del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, indica que: “De la Seguridad Digital La seguridad digital es el estado de confianza en el entorno digital que resulta de la gestión y aplicación de un conjunto de medidas proactivas y reactivas frente a los riesgos que afectan la seguridad de las personas, la prosperidad económica y social, la seguridad nacional y los objetivos nacionales en dicho entorno. Se sustenta en la articulación con actores del sector público, sector privado y otros quienes apoyan en la implementación de controles, acciones y medidas”;

Que, el artículo 2 de la Ley N° 28551, Ley que establece la obligación de elaborar y presentar planes de contingencia, se define a los planes de contingencia como instrumentos de gestión que definen los objetivos, estrategias y programas que orientan las actividades institucionales para la prevención, la reducción de riesgos, la atención de emergencias y la rehabilitación en casos de desastres permitiendo disminuir o minimizar los daños, las víctimas u pérdidas que podrían ocurrir a consecuencia de fenómenos naturales, tecnológicos o de la producción industrial, potencialmente dañinos;

Que, mediante la Resolución de Contraloría N° 320-2006-CG, la Contraloría General de la República aprueba las Normas de Control Interno, que son aplicables a las Entidades del Estado de conformidad con lo establecido por la Ley N° 28716. Al respecto, el comentario 07 del numeral 3.10 "Controles para las Tecnologías de la Información y Comunicaciones” de las referidas normas, dispone que, “Para el adecuado ambiente de control en los sistemas informáticos, se requiere que éstos sean preparados y programados con anticipación para mantener la continuidad del servicio. Para ello se debe elaborar, mantener y actualizar periódicamente un plan de contingencia debidamente autorizado y aprobado por el titular o funcionario designado donde se establezcan procedimientos para la recuperación de datos con el fin de afrontar situaciones de emergencia”;

Que, mediante el artículo 1 de la Ley N° 29664, Ley que crea el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD) y modificatorias señala que el SINAGERD es el sistema interinstitucional, sinérgico, descentralizado, transversal y participativo, con la finalidad de identificar los riesgos asociados a peligros, priorizar la prevención para evitar la generación de nuevos riesgos, reducir o minimizar sus efectos, así como, la preparación y respuesta ante situaciones de emergencia o desastre mediante el establecimiento de principios, lineamientos de política, componentes, procesos e instrumentos de la Gestión del Riesgo de Desastres.”

Que, mediante Resolución Ministerial N° 004-2016-PCM, se aprueba el uso obligatorio de la Norma Técnica Peruana “NTP-ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistema de Gestión de Seguridad de la Información. Requisitos. 2a. Edición”, en todas las entidades integrantes del Sistema Nacional de Informática, precisando en su numeral 4.4 que “La organización debe establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información”;

Que, conforme a lo establecido en el artículo 29 del Manual de Operaciones, la Unidad de Tecnologías de la Información es responsable de "*Elaborar y proponer los lineamientos, planes, proyectos, procedimientos y directivas de seguridad de la información y contingencias de los servicios informáticos, en el marco de lo dispuesto por el MIDIS y PCM*";

Que, por otra parte, el inciso l) del artículo 10 del Manual de Operaciones del Programa Nacional Plataformas de Acción para la Inclusión Social – PAIS, aprobado mediante Resolución Ministerial Nº 263-2017-MIDIS, se establece la facultad de la Dirección Ejecutiva para emitir resoluciones en asuntos de su competencia;

Que, con Memorándum N° D000580-2024-MIDIS/PNPAIS-UTI de fecha 18 de octubre de 2024, sustentado en el Informe D00439-2024-MIDIS/PNPAIS-UTI-MCP la Unidad de Tecnologías de la Información, remite la propuesta "Plan Multianual de Contingencia de Tecnologías de la Información y Comunicaciones del Programa Nacional "Plataformas de Acción para la Inclusión Social" 2024-2025, el cual tiene como finalidad asegurar que el Programa esté preparado para enfrentar situaciones inesperadas de manera eficaz y ordenada, asegurando la continuidad de los sistemas de información y servicios digitales; así como, la protección de la información;

Que, mediante Informe N° D000488-2024-MIDIS/PNPAIS-UPP de fecha 22 de octubre de 2024, la Unidad de Planeamiento y Presupuesto emite opinión favorable respecto a la aprobación de la propuesta de "Plan Multianual de Contingencia de Tecnologías de la Información y Comunicaciones del Programa Nacional "Plataformas de Acción para la Inclusión Social" 2024-2025; señalando, además, que se encuentra acorde a la Directiva N° 003-2022-MIDIS denominada Catálogo de Documentos Oficiales el Ministerio de Desarrollo e Inclusión Social";

Que, con Informe N° D000532-2024--MIDIS/PNPAIS-UAJ, de fecha 24 de octubre de 2024, la Unidad de Asesoría Jurídica señala que resulta viable que el Director Ejecutivo, en su calidad de máxima autoridad administrativa emita el acto resolutivo que apruebe el Plan Multianual de Contingencia de Tecnologías de la Información y Comunicaciones del Programa Nacional "Plataformas de Acción para la Inclusión Social" 2024-2025;

Con el visto de la Unidad de Tecnologías de la Información, Unidad de Planeamiento y Presupuesto y de la Unidad de Asesoría Jurídica;

De conformidad con lo dispuesto en el Decreto Supremo N° 013-2017-MIDIS, mediante el cual se crea el Programa Nacional "Plataformas de Acción para la Inclusión Social – PAIS" sobre la base del Programa Nacional Tambos, y la Resolución Ministerial N° 263-2017-MIDIS que aprueba el Manual de Operaciones del Programa Nacional "Plataformas de Acción para la Inclusión Social" – PAIS;

SE RESUELVE:

Artículo 1º.- Aprobar el Plan Multianual de Contingencia de Tecnologías de la Información y Comunicaciones del Programa Nacional "Plataformas de Acción para la Inclusión Social" 2024-2025 y sus anexos contenidos en el mismo, que forma parte integrante de la presente Resolución.

Artículo 2º.- Disponer a la Unidad de Tecnologías de la Información, la implementación y ejecución del Plan aprobado en el artículo 1 de la presente resolución.

Artículo 3º.- Encargar a la Unidad de Administración que disponga las acciones necesarias para la debida y oportuna notificación de la presente resolución a las unidades

orgánicas, unidades territoriales, al Especialista de Gestión de Calidad y al Coordinador Técnico del Programa.

Artículo 4°.- Disponer que la Unidad de Comunicación e Imagen publique la presente Resolución en el Portal de Transparencia Estándar y en el Portal Institucional del Programa

Regístrese, comuníquese, notifíquese y/o publíquese.

Documento firmado digitalmente

FIDEL PINTADO PASAPERA
DIRECTOR EJECUTIVO
PROGRAMA NACIONAL PAIS

Exp. N°: UTI00020240000382

PLAN MULTIANUAL DE CONTINGENCIA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES DEL PROGRAMA NACIONAL "PLATAFORMAS DE ACCIÓN PARA LA INCLUSIÓN SOCIAL" 2024-2025

Plan N° PAIS.GTI.PLA.19-2024-MIDIS/PAIS

Versión N° 01

Plan aprobado mediante Resolución de Dirección Ejecutiva N° -2024-MIDIS/PAIS

Etapa	Responsable	Cargo	Visto Bueno y sello:
Formulado por:	Jorge Luis Távara Vallejos	Ejecutivo(a) de la Unidad de Tecnologías de la Información	PAIS Plataformas de Acción para la Inclusión Social Fecha: Firmado digitalmente por TAVARA VALLEJOS Jorge Luis FAU 20601993181 soft Motivo: Soy el autor del documento Fecha: 22.10.2024 15:00:25 -05:00
Revisado por:	Irma Jennypher Cuba Araoz	Ejecutivo(a) de la Unidad de Planeamiento y Presupuesto	PAIS Plataformas de Acción para la Inclusión Social Fecha: Firmado digitalmente por CUBA ARAOZ Irma Jennypher FAU 20601993181 soft Motivo: Soy el autor del documento Fecha: 22.10.2024 15:54:27 -05:00
	Igor Elías Mejía Verástegui	Ejecutivo(a) de la Unidad de Asesoría Jurídica	PAIS Plataformas de Acción para la Inclusión Social Fecha: Firmado digitalmente por MEJIA VERASTEGUI Igor Elias FAU 20601993181 soft Motivo: Soy el autor del documento Fecha: 25.10.2024 09:18:06 -05:00
Aprobado por:	Fidel Pintado Pasapera	Director Ejecutivo	PAIS Plataformas de Acción para la Inclusión Social Fecha: Firmado digitalmente por PINTADO PASAPERA Fidel FAU 20601993181 soft Motivo: Soy el autor del documento Fecha: 25.10.2024 09:41:54 -05:00

PLAN MULTIANUAL DE CONTINGENCIA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES DEL PROGRAMA NACIONAL "PLATAFORMAS DE ACCIÓN PARA LA INCLUSIÓN SOCIAL" 2024-2025

ÍNDICE

1. INTRODUCCIÓN

Un Plan de Contingencia de Tecnologías de la Información y Comunicación (PCTIC) es un documento estratégico dentro la gestión de riesgos y continuidad operativa de cualquier organización moderna. Los sistemas de Información y servicios digitales juegan actualmente un rol crucial en la mayoría de los procesos organizacionales, ya que permiten la gestión de datos, la comunicación interna y externo, la automatización de tareas y el acceso a información en tiempo real. En ese sentido, una interrupción en los sistemas de información y/o servicios digitales, ya sea causado por fallas técnicas, desastres naturales, ataques cibernéticos o errores humanos, puede generar consecuencias graves, como la paralización de los servicios críticos, perdida de datos, daños a la reputación, entre otros.

El presente documento define el Plan de Contingencia de Tecnologías de la Información y Comunicación del Programa Nacional "Plataformas de Acción para la Inclusión Social" como un proceso continuo de planeación, desarrollo, prueba e implantación de procesos y procedimientos estructurados que deben implementarse en caso de una emergencia. Estas acciones buscan asegurar la rápida restauración y recuperación de los sistemas de información y servicios digitales minimizando el tiempo de inactividad y reduciendo el impacto negativo sobre las operaciones del Programa.

A través de este Plan, se pretende asegurar que el Programa Nacional "Plataformas de Acción para la Inclusión Social" esté preparado para enfrentar situaciones inesperadas de manera eficaz y ordenada, asegurando la continuidad de los sistemas de información y servicios digitales; así como, la protección de la información.

2. MARCO NORMATIVO

2.1. Ley N° 29664, Ley que crea el Sistema Nacional de Gestión de Desastres (SINAGERD)

2.2. Ley N° 29733, Ley de Protección de Datos Personales

2.3. Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital

2.4. Decreto Supremo N° 003-2013-JUS, que aprueba el Reglamento de la Ley N° 29733; Ley de Protección de Datos Personales

2.5. Decreto Supremo N° 106-2027-PCM, que aprueba el Reglamento para la identificación, evaluación y gestión de riesgos de los activos críticos nacionales (ACN)

2.6. Decreto Supremo N° 029-2021-PCM, que aprueba el Reglamento del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo

2.7. Decreto Supremo N° 085-2023-PCM. que aprueba la Política Nacional de Transformación Digital al 2030

2.8. Decreto de Urgencia N° 007-2020, que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento.

2.9. Decreto Supremo N.° 005-2024-MIDIS, que aprobó la Sección Primera del Reglamento de Organización y Funciones del Ministerio de Desarrollo e Inclusión Social.

2.10. Decreto Supremo N.° 006-2024-MIDIS, que aprobó la Sección Primera del Reglamento de Organización y Funciones del Organismo de Focalización e Información Social (OFIS).

2.11. Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023-PCM/SGTD que establece la implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información en las Entidades Públicas

2.12. Resolución Ministerial N° 028-2015-PCM, que aprueba los lineamientos para la Gestión de la Continuidad Operativa en las entidades públicas en los tres niveles de gobierno

2.13. Resolución Ministerial N° 188-2015-PCM, que aprueba los lineamientos para la formulación y aprobación de Planes de Contingencia

2.14. Resolución Ministerial N° 002-2021-MIDIS, que aprueba los lineamientos de Seguridad de la Información del Ministerio de Desarrollo e Inclusión Social

2.15. Resolución Ministerial N° 111-2021-MIDIS, que aprueba el Plan de Continuidad Operativa del MIDIS

2.16. Resolución Ministerial N° 138-2021-MIDIS, que aprueba el manual N° 004-2021-MIDIS, manual para la gestión de riesgos de procesos

2.17. Resolución Ministerial N° 159-2022-MIDIS, que aprueba la Directiva N° 003-2022-MIDIS denominada "Catálogo de Documentos Oficiales del Ministerio de Desarrollo e Inclusión Social"

2.18. Resolución Ministerial N° 061-2023-MIDIS, que aprueba el Plan de Gestión de Riesgos de Desastres del MIDIS.

2.19. Resolución Ministerial N° 100-2023-MIDIS, que aprueba el Plan Estratégico Institucional del MIDIS

2.20. Resolución de Secretaría General N.° 030-2024-MIDIS-SG, que aprueba el Plan Nº 02-2024-MIDIS-SG "Plan de Contingencia y Recuperación de los Servicios Informáticos del Centro de Datos de la Sede Central del Ministerio de Desarrollo e Inclusión Social"

2.21. Resolución Directoral N° 060-2023-MIDIS/PNPAIS-DE, que aprueba el "Plan de Implementación del Sistema de Gestión de Seguridad de la Información del PNPAIS"

2.22. Resolución de Dirección Ejecutiva N° 062-2023-MIDIS-PNPAIS-DE, que conforma el Equipo de Respuesta ante Incidentes de Seguridad Digital (CSIRT) del Programa Nacional "Plataformas de Acción para la Inclusión Social – PAIS"

2.23. Resolución de Dirección Ejecutiva N° 055-2024-MIDISPNPAIS-DE, que aprobó el Instructivo "Formulación revisión y aprobación de documentos normativos del Programa Nacional Plataformas de Acción para la Inclusión Social – PAIS" (PAIS.GPP. I.06-2024-MIDIS)

2.24. Resolución de Dirección Ejecutiva N° 065-2024-MIDIS-PNPAIS-DE, que aprueba el Mapa de Procesos del Programa Nacional "Plataformas de Acción para la Inclusión Social – PAIS".

3. ALCANCE

3.1. ÁMBITO DE APLICACIÓN

De cumplimiento obligatorio de todas las unidades de organización del Programa Nacional "Plataformas de Acción para la Inclusión Social – PAIS".

3.2. ACTORES INVOLUCRADOS

a. **Director Ejecutivo**: Es la máxima autoridad administrativa de la entidad, quién aprueba el plan y le corresponde prever los recursos presupuestales para el financiamiento de este.

b. **Ejecutivo de la Unidad de Tecnologías de la Información**: Es responsable de ejecutar y velar por el cumplimiento del Plan de Contingencia de Tecnologías de la Información y Comunicaciones (PCTIC). Asimismo, es responsable de supervisar las decisiones y dirigirlas estrategias tecnologías que aseguren que la infraestructura tecnológica esté protegida y pueda ser recuperada en caso de incidentes.

c. **Oficial de Seguridad y Confianza Digital**: Es el principal responsable de la gestión de riesgos relacionados con la seguridad de la información. Debe liderar la identificación de amenazas, la definición de medidas de protección y garantizar que los sistemas estén protegidos contra ataques. Asimismo, es responsable del mantenimiento (actualización y/o adaptación) del Plan de Contingencia TIC.

d. **Equipo de respuestas ante incidentes de seguridad digital – CSIRT**: Responsables de la identificación de sistemas vulnerables, la implementación de mecanismos de respaldo y recuperación, y la creación de procedimientos técnicos específicos para restaurar servicios afectados. Asimismo, son responsables de ejecutar las acciones de prevención, protección y recuperación de servicios tecnológicos y sistemas de información.

4. DIAGNÓSTICO

La Unidad de Tecnologías de la Información planifica y gestiona los recursos de hardware, software y telecomunicaciones, garantizando que los sistemas de información y los servicios digitales se mantengan operativos. Esta actividad asegura el soporte continuo a los procesos y actividades tanto administrativas como operativas que desarrolla el personal del Programa.
Los sistemas de información y servicios digitales son vulnerables a una variedad de interrupciones, que van desde leves, como cortes de energía a corto plazo o fallas en las unidades de disco, hasta eventos severos, como la destrucción de equipos, incendios o ciberataques. Estas amenazas, aunque en su mayoría mitigables, no pueden ser completamente eliminadas, lo que genera un riesgo inherente.

Actualmente, gran parte de las vulnerabilidades puede minimizarse o eliminarse mediante controles administrativos, operativos o técnicos. El PNPAIS ha implementado medidas como el

monitoreo continuo de sistemas, respaldo periódico de datos y protocolos de seguridad cibernética, lo que contribuye significativamente a la resiliencia ante posibles fallos o ataques. Sin embargo, sigue existiendo la posibilidad de interrupciones imprevistas que podrían afectar gravemente la continuidad operativa del Programa.

Los riesgos identificados también incluyen la dependencia de terceros para servicios críticos como el acceso a Internet y proveedores de hardware, lo que puede amplificar las vulnerabilidades frente a fallos externos. A pesar de contar con una infraestructura robusta, el Programa depende de la gestión oportuna de incidentes y la disponibilidad de recursos alternativos para garantizar una rápida recuperación en caso de contingencia.

Finalmente, aunque el equipo técnico tiene procedimientos internos establecidos para la recuperación de desastres, la falta de pruebas regulares y la capacitación continua del personal pueden limitar la efectividad de la respuesta en situaciones de emergencia. Por lo tanto, es fundamental fortalecer estos aspectos y garantizar que se mantengan protocolos de comunicación eficaces para informar a las partes interesadas en caso de incidentes mayores.

En conclusión, el diagnóstico revela que, si bien existen medidas importantes para reducir los riesgos implementadas en el PNPAIS, es necesario reforzar estos aspectos desarrollando planes de contingencia, realizando simulacros periódicos y actualizando continuamente las políticas de seguridad para mejorar la capacidad de respuesta ante interrupciones.

5. MARCO ESTRATÉGICO

5.1. OBJETIVO ESTRATÉGICO / ACCIÓN ESTRATÉGICA

La formulación del presente Plan se encuentra relacionado de manera general con el objetivo estratégico institucional OEI.05 "Incrementar el acceso a infraestructura y servicios básicos de la población en centros poblados rurales, rurales dispersos, en situación de pobreza, pobreza extrema y vulnerabilidad" y a las acciones estratégicas "Servicios públicos con plataformas itinerantes accesibles a las poblaciones rurales en situación de pobreza y pobreza extrema" y "Servicios públicos con plataformas fijas accesibles a las poblaciones rurales y rurales dispersas en situación de pobreza y pobreza extrema" aprobado en el marco del Plan Estratégico Institucional 2024-2030 del Ministerio de Desarrollo e Inclusión Social, según Resolución Ministerial N° 00060-2024-MIDIS.

5.2. OBJETIVO GENERAL

Garantizar la continuidad de las operaciones del Programa Nacional "Plataformas de Acción para la Inclusión Social – PAIS" mediante la implementación de acciones estructuradas que permitan la rápida recuperación de sistemas de información y servicios digitales, en caso de interrupciones no previstas, minimizando así el impacto operativo y reputacional.

6. PROGRAMACIÓN DE ACTIVIDADES

6.1. ANÁLISIS DE IMPACTO (BIA)

En esta etapa se identifica la correlación de los sistemas de información y servicios digitales con los procesos y servicios críticos del PNPAIS; así como, los efectos de sus interrupciones. Este análisis consta de tres (03) pasos:

Nro.	Paso	Descripción
1.	Determinar los procesos de misión/negocio y la criticidad de su recuperación	• Actualizar la matriz de procesos de misión / negocios respaldados por los sistemas de información y/o servicios digitales (ANEXO N° 3) • Determinar el impacto de una interrupción de cada sistema de información y servicio digital en sus procesos identificados, junto con los impactos de la inactividad y el tiempo estimado de inactividad.
2.	Identificar los requisitos de recuperación	Para una recuperación óptima es necesario una evaluación exhaustiva de los recursos necesarios para reanudar los sistemas de información y servicios digitales lo más rápido posible. Entre los recursos claves se encuentran: • Instalaciones • Personal • Equipos • Software • Archivos de datos • Componentes de los sistemas • Registros vitales • Entre otros
3.	Identificar las prioridades de recuperación	Con los resultados de las actividades anteriores, los recursos de los sistemas de información y servicios digitales se pueden vincular de manera más clara a los procesos y funciones críticas del PNPAIS. Con ello, se puede establecer niveles de prioridad para secuenciar las actividades y recursos de recuperación.

Fuente: NIST Special Publication 800-34 Rev. 1 Contingency Planning Guide for Federal Information Systems

Para complementar los pasos del Análisis de Impacto es necesario utilizar la Matriz de riesgos (ANEXO N° 4), la cual permitirá establecer el Tiempo Objetivo de Recuperación (RTO) y el Punto Objetivo de Recuperación (RPO) para cada sistema, garantizando que las estrategias de contingencia estén alineadas con los riesgos identificados y enfocadas en restaurar primero los servicios más esenciales:

"Como apoyo para la ejecución del Análisis de Impacto del Negocio, se puede revisar la información (mejores prácticas y estándares) recopilada en el ANEXO N° 5 del presente documento".

6.2. IDENTIFICACIÓN DE CONTROLES PREVENTIVOS

El impacto de las interrupciones identificadas en el BIA puede ser mitigado o eliminado mediante la implementación de controles (medidas) preventivos que disuadan, detecten y/o reduzcan los impactos en los sistemas de información y/o servicios digitales. Los controles preventivos implementados por la Unidad de Tecnologías de la Información se listan en la Matriz de Riesgos (ANEXO N° 3).

Para la actualización de los controles preventivos se debe tomar como referencia la información (estándares) recopilada en el Anexo B del presente documento.

6.3. MPLEMENTACIÓN DE ESTRATEGIAS DE CONTINGENCIA

En esta etapa se crean estrategias de contingencia para mitigar adecuadamente los riesgos que surge al usar los sistemas de información y sistemas digitales. Entre estas estrategias se puede formular planes, protocolos, procedimientos, cartillas u otros instrumentos de gestión que sean necesarios.

Según el Manual N° 004-2021-MIDIS – Manual para la Gestión de Riesgos de Procesos en el Ministerio de Desarrollo e Inclusión Social, aprobado mediante Resolución Ministerial N° 138-2021-MIDIS. Las estrategias para la gestión de riesgos son las siguientes:

Nro.	Estrategia	Descripción
1.	Evitar	Consiste en implementar controles para eliminar las condiciones o situaciones que generan el riesgo, inclusive no iniciar o evitar realizar la actividad o proteger el proceso del impacto que pueda generar el riesgo
2.	Mitigar	Consiste en implementar controles para reducir el nivel de riesgo; incluye optimizar los procesos o acciones que se ejecutan, así como implementar nuevos controles y/o cambiar los controles existentes
3.	Compartir	Consiste en trasladar o compartir el riesgo a un tercero, junto con la responsabilidad de respuesta. No implica que el riesgo haya sido eliminado, tampoco que el dueño del proceso o del riesgo transfiera su responsabilidad
4.	Asumir	Consiste en aceptar el riesgo, no se emprende ningún control, no requiere un plan de tratamiento. Sin embargo, implica revisar periódicamente el riesgo a fin de identificar oportunamente posibles cambios significativos

Fuente: Resolución Ministerial N.° 138-2021-MIDIS

Estas estrategias son incluidas en la Matriz de Riesgos (ANEXO N° 3). Para su actualización, se puede revisar la información (estándares) recopilada en el Anexo C del presente documento.

6.4. PLANES DE PRUEBAS, CAPACITACIÓN Y EJERCICIOS

Como parte del PCTIC es necesario mantener en un estado de preparación al PNPAIS, lo que recae en tener al personal con capacitación constante para cumplir con sus roles y responsabilidades, tener planes de ensayo para validar el contenido del plan, y tener los resultados del funcionamiento correcto de controles implementados que aseguren la operatividad de los sistemas de información y servicios digitales.

a. Pruebas

Las pruebas permiten identificar y abordar las deficiencias del plan mediante la validación de uno o más de sus componentes. Las pruebas pueden adoptar varias formas y lograr varios objetivos, pero deben realizarse lo más cerca posible de un entorno operativo. Cada componente del sistema de información o servicio digital debe probarse para confirmar la precisión de los procedimientos de recuperación individuales. El plan de pruebas debe contar como mínimo con lo siguiente:

- Procedimientos de notificación

- Recuperación del sistema en una plataforma alternativa a partir de medios de respaldo
- Conectividad interna y externa
- Rendimiento del sistema utilizando equipo alternativo
- Restauración de operaciones normales

b. Capacitaciones

Las capacitaciones para la ejecución del PCTIC debe estar relacionado a los roles del personal y al perfeccionamiento de las habilidades necesarias para cumplir con sus responsabilidades. Con las capacitaciones se debe garantizar que el personal esté preparado para participar en todas las pruebas y ejercicios programados, así como en eventos de interrupciones reales. Las capacitaciones deben abarcar como mínimo lo siguiente:

- Propósito del plan.
- Coordinación y comunicación entre equipos.
- Procedimientos de informes.
- Requisitos de seguridad.
- Procesos específicos del equipo (fases de activación y notificación, recuperación y reconstitución).
- Responsabilidades individuales (fases de activación y notificación, recuperación y reconstitución).

c. Ejercicios

De acuerdo con el cronograma de actividades definido en la Tabla 3 "Matriz de programación para pruebas y ejercicios" del numeral 6.6 del presente Plan, se ejecutarán ejercicios relacionados al manejo de los controles preventivos de los Riesgos identificados en el ANEXO N° 4.

La estructura que se trabajará para la ejecución de estos ejercicios será la siguiente:

Nro.	Tipo de Ejercicio	Descripción
1.	Ejercicio de mesa	Ejercicios basados en debates en los que el personal se reúne en un aula o en grupos de trabajo para analizar sus funciones durante una emergencia y sus respuestas a una situación de emergencia particular
2.	Ejercicios funcionales	Los ejercicios funcionales permiten al personal validar su preparación operativa para emergencias al realizar sus tareas en un entorno operativo simulado

Fuente: ISO/IEC 27031:2011, Tecnologías de la Información

Como apoyo para el plan de pruebas, capacitaciones y ejercicios, se puede revisar la información (estándares) recopilada en el Anexo D del presente documento.

6.5. MANTENIMIENTO DEL PLAN DE CONTINGENCIA DE TIC

Es necesario que el Oficial de Seguridad y Confianza Digital o quien haga sus veces revise y actualice regularmente el listado de sistemas de información y sistemas digitales, así como las medidas de control y contingencia, lista de contactos, entre otros.

El proceso de monitoreo continuo es una herramienta eficaz para el mantenimiento del PCTIC, produciendo actualizaciones continuas de los planes de seguridad, informes de evaluación de seguridad y planes de acción y documentos de hitos.

Nro.	Alcance de revisión del PCTIC
1.	Procedimientos técnicos
2.	Hardware, software y otros equipos (tipos, especificaciones y cantidad)
3.	Nombres e información de contacto de los miembros del equipo
4.	Nombres e información de contacto de los proveedores, incluidos los de proveedores alternativos y externos
5.	Requisitos de instalaciones alternativas y externas
6.	Registros vitales (electrónicos e impresos)

Fuente: NIST Special Publication 800-34 Rev. 1 Contingency Planning Guide for Federal Information Systems

Asimismo, el plan debe revisarse para comprobar su precisión e integridad con una frecuencia definida por el PNPAIS o siempre que se produzcan cambios significativos en cualquier elemento del plan.

Como apoyo para el mantenimiento del PCTIC, se puede revisar la información (estándares) recopilada en el Anexo E del presente documento.

6.6. PLAN DE DESPLIEGUE Y EJECUCIÓN DEL PLAN DE CONTINGENCIA DE TI

Toda la programación de actividades se desarrolla mediante un cronograma secuencial especificado en las matrices del ANEXO N° 2.

7. SEGUIMIENTO Y EVALUACIÓN

El seguimiento y evaluación del PCTIC estará a cargo del CSIRT, quienes remitirán un informe (reporte) trimestral del cumplimiento de las pruebas, capacitaciones y aplicaciones del plan, así como la evaluación de actualizaciones al plan como medida de mantenimiento; al Comité de Gobierno y Transformación Digital y a la Dirección Ejecutiva.

La CSIRT informará el cumplimiento de las actividades y metas del PCTIC. Esta información a su vez servirá para el diagnóstico de la propuesta de actualización del PCTIC. La información de los Apéndices será actualizada con una periodicidad bimestral y serán publicadas en el portal de Intranet del Programa Nacional PAIS.

8. ANEXOS

Anexo N° 1: Definiciones y abreviaturas
Anexo N° 2: Matrices de despliegue y ejecución del plan de contingencia de TI
Anexo N° 3: Matriz de amenazas, vulnerabilidades y riesgos
Anexo N° 4: Cartilla de instrucción para la gestión de la emergencia y/o de crisis
Anexo N° 5: Cartilla de instrucción para el control de las operaciones de recuperación

ANEXO N° 1 DEFINICIONES Y ABREVIATURAS

I. Definiciones

a) **Activo**: Es cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización, pueden ser procesos de negocio, datos, aplicaciones, equipos informáticos, personal, soportes de información, redes, equipamiento auxiliar o instalaciones. Es susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. El activo es algo que presenta valor para la organización.

b) **Amenaza**: Causa potencial de un incidente no deseado que puede resultar en daño al sistema del entorno digital o a la propia organización.

c) **Actividades Críticas**: Están constituidas por las actividades que la entidad haya identificado como indispensables y que no pueden dejar de realizarse, conforme a sus competencias y atribuciones señaladas en las normas de la materia. En el marco del gobierno digital, se le define también como la actividad económica y/o social cuya interrupción tiene graves consecuencias en la salud y seguridad de los ciudadanos, en el funcionamiento efectivo de los servicios esenciales que mantienen la economía, sociedad y el gobierno, o afectan la prosperidad económica y social en general.

d) **Confianza Digital**: Es el estado que emerge como resultado de cuan veraces, predecibles, éticas, proactivas, transparentes, seguras, inclusivas y confiables son las interacciones digitales que se generan entre personas, empresas, entidades públicas o cosas en el entorno digital, con el propósito de impulsar el desarrollo de la economía digital y la transformación digital. Es un componente de la transformación digital y tiene como ámbitos la protección de datos personales, la ética, la transparencia, la seguridad digital y la protección del consumidor en el entorno digital.

e) **Confidencialidad**: Garantizar que la información sea accesible únicamente para quienes tengan acceso autorizado.

f) **Ciberseguridad**: Capacidad tecnológica de preservar el adecuado funcionamiento de las redes, activos y sistemas informáticos, y protegerlos ante amenazas y vulnerabilidades en el entorno digital. Comprende la perspectiva técnica de la Seguridad Digital y es un ámbito del marco de la Seguridad Digital del país.

g) **Disponibilidad**: Garantizar que los usuarios autorizados tengan acceso a la información y activos asociados cuando sea necesario.

h) **Evaluación del Riesgo**: Proceso que consiste en comparar el riesgo calculado con ciertos criterios de riesgos para determinar la importancia del riesgo, involucra a la valoración y al tratamiento de los riesgos.

i) Equipo de Respuestas ante incidentes de Seguridad Digital – CSIRT Es aquel equipo responsable de la gestión de incidentes de seguridad digital que afectan los activos de una entidad pública o una red de confianza. Su implementación y conformación se realiza en base a las disposiciones que determine la Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros – PCM.

j) **Entorno Digital**: Es el dominio o ámbito habilitado por las tecnologías y dispositivos digitales, generalmente interconectados a través de redes de datos o comunicación, incluyendo el internet, que soporta los procesos, servicios, infraestructuras y la interacción entre personas.

k) **Gestión de Incidentes de seguridad digital**: Es el proceso formal que tiene por finalidad planificar, preparar, identificar, analizar, contener, investigar incidentes de seguridad digital, así como la recuperación y la determinación de acciones correctivas para prevenir incidentes similares.

l) **Gestión de Riesgos**: Actividades coordinadas para dirigir o controlar el efecto de la incertidumbre de un resultado esperado. En el marco del gobierno digital se le define como [23]; La gestión de riesgos de seguridad en el entorno digital está integrada en la toma de decisiones, diseño de controles de seguridad en los servicios digitales y procesos de la entidad. Es responsabilidad de la alta dirección dirigirla, mantenerla e incorporarla en la gestión integral de riesgos de la entidad.

m) **Integridad**: Es salvaguardar la exactitud e integridad de la información y activos asociados.

n) **Incidente de seguridad digital**: Se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a una política de seguridad de la Información.

o) **Infraestructura TIC**: Hace referencia a todos los sistemas computacionales entre hardware y software, estando comprendido en ello todos los bienes catalogados como recursos de informática.

p) **Servicio Digital**: Es aquel provisto de forma total o parcial a través de internet u otra red equivalente, que se caracteriza por ser automático, no presencial y utilizar de manera intensiva las tecnologías digitales, para la producción y acceso a datos y contenidos que general valor público para los ciudadanos y personas en general.

q) **Seguridad Digital**: Es el estado de confianza en el entorno digital que resulta de la gestión y aplicación de un conjunto de medidas proactivas y reactivas frente a los riesgos que afectan la seguridad de las personas, la prosperidad económica y social, la seguridad nacional y los objetivos nacionales en dicho entorno. Se sustenta en la articulación con actores del sector público, sector privado y otros quienes apoyan en la implementación de controles, acciones y medidas.

r) **Seguridad de la Información**: Es preservar la confidencialidad, integridad y disponibilidad de la información, además, también pueden ser involucradas otras características como la autenticación, responsabilidad, no repudio y fiabilidad.

s) **Seguridad Informática**: Se define a la seguridad informática como el proceso de prevenir y detectar el uso no autorizado o indebido de un sistema informático en particular, cuyo propósito es la de asegurar la operatividad del sistema computacional tanto a nivel de hardware como de software.

t) **Tecnologías Digitales**: Se refieren a las tecnologías de la información y la Comunicación – TIC, incluidos internet, las tecnologías y dispositivos móviles, así como la analítica de

datos utilizados para mejorar la generación, recopilación, intercambio, agregación, combinación, análisis, acceso, búsqueda y presentación de contenido digital, incluido el desarrollo de servicios y aplicaciones aplicables a la materia de gobierno digital.

u) **Vulnerabilidad**: Debilidad o fallo de un sistema que puede ser aprovechado con fines maliciosos (normalmente mediante un programa que se denomina exploit). La debilidad involucra también a una infraestructura, arquitectura, archivo o grupo de archivos en un entorno digital, que puede ser explotado por una o más amenazas.

II. Abreviaturas

a) **CSIRT** : Computer Security Incident Response Team (Equipo de Respuesta ante Incidentes de Seguridad Digital)

b) **MIDIS** : Ministerio de Desarrollo e Inclusión Social

c) **OGTI** : Oficina General de Tecnologías de la Información

d) **PCTIC** : Plan de Contingencia TIC (Tecnologías de Información y Comunicaciones)

e) **PNPAIS** : Programa Nacional "Plataformas de Acción para la Inclusión Social"

f) **SGTD** : Secretaría de Gobierno y Transformación Digital

g) **TIC** : Tecnologías de Información y Comunicaciones

h) **UA** : Unidad de Administración

i) **UAGS** : Unidad de Articulación de Servicios

j) **UPS** : Unidad de Plataforma de Servicios

k) **URRHH** : Unidad de Recursos Humanos

l) **UT** : Unidad Territorial

m) **UTI** : Unidad de Tecnologías de la Información

ANEXO N° 2 MATRICES DE DESPLIEGUE Y EJECUCIÓN DEL PLAN DE CONTINGENCIA DE TI

Tabla N° 1: MATRIZ DE PROGRAMACIÓN PARA EL DESPLIEGUE Y EJECUCIIÓN DEL PLAN DE CONTIGENCIA DE TIC

Etapa	Actividad	Descripción	2024			2025												Unidad Responsable
			IV TRIM			I TRIM			II TRIM			III TRIM			IV TRIM			
			Oct	Nov	Dic	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Set	Oct	Nov	Dic	
Análisis de impacto (BIA)	Iniciar y formar equipo BIA	Formar el equipo responsable del BIA y realizar una sesión de apertura.																UTI
	Identificar procesos críticos	Recopilar información sobre procesos, los sistemas de información y servicios digitales que son críticos para el PNPAIS.																UTI / UUOO
	Evaluar impactos potenciales	Identificar los impactos operacionales y legales que resultarían de la interrupción de procesos.																UTI / UUOO
	Determinar los tiempos máximos de inactividad aceptable (RTO y RPO)	Determinar el tiempo máximo que los sistemas de información y servicios digitales pueden estar fuera de operación antes de generar problemas graves.																UTI / UUOO
	Identificar los requisitos de recuperación	Evaluar los recursos necesarios para reanudar los sistemas de información y servicios digitales lo más rápido posible																UTI
	Identificar las prioridades de recuperación	Establecer niveles de prioridad para secuenciar las actividades y recursos de recuperación.																UTI / UUOO
	Aprobar el Informe final BIA	Redactar un informe detallado con los hallazgos del análisis de impacto.																DE / UTI
Identificación de controles preventivos	Identificar los riesgos y vulnerabilidades	Revisar los resultados del BIA para identificar posibles vulnerabilidades en los sistemas críticos.																UTI
	Identificar controles preventivos	Identificar controles de seguridad (físicos, técnicos y administrativos) que pueden mitigar riesgos.																UTI

Etapa	Actividad	Descripción	2024			2025												Unidad Responsable
			IV TRIM			I TRIM			II TRIM			III TRIM			IV TRIM			
			Oct	Nov	Dic	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Set	Oct	Nov	Dic	
	Evaluar la efectividad de los controles actuales	Revisar controles actuales y su eficacia en la prevención de interrupciones o fallos.					■											UTI
	Desarrollar recomendaciones para nuevos controles	Proponer nuevos controles preventivos o mejoras a los existentes para proteger los sistemas críticos.						■										UTI
	Presentar el plan de controles preventivos	Documentar y presentar las medidas preventivas identificadas para su implementación.						■										UTI
Implementación de estrategias de contingencia	Revisar las estrategias de contingencia disponibles	Revisar diferentes enfoques de contingencia: recuperación de desastres, respaldo de datos, redundancia, etc.							■	■								UTI
	Seleccionar la estrategia de contingencia	Elegir la estrategia más adecuada en función del BIA y los controles preventivos identificados.								■								UTI
	Actualizar el plan de contingencia	Actualizar el plan detallado que incluirá procedimientos de recuperación, contactos de emergencia y tiempos de restauración.								■	■							UTI
	Implementar nuevas pruebas de recuperación	Actualizar el plan de pruebas de recuperación (ejercicios de mesa, simulaciones) para verificar la efectividad del plan.										■	■					UTI
	Revisar y ajustar el plan según el resultado de las pruebas	Ajustar el plan de contingencia según los resultados de las pruebas y simulaciones realizadas.														■	■	UTI
	Capacitar al personal	Entrenar al personal involucrado en los procedimientos de contingencia												■				UTI

Tabla N° 2: MATRIZ DE PROGRAMACIÓN DE ACTIVIDADES – PLAN DE RESPUESTA Y RECUPERACIÓN

Etapa	Actividad	Tiempo de respuesta	Unidad Responsable	Indicador		
				Indicador Clave de Rendimiento (PKI)	Descripción	Objetivo
Notificación y Activación	Contactar al equipo de respuesta de TI a través de la línea de emergencia interna.	Dentro de los 15 min de la identificación del incidente	Colaborador de PNPAIS	Tasa de Notificación Temprana	Porcentaje de incidentes notificados dentro del plazo de 15 minutos	95%
	Notificar a los responsables de las áreas críticas afectadas.	Dentro de los 30 min de la identificación del incidente	UTI	Tiempo Promedio de Notificación	Tiempo promedio desde la detección del incidente hasta la notificación del equipo de respuesta.	≤ 10 min
	Informar a la alta dirección y a las partes interesadas clave.		UTI			
Evaluación Inicial del Incidente	Evaluar el alcance y el impacto del incidente.	Dentro de los primeros 30 minutos después de la notificación	CSIRT	Tasa de Evaluación Completa	Porcentaje de incidentes evaluados dentro del plazo de 30 minutos.	90%
	Determinar las funciones críticas afectadas y los recursos necesarios para la recuperación.		CSIRT	Exactitud de la Evaluación Inicial	Evaluaciones que identifican correctamente el alcance y el impacto del incidente.	95%
	Identificar la causa raíz si es posible.		CSIRT			
Activación del Plan de Recuperación	Activar el equipo de recuperación de TI.	Dentro de los primeros 60 minutos después de la evaluación inicial	CSIRT	Tasa de Activación Temprana	Porcentaje de incidentes que activan el plan de recuperación dentro del plazo de 60 minutos.	85%
	Implementar procedimientos de recuperación según las estrategias definidas (recuperación de datos, conmutación a sitios alternativos, etc.).		Especialista TI	Tiempo Promedio de Activación	Tiempo promedio desde la evaluación inicial hasta la activación del plan de recuperación	≤ 45 min
	Comunicarse con las partes interesadas sobre el estado de la recuperación y los plazos estimados.		UTI			

Etapa	Actividad	Tiempo de respuesta	Unidad Responsable	Indicador		
				Indicador Clave de Rendimiento (PKI)	Descripción	Objetivo
Comunicaciones Durante el Incidente	Proporcionar actualizaciones regulares sobre el progreso de la recuperación a todas las partes interesadas.	Actualizaciones cada 30 minutos o según sea necesario	UTI	Frecuencia de Actualizaciones	Cumplimiento de la frecuencia de actualizaciones establecida.	100%
	Mantener una comunicación clara y coherente para evitar malentendidos y pánico.		UTI	Satisfacción de Comunicación	Nivel de satisfacción de las partes interesadas con la comunicación durante el incidente.	≥ 90%
Recuperación de Datos	Restaurar datos desde las copias de seguridad más recientes	Dentro de las primeras 2 horas para datos críticos	Especialista TI	Tasa de Recuperación de Datos	Porcentaje de datos críticos restaurados dentro del plazo de 2 horas.	90%
	Verificar la integridad y la completitud de los datos restaurados		Especialista TI	Integridad de Datos	Porcentaje de datos restaurados sin errores.	99%
Recuperación de Sistemas	Restaurar servidores, aplicaciones y servicios críticos.	Dentro de las primeras 4 horas para sistemas críticos	Especialista TI	Tasa de Recuperación de Sistema	Porcentaje de sistemas críticos restaurados dentro del plazo de 4 horas.	85%
	Validar la funcionalidad de los sistemas recuperados.		Especialista TI	Funcionamiento de Sistemas Recuperados	Porcentaje de sistemas que funcionan correctamente después de la recuperación.	95%
Validación y Verificación	Verificar la integridad y funcionalidad de los sistemas y datos restaurados.	Dentro de las primeras 6 horas después de la recuperación	Usuario final	Tasa de Validación Completa	Porcentaje de validaciones completadas dentro del plazo de 6 horas.	95%
	Realizar pruebas de aceptación con los usuarios finales para asegurar que los sistemas funcionan como se espera.		Usuario final	Satisfacción del Usuario	Nivel de satisfacción de los usuarios finales con la funcionalidad de los sistemas recuperados.	≥ 90%

Etapa	Actividad	Tiempo de respuesta	Unidad Responsable	Indicador		
				Indicador Clave de Rendimiento (PKI)	Descripción	Objetivo
Retorno a la Operación Normal	Transición de las operaciones desde el entorno de recuperación al entorno normal.	Dentro de las primeras 24 horas después de la recuperación completa	PNPAIS	Tasa de Retorno a Operación Normal	Porcentaje de operaciones que regresan al entorno normal dentro del plazo de 24 horas.	90%
	Desactivar el sitio alternativo y reintegrar cualquier sistema temporal utilizado durante la recuperación.		Especialista TI	Funcionamiento Post-Restauración	Porcentaje de sistemas que funcionan correctamente después del retorno a la operación normal.	98%
Evaluación Post-Incidente	Revisión de la respuesta y recuperación para identificar lecciones aprendidas y áreas de mejora.	Dentro de las 48 horas posteriores al retorno a la operación normal	CSIRT	Tasa de Evaluación Completa	Porcentaje de evaluaciones completadas dentro del plazo de 48 horas.	100%
	Documentar las observaciones y recomendaciones para mejorar el plan de contingencia.		CSIRT	Implementación de Mejoras	Porcentaje de recomendaciones implementadas después de la evaluación post-incidente.	80%
Actualización del Plan	Actualización del plan de contingencia basándose en las lecciones aprendidas y recomendaciones.	Dentro de los 7 días posteriores a la evaluación post-incidente	CSIRT	Tasa de Actualización del Plan	Porcentaje de planes actualizados dentro del plazo de 7 días.	100%
	Revisión y aprobación del plan actualizado por la alta dirección.	Dentro de los 14 días posteriores a la evaluación post-incidente	Dirección Ejecutiva	Aprobación del Plan Actualizado	Porcentaje de planes actualizados aprobados por la alta dirección.	100%

Tabla N° 3: MATRIZ DE PROGRAMACIÓN PARA PRUEBAS Y EJERCICIOS

Etapa	Actividad	2024			2025						Unidad Responsable
		IV TRIM			I TRIM			II TRIM			
		Oct	Nov	Dic	Ene	Feb	Mar	Abr	May	Jun	
PRUEBAS	Recuperación de Datos			■			■			■	UTI
	Recuperación de Sistemas	■						■			UTI
	Redundancia de Redes				■						UTI
	Planes de Respuesta a Incidentes					■					UTI
EJERCICIOS	Simulación de uno o más incidentes relacionados a los riesgos identificado en el Anexo N° 2.			■						■	UTI
	Recuperación Completa				■						UTI
	Comunicación de Crisis						■				UTI

ANEXO N° 3 MATRIZ DE AMENAZAS, VULNERABILIDADES Y RIESGOS

IDENTIFICACIÓN, ANÁLISIS DEL RIESGO /OPORTUNIDAD							VALOR DEL RIESGO / OPORTUNIDAD				PLAN DE TRATAMIENTO			
N°	R/O	RIESGO / OPORTUNIDAD	TIPO DE RIESGO	CAUSA	EFECTO	CONTROLES ACTUALES	PROBABILIDAD	IMPACTO	VALOR	NIVEL	ESTRATEGIA (ver comentario)	APLICA PLAN (SI/NO)	MEDIDA DE CONTROL / ACCIÓN	ESTADO
1	R	Podría filtrarse información no pública o datos protegidos por ley, por desconocimiento de la norma y baja conciencia de seguridad digital, comprometiendo la seguridad personal y de la entidad	Seguridad Digital	Desconocimiento de la norma y baja conciencia de seguridad digital	Compromete la seguridad personal e institucional	Declaración de Compromiso con la Seguridad de la Información de los servidores (RD. 213-2020- MIDIS/PNPAIS), SGSI en proceso de implementación (RD. N° 060-2023-MIDIS/PNPAIS-DE)	4	10	40	Medio	Mitigar	Si	Implementar el Sistema de Gestión de Seguridad de la Información	Parcialmente implementado
2	R	Podría darse el acceso libre a espacios restringidos de procesamiento de datos, producción de software y administración del DATA CENTER, por falta de regulación (avisos e indicativos de zonas restringidas), incrementando los riesgos de seguridad digital.	Seguridad Digital	Falta de regulación (avisos e indicativos de zonas restringidas)	Incremento de los riesgos de la seguridad digital	1) RD. N° 213-2020-MIDIS/PNPAIS 2) RM. N° 002-2021-MIDIS 3) Memo Múltiple N° D000033-2023-MIDIS/PNPAIS-UTI 04/05	6	8	48	Alto	Evitar	Si	Implementar el Procedimiento de Control de Acceso al Centro de Datos - PNPAIS	Parcialmente implementado
3	R	Existiría baja efectividad de respuesta a incidentes de seguridad digital, por parte del equipo CSIRT, comprometiendo la operatividad de la Infraestructura de TI	Seguridad Digital	No conformación del equipo CSIRT	Compromete la operatividad de la infraestructura de TI	CSIRT conformado con la RD. N° 062-2023-MIDIS/PNPAIS-DE	6	10	60	Alto	Compartir	Si	Someter al CSIRT a entrenamientos en escenarios de riesgos simulados	Parcialmente implementado

IDENTIFICACIÓN, ANÁLISIS DEL RIESGO /OPORTUNIDAD							VALOR DEL RIESGO / OPORTUNIDAD				PLAN DE TRATAMIENTO			
N°	R/O	RIESGO / OPORTUNIDAD	TIPO DE RIESGO	CAUSA	EFECTO	CONTROLES ACTUALES	PROBABILIDAD	IMPACTO	VALOR	NIVEL	ESTRATEGIA (ver comentario)	APLICA PLAN (SI/NO)	MEDIDA DE CONTROL / ACCIÓN	ESTADO
4	R	Podría darse mal uso a los recursos de tecnologías y sistemas de información (TI/SI), por desconocimiento de la norma de tenencia y custodia de los bienes informáticos, comprometiendo la vida útil del bien.	Seguridad Digital	Desconocimiento de la norma de tenencia y custodia de los bienes informáticos	Compromete la vida útil del bien	Directiva de gestión de bienes muebles del Estado (RD. N° 009-2018- MIDIS/PNPAIS-DE)	4	8	32	Medio	Compartir	Si	Sensibilizar al personal en el uso, custodia y tenencia de recursos informáticos	Parcialmente implementado
5	R	Existirían Productos de software desarrollados de baja calidad, por la falta de procedimientos que regulen el testing y control de calidad de software, comprometiendo la operatividad de los servicios digitales implementados	Seguridad Digital	Falta de Personal especializado en testing y control de calidad de TI	Compromete la operatividad de los servicios digitales implementados	Procedimiento del Ciclo de Vida del SW (RD 028-2020-MIDIS/PNPAIS) y (RM. 121- 2021-MIDIS)	6	10	60	Alto	Compartir	No	Impulsar cumplimiento de la normativa del Ciclo de Vida del SW y Gestión de proyectos emitido por el MIDIS	Parcialmente implementado
6	R	Podría darse el uso ilegal de productos de software, por la no identificación oportuna de la necesidad para la adquisición de la licencia respectiva, afectando el derecho de propiedad intelectual y autoría, comprometiendo la imagen institucional	Seguridad Digital	No identificar de forma oportuna la necesidad para adquirir la licencia respectiva	Afecta el derecho de la propiedad intelectual y autoría, y compromete la imagen institucional	Restricciones de uso ilegal de SW se contempla en la RD 213-2020-MIDIS/PNPAIS	4	10	40	Medio	Evitar	Si	Difundir las restricciones sobre uso legal de productos de SW, a través de Alertas de Seguridad Digital	Implementado

IDENTIFICACIÓN, ANÁLISIS DEL RIESGO /OPORTUNIDAD							VALOR DEL RIESGO / OPORTUNIDAD				PLAN DE TRATAMIENTO			
N°	R/O	RIESGO / OPORTUNIDAD	TIPO DE RIESGO	CAUSA	EFECTO	CONTROLES ACTUALES	PROBABILIDAD	IMPACTO	VALOR	NIVEL	ESTRATEGIA (ver comentario)	APLICA PLAN (SI/NO)	MEDIDA DE CONTROL / ACCIÓN	ESTADO
7	R	Existirían Bases de Datos de los Sistemas de Información con datos no confiables e inconsistentes, por el alto índice de error con que estos son ingresados, comprometiendo la toma de decisiones gerenciales	Seguridad Digital	Alto índice de error con que son ingresados los datos	Compromete la toma de decisiones gerenciales	Se asignó el Rol de Gobierno de Datos con la RD. 144- 2021-MIDIS/PNPAIS	6	10	60	Alto	Mitigar	Si	Sensibilizar y auditar bases de datos	Parcialmente implementado
8	R	Podría interrumpirse los servicios proveídos por terceros (internet, correo electrónico, telefonía IP, etc.) por cuestiones técnicas propias de la tecnología, restringiendo la continuidad de las operaciones del programa,	Seguridad Digital	Cuestiones técnicas propias de la tecnología	Restringe la continuidad de las operaciones del programa	Se gestiona alta disponibilidad de los servicios de terceros (conectividad, correo electrónico y telefonía IP) según contrato de las partes	4	8	32	Medio	Mitigar	No	Establecer y mantener un canal de comunicación efectiva con los proveedores para reportar incidencias y/o averías orientado a su recuperación.	Implementado
9	R	Podría la infraestructura tecnológica del Programa, ser objeto de ataques informáticos dirigidos, por las vulnerabilidades de seguridad que tendrían, comprometiendo la continuidad de las operaciones en el programa.	Seguridad Digital	Vulnerabilidades de seguridad	Compromete la continuidad de las operaciones del Programa	Se dispone de procedimiento interno de Copias de Respaldo	6	10	60	Alto	Mitigar	Si	Implementar el Plan de Contingencia de TIC y el Sistema de Gestión de Seguridad de la Información	Parcialmente implementado

IDENTIFICACIÓN, ANÁLISIS DEL RIESGO /OPORTUNIDAD							VALOR DEL RIESGO / OPORTUNIDAD				PLAN DE TRATAMIENTO			
N°	R/O	RIESGO / OPORTUNIDAD	TIPO DE RIESGO	CAUSA	EFECTO	CONTROLES ACTUALES	PROBABILIDAD	IMPACTO	VALOR	NIVEL	ESTRATEGIA (ver comentario)	APLICA PLAN (SI/NO)	MEDIDA DE CONTROL / ACCIÓN	ESTADO
10	R	Podría el Centro de Datos del programa (DATACENTER) sufrir inundación por deterioro y falta de mantenimientos de los sistemas de suministro de agua, paralizando las operaciones del Centro de Gestión de Datos	Seguridad Digital	Deterioro y falta del mantenimiento de los sistemas de suministro de agua	Paralización de las operaciones del Centro de Datos	Se cuenta con nuevo Centro de Datos implementado bajo estándares en nueva sede del PNPAIS	4	8	32	Medio	Evitar	Si	Implementar el Plan de Contingencia de TIC	Parcialmente implementado
11	R	Podría fallar las copias de respaldo de datos, sistemas, fuentes y configuraciones efectuadas, por la no verificación y ausencia de pruebas de efectividad, comprometiendo la recuperación de la operatividad de los servicios digitales	Seguridad Digital	No verificación y ausencia de pruebas de efectividad de las copias de respaldo	Compromete la recuperación de la operatividad de los servicios digitales	Se hacen copias de respaldo en varios momentos (diario, semanal, mensual), y en adición se realiza la prueba de efectividad de las copias según procedimiento interno	4	10	40	Medio	Evitar	Si	Ejecutar el procedimiento de restauración de datos a modo de simulacro con participación del CSIRT-PNPAIS	Parcialmente implementado
12	R	Podrían ocurrir accesos no controlados de usuarios no autorizados al dominio de la red del programa, por la falta de control en la gestión de permisos de acceso, comprometiendo la seguridad digital de la infraestructura de TI.	Seguridad Digital	Falta de control en la gestión de permisos de accesos a la red de datos del Programa	Compromete la seguridad digital de la Infraestructura de TI	La RD 213-2020-MIDIS/PNPAIS regula el control de acceso a los servicios digitales	4	8	32	Medio	Evitar	No	Efectuar acciones de supervisión y control de usuarios concedidos por unidades orgánicas	Parcialmente implementado

IDENTIFICACIÓN, ANÁLISIS DEL RIESGO /OPORTUNIDAD							VALOR DEL RIESGO / OPORTUNIDAD				PLAN DE TRATAMIENTO			
N°	R/O	RIESGO / OPORTUNIDAD	TIPO DE RIESGO	CAUSA	EFECTO	CONTROLES ACTUALES	PROBABILIDAD	IMPACTO	VALOR	NIVEL	ESTRATEGIA (ver comentario)	APLICA PLAN (SI/NO)	MEDIDA DE CONTROL / ACCIÓN	ESTADO
13	R	Podría no ejecutarse el Plan de Mantenimiento Preventivo de Informática por la carencia de medios y recursos, perjudicando la operatividad de los equipos informáticos y su ciclo de vida útil	Seguridad Digital	Carencia de medios y recursos	Perjudica la operatividad de los equipos informáticos y su ciclo de vida útil	RD 269-2020-MIDIS/PNPAIS regula la presentación del Plan de Mantenimiento de Informática de forma oportuna	6	8	48	Alto	Mitigar	Si	Identificar los puntos de atención a priorizar y gestionar los medios y recursos necesarios de forma oportuna	Parcialmente implementado
14	R	Podría ocurrir Incendio en las instalaciones del Programa, con incidencia en el Centro de Datos, por circunstancias generalmente imprevistas, comprometiendo la seguridad física de la instalación, infraestructura de TI y el personal	Seguridad Digital	Circunstancias generalmente imprevistas	Compromete la seguridad física de la instalación, infraestructura de TI y el personal	Vigilancia física externa y disposición de extintores en puntos clave	4	8	32	Medio	Compartir	Si	Asegurar la vigencia de los sistemas de seguridad contra incendios y capacitar al personal en el uso de los sistemas de seguridad	Parcialmente implementado
15	R	Podría ocurrir el corte del suministro eléctrico por hechos diversos, con incidencia en el Centro de Datos.	Seguridad Digital	Hechos diversos (caída de torres, falta de pago, sabotaje, vandalismo, etc.)	Incide en la operatividad del Centro de Gestión de Datos (DATA CENTER)	Se cuenta con UPS en el Centro de Gestión de Datos	4	8	32	Medio	Compartir	No	Disponer de fuente de energía acumulable para el Centro de Datos	Implementado

IDENTIFICACIÓN, ANÁLISIS DEL RIESGO /OPORTUNIDAD							VALOR DEL RIESGO / OPORTUNIDAD				PLAN DE TRATAMIENTO			
N°	R/O	RIESGO / OPORTUNIDAD	TIPO DE RIESGO	CAUSA	EFECTO	CONTROLES ACTUALES	PROBABILIDAD	IMPACTO	VALOR	NIVEL	ESTRATEGIA (ver comentario)	APLICA PLAN (SI/NO)	MEDIDA DE CONTROL / ACCIÓN	ESTADO
16	R	Podría presentarse averías en la Infraestructura de TI/SI, y cableado estructurado de Redes y Comunicaciones, por falta de control y mantenimiento preventivo, comprometiendo la operatividad de la infraestructura de TI.	Seguridad Digital	Falta de control y mantenimiento preventivo	Compromete la operatividad de la infraestructura de TI	Se cuenta con el servicio de Administración del Centro de Datos, quien ejerce control operacional y planifica los mantenimientos preventivos	4	8	32	Medio	Mitigar	Si	Incluir en el Plan de Mantenimiento Preventivo Anual de Informática, los elementos que conforman el Centro de Datos e Infraestructura de red del PNPAIS:	Parcialmente implementado
17	R	Podría detectarse hurto o pérdida de equipos informáticos del programa, por la falta de control y actualización permanente del inventario, restringiendo la disponibilidad de herramientas de trabajo para el personal	Seguridad Digital	Falta de control y actualización permanente del inventario de equipos informáticos	Restringe la disponibilidad de herramientas de trabajo para el personal	Directiva de gestión de bienes muebles del Estado (RD. N° 009-2018- MIDIS/PNPAIS)	4	6	24	Bajo	Compartir	Si	Concientizar al personal en temas de uso y custodia de los bienes informáticos	Parcialmente implementado
18	R	Podría el parque informático del programa presentar un alto índice de obsolescencia, por la antigüedad de las adquisiciones y uso del protocolo IPV6 para los recursos de HW y SW, reduciendo la capacidad operativa por el limitado número de equipos informáticos con vigencia tecnológica.	Seguridad Digital	Antigüedad de las adquisiciones y uso del protocolo IPV6 para los recursos de HW y SW	Reduce la capacidad operativa por el limitado número de equipos informáticos con vigencia tecnológica	Proyecto del Plan de Migración al Protocolo IPV6	8	10	80	Muy Alto	Mitigar	Si	Gestionar la aprobación del Proyecto de Plan de Migración al protocolo IPV6.	Parcialmente implementado

IDENTIFICACIÓN, ANÁLISIS DEL RIESGO /OPORTUNIDAD							VALOR DEL RIESGO / OPORTUNIDAD				PLAN DE TRATAMIENTO			
N°	R/O	RIESGO / OPORTUNIDAD	TIPO DE RIESGO	CAUSA	EFECTO	CONTROLES ACTUALES	PROBABILIDAD	IMPACTO	VALOR	NIVEL	ESTRATEGIA (ver comentario)	APLICA PLAN (SI/NO)	MEDIDA DE CONTROL / ACCIÓN	ESTADO
19	R	Podría no lograrse promover e impulsar el marco de Gobierno y Transformación Digital en el programa, por la ausencia de especialistas que ayuden en su implementación, afectando el cumplimiento del marco del Gobierno y la Transformación Digital	Seguridad Digital	Ausencia de especialista en Gobierno y Transformación Digital	Afecta el cumplimiento del marco del Gobierno y la Transformación Digital	Con la RD. 144-2021-MIDIS/PNPAIS, se actualizó la conformación del Comité de Gobierno y Transformación Digital	4	8	32	Medio	Mitigar	No	Facilitar información de las normas de Gobierno y Transformación Digital al Comité de Gobierno y Transformación Digital del PNPAIS durante las sesiones de trabajo planificadas.	Parcialmente implementado
20	R	El personal de la Unidad de Tecnologías de la Información, podría apropiarse o usar indebidamente los accesorios y/o periféricos de hardware que el PNPAIS adquiere para los mantenimientos correctivos, comprometiendo la continuidad operativa del parque informático.	Corrupción	Deficiente control en la asignación de repuestos y accesorios de informática para los mantenimientos correctivos	Compromete la continuidad operativa del parque informático	Vales de entrega generados por la Unidad de Administración	4	8	32	Medio	Mitigar	No	Exigir informe de uso con vales o guías de entrega de los recursos de hardware, al término de la acción de mantenimiento correctivo.	No implementado
21	R	El personal del proceso de Gestión de los Sistemas de Información y Bases de Datos, podría apropiarse o usar indebidamente los datos personales que se gestiona en el PNPAIS, comprometiendo la seguridad digital de la entidad.	Corrupción	Falta de controles en el marco del Sistema de Gestión de Seguridad de la Información	Compromete la imagen institucional y vulnera la seguridad de los datos del personal y de la entidad	La RD 213-2020-MIDIS/PNPAIS regula el control de acceso a los servicios digitales	4	8	32	Medio	Evitar	Si	Implementar el Sistema de Gestión de Seguridad de la Información	Parcialmente implementado

IDENTIFICACIÓN, ANÁLISIS DEL RIESGO /OPORTUNIDAD							VALOR DEL RIESGO / OPORTUNIDAD				PLAN DE TRATAMIENTO			
N°	R/O	RIESGO / OPORTUNIDAD	TIPO DE RIESGO	CAUSA	EFECTO	CONTROLES ACTUALES	PROBABILIDAD	IMPACTO	VALOR	NIVEL	ESTRATEGIA (ver comentario)	APLICA PLAN (SI/NO)	MEDIDA DE CONTROL / ACCIÓN	ESTADO
22	O	Vigencia del marco normativo de las TIC (estándares, normas técnicas, leyes, etc.), con énfasis en el gobierno y la transformación digital, así como las buenas prácticas de la gestión de TI.	Seguridad Digital	El PNPAIS no dispone de marco normativo que promueva de forma integral el Gobierno y la Transformación Digital, en función de sus tres ejes: Personal - Proceso - Tecnología	Dificulta la implementación del Gobierno y Transformación Digital	RD. 144-2021-MIDIS/PNPAIS, actualiza la conformación del Comité de Gobierno y Transformación Digital	4	8	32	Medio	Compartir	No	Fortalecer las capacidades del Comité de Gobierno y Transformación Digital y del Personal	Parcialmente implementado
23	O	Diversidad de proveedores y ventajas tecnológicas del Icloud (Computación en la nube) para la gestión de servicios de tecnologías de la información y comunicaciones	Seguridad Digital	El PNPAIS cuenta con servicios digitales que demandan alta disponibilidad	Asegurar la operatividad y la continuidad de los servicios digitales	Se hace uso de IaaS bajo el contrato de conectividad con Telefónica del Perú.	6	10	60	Alto	Asumir	No	Asegurar el uso de la computación en la nube para los servicios digitales críticos del PNPAIS, aplicando mejora continua.	Implementado

IDENTIFICACIÓN, ANÁLISIS DEL RIESGO /OPORTUNIDAD							VALOR DEL RIESGO / OPORTUNIDAD				PLAN DE TRATAMIENTO			
N°	R/O	RIESGO / OPORTUNIDAD	TIPO DE RIESGO	CAUSA	EFECTO	CONTROLES ACTUALES	PROBABILIDAD	IMPACTO	VALOR	NIVEL	ESTRATEGIA (ver comentario)	APLICA PLAN (SI/NO)	MEDIDA DE CONTROL / ACCIÓN	ESTADO
24	O	Soluciones de Blockchain, Big Data, herramientas de analítica de datos y de IA cuando corresponda	Seguridad Digital	El PNPAIS requiere de servicios digitales que den soporte a la toma de decisiones gerenciales	Facilita la toma de decisiones gerenciales, el cual tiene como soporte a sistemas de información especializados (Analítica de Datos/Inteligencia de Negocios y la Inteligencia Artificial)	Se hace uso de la Analítica de Datos a través de la plataforma del Office 365	6	10	60	Alto	Asumir	No	Identificar las necesidades e impulsar el uso de la tecnología de Analítica de Datos	Parcialmente implementado
25	O	Plataformas diversas, flexibles y multifuncionales para trabajos colaborativos (one drive, ms teams, outlook, etc.)	Seguridad Digital	El PNPAIS tiene la obligación de usar plataformas de colaboración en el marco del Gobierno y Transformación Digital	Mejora la imagen institucional y la relación de confianza entre el PNPAIS y su público objetivo	Se cuenta con la Plataforma Zoom licenciada para usuarios externos y el MS Teams para usuarios internos.	6	10	60	Alto	Asumir	No	Asegurar la continuidad del servicio de colaboración para usuarios internos y externos	Implementado

IDENTIFICACIÓN, ANÁLISIS DEL RIESGO /OPORTUNIDAD							VALOR DEL RIESGO / OPORTUNIDAD				PLAN DE TRATAMIENTO			
N°	R/O	RIESGO / OPORTUNIDAD	TIPO DE RIESGO	CAUSA	EFECTO	CONTROLES ACTUALES	PROBABILIDAD	IMPACTO	VALOR	NIVEL	ESTRATEGIA (ver comentario)	APLICA PLAN (SI/NO)	MEDIDA DE CONTROL / ACCIÓN	ESTADO
26	O	Presencia e importante crecimiento de la era digital en el contexto de la prestación de servicios con enfoque al cliente	Seguridad Digital	La evolución de la tecnología y la digitalización masiva de procesos empresariales genera una brecha en algunas organizaciones	Facilita el acceso a los servicios digitales a los ciudadanos, quienes pueden consumir servicios usando tecnología digital.	RD. 144-2021-MIDIS/PNPAIS, actualiza la conformación del Comité de Gobierno y Transformación Digital	6	10	60	Alto	Asumir	No	Impulsar y promover la digitalización de procesos en el marco del Gobierno y la Transformación Digital	Parcialmente implementado

Fuente: Elaboración propia

ANEXO N° 4 CARTILLA DE INSTRUCCIÓN PARA LA GESTIÓN DE LA EMERGENCIA Y/O DE CRISIS

PROPÓSITO

Establecer las instrucciones que debe seguir el CSIRT del PNPAIS o de quien haga sus veces, en situaciones de emergencia y/o de crisis declarados y confirmados ante la ocurrencia de incidentes de seguridad digital.

Las instrucciones que se desarrollan en esta cartilla atienden las siguientes interrogantes:

a. ¿Cuáles son o podrían ser los escenarios de emergencia y/o de crisis, que afectaría la capacidad operativa de la infraestructura tecnológica, entorno y los servicios digitales del PNPAIS?

b. ¿Cómo se convoca al CSIRT del PNPAIS, ante la declaración y confirmación del escenario de emergencia y/o de crisis?

c. ¿Cuáles son las consideraciones y el flujo de trabajo para tener cuenta de forma previa a las acciones de respuesta?

d. ¿Cuál debe ser la actuación del CSIRT del PNPAIS o de quien haga sus veces durante la situación de emergencia y/o de crisis?

DE LOS ESCENARIOS DE EMERGENCIA Y/O DE CRISIS

Los posibles escenarios de emergencia y/o de crisis que pueden darse e impactar en el entorno digital, infraestructura TIC y los servicios digitales, según su tipología y clasificación, son los que se describen en la tabla siguiente, los cuales pueden inclusive ser contrastados con la matriz de riesgos:

Grupo	Emergencia o Crisis	Tipo	Clasificación
1	Movimiento telúrico	Natural	Avería crítica
	Huracanes	Natural	
	Tsunamis	Natural	
	Inundación	Natural o provocado	
	Incendios	Natural o provocado	
	Robo / hurtos	Provocado	
	Fraudes / estafas	Provocado	
	Escándalo por protección de datos	Provocado	
	Ataque cibernético / Ciberdelincuencia	Provocado	
	Ataque terrorista y/o sabotaje	Provocado	

<table>
<tr><th>Grupo</th><th>Emergencia o Crisis</th><th>Tipo</th><th>Clasificación</th></tr>
<tr><td colspan="4">Son situaciones de crisis que se generan como consecuencia de un evento natural, casi siempre difícil de prever; lo son también aquellas situaciones provocadas por el ser humano. En ambos casos el impacto de estas emergencias o de crisis, impacta en la organización de forma negativa, podría implicar la pérdida de materiales, afectación a la operatividad del entorno digital e infraestructura TIC, y lo que es peor podría comprometer la vida y la salud de las personas.</td></tr>
<tr><td rowspan="4">2</td><td>Intoxicación</td><td>Provocado</td><td rowspan="4">Emergencia sanitaria</td></tr>
<tr><td>Epidemias, pandemias</td><td>Natural o provocado</td></tr>
<tr><td>Amenazas biológicas</td><td>Natural o provocado</td></tr>
<tr><td>Accidentes Personales muy frecuentes</td><td>Provocado</td></tr>
<tr><td colspan="4">Son situaciones de emergencia o de crisis, que pueden ocurrir en la organización y que pueden afectar la salud ocupacional y/o salud pública. Este sería el caso, por ejemplo, si los participantes a un evento promovido por la organización se intoxicaran porque la comida estaba en mal estado. Lo son también las emergencias médicas no atendidas por la organización a nivel de primeros auxilios o en las que no se adopten acciones de prevención y de protección de la salud ocupacional, o simplemente cuando no se cumplan con los protocolos de salud establecidos.</td></tr>
<tr><td rowspan="4">3</td><td>Fuga de información no autorizada</td><td>Provocado</td><td rowspan="4">Ataques a la reputación / integridad</td></tr>
<tr><td>Actos de corrupción en el entorno</td><td>Provocado</td></tr>
<tr><td>Comportamiento no ético del personal</td><td>Provocado</td></tr>
<tr><td>Uso de recursos de TIC con fines particulares</td><td>Provocado</td></tr>
<tr><td colspan="4">Son situaciones de emergencia o de crisis porque afectan la buena imagen y reputación de la organización, pues se convierten con gran facilidad en una amenaza si es que no se desactivan de forma inmediata. La mala conducta de la administración también pone en peligro la imagen y la integridad de una organización.</td></tr>
</table>

ANEXO N° 5 CARTILLA DE INSTRUCCIÓN PARA EL CONTROL DE LAS OPERACIONES DE RECUPERACIÓN

PROPÓSITO

Establecer las instrucciones que se deben seguir para recuperar la operatividad de la infraestructura TIC y/o de los servicios digitales afectados por incidente de seguridad digital.

En este apartado se desarrollan las siguientes interrogantes:

a. ¿Cuáles son los roles, responsabilidades y la organización del CSIRT, personal de la UTI y CGTD-PNPAIS?

b. ¿Cuáles son los aspectos básicos a tener en cuenta para preservar y recuperar la operatividad?

c. ¿Qué hacer para recuperar y asegurar la operatividad?

d. ¿Cómo debe ser la evaluación y el control de la recuperación?

ROLES, RESPONSABILIDADES Y ORGANIZACIÓN

Los roles, las responsabilidades y la organización del CSIRT, personal de UTI y del CGTD-PNPAIS se derivan de las normativas siguientes:

a. Manual de Operaciones del PNPAIS

b. Resolución de conformación del CGTD-PNPAIS

c. Resolución de conformación del CSIRT-PNPAIS

d. Marco normativo de Gobierno y Transformación Digital

Para los efectos de la presente cartilla, los roles y responsabilidades del CSIRT, es como sigue:

N°	Conformación	Roles / Responsabilidades
1	Ejecutivo/a de la Unidad de Tecnologías de la Información, o quien haga sus veces.	**Coordinador del CSIRT**: Es el encargado de realizar todas las actividades de gestión del CSIRT, así mismo es el punto de contacto con el CSIRT Nacional del Centro Nacional de Seguridad Digital.
2	Administrador/a de la Red de Datos y Comunicaciones, o quien haga sus veces.	**Gestor de Incidentes:** Es el responsable de la gestión de los incidentes de seguridad digital, así como también de la comunicación del incidente al Centro Nacional de Seguridad Digital.
3	El/la Coordinador/a de Soporte Técnico y Mesa de Ayuda, o quien haga sus veces.	**Gestor de Redes y Comunicaciones:** Es responsable de la seguridad de las redes de comunicación de la entidad, implementa medidas de cifrado para la protección de la confidencialidad de las comunicaciones y determina el modelo de monitorización de las mismas.

N°	Conformación	Roles / Responsabilidades
4	El/la Coordinador/a de Infraestructura de TI y/o el Coordinador de Desarrollo de Software, o quien haga sus veces.	**Gestor de Infraestructuras Digitales:** Es el responsable de la seguridad de los servidores e infraestructuras de nube, determina las reglas de seguridad a nivel del sistema operativo y aplicaciones.
5	Oficial de Seguridad y Confianza Digital	**Oficial de Seguridad y Confianza Digital:** Participa como miembro del CSIRT para realizar las funciones de apoyo en la gestión de incidentes y articulador de los ámbitos de seguridad y confianza digital que sean relevantes al incidente.

Asimismo, teniendo en cuenta que, siendo la misión principal del CSIRT durante una situación de emergencia y/o de crisis, controlar los riesgos y recuperar la operatividad de la infraestructura TIC y/o de los servicios digitales, las actividades principales que deben gestionar de forma alineada a los ámbitos de la prevención y contención de riesgos, y con cierta regularidad son:

N°	Actividad	Descripción / Condición
1	Revisar arreglos y procedimientos estándar de seguridad.	Actividad de seguridad que será ejecutado en tiempos normales de operación y funcionamiento de las TIC, regularmente es fuera de una situación de emergencia y/o de crisis.
2	Gestionar auditorías y entrenamiento ante nuevas amenazas.	
3	Investigar nuevas formas de amenazas.	
4	Gestionar el manejo remoto de la información crítica como contraseñas o configuraciones de red.	
5	Mantener un registro de normas y regulaciones y controlar su cumplimiento	
6	Detectar, analizar, responder y prevenir ciber-amenazas.	Actividad de seguridad que será ejecutado en tiempos normales de operación y funcionamiento de las TIC, puede ser fuera o dentro de una situación de emergencia y/o de crisis.
7	Mantener un registro de todas las actividades sobre gestión de riesgos para referencias futuras.	
8	Priorizar y escalar alertas y tareas de gestión de riesgos	Actividad de seguridad que será ejecutado en circunstancias previas a una situación de emergencia y/o de crisis.
9	Coordinar y ejecutar las estrategias de respuesta.	Actividad de seguridad que será ejecutado en situaciones de emergencia y/o de crisis.
10	Realizar estudios forenses sobre los incidentes.	Actividad de seguridad que será ejecutado de forma posterior a una situación de emergencia y/o de crisis, cuando corresponda.

ANEXO N° 6 CONSIDERACIONES PARA EL ANÁLISIS DE IMPACTO

1. Determinar los procesos de misión/negocio y la criticidad de su recuperación

- Procesos del PNPAIS y su posible criticidad de recuperación:

Proceso				Impacto			
N°	Tipo de proceso	Macroproceso (Nivel 0)	Proceso (Nivel 1)	Muy Alto	Alto	Medio	Bajo
1	**Estratégico**	Gestión de la Dirección	Revisión de Indicadores Estratégicos			X	
2			Dirigir el Sistema de Gestión de Calidad			X	
3		Planeamiento, Presupuesto y Modernización	Planeamiento Estratégico y Operativo			X	
4			Gestión del Proceso Presupuestario		X		
5			Gestión Organizacional y Normativo				X
6		Gestión de Calidad	Diseño e implementación del Sistema de Gestión de la Calidad			X	
7			Monitoreo y Evaluación al Sistema de Gestión de la Calidad			X	
8			Implementación de mejoras continua del Sistema de Gestión de la Calidad			X	
9		Monitoreo y Evaluación	Monitoreo			X	
10			Evaluación			X	
11		Gestión del Control Institucional	Servicios de Control Institucional			X	
12			Servicios Relacionados de Control				X
13	**Misionales**	Gestión de Focalización, Ejecución y Operatividad de las Plataformas de Servicio	Formulación y evaluación (Pre - inversión)	X			
14			Ejecución de las plataformas de servicio	X			
15			Operatividad y mantenimiento de las plataformas de servicio	X			
16		Gestión de Articulación de Servicios	Diagnóstico	X			
17			Articulación	X			
18		Gestión de Ejecución de la Articulación	Ejecución de la Intervención	X			
19			Gestión de Riesgo de Desastres	X			
20	**De Apoyo**	Gestión Administrativa	Gestión Abastecimiento y Control Patrimonial		X		
21			Gestión Financiera y Contable		X		
22			Gestión Documentaria y Atención al Ciudadano			X	
23		Gestión de Recursos Humanos	Gestión del Empleo y Administración de Personal		X		

Proceso				Impacto			
N°	Tipo de proceso	Macroproceso (Nivel 0)	Proceso (Nivel 1)	Muy Alto	Alto	Medio	Bajo
24			Gestión del Desarrollo de Capacidades y de las Relaciones Humanas		X		
25		Gestión de Comunicación e Imagen	Gestión de Imagen y Posicionamiento del Programa			X	
26			Gestión de la Información y Comunicación del Programa		X		
27		Gestión de Sistemas y Tecnologías de la Información	Gestión de la Seguridad de la Información y Calidad de TI	X			
28			Gestión de los Sistemas de Información y Bases de Datos	X			
29			Gestión de la Infraestructura y Redes de Comunicaciones	X			
30			Gestión de Soporte Operacional y Servicios de TI	X			
31		Asesoría Jurídica	Asistencia Jurídica Legal			X	
32			Gestión de Información sobre Procesos Administrativos, Arbitrales o Judiciales			X	

Fuente: Elaboración propia.

- Conceptos relacionados con el tiempo de inactividad aceptable de los sistemas de información y servicios digitales:

Concepto	Descripción
Tiempo Máximo Tolerable de Inactividad (MTD).	El MTD representa la cantidad total de tiempo que el propietario del sistema/oficial de autorización está dispuesto a aceptar para una interrupción de un proceso de misión/negocio, e incluye todas las consideraciones de impacto.
Objetivo de Tiempo de Recuperación (RTO)	El RTO define la cantidad máxima de tiempo que un recurso del sistema puede permanecer no disponible antes de que haya un impacto inaceptable en otros recursos del sistema, los procesos de misión/negocios respaldados y el MTD.
Objetivo de Punto de Recuperación (RPO)	El RPO representa el punto en el tiempo, antes de una interrupción o caída del sistema, hasta el cual los datos del proceso de misión/negocio pueden ser recuperados (dado que se cuenta con la copia de seguridad más reciente) después de una interrupción.

Fuente: NIST Special Publication 800-34 Rev. 1 Contingency Planning Guide for Federal Information Systems

2. Identificar los requisitos de recuperación

- Modelo para la jerarquía de prioridades de recuperación del sistema de información

Recurso/componente del sistema	Plataforma / Sistema Operativo / Versión	Descripción

Fuente: NIST Special Publication 800-34 Rev. 1 Contingency Planning Guide for Federal Information Systems

3. Identificar las prioridades de recuperación

- Prioridades básicas de infraestructura tecnológica previamente identificados:

N°	Incidente / Contingencia	Causas probables	Métrica / Parámetro		
			RTO	MTD	RPO
1	**(01)** Inoperatividad del Centro de Gestión de Datos (DATA CENTER)	Movimiento telúrico	06 H	1 D	90%
		Incendio	06 H	1 D	90%
		Inundación	06 H	1 D	90%
		Acciones de Sabotaje, terrorismo, vandalismo, etc.	06 h	1 D	90%
		Ciberataque	06 H	1 D	90%
2	**(02)** Inoperatividad de la Infraestructura de Comunicaciones (enlace/conectividad)	Inoperancia del Switch Core	05 H	1 D	80%
		Fallas técnicas en el cableado estructurado	03 H	1 D	80 %
		Caída del servicio de Internet	02 H	1 D	80%
		Caída del suministro eléctrico	02 H	1 D	80%
		Ciberataque	08 H	1 D	80%
3	**(03)** Inoperatividad de Servicios Digitales (incluye bases de datos)	Caída del servidor de dominio	2 H	1 D	80%
		Caída del servidor de alojamiento (Interfaz y base de datos)	2 H	1 D	80%
		Inoperancia del sistema de energía estabilizada	6 H	1 D	80%
		Inoperancia del sistema de refrigeración	2 H	1 D	80%
		Interrupción del servicio por parte del proveedor	2 H	1 D	80%
		Ciberataque	08 H	1 D	80%
4	**(04)** Condiciones inseguras para el personal (Que afecten o pongan en riesgo la vida y la salud)	Acciones de sabotaje, terrorismo, vandalismo, otros	48 H	3 D	80%
		Condiciones ambientales no aptas para la salud humana	72 H	7 D	80%

N°	Incidente / Contingencia	Causas probables	Métrica / Parámetro		
			RTO	MTD	RPO

Leyenda:

- **RTO** (Recovery Time Objetive): Tiempo de recuperación (recursos humanos y tecnológicos) - Es el tiempo que un proceso permanecerá o puede permanecer detenido antes de que su funcionamiento sea restaurado. Este valor suele ser muy subjetivo, por lo que los líderes de las acciones de respuesta deberán previamente haber evaluado y valorado la infraestructura tecnológica sobre la que aplicará esta métrica.

- **MTD** (Maximum Tolerable Downtime): Tiempo máximo tolerable de caída - Es el tiempo que un pro-ceso puede permanecer caído antes de que se produzcan consecuencias devastadoras para la organización. Hay que tener en cuenta que esta valoración es en la mayoría de casos subjetiva, puesto que, si bien es posible medir cuantitativamente el impacto de una contingencia a nivel de usuarios finales, clientes o proveedores, servicios ofertados por la web no disponibles, determinar en qué momento dicho impacto pone en riesgo la continuidad de la organización resulta ser complejo.

- **RPO**: Grado de dependencia de la actualidad de los datos - (Recovery Point Objetive) Este valor determina el impacto que tiene sobre la actividad la pérdida de datos. Este valor es crítico a la hora de determinar las políticas de copias de la organización y no guarda relación con el RTO.

H: Horas **D**: Días

Fuente: Elaboración propia.

- Prioridades básicas de los sistemas de información y servicios digitales previamente identificados:

N°	Incidente / Contingencia	Causas probables	Métrica / Parámetro		
			RTO	MTD	RPO
1	Sistema de información y monitoreo sismonitor - libro de reclamaciones	Aplicativo WEB para el registro de los reclamos reportados por los pobladores o personas externas al programa.	2 H	8 H	95%
2	Sistema de información interna (intranet) - indicadores de control	Aplicativo WEB que permite el registro de la información de los usuarios del programa en relación al cumplimiento de las funciones encomendadas - Registro de los Indicadores de Gestión e Indicadores Operativos del Programa Nacional PAIS	8 H	1 D	70%
3	Sistema de información interna (intranet) - módulo de asesoría jurídica	Aplicativo WEB que permite el registro de la información de los usuarios del programa en relación al cumplimiento de las funciones encomendadas - Registro de los Laudos arbitrales	8 H	1 D	70%
4	Sistema de información interna (intranet) - módulo de asesoría jurídica	Aplicativo WEB que permite el registro de la información de los usuarios del programa en relación al cumplimiento de las funciones encomendadas - Gestión y Mantenimiento de la WEB del Sistema de Control Interno	8 H	1 D	70%

N°	Incidente / Contingencia	Causas probables	Métrica / Parámetro		
			RTO	MTD	RPO
5	Sistema de información y monitoreo sismonitor - carpetas regionales	Módulo para la Unidad de Planeamiento y Presupuesto que mostrará un repositorio subdividido en Resumen Ejecutivo, Resumen de Proyectos e Inversiones y Ficha Coyuntural; para acompañar documentos técnicos de información elaborados para las diferentes reuniones bilaterales entre los diferentes niveles de gobiernos en los cuales tiene participación el PN País a través de la Dirección Ejecutiva.	2 H	8 H	95%
6	Sistema de información y monitoreo sismonitor - repositorio documental del programa	Aplicativo WEB donde se almacenan todos los documentos, directivas, encuestas, manuales, reportes de otras instituciones en relación con el programa nacional PAIS	2 H	8 H	95%
7	Sistema de información y monitoreo sismonitor - recursos humanos	Aplicativo WEB para el registro de las convocatorias, puestos, procesos	2 H	8 H	95%
8	Plataforma e-learning chamilo	Herramienta WEB para la Gestión de la Plataforma e-learning Chamilo para gestionar el aprendizaje en los tambos como apoyo al gobierno: "Yo aprendo en casa".	8 H	1 D	70%
9	Módulo de encuesta de satisfacción	Módulo de Gestión de las encuestas de satisfacción de la calidad del servicio brindado a los usuarios en los tambos. Solicitado por el especialista de CALIDAD de la Dirección Ejecutiva.	8 H	1 D	70%
10	Módulo de gestión integrada para URRHH	Módulo de información integrada de Recursos Humanos, para la Gestión de la Información sobre los datos personales, académicos y laborales de los servidores del programa.	8 H	1 D	70%
11	Módulo de sistema de gestión documental - SGD	Aplicativo WEB para la Gestión de Documentos, en el marco de Cero Papeles.	4 H	12 H	80%
12	Sistema de información interna (intranet) - tablero de control - usuario	Reporte BI que permite la visualización de las atenciones realizadas en las plataformas TAMBOS y PIAS	8 H	1 D	70%
13	Sistema de información interna (intranet) - tambo bicentenario	Aplicativo WEB que permite el registro de la información de los usuarios del programa en relación al cumplimiento de las funciones encomendadas - Registro de documentos, encuestas y reporte general en el marco del tambo bicentenario del Programa Nacional PAIS	4 H	12 H	80%

N°	Incidente / Contingencia	Causas probables	Métrica / Parámetro		
			RTO	MTD	RPO
14	Sistema de información interna (intranet) - hambre cero	Aplicativo WEB que permite el registro de la información de los usuarios del programa en relación al cumplimiento de las funciones encomendadas - Reporte de Actividades Ejecutadas, en el marco de las funciones por Hambre Cero a cargo de los gestores de los tambos	4 H	12 H	80%
15	Sistema de información interna (intranet) - reporte de género BI	Aplicativo WEB que permite el registro de la información de los usuarios del programa en relación al cumplimiento de las funciones encomendadas - Reporte BI para la visualización de las atenciones e intervenciones, alineadas a la igualdad de genero	8 H	1 D	70%
16	Landing page _ amachay	Aplicativo web que permite mostrar las actividades y servicios realizados a nivel regional a los 152 distritos priorizados en el marco del COVID19	8 H	1 D	70%
17	Sistema de información interna (intranet) - consulta SGD	Aplicativo WEB que permite a todos los usuarios del programa ver el seguimiento de los documentos (expedientes) del Sistema de Gestión Documental	4 H	12 H	80%
18	Sistema de información interna (intranet) - registro SGD	Aplicativo WEB que permite a los encargados de la documentación de la Unidad de Administración registrar las entidades adicionales a los usuarios del programa de acuerdo con la necesidad	4 H	12 H	80%
19	Sistema de información interna (intranet) - reporte SGD	Aplicativo WEB que permite a todos los usuarios del programa ver los documentos (expedientes) del Sistema de Gestión Documental que se visualizan en las bandejas de cada una de las unidades del programa nacional PAIS	8 H	1 D	70%
20	Sistema de información interna (intranet) - tambo bicentenario - tambo productivo	Aplicativo WEB que permite el registro de la información de los usuarios del programa en relación al cumplimiento de las funciones encomendadas - Bandeja para la Gestión de los cuestionarios registrados por los gestores de los TAMBOS, en relación a sus módulos productivos.	8 H	1 D	70%
21	Sistema de información interna (intranet) - módulos recursos humanos - selección NE	Aplicativo WEB que permite el registro de la información de los usuarios del programa en relación al cumplimiento de las funciones encomendadas - Gestión de Convocatorias para el Comité de Convocatorias de Supervisores y Residentes de los Núcleos Ejecutores del Programa Nacional PAIS	8 H	1 D	70%
22	Sistema de información interna (intranet) - módulos de encuestas de satisfacción	Aplicativo WEB que permite el registro de la información de los usuarios del programa en relación al cumplimiento de las funciones encomendadas - Gestión de las encuestas de satisfacción generadas producto de las atenciones a los usuarios de los centros poblados	8 H	1 D	70%

N°	Incidente / Contingencia	Causas probables	Métrica / Parámetro		
			RTO	MTD	RPO
23	Sistema de información interna (intranet) - reporte de plataformas BI	Aplicativo WEB que permite el registro de la información de los usuarios del programa en relación al cumplimiento de las funciones encomendadas - Reporte para el seguimiento y monitoreo del estado del INTERNET en los TAMBOS	8 H	1 D	70%
24	Sistema de información interna (intranet) - seguimiento de expedientes SGD	Aplicativo WEB que permite a todos los usuarios del programa hacer el seguimiento a los documentos (expedientes) del Sistema de Gestión Documental, considera el flujo de la ruta de los documentos de cada una de las unidades del programa nacional PAIS	8 H	1 D	70%
25	Sistema de información interna (intranet) - documentos pendientes SGD	Aplicativo WEB que permite a todos los usuarios del programa generar el reporte de todos los documentos (expedientes) pendientes del Sistema de Gestión Documental, considera todos los documentos pendientes de cada una de las bandejas de las unidades del programa nacional PAIS	4 H	12 H	80%
26	Sistema de información interna (intranet) - reporte SGD BI	Aplicativo WEB que permite a todos los usuarios del programa ver los indicadores de la documentación de acuerdo con la gestión de los documentos en el Sistema de Gestión Documental	8 H	1 D	70%
27	Sistema de información interna (intranet) - sistema de gestión integrado	Aplicativo WEB que permite el registro de la información de los usuarios del programa en relación al cumplimiento de las funciones encomendadas - Registro en el Sistema de Gestión Integrado (Repositorio de Documentación del Sistema de Gestión Integrado)	8 H	1 D	70%
28	Sistema de información interna (intranet) - gestión de riesgo	Aplicativo WEB que permite el registro de la información de los usuarios del programa con relación al cumplimiento de las funciones encomendadas - Registro de los riesgos encontrados en cumplimiento de las funciones del Programa Nacional PAIS	4 H	12 H	80%
29	Sistema de información interna (intranet) - reporte matriz de riesgos	Aplicativo WEB que permite el registro de la información de los usuarios del programa en relación con el cumplimiento de las funciones encomendadas - Seguimiento y Monitoreo de la Matriz de Riesgos de las UUOO y UUTT del Programa Nacional PAIS	8 H	1 D	70%
30	Sistema de información interna (intranet) - consultas de reniec en línea	Aplicativo WEB que permite el registro de la información de los usuarios del programa con relación al cumplimiento de las funciones encomendadas - Consulta de DNI en línea a la base de datos de la Reniec para los usuarios de Mesa de Partes del Programa Nacional	4 H	12 H	80%
31	Sistema de información interna (intranet) - tablero de control - ejecución presupuestal	Reporte BI que permite la visualización de la ejecución presupuestal del Programa Nacional PAIS, así como la ejecución presupuestal detallada de las UUTTs y UUOOs	8 H	1 D	70%

N°	Incidente / Contingencia	Causas probables	Métrica / Parámetro		
			RTO	MTD	RPO
32	Sistema de información interna (intranet) - módulos administrativos	Aplicativo WEB que permite el registro de la información de los usuarios del programa en relación al cumplimiento de las funciones encomendadas - Registro de visitas, Ordenes de Servicio y Fondos por Encargo del Programa Nacional PAIS	4 H	12 H	80%
33	Sistema de información interna (intranet) - módulos de seguridad	Aplicativo WEB que permite el registro de la información de los usuarios del programa en relación al cumplimiento de las funciones encomendadas - Gestión de los Usuarios de la INTRANET del Programa Nacional PAIS	8 H	1 D	70%
34	Sistema de información interna (intranet) - módulos de gestion de actividades e intervenciones	Aplicativo WEB que permite el registro de la información de los usuarios del programa en relación al cumplimiento de las funciones encomendadas - Gestión de las actividades e intervenciones de las entidades en los tambos del Programa Nacional PAIS	8 H	1 D	70%
35	Sistema de información interna (intranet) - módulos de diagnóstico participativo	Aplicativo WEB que permite el registro de la información de los usuarios del programa en relación al cumplimiento de las funciones encomendadas - Gestión del Padrón nominal, participación, ámbito de influencia, identificación de actores e información	8 H	1 D	70%
36	Sistema de información interna (intranet) - programación de planes de trabajo	Aplicativo WEB que permite el registro de la información de los usuarios del programa con relación al cumplimiento de las funciones encomendadas	8 H	1 D	70%
37	Sistema de información interna (intranet) - soporte	Aplicativo WEB que permite el registro de la información de los usuarios del programa en relación con el cumplimiento de las funciones encomendadas - Gestión de los tickets	4 H	12 H	80%
38	Sistema de información interna (intranet) - registro de incidencias del internet	Aplicativo WEB que permite el registro de la información de los usuarios del programa en relación con el cumplimiento de las funciones encomendadas - Registro de las INCIDENCIAS reportadas a las empresas externas al programa nacional PAIS	4 H	12 H	80%
39	Módulo de evaluación de conocimientos	Módulo que permite la virtualización de la toma de exámenes de conocimiento a los postulantes a los diferentes puestos del PNPAIS que requerían dicha evaluación, la que	8 H	1 D	70%
40	Plataforma de votación virtual	Plataforma WEB de votación para el proceso de elecciones de los representantes Titulares y Suplentes de los trabajadores en el Comité de Seguridad y Salud en el Trabajo	8 H	1 D	70%
41	Sistema de información externa (TAMBOOK) - web site informativo general del PNPAIS	Aplicativo WEB Informativo de las operaciones que se realizan en el Programa, así como información importante conteniendo datos personales de los gestores de tambos	4 H	12 H	80%

N°	Incidente / Contingencia	Causas probables	Métrica / Parámetro		
			RTO	MTD	RPO
42	Sistema de información interna (intranet) - asignación de tambos	Aplicativo Web informativo que permite asignar a los monitores lo tambos que deben monitorear	4 H	12 H	80%
43	Sistema de información interna (intranet) - programación de actividades JUT's y monitores	Aplicativo Web Informativo que registrar las actividades que realizan los JUT y Monitores	8 H	1 D	70%
44	Sistema de control de pago de servicios básicos en tambos (agua, luz) (intranet)	Aplicativo Web que permite a los GIT, JUT y Coordinador de Abastecimiento el registro de recibos correspondiente a un periodo determinado	4 H	12 H	80%
45	Sistema de información interna (intranet) - sistema de evaluación de buenas prácticas	Aplicativo Web que permite a los GIT, el registro de sus experiencias exitosas implementadas en los tambos del PNPAIS	8 H	1 D	70%
46	Módulo casillas electrónicas dentro del marco de la ley N° 31736.	Aplicativo Web que permite obtener el documento del SGD de acuerdo a un número de expediente solicitado por el usuario	8 H	1 D	70%
47	Sistema de información interna (intranet) - módulo de gestión y monitoreo del avance de obra	Aplicativo Web que gestiona la información de proyectos, permitiendo registrar actualizaciones, verificar estados, visualizar imágenes detalladas y decidir sobre la aprobación o rechazo del progreso del proyecto.	8 H	1 D	70%
48	Sistema de información interna (intranet) - módulo registro pias	Aplicativo Web que permite registrar todas las intervenciones realizadas en las plataformas itinerantes móviles (PIAS)	8 H	1 D	70%
49	Sistema de información interna (intranet) - módulo registro PIM	Aplicativo Web que permite listar el Plan de Intensión de Movimiento (PIM), asimismo permite visualizar la geolocalización del punto de atención	4 H	12 H	80%
50	Sistema de información interna (intranet) - módulo registro de incidencias en las pias	Aplicativo Web que permite registrar todas las incidencias ocurridas en las PIAS	8 H	1 D	70%
51	Sistema de información interna (intranet) - módulo registro nacimiento en las pias	Aplicativo Web que permite registrar todos los nacimientos ocurridos en las PIAS	8 H	1 D	70%

N°	Incidente / Contingencia	Causas probables	Métrica / Parámetro		
			RTO	MTD	RPO
52	Sistema de información interna (intranet) - módulo encuesta satisfacción PIAS	Aplicativo Web que permite registrar encuesta de satisfacción PIAS	8 H	1 D	70%
53	Sistema de información interna (intranet) - módulo actividades diarias en las PIAS	Aplicativo Web que permite listar las intervenciones cerradas por campaña, asimismo como el total de atenciones y beneficiarios	8 H	1 D	70%
54	Sistema de información interna (intranet) - módulo de diagnóstico para las PIAS	Aplicativo Web permite registrar y cargar toda la información relacionada a los puntos de atención y sus pobladores de las PIAS	8 H	1 D	70%
55	Sistema de información interna (intranet) - módulo de programación de actividades de soporte en las PIAS	Aplicativo Web que permite registrar todas las actividades de soporte que realiza en el gestor de las PIAS	8 H	1 D	70%
56	Sistema de información interna (intranet) - módulo de registro de referencias en las PIAS	Aplicativo Web que permite registrar todas las referencias ocurridas en las PIAS	8 H	1 D	70%
57	Sistema de información interna (intranet) - módulo de registro del plan de intensión de movimiento de las PIAS	Aplicativo Web que permite registrar todos los planes de trabajo y las actividades correspondientes que son necesarias previamente para la programación de las intervenciones	8 H	1 D	70%
58	Sistema de información interna (intranet) - calendario intervenciones	Aplicativo Web que permite visualizar de manera óptima las intervenciones programadas, aprobado y ejecutadas	8 H	1 D	70%
59	Landing page para tambos y PIAS	Página Informativa de Tambos y PIAS	8 H	1 D	70%

N°	Incidente / Contingencia	Causas probables	Métrica / Parámetro		
			RTO	MTD	RPO

Leyenda:

- **RTO** (Recovery Time Objetive): Tiempo de recuperación (recursos humanos y tecnológicos) - Es el tiempo que un proceso permanecerá o puede permanecer detenido antes de que su funcionamiento sea restaurado. Este valor suele ser muy subjetivo, por lo que los líderes de las acciones de respuesta deberán previamente haber evaluado y valorado la infraestructura tecnológica sobre la que aplicará esta métrica.

- **MTD** (Maximum Tolerable Downtime): Tiempo máximo tolerable de caída - Es el tiempo que un pro-ceso puede permanecer caído antes de que se produzcan consecuencias devastadoras para la organización. Hay que tener en cuenta que esta valoración es en la mayoría de casos subjetiva, puesto que, si bien es posible medir cuantitativamente el impacto de una contingencia a nivel de usuarios finales, clientes o proveedores, servicios ofertados por la web no disponibles, determinar en qué momento dicho impacto pone en riesgo la continuidad de la organización resulta ser complejo.

- **RPO**: Grado de dependencia de la actualidad de los datos - (Recovery Point Objetive) Este valor determina el impacto que tiene sobre la actividad la pérdida de datos. Este valor es crítico a la hora de determinar las políticas de copias de la organización y no guarda relación con el RTO.

H: Horas **D**: Días

Fuente: Elaboración propia.

ANEXO N° 7 CONSIDERACIONES PARA LA IDENTIFICACIÓN DE CONTROLES PREVENTIVOS

1. Tipos de controles

Control	Objetivo	Medida
Controles de Seguridad Física	Proteger las instalaciones y activos físicos contra accesos no autorizados y daños	Instalación de sistemas de seguridad (cámaras, alarmas, control de acceso)
Controles de Seguridad de la Información	Proteger la integridad, confidencialidad y disponibilidad de la información	Implementación de firewalls, sistemas de detección de intrusos (IDS), políticas de contraseñas robustas
Controles de Respaldo de Datos	Asegurar la disponibilidad de datos críticos en caso de pérdida o corrupción de datos	Realización de copias de seguridad regulares, almacenamiento de copias en sitios remotos.
Controles de Redundancia	Asegurar la continuidad de operaciones críticas mediante la eliminación de puntos únicos de falla	Implementación de sistemas y componentes redundantes (servidores, redes, almacenamiento).
Controles de Mantenimiento Preventivo	Prevenir fallos operativos mediante el mantenimiento y actualización proactiva de sistemas y equipos	Programación de mantenimiento regular para hardware y software, actualización de sistemas
Controles de Capacitación y Concienciación	Asegurar que los empleados estén capacitados y sean conscientes de su papel en la protección de los activos de la organización	Programas de capacitación regular para empleados en seguridad de la información y procedimientos de continuidad del negocio
Controles de Gestión de Proveedores	Garantizar que los proveedores cumplan con los requisitos de continuidad del negocio y seguridad	Evaluación y selección rigurosa de proveedores, establecimiento de acuerdos de nivel de servicio (SLA)
Controles de Gestión de Configuración	Asegurar, que los cambios en los sistemas se gestionen de manera controlada para minimizar el riesgo de interrupciones	Implementación de procesos de gestión de cambios y configuración para todos los sistemas críticos

Fuente: Elaboración propia.

2. Controles preventivos más comunes para implementarse

N°	Control preventivo	Descripción
01	Suministro de energía ininterrumpida (UPS)	Proporcionar energía de respaldo a corto plazo a todos los componentes del sistema (incluyendo controles ambientales y de seguridad)
02	Generadores de energía de respaldo	Proporcionar energía de respaldo a largo plazo
03	Sistema de aire acondicionado	Evitar fallos de ciertos componentes, como un compresor
04	Sistema de supresión de incendios	Implementado en el centro de datos
05	Detectores de humo y fuego	Instalados en el techo y piso de la sala de computadoras
06	Sensores de agua	Instalados en el techo y piso de la sala de computadoras

N°	Control preventivo	Descripción
07	Contenedores	Resistentes al calor y al agua para medios de respaldo.
08	Interruptor maestro	Para el apagado de emergencia de los sistemas de información y/o servicios digitales.
09	Almacenamiento externo de medios de respaldo	Por ejemplo: Respaldos en cintas tape
10	Controles de seguridad digital	Por ejemplo: Gestión de claves criptográficas
11	Respaldos programados frecuentemente	Que incluyan dónde se almacenan los respaldos (en el sitio o fuera de él) y con qué frecuencia se recirculan y trasladan al almacenamiento

Fuente: NIST Special Publication 800-34 Rev. 1 Contingency Planning Guide for Federal Information Systems

3. Nivel de actividad

Control preventivo	Descripción
Suministro de energía ininterrumpida (UPS)	Proporcionar energía de respaldo a corto plazo a todos los componentes del sistema (incluyendo controles ambientales y de seguridad)
Generadores de energía de respaldo	Proporcionar energía de respaldo a largo plazo

Fuente: Resolución Ministerial N.° 138-2021-MIDIS

4. Estado de la medida de control / acción

ESTADO DE LA MEDIDA DE CONTROL / ACCIÓN	
Descripción	Estado
De 0% hasta el 50% de las actividades culminadas, la medida de control / acción es:	No implementada
De 51% hasta el 99% de actividades culminadas, la medida de control / acción es:	Parcialmente implementada
El 100% de las actividades culminadas, la medida de control / acción es:	Implementada

Fuente: Resolución Ministerial N.° 138-2021-MIDIS

ANEXO N° 8 CONSIDERACIONES PARA LA IMPLEMENTACIÓN DE ESTRATEGIAS DE CONTINGENCIA

1. Estrategias de contingencia según ámbito de aplicación

Ámbito	Medida
Prevención	Realización de análisis de riesgos periódicos para identificar vulnerabilidades.
	Implementación de controles de acceso, firewalls y herramientas de detección de intrusiones.
	Actualización constante de software y parches de seguridad.
	Capacitación y concientización del personal en ciberseguridad y buenas prácticas.
	Realización de pruebas de penetración y auditorías de seguridad para detectar posibles debilidades.
	Desarrollo de políticas de seguridad de la información, como la gestión de contraseñas, acceso remoto seguro, etc.
Contención	Activación de protocolos de respuesta a incidentes de seguridad para detener la amenaza.
	Aislamiento de los sistemas afectados para evitar la propagación del incidente a otras áreas.
	Identificación y bloqueo de usuarios no autorizados o dispositivos comprometidos.
	Uso de soluciones de respaldo en tiempo real para mantener la operación de los servicios esenciales mientras se resuelve el incidente.
	Comunicación clara y rápida a los equipos de TI y a los usuarios sobre el incidente y las medidas tomadas.
Recuperación	Implementación de planes de recuperación ante desastres, que incluyan procedimientos de restauración de datos desde copias de seguridad.
	Verificación de la integridad de la información y sistemas restaurados para asegurar que no haya sido comprometida.
	Monitoreo post-incidente para detectar posibles nuevas amenazas o comportamientos anómalos.
	Actualización de los planes de contingencia y procedimientos basados en las lecciones aprendidas del incidente.
	Ejecución de simulacros de recuperación para mejorar los tiempos de respuesta y la efectividad de los planes de recuperación de desastres.

Fuente: Elaboración propia.

2. Estrategias de contención personalizadas

Estrategia de Continuidad TIC	Sub estrategia de Continuidad TIC	Descripción
Copias de Seguridad y Recuperación de Datos	Copias de Seguridad (backups)	✓ Frecuencia: Realizar copias de seguridad diarias, semanales y mensuales de todos los datos críticos. ✓ Ubicación: Almacenar copias de seguridad en múltiples ubicaciones, incluyendo sitios remotos y servicios en la nube. ✓ Pruebas: Realizar pruebas periódicas de restauración para asegurar la integridad y disponibilidad de los datos.
	Recopilación de Datos	✓ Replicación Síncrona: Implementar replicación de datos en tiempo real a un sitio alterno para datos críticos. ✓ Replicación Asíncrona: Utilizar replicación asíncrona para datos menos críticos, con un retraso temporal aceptable.

Estrategia de Continuidad TIC	Sub estrategia de Continuidad TIC	Descripción
Redundancia de Sistemas y Redes	Sistemas Redundantes	✓ Hardware: Implementar servidores y almacenamiento redundante para eliminar puntos únicos de falla. ✓ Software: Utilizar sistemas operativos y aplicaciones redundantes configurados en alta disponibilidad.
	Redes Redundantes	✓ Conexiones de Red: Configurar múltiples conexiones a internet y redes redundantes para asegurar la conectividad continua. ✓ Dispositivos de Red: Implementar enrutadores, switches y firewalls redundantes.
Sitios de Recuperación	Sitios Alternativos	✓ Sitio Caliente: Un sitio completamente operativo y disponible de inmediato, con hardware y software duplicados. ✓ Sitio Templado: Un sitio equipado que puede estar operativo en cuestión de horas o días. ✓ Sitio Frío: Un sitio físico sin equipamiento preparado, que necesita ser configurado antes de su uso.
	Trabajo Remoto	✓ Acceso Remoto: Configurar VPNs seguras y acceso remoto para que los empleados puedan trabajar desde cualquier ubicación. ✓ Equipamiento: Proporcionar laptops y dispositivos móviles a los empleados clave.
Mantenimiento y Actualización de Sistemas	Mantenimientos programados	✓ Parcheo y Actualizaciones: Realizar actualizaciones regulares de sistemas operativos, aplicaciones y firmware. ✓ Inspección de Hardware: Programar inspecciones periódicas y mantenimiento de hardware crítico.
	Gestión de Cambios	✓ Procesos de Gestión de Cambios: Implementar procesos formales para gestionar cambios en la infraestructura de TI. ✓ Documentación: Mantener una documentación detallada de todos los cambios realizados en los sistemas.
Plan de Respuesta y Recuperación	Plan de Respuesta a Incidentes	✓ Procedimientos de Notificación: Establecer procedimientos claros para la notificación de incidentes. ✓ Equipos de Respuesta: Formar equipos de respuesta a incidentes con roles y responsabilidades definidos.
	Plan de Recuperación de TI	✓ Procedimientos de Recuperación: Documentar procedimientos específicos para la recuperación de sistemas y aplicaciones críticas. ✓ Prioridades de Recuperación: Establecer prioridades de recuperación basadas en el análisis de impacto en el negocio.
Monitoreo y Detección	Sistemas de Monitoreo	✓ Monitoreo Continuo: Implementar sistemas de monitoreo continuo para detectar anomalías y fallos en tiempo real. ✓ Alertas Automáticas: Configurar alertas automáticas para notificar al personal de TI sobre posibles incidentes.
	Análisis de Logs	✓ Recolección de Logs: Recopilar y analizar logs de sistemas y aplicaciones para identificar patrones de incidentes. ✓ SIEM (Security Information and Event Management): Implementar soluciones SIEM para una mejor correlación y análisis de eventos de seguridad.
Capacitación y Pruebas	Entrenamiento del Personal	✓ Capacitación Regular: Realizar capacitaciones periódicas para el personal de TI sobre procedimientos de contingencia y recuperación. ✓ Simulacros: Llevar a cabo simulacros de recuperación para evaluar la preparación del equipo y la efectividad de los planes.

Estrategia de Continuidad TIC	Sub estrategia de Continuidad TIC	Descripción
	Pruebas de Recuperación	✓ Pruebas Regulares: Realizar pruebas regulares de los planes de recuperación de TI para identificar y corregir posibles fallos. ✓ Revisión de Resultados: Analizar los resultados de las pruebas y actualizar los planes de recuperación según sea necesario.
Gestión de Proveedores y Contratos	Evaluación de Proveedores	✓ Selección de Proveedores: Evaluar proveedores de servicios críticos para asegurar que cumplan con los requisitos de continuidad. ✓ Acuerdos de Nivel de Servicio (SLA): Establecer SLA claros con proveedores para asegurar tiempos de respuesta y recuperación.
	Alternativas de Proveedores	✓ Procesos de Gestión de Cambios: Implementar procesos formales para gestionar cambios en la infraestructura de TI. ✓ Documentación: Mantener una documentación detallada de todos los cambios realizados en los sistemas.

Fuente: Elaboración propia.

ANEXO N° 9 CONSIDERACIONES PARA LAS PRUEBAS, CAPACITACIONES Y EJERCICIOS

1. Pruebas

Con la finalidad de validar la eficacia del PCTIC, asegurar que el personal esté adecuadamente preparado para responder a incidentes, y para identificar y corregir deficiencias en los procedimientos de recuperación y respuesta. Se deberá realizar pruebas regulares, según el siguiente cuadro:

N°	Tipo de prueba	Objetivo	Frecuencia	Método
1	Recuperación de Datos	Asegurar que las copias de seguridad se pueden restaurar correctamente	Trimestral	Seleccionar datos críticos y realizar una restauración completa en un entorno de prueba
2	Recuperación de Sistemas	Verificar la capacidad de restaurar sistemas y aplicaciones críticas	Semestral	Simular la pérdida de un servidor crítico y realizar una recuperación completa en un entorno de prueba
3	Redundancia de Redes	Validar la efectividad de las configuraciones de red redundantes	Anual	Simular la falla de una conexión de red primaria y verificar la conmutación por error a la conexión secundaria
4	Planes de Respuesta a Incidentes	Evaluar la capacidad del equipo de TI para responder a diferentes tipos de incidentes	Anual	Realizar simulaciones de incidentes (ciberataques, fallos de energía) y evaluar la respuesta del equipo

Fuente: Elaboración propia.

2. Capacitación

Asimismo, debe realizar capacitaciones y talleres constantes con la finalidad de asegurar que el personal pueda comunicar y/o reportar los incidentes que puedan ocurrir en los servicios tecnologías y/o sistemas de información del PNPAIS, con la finalidad que pueda detectarse a tiempo:

N°	Entrenamiento	Contenido	Frecuencia	Método
1	Capacitación del Personal de la UTI	Procedimientos de recuperación, Manejo de copias de seguridad, Gestión de incidentes.	Semestral	Talleres, Cursos en línea, y Seminarios
2	Concienciación de Seguridad para los colaboradores	Buenas prácticas de seguridad, Políticas de contraseñas, Reconocimiento de phishing	Anual	Seminarios, Campañas de concienciación, y Módulos de e-learning
3	Formación Cruzada	Capacitación cruzada en roles y responsabilidades clave para asegurar la redundancia del conocimiento	Anual	Talleres de intercambio de roles, Sesiones de capacitación en el puesto

Fuente: Elaboración propia.

3. Ejercicios

Para complementar las pruebas debe ejecutarse los siguientes ejercicios como talleres para el personal de la Unidad de Tecnologías de la Información:

N°	Entrenamiento	Objetivo	Frecuencia	Método
1	Simulación de Incidentes	Probar la capacidad de respuesta del equipo ante incidentes específicos.	Trimestral	Ejercicios de mesa (tabletop exercises) donde se simulan escenarios y se discuten las respuestas en tiempo real
2	Recuperación Completa	Validar la recuperación completa de todas las funciones críticas	Anual	Simular un desastre mayor y realizar una recuperación completa en un entorno de prueba, involucrando a todos los equipos pertinentes
3	Comunicación de Crisis	Probar los protocolos de comunicación interna y externa durante una crisis	Semestral	Simulaciones donde se prueba la comunicación entre equipos internos y con partes interesadas externas.

Fuente: Elaboración propia.

ANEXO N° 10 CONSIDERACIONES PARA EL MANTENIMIENTO DEL PCTIC

A continuación, se presenta la estructurada para el mantenimiento del PCTIC:

N°	Etapa	Actividad / Frecuencia		Método
1	Revisión y Actualización	Frecuencia	Revisión Trimestral	Revisión de componentes críticos del plan, como contactos de emergencia y procedimientos de recuperación
2			Revisión Anual	Revisión exhaustiva de todo el plan de continuidad del negocio
3		Proceso	Asignación de Responsabilidades	Asignar responsabilidades claras a un equipo de continuidad del negocio
4			Evaluación de Cambios	Identificar y evaluar cambios en la organización, tecnología, procesos y entorno que puedan afectar el PCTIC
5			Actualización de Documentación	Actualizar todos los documentos del PCTIC para reflejar los cambios identificados
6	Gestión de Cambios	Procedimientos de Cambio	Solicitud de Cambio	Establecer un procedimiento formal para la solicitud de cambios en el PCTIC
7			Aprobación de Cambios	Implementar un proceso de revisión y aprobación de cambios por parte del equipo de continuidad del negocio
8			Implementación y Documentación	Implementar los cambios aprobados y actualizar la documentación del BCP en consecuencia
9	Registro de Cambios	Registro de Cambios		Mantener un registro de todos los cambios realizados en el BCP, incluyendo detalles de la naturaleza del cambio, la razón del cambio, la fecha de implementación y las personas responsables

ANEXO N° 11 DIRECTORIO DE CONTACTOS

DIRECTORIO DE CONTACTOS DE UTI

N°	Contacto	Rol	Teléfono	Correo electrónico
1	Ejecutivo de Unidad de Tecnologías de la Información	Líder del equipo CSIRT	(01) 390 6630 Anexo 6686	jtavara@pais.gob.pe
2	Apoyo administrativo	Secretario Administrativo		ghuaman@pais.gob.pe
3	Analista de Soporte Operacional y Servicios Tecnológicos	Equipo CSIRT		mcruz@pais.gob.pe
4	Analista de Base de Datos	Equipo CSIRT		mpanduro@pais.gob.pe
5	Oficial de Confianza y Seguridad Digital	Equipo CSIRT		jmori@pais.gob.pe
6	Soporte Técnico Informático	Soporte Técnico Informático		oponte@pais.gob.pe

Fuente: Elaboración propia.

DIRECTORIO DE CONTACTOS DE ENTIDADES DE APOYO

N°	Entidad / Organización	Teléfono	Correo electrónico
1	**SEGDI – PCM** Secretaría de Gobierno y Transformación Digital	219-7000 Anexo 5120	
2	**SEGDI – PCM** Sub Secretaría de Tecnologías Digitales	219-7000 Anexo 5120	
3	**SEGDI – PCM** Sub Secretaría de Transformación Digital	219-7000 Anexo 5120	
4	**SEGDI – PCM** CSIRT – SEGDI Centro Nacional de Seguridad Digital (CNSD)	219-7000	cnsd@pcm.gob.pe pecert@pcm.gob.pe gobierno.digital@pcm.gob.pe
5	**OSDN - MIDIS** Oficina de Seguridad y Defensa Nacional	631-8000 Anexo 1586	
6	**OGTI – MIDIS** Oficina General de Tecnologías de Información	631-8000 Anexo 1652 y 1371	
7	**MININTER** Director General de la Oficina de Seguridad y Defensa Nacional	418-4030 475-6690	
8	**DIVINDAT – PNP** División de Alta Tecnología de la Policía Nacional	942440729	

Fuente: Elaboración propia.

DIRECTORIO DE CONTACTOS DE PROVEEDORES UTI

N°	Contacto	Servicio	Cargo	Empresa	Teléfono	Correo electrónico
1	Juan Atalaya Goicochea	Telecomunicaciones / servicios TI	Gerente de cuenta	Telefónica del Perú SAA	978 437 401	juan.atalayagoicochea@telefonica.com
2	Oscar Lindo Turin	Telecomunicaciones / servicios TI	Service manager	Telefónica del Perú SAA	975 455 481	oscar.lindo@telefonica.com
3	Fabiola Lugo Campos	Telecomunicaciones / servicios TI	Asesor comercial	Axess	945 426 985	fabiola.lugo@axessnet.com
4	Cesar Castro Juarez	Telecomunicaciones / servicios TI	Jefe servicio técnico	Axess	945 645 742	cesar.castro@axessnet.com
5	Alex Crucez	Correo electrónico	Soporte técnico	DailyTech	957 334 068	alex.cruces@dailytech.pe
6	Luis Sumarriva Rubio	Correo electrónico	Jefe soporte técnico	DailyTech	941 564 725	luis.sumarriva@dailytech.pe
7	Carlos Uriarte	Antivirus	Administrador de proyectos	JL Busines	961 780 122	curiarte@jlbusiness.com
8	Victor Gutierrez	Antivirus	Administrador de cuenta	ESET Perú	992 214 073	vgutierrez@eset.pe
9	Steven Calero	Impresoras	Jefe soporte tecnico	CODESA	988 567 385	scalero@codesaperu.com
10	Abdel Ramirez	Telecomunicaciones/servicios ti	Ventas	GTD	995 139 430	abdel.ramirez@grupogtd.com
11	Jeronimo Medina	Telecomunicaciones/servicios ti	Gestor de proyectos	GTD	921 885 675	jeronimo.medina@grupogtd.com
12	Richard Baldeon	Internet satelital	Ventas	Colinanet	963 616 761	rbaldeon@colinanet.com
13	Fiorela Benavides	Internet satelital	Gestor de proyectos	Colinanet	969 912 183	benavides@colinanet.com
14	Raul Donayre Tello	Telecomunicaciones / servicios TI	Ventas	Entel	990 352 790	raul.donayre@entel.pe

Fuente: Elaboración propia.

ANEXO N° 12 FORMATO-003-UTI-SEGDI – HISTORIAL DE ACCIONES DE ACCIONES DE RESPUESTA

<table>
<tr><th colspan="5">Parte 1 de 3 de la ficha</th></tr>
<tr><th>Valoración N°</th><th colspan="2">Parámetro</th><th>Res</th><th>Descripción del Incidente Reportado</th><th>Causa probable</th></tr>
<tr><td rowspan="6">I</td><td rowspan="5">NIVEL DE RIESGO (Probabilidad por Impacto)</td><td>(1) Riesgo Muy Alto (de 80 a 100 puntos)</td><td></td><td rowspan="5"></td><td rowspan="5"></td></tr>
<tr><td>(2) Riesgo Alto (de 48 a 64 puntos)</td><td></td></tr>
<tr><td>(3) Riesgo Moderado (4 puntos)</td><td></td></tr>
<tr><td>(4) Riesgo Medio (de 32 - 40 puntos)</td><td></td></tr>
<tr><td>(5) Riesgo Bajo (de 16 a 24 punto)</td><td></td></tr>
<tr><td colspan="2">Resultado de la valoración (nivel de riesgo:</td><td colspan="3">Emergencia o crisis confirmada:
SI ( ) NO ( ),
se activa el PCTIC:
SI ( ) NO( )</td></tr>
<tr><td rowspan="2">II</td><td colspan="5">DECISIONES ADOPTADAS</td></tr>
<tr><td colspan="4">(1) Evacuar a todo el personal
(2) Evacuar al personal de zonas contiguas
(3) Cortar el suministro de energía eléctrica
(4) Cortar el suministro de agua potable
(5) Cortar las líneas de comunicación (conectividad / telefonía)
(6) Ejecutar tareas básicas de control y mitigación
(7) Solicitar apoyo externo especializado
(8) No realizar acción alguna por alto riesgo para la vida
(9) No realizar acción alguna por la complejidad del incidente
(10) _____
(11) _____
(12) _____
(13) _____
(14) _____
(15) _____</td><td>( )
( )
( )
( )
( )
( )
( )
( )
( )
( )
( )
( )
( )
( )
( )</td></tr>
</table>

Parte 2 de 3 de la ficha

OBSERVACIONES, COMENTARIOS Y ANOTACIONES

1) .....
2) .....
3) .....
4) .....
5) .....
6) .....
7) .....
8) .....
9) .....
10) .....
11) .....
12) .....
13) .....
14) .....
15) .....
16) .....
17) .....
18) .....
19) .....
20) .....
21) .....
22) .....
23) .....
24) .....
25) .....
26) .....
27) .....
28) .....
29) .....
30) .....

Registrador / Operador

Líder del CSIRT

Lugar: _____
Fecha: _____
Hora: _____

PARTE 3 de 3 de la ficha

INSTRUCCIÓN DE USO DE LA FICHA

Para encontrar las respuestas (RES) a los parámetros y determinar el impacto que se indica en la parte primera de la ficha, se debe aplicar los parámetros que establecidos en la metodología de gestión de riesgos de la entidad.

ANEXO N° 13 FORMATO-005-UTI-SEGDI – FORMATO DE CONTROL DE PRUEBA Y ERROR

Acta de Pruebas ( ) y/o Conformidad ( ) **De: .....**	Hoja ( ) de ( )

En _____, a los ____ días del mes de _____ del año _____, las personas cuyos nombres se listan a continuación se reunieron para participar de las pruebas de control de la operatividad y funcionamiento de:

1) _____

2) _____

3) _____

N°	DNI N°	Apellido y nombres	Por parte de:
1			
2			
3			
4			

Las tareas y actividades que se ejecutaron, con los resultados alcanzados son:

N°	ACTIVIDAD REALIZADA	EJECUTADO POR	RESULTADO		
			Excelente	Bueno	Malo
1					
2					
3					
4					
5					

a) Excelente: Los resultados alcanzados son totalmente favorables y satisfacen las expectativas del usuario final

b) Bueno: Los resultados alcanzados son favorables y satisfacen moderadamente las expectativas del usuario final

c) Malo: Los resultados alcanzados no son favorables y no satisfacen las expectativas del usuario final

Acta de Pruebas ( ) y/o Conformidad ( ) **De: ……**	Hoja ( ) de ( )

Los participantes que participaron de la prueba, declaran su:

CONFORMIDAD ( ) NO CONFORMIDAD ( ) sobre la prueba realizada, en señal de lo cual firman:

---	---	---
---	---	---

……
V° B°
Líder del equipo CSIRT y/o
Ejecutivo de la Unidad de TI