ACUERDO MINISTERIAL NÚMERO 359-2026
GUATEMALA, 10 DE JULIO DE 2026
LA MINISTRA DE TRABAJO Y PREVISIÓN SOCIAL

CONSIDERANDO

Que de conformidad con lo que establece el artículo 194 literales a) y f) de la Constitución Política de la República de Guatemala, corresponde a los Ministros de Estado, ejercer jurisdicción sobre todas las dependencias de su ministerio y dirigir, tramitar, resolver e inspeccionar todos los negocios relacionados con su ministerio; y en virtud que la Ley del Organismo Ejecutivo, Decreto 114-97 del Congreso de la República de Guatemala establece que son atribuciones generales de los Ministros, entre otras, dictar los acuerdos, resoluciones, circulares y otras disposiciones relacionadas con el despacho de los asuntos de su ramo, conforme la ley; cumplir y hacer que se cumpla el ordenamiento jurídico en los diversos asuntos de su competencia y dirigir y coordinar la labor de las dependencias y entidades bajo su competencia, así como la administración de los recursos financieros, humanos y físicos bajo su responsabilidad, velando por la eficiencia y la eficacia en el empleo de los mismos.

CONSIDERANDO

Que por medio de oficio -DISI-OF-653-2026-EOCG/fa de fecha seis de julio de dos mil veintiséis, el Director de Sistemas de Información del Ministerio de Trabajo y Previsión Social trasladó para su aprobación el **"Plan de Contingencia y Recuperación Ante Desastres", Versión 1-2026** a la Unidad de Planificación y Cooperación del Ministerio de Trabajo y Previsión Social.

CONSIDERANDO

Que por medio de Oficio No. 492-2026 de fecha nueve de julio de dos mil veintiséis, el Viceministerio Administrativo Financiero del Ministerio de Trabajo y Previsión Social solicita las gestiones de emisión de Acuerdo Ministerial para aprobar el proyecto denominado **"Plan de Contingencia y Recuperación Ante Desastres", Versión 1-2026**, de la Dirección de Sistemas de Información del Ministerio de Trabajo y Previsión Social.

CONSIDERANDO

Que para el efecto, el **"Plan de Contingencia y Recuperación Ante Desastres", Versión 1-2026**, de la Dirección de Sistemas de Información del Ministerio de Trabajo y Previsión Social, es un instrumento técnico en el cual se establece el conjunto de estrategias, tareas, recursos, roles y responsabilidades orientados a mitigar el impacto de incidentes mayores, asegurando la recuperación ordenada y eficiente de los sistemas y servicios críticos de Tecnologías de Información y Comunicación (TIC) en el menor tiempo posible, garantizando la continuidad operativa del del Ministerio de Trabajo y Previsión Social.

POR TANTO

Con base en lo considerando, leyes citadas y lo que para el efecto preceptúan los artículos 194, literales a) y f) de la Constitución Política de la Republica de Guatemala; 27 literales f) y m) de la Ley del Organismo Ejecutivo, Decreto Número 114-97 del Congreso de la República de Guatemala.

ACUERDA

Artículo 1. APROBACIÓN. Aprobar en todo su contenido el **"Plan de Contingencia y Recuperación Ante Desastres", Versión 1-2026**, de la Dirección de Sistemas de Información del Ministerio de Trabajo y Previsión Social en su versión 01, el cual consta de cincuenta y cinco (55) hojas, impresas únicamente en su lado anverso, y que forman parte del presente acuerdo.

Artículo 2. RESPONSABILIDAD. La Dirección de Sistemas de Información del Ministerio de Trabajo y Previsión Social, será responsable de revisar periódicamente el **"Plan de Contingencia y Recuperación Ante Desastres", Versión 1-2026**, de la Dirección de Sistemas de Información del Ministerio de Trabajo y Previsión Social, conforme a las necesidades en el servicio o cambios que surjan en las normas legales o aspectos administrativos, que mejoren la eficiencia de los procesos; así como realizar las modificaciones y actualizaciones correspondientes.

Artículo 3. DEROGATORIA. Se deroga cualquier otra disposición legal previa que se refiera a lo dispuesto en el **"Plan de Contingencia y Recuperación Ante Desastres", Versión 1-2026**, de la Dirección de Sistemas de Información del Ministerio de Trabajo y Previsión Social.

Artículo 4. VIGENCIA. El presente Acuerdo Ministerial surte sus efectos de manera inmediata.

Artículo 5. Notifíquese a la Dirección de Sistemas de Información y a la Unidad de Planificación y Cooperación del Ministerio de Trabajo y Previsión Social, para lo que corresponda.

Miriam Catarina Roquel
Ministra de Trabajo y Previsión Social
Ministerio de Trabajo y Previsión Social

MINISTERIO DE TRABAJO Y PREVISION SOCIAL
REPUBLICA DE GUATEMALA, C.A.

MINISTERIO DE TRABAJO Y PREVISION SOCIAL
SECRETARIA GENERAL
GUATEMALA, C.A.

Lic. Erwin Eduardo Velásquez Herrera
Secretario General
Ministerio de Trabajo y Previsión Social

VERSIÓN-01-2026
PLAN DE CONTINGENCIA Y RECUPERACIÓN ANTE DESASTRES
DIRECCIÓN DE SISTEMAS DE INFORMACIÓN

Ministerio de Trabajo y Previsión Social

UTZ SAMAJ

Aprobación del Plan de Contingencia y Recuperación Ante Desastres "Dirección de Sistemas de Información"

Nombre del Documento:	Plan de Contingencia y Recuperación Ante Desastres de la Dirección de Sistemas de Información del Ministerio de Trabajo y Previsión Social			
Identificación:	**Versión:**		01	**Fecha de aprobación:** Julio 2026
	Nombre Completo	Puesto que Ocupa	Firma	
VALIDADO POR:	Ing. Edwin Omar de la Cruz García	Director de Sistemas de Información -DISI-	Ing. Edwin Omar de la Cruz García Director de Sistemas de Información Ministerio de Trabajo y Previsión Social	
Vo. Bo.:	Lcda. Karen Elizabeth Reyes Crúz	Viceministra Administrativa Financiera	Vo.Bo. Lcda. Karen Elizabeth Reyes Crúz Viceministra Administrativa Financiera Ministerio de Trabajo y Previsión Social	

ÍNDICE GENERAL

1 INTRODUCCIÓN 7
2 JUSTIFICACIÓN Y CONTEXTO 7
3 MARCO NORMATIVO Y ALCANCE SINTÉTICO 9
4 OBJETIVOS 11
4.1 Objetivo general 11
4.2 Objetivos específicos 11
5 PREMISAS PARA LA IMPLEMENTACIÓN 12
5.1 Premisas para la ejecución 14
5.2 Condicionamiento de ejecución 15
6 ALCANCE 15
7 SERVICIOS Y SISTEMAS CUBIERTOS 16
7.1 Sistemas de Cumplimiento Legal y Registro: 16
7.2 Servicios de Intermediación y Empleo: 16
7.3 Sistemas de Gestión de Conflictos Laborales: 16
7.4 Sistemas de Seguridad y Administración: 16
7.5 Infraestructura de Soporte Crítico: 17
8 TIPO DE DESASTRE CUBIERTO 17
9 ROLES, RESPONSABILIDADES Y EQUIPO 17
9.1 Despacho Ministerial 17
9.2 Comité de Dirección 18
9.2.1 Tareas Específicas del Comité de Dirección 20
9.3 Liderazgo operativo 23
9.4 Responsabilidades del Coordinador Operativo 23
9.5 Equipos de respuesta 25
9.5.1 Objetivo y composición 26
9.5.2 Equipo de Recuperación Tecnológica (ERT) 26

9.5.3 Equipo de Enlace de Procesos y Validación Funcional 26
9.5.4 Movilización 26
9.6 Tareas del ERT 26
9.7 Tareas de los enlaces de procesos y validación funcional 28
10 ANÁLISIS DE IMPACTO AL NEGOCIO 29
10.1 Criterios de medición de impacto 30
10.2 Clasificación de criticidad, RTO Y RPO 31
11 MATRIZ DE SISTEMAS CRÍTICOS DEL MINTRAB 32
12 CLÁUSULA DE RESPONSABILIDAD Y ÉTICA 34
13 ESTRATEGIA DE RECUPERACIÓN TECNOLÓGICA 35
13.1 Estrategia general 35
13.2 Componentes clave de la estrategia 36
13.2.1 Infraestructura del sitio alterno 36
13.2.2 Mecanismos de replicación y backup 36
13.2.3 Estrategia de recuperación de datos 37
14 INFRAESTRUCTURA TECNOLÓGICA 38
14.1 Arquitectura del sitio primario 38
14.2 Arquitectura del sitio de contingencia 38
14.3 Esquema de replicación de datos 39
15 PROCESO DE DECLARACIÓN DE DESASTRE 40
15.1 Fases del proceso de activación 40
15.1.1 Fase 1: Detección e inicialización 41
15.1.2 Fase 2: Evaluación y notificación (coordinación táctica) 42
15.1.3 Fase 3: Declaración formal y activación operativa 43
15.1.4 Criterios de declaración formal 44
15.2 Proceso de cierre de desastre 44
16 PLAN DE COMUNICACIÓN Y COORDINACIÓN 44

16.1 CANALES DE COMUNICACIÓN OFICIAL 45
16.2 Comunicación externa (ciudadanía y sector laboral) 45
16.3 Coordinación con proveedores críticos 46
16.4 Matriz de notificación (escalamiento) 47
16.5 Protocolo de control de información 47
17 PROCEDIMIENTOS DE RECUPERACIÓN 47
17.1 Secuencia general de recuperación 47
17.1.1 Procedimiento de recuperación de infraestructura core (P1) 48
17.1.1.1 Servicios de identidad y acceso 48
17.1.1.2 Procedimiento de recuperación de sistemas misionales (p1) 48
17.1.1.3 Procedimiento de recuperación de sistemas de apoyo (p2/p3) 48
17.1.1.4 Tabla de verificación de salida 48
18 PROCEDIMIENTOS DE RETORNO 49
18.1 Criterios de retorno a la normalidad 49
18.2 Pasos operativos para el failback 49
18.3 Validación post-retorno 51
19 MANTENIMIENTO Y PRUEBAS DEL PLAN 51
19.1 Programa de pruebas anuales 52
19.2 Actualización del plan 52
19.2.1 Disparadores de actualización obligatoria: 52
19.2.2 Cláusula de inmutabilidad: 53
19.3 Requisito de certificación de premisas 53
Glosario 54

ÌNDICE DE TABLAS

1. Marco normativo y alcance sintético 10
2. Premisas para la implementación 12
3. Comité de Dirección 18
4. Tareas Específicas del Comité de Dirección 21
5. Responsabilidades del Coordinador Operativo 24
6. Tareas del ERT 27
7. Tareas de los enlaces de procesos y validación funcional 28
8. Criterios de medición de impacto 30
9. Clasificación de criticidad, RTO Y RPO 31
10. Matriz de sistemas críticos del MINTRAB 32
11. Mecanismos de replicación y backup 36
12. Arquitectura del sitio de contingencia 38
13. Detección e inicialización 41
14. Evaluación y notificación 42
15. Declaración formal y activación operativa 43
16. Comunicación externa 45
17. Coordinación con proveedores críticos 46
18. Tabla de verificación de salida 49
19. Criterios de retorno a la normalidad 49

1 INTRODUCCIÓN

El Ministerio de Trabajo y Previsión Social (MINTRAB), en su calidad de entidad rectora en la promoción del empleo digno, la supervisión del cumplimiento de la legislación laboral y el desarrollo de la previsión social en Guatemala depende de manera crítica de la operatividad continua de sus Sistemas de Tecnologías de Información y Comunicación (TIC). Estos sistemas constituyen un componente esencial para garantizar la prestación eficaz y oportuna de los servicios públicos bajo su competencia.

La ocurrencia de eventos disruptivos, tales como fallas graves de infraestructura tecnológica, desastres naturales o ciberataques, representa una amenaza significativa para la confidencialidad, integridad y disponibilidad de la información institucional, así como para la continuidad de los servicios brindados a la ciudadanía. Ante estos riesgos, resulta imprescindible contar con mecanismos estructurados que permitan responder de manera oportuna y efectiva.

En este contexto, el presente Plan Contingencia y Recuperación Ante Desastres (PCRAD) establece el conjunto de estrategias, tareas, recursos, roles y responsabilidades orientados a mitigar el impacto de incidentes mayores. Su propósito es asegurar la recuperación ordenada y eficiente de los sistemas y servicios críticos de Tecnologías de Información y Comunicación (TIC) en el menor tiempo posible, garantizando así la continuidad operativa del Ministerio y el cumplimiento de su mandato legal y constitucional.

2 JUSTIFICACIÓN Y CONTEXTO

El Ministerio de Trabajo y Previsión Social (MINTRAB), en su calidad de institución rectora encargada de la promoción del empleo digno, la vigilancia estricta del cumplimiento de la legislación laboral y el desarrollo integral de la previsión social en la República de Guatemala sustenta la eficacia de su gestión en la disponibilidad, robustez y continuidad de sus Sistemas de Tecnologías de Información y Comunicación (TIC).

En la era de la transformación digital de la administración pública, estos activos tecnológicos han dejado de ser herramientas de soporte secundario para convertirse en el núcleo operativo y estratégico indispensable que permite garantizar el ejercicio de los derechos fundamentales de la población trabajadora y empleadora, viabilizando la prestación de servicios públicos esenciales de forma ágil, transparente y con estricto apego al mandato constitucional y legal de la institución.

Consiguientemente, la materialización de amenazas catastróficas o incidentes mayores —clasificados de origen natural (como sismos de gran magnitud, inundaciones o tormentas), fallas críticas de infraestructura (como interrupciones prolongadas del suministro eléctrico o incendios en el Data Center) o eventos de seguridad digital provocados por la delincuencia cibernética (tales como ataques de denegación de servicio distribuido [DDoS], inyecciones de código o incidentes de ransomware de última generación)— posee el potencial latente de quebrantar los pilares fundamentales de la seguridad de la información: Confidencialidad, Integridad y Disponibilidad.

Un escenario de esta naturaleza no solo interrumpiría los flujos de trabajo internos, sino que expondría al Ministerio a la alteración o pérdida irrecuperable de registros transaccionales críticos, provocando la paralización inmediata de la atención ciudadana y vulnerando gravemente la resiliencia operativa e institucional ante la opinión pública y los entes de fiscalización del Estado.

Vinculación Normativa con el Reglamento Orgánico Interno (ROI)

El Plan se fundamenta en el Acuerdo Gubernativo 215-2012 (Reglamento Orgánico Interno del MINTRAB). El presente PCRAD es la herramienta técnica para dar cumplimiento a las atribuciones de la Dirección de Sistemas de Información (DISI), específicamente lo establecido en el Artículo 14, numerales 53 y 56, que obligan a esta dirección a proponer y aplicar políticas de seguridad informática, así como administrar y mantener actualizados los sistemas de información institucionales para garantizar su disponibilidad.

Análisis de Viabilidad y Continuidad Institucional

La implementación de este plan representa una inversión estratégica cuya viabilidad se justifica por la protección de programas de alto impacto social, como por ejemplo el Programa de Aporte Económico del Adulto Mayor (PAM) y el sistema RECIT. La continuidad de estos servicios evita perjuicios económicos al Estado derivados de la suspensión de plazos legales y garantiza que los beneficios lleguen a la población vulnerable sin interrupciones, cumpliendo con los principios de eficiencia y eficacia que rigen la administración pública.

3 MARCO NORMATIVO Y ALCANCE SINTÉTICO

El presente plan se ha estructurado de manera ejecutiva para facilitar su consulta durante una crisis, alineándose a los siguientes marcos regulatorios y técnicos:

- Cumple con las Normas de Control Interno de la Contraloría General de Cuentas (CGC) y el Acuerdo Gubernativo 215-2012 (ROI).

1. Marco normativo y alcance sintético

Norma de Control Interno (CGC)	Aplicación en el Plan de Contingencia	Objetivo de Cumplimiento
Norma 5.4: Planes de Contingencia	Definición de la metodología de respuesta ante desastres.	Garantizar la continuidad de los servicios institucionales ante eventos disruptivos.
Norma 5.5: Seguridad de Aplicaciones y Datos	Implementación de mecanismos de replicación síncrona y asíncrona para sistemas P1 y P2.	Asegurar la integridad y disponibilidad de la información procesada en la DISI.
Norma 5.6: Respaldo y Recuperación de Datos	Establecimiento de métricas RTO (Tiempo) y RPO (Punto de recuperación) en el numeral 9.2.	Limitar la pérdida de datos a los niveles máximos aceptables para el Ministerio.
Norma 5.2: Continuidad de la Operación de TI	Configuración de un Sitio Alterno (Hot Site) con arquitectura espejo.	Mantener la operatividad de los sistemas misionales fuera del centro de datos primario.
Norma 1.3: Segregación de Tareas	Matriz de roles donde la declaración de desastre es administrativa y la ejecución es técnica.	Evitar que una sola persona controle todas las etapas de una emergencia institucional.

4 OBJETIVOS

4.1 Objetivo general

Establecer la metodología, las tareas, los roles y los recursos técnicos y humanos requeridos para responder de manera efectiva a un desastre tecnológico mayor, con el fin de restaurar la infraestructura, las plataformas y los servicios de Tecnologías de Información y Comunicación (TIC) críticos del Ministerio de Trabajo y Previsión Social (MINTRAB).

Todo esto debe realizarse dentro de los tiempos máximos predefinidos (RTO y RPO), garantizando la continuidad operacional de las funciones misionales del MINTRAB en beneficio de los trabajadores, empleadores y la ciudadanía de Guatemala.

4.2 Objetivos específicos

- **Minimizar el Impacto:** Reducir al máximo el tiempo de inactividad de los sistemas críticos y la potencial pérdida de datos resultante de un evento disruptivo.
- **Definir la Gobernanza:** Asignar y documentar las responsabilidades, la autoridad y el flujo de comunicación de los equipos de respuesta y las autoridades Ministeriales antes, durante y después de un desastre.
- **Priorizar la Recuperación:** Utilizar el Análisis de Impacto al Negocio (BIA) para determinar la secuencia de recuperación de los sistemas, asegurando que los servicios más críticos (Ej.: RECIT, Portal Tu Empleo, Sistemas de Denuncias) se restablezcan primero.
- **Asegurar la Confiabilidad:** Implementar tareas técnicas (Sección 10) que permitan el retorno seguro a la operación normal en el sitio de contingencia y la posterior vuelta a la normalidad (Failback) al sitio principal.
- **Validar la Respuesta:** Establecer una estrategia formal de pruebas y mantenimiento para asegurar que el PCRAD se mantenga vigente y que el personal esté preparado para ejecutar los procedimientos.

5 PREMISAS PARA LA IMPLEMENTACIÓN

Este PCRAD se centra exclusivamente en la recuperación de la infraestructura y servicios de TIC. Por lo tanto, no cubre los siguientes escenarios o áreas, las cuales no son responsabilidad del presente PCRAD, el Plan de Seguridad Institucional o los procedimientos operativos estándar del MINTRAB:

2. Premisas para la implementación		
Categoría	**Exclusión Específica**	**Justificación**
Respuesta No Tecnológica	Seguridad Física y Evacuación: La respuesta a amenazas que ponen en riesgo la vida humana (incendios, sismos, emergencias médicas) y la gestión de la evacuación de las instalaciones.	Esta es responsabilidad del Plan de Emergencia y Seguridad Institucional del MINTRAB.
	Procedimientos Manuales de Continuidad (Workarounds): El plan no detalla las operaciones temporales manuales que las áreas usuarias deben ejecutar para suplir la falta del sistema.	La definición de estos procesos y formularios de emergencia son parte del Plan de Continuidad del Negocio (BCP) de cada unidad administrativa.
	Recuperación de Archivos Físicos: La restauración y reorganización de archivos físicos o documentos que no hayan sido digitalizados o no	Esto corresponde a la gestión documental y operativa de cada Dirección.

2. Premisas para la implementación		
Categoría	**Exclusión Específica**	**Justificación**
	residan en los sistemas de almacenamiento crítico.	
Infraestructura No Crítica	Sistemas No Críticos: La recuperación de sistemas clasificados como P3 (Soporte) o P4 (Administrativos/No Críticos) en el BIA.	Estos sistemas serán restaurados después de la recuperación de los sistemas P1 y P2, utilizando los procedimientos operativos estándar y no la activación del PCRAD.
	Infraestructura de Usuarios Finales (End-Points): La recuperación, reemplazo o configuración de equipos de escritorio, laptops, impresoras y teléfonos fijos individuales.	Esta es una función de soporte técnico rutinario y no requiere la activación de un PCRAD.
Dependencias Externas	Fallas de Servicios Públicos: Fallas prolongadas en servicios públicos fuera de las instalaciones del MINTRAB (redes públicas de agua, gas, fallas regionales de telecomunicaciones).	El plan cubre la respuesta dentro de la esfera de control del Ministerio, asumiendo que el sitio de contingencia es accesible y funcional.

2. Premisas para la implementación		
Categoría	**Exclusión Específica**	**Justificación**
	Sistemas Gubernamentales Externos: La indisponibilidad de sistemas de otras entidades de gobierno (Ej: RENAP, Ministerio de Finanzas, Bancos Centrales, IGSS y SAT) de las que el MINTRAB dependa para sus operaciones.	El MINTRAB solo puede mitigar el impacto, no puede ejecutar la recuperación de sistemas externos.

5.1 Premisas para la ejecución

- **Estrategia de Recuperación (Sitio Alterno y Réplica):** Se asume la existencia y operatividad de un Sitio Alterno/de Contingencia (DR Site), el cual ha sido diseñado para albergar la infraestructura necesaria para la recuperación. Además, se asume que existe un mecanismo de replicación de datos activo y funcional, lo que garantiza la disponibilidad de los datos dentro del RPO establecido.
- **Personal Clave:** Se asume que el personal crítico de TI y los líderes de los procesos de negocio están disponibles y pueden ser contactados y movilizados al sitio de contingencia o al punto de encuentro alterno dentro del tiempo requerido.
- **Energía y Conectividad (DR Site):** Se asume que el sitio de contingencia cuenta con el suministro de energía eléctrica y la conectividad a Internet/WAN necesarios para operar las funciones críticas durante el tiempo que dure la contingencia.
- **Recursos Financieros y Legales:** Se asume que la activación del PCRAD cuenta con el respaldo y la aprobación del Despacho Ministerial para incurrir en los gastos y tomar las decisiones operativas extraordinarias necesarias para la recuperación.

- **Comunicación Operacional:** Se asume la existencia de canales de comunicación fuera de la infraestructura del MINTRAB (teléfonos celulares, redes sociales, correo electrónico externo) para la notificación inicial del desastre.

5.2 Condicionamiento de ejecución

La operatividad y el éxito del presente PCRAD están sujetos estrictamente al cumplimiento de las premisas anteriormente descritas. El PCRAD se podrá ejecutar y probar SI Y SOLO SI las premisas técnicas, logísticas y financieras han sido cumplidas y garantizadas por el Ministerio.

Cualquier degradación en los servicios de soporte (como fallas en el sitio alterno, falta de enlaces de replicación o ausencia de copias de seguridad) invalida las garantías de tiempo de recuperación (RTO) y punto de recuperación (RPO) establecidas en este documento.

6 ALCANCE

El Plan de Contingencia y Recuperación Ante Desastres (PCRAD) del Ministerio de Trabajo y Previsión Social (MINTRAB) tiene por objeto la recuperación de los siguientes activos y servicios, clasificados como Críticos (P1) o Esenciales (P2), y se delimita de la siguiente manera:

- El Plan se limita estrictamente a la recuperación de los servicios de TIC del MINTRAB. No sustituye los protocolos de salud, seguridad ocupacional o evacuación física de las instalaciones, los cuales se rigen por sus propios manuales.
- La estructura del plan permite una respuesta modular; cada equipo (Táctico, Estratégico y de Recuperación) posee guías de acción rápidas que evitan la ambigüedad en la toma de decisiones bajo presión.

7 SERVICIOS Y SISTEMAS CUBIERTOS

El alcance se centra en la continuidad de las funciones misionales con mayor impacto legal, social y económico, incluyendo, pero no limitándose a:

7.1 Sistemas de Cumplimiento Legal y Registro:

- Registro Electrónico de Contratos Individuales de Trabajo (RECIT): Base de datos y plataforma de la aplicación.
- Libro Electrónico de Salarios: Incluyendo la base de datos de nóminas e informes.
- Registro de Organizaciones Sindicales y Asociaciones Solidarias.
- Sistema de Permisos a Extranjeros (PEX): Gestión de la legalidad laboral y la migración controlada.
- Legalidad Laboral: Sistemas y bases de datos que soportan la verificación del cumplimiento normativo.

7.2 Servicios de Intermediación y Empleo:

- Portal Electrónico "Tu Empleo": Incluyendo la base de datos de oferentes y demandantes de empleo.
- Programas de Movilidad Laboral (Oportuguate): Plataformas de gestión y seguimiento de los programas de trabajo temporal en el extranjero.

7.3 Sistemas de Gestión de Conflictos Laborales:

Sistemas de soporte a la Inspección General de Trabajo (IGT) y plataformas de recepción de denuncias en línea.

7.4 Sistemas de Seguridad y Administración:

- Sistema de Gestión de PAM (Programa de Aporte al Adulto Mayor): Sistema encargado de gestionar los aportes a Adulto Mayor.
- Sistema de Gestión de Reservas para los Centros Recreativos y Vacacionales: Soporte a la función de previsión social.

7.5 Infraestructura de Soporte Crítico:

- Servicios de Directorio Activo (Active Directory) y Servidores DNS.
- Sistemas de correo electrónico institucional (Excluyendo la recuperación individualizada de buzones de usuario).
- Sistemas de almacenamiento de datos críticos (SAN/NAS).

8 TIPO DE DESASTRE CUBIERTO

El plan está diseñado para la respuesta, contención y recuperación de desastres que causen la indisponibilidad total o parcial del Data Center Primario por un período que exceda el RTO de los sistemas P1, incluyendo:

- Desastres naturales (sismos, inundaciones, tormentas mayores).
- Fallas graves de infraestructura (incendio, fallo eléctrico prolongado no mitigable con UPS/Generadores).
- Eventos de seguridad (ciberataques, ransomware o destrucción lógica de datos)

9 ROLES, RESPONSABILIDADES Y EQUIPO

La estructura de respuesta aquí definida se fundamenta en las competencias establecidas en el Acuerdo Gubernativo 215-2012 (Reglamento Orgánico Interno del MINTRAB). La ejecución de estas responsabilidades garantiza que el Ministerio cumpla con su función de administrar sistemas de información actualizados y velar por la seguridad informática institucional (Art. 14, numerales 5, 52 y 56 del ROI).

9.1 Despacho Ministerial

El Despacho Ministerial es la Máxima Autoridad para la toma de decisiones durante un evento disruptivo. Su función no es técnica, sino de gobernanza, comunicación estratégica y gestión de impacto institucional.

9.2 Comité de Dirección

El Comité de Dirección estará integrado, y será de carácter temporal, por los Directores que considere el Despacho Ministerial, quienes deben mantener un contacto y disponibilidad constante durante el incidente:

3. Comité de Dirección			
Rol en el Comité de Dirección	**Designación Típica en MINTRAB**	**Rol en el PCRAD**	**Suplente Recomendado**
Presidente del Comité	Ministro(a) o Viceministro(a) Delegado	Máxima autoridad. Único facultado para la Declaración Formal de Desastre y la aprobación de gastos extraordinarios.	Viceministro de Administración Financiera
Coordinador General del PCRAD	Director(a) de Sistemas de Información	Líder estratégico de la respuesta. Sirve de enlace entre el Comité y el Equipo de Recuperación Tecnológica (ERT).	Subdirector de Sistemas de Información
Coordinador de Comunicaciones	Director(a) de Comunicación Social	Administra la información que se divulga a la prensa, la ciudadanía y las	Subdirector(a) de Comunicación Social

3. Comité de Dirección			
Rol en el Comité de Dirección	**Designación Típica en MINTRAB**	**Rol en el PCRAD**	**Suplente Recomendado**
		dependencias gubernamentales.	
Coordinador de Procesos Críticos	Directores(as) de las unidades priorizadas	Valida el impacto en la operación del negocio, confirma el cumplimiento de los RTO y aprueba la reanudación del servicio al público.	Subdirector(a) de la Unidad
Coordinador Legal	Jefe de Consejo Técnico y Asesoría Legal	Revisa las implicaciones legales, contractuales y de cumplimiento normativo derivadas del desastre y también Emitir dictámenes jurídicos sobre la suspensión de plazos legales en procesos administrativos y de inspección mientras	Subjefe de Consejo Técnico y Asesoría Legal

3. Comité de Dirección			
Rol en el Comité de Dirección	**Designación Típica en MINTRAB**	**Rol en el PCRAD**	**Suplente Recomendado**
		dure la contingencia tecnológica, según el Art. 18 del ROI	
Coordinador Financiero	Director(a) Financiero(a)	Gestionar los recursos extraordinarios bajo los principios de transparencia y rendición de cuentas que supervisa la Unidad de Auditoría Interna (UDAI)	Subdirector Financiero

9.2.1 Tareas Específicas del Comité de Dirección

Las tareas específicas del Comité se dividen en tres fases:

4. Tareas Específicas del Comité de Dirección		
Fase	**Tarea Específica**	**Impacto Estratégico**
1. Declaración y Activación	Evaluación de la Escala: Analiza la situación y el impacto real en los servicios P1 y P2.	Decide si el evento justifica la activación del PCRAD o si puede manejarse con procedimientos de soporte estándar.
	Declaración Formal: El Presidente del Comité emite la orden formal de activación del PCRAD , notificando a todas las partes interesadas internas y externas.	Pone en marcha la movilización del ERT al Sitio de Contingencia.
2. Seguimiento y Gestión (Durante la Crisis)	Gestión de Prioridades: Reconfirma que el ERT está enfocando sus esfuerzos en los sistemas con el RTO más estricto.	Asegura que los esfuerzos de recuperación cumplan con las necesidades del negocio.
	Gestión de la Comunicación: Aprueba los	Protege la reputación y mantiene la confianza ciudadana y empresarial.

4. Tareas Específicas del Comité de Dirección		
Fase	**Tarea Específica**	**Impacto Estratégico**
	comunicados oficiales sobre el estado de los servicios (Ej.: Notificación de la indisponibilidad de Portal Tu Empleo).	
	Gestión de Recursos: Resuelve los escalamientos técnicos, logísticos o de recursos que el Coordinador PCRAD no pueda resolver (Ej.: Contratación urgente de servicios o compra de equipo).	Elimina obstáculos para la recuperación técnica.
3. Cierre y Post-Desastre	Declaración de Cierre: Aprueba el inicio de la Vuelta a la Normalidad (Failback) al sitio primario y declara el fin de la emergencia.	Finaliza el PCRAD y devuelve la operación al estado pre-desastre.

4. Tareas Específicas del Comité de Dirección		
Fase	**Tarea Específica**	**Impacto Estratégico**
	Revisión Post-Incidente: lidera la reunión de lecciones aprendidas, revisando la ejecución del PCRAD para identificar mejoras en el plan.	Mejora la resiliencia institucional futura.

9.3 Liderazgo operativo

El Director(a) de Sistemas de Información (DISI) asume el rol de Coordinador General Operativo del PCRAD. Este rol es fundamentalmente técnico y táctico. El Director de DISI lidera la ejecución de la respuesta tecnológica una vez que el desastre ha sido detectado por el personal de monitoreo y la situación ha sido escalada para la evaluación del Comité de Dirección.

9.4 Responsabilidades del Coordinador Operativo

El Director(a) de la DISI es el líder de la respuesta técnica y el principal punto de contacto con el Comité de Dirección. Sus responsabilidades se centran en la gestión, dirección y aseguramiento de los procedimientos:

5. Responsabilidades del Coordinador Operativo

Fase del PCRAD	Responsabilidad Específica	Impacto Operativo
I. Preparación (Pre-Desastre)	Mantenimiento del PCRAD : Gestiona la actualización del presente plan y que los miembros del ERT conozcan sus roles.	Gestiona la vigencia y ejecución del PCRAD .
II. Activación (Durante el Evento)	Evaluación y Reporte: Recibir el informe técnico inicial del incidente del personal de infraestructura, evaluar la afectación a los sistemas P1/P2 e informa la situación al Comité de Dirección.	Permite al Comité de Dirección tomar la decisión de Declarar el Desastre.
	Movilización y Dirección: Una vez activado el PCRAD, ordenar la movilización inmediata del Equipo de Recuperación Tecnológica (ERT) al sitio de contingencia.	Inicia la fase de ejecución técnica (Recuperación).
III. Recuperación y Ejecución	Dirección del ERT: Liderar, dirigir y supervisar directamente al ERT en el sitio de contingencia para ejecutar los procedimientos técnicos dentro de los tiempos RTO definidos.	Asegura la adhesión a los procedimientos para una restauración ordenada.

5. Responsabilidades del Coordinador Operativo		
Fase del PCRAD	**Responsabilidad Específica**	**Impacto Operativo**
	Dirección del ERT: Liderar, dirigir y supervisar directamente al ERT en el sitio de contingencia para ejecutar los procedimientos técnicos (Capítulo 10) dentro de los tiempos RTO definidos.	Desbloquea la operación del ERT.
IV. Cierre y Failback	Validación Técnica: Revisa informe técnico donde indica que los sistemas han sido restaurados y cumplen con los requisitos funcionales mínimos para la operación continua.	Proporciona la luz verde técnica al Comité para la reanudación del servicio.
	Coordinación de Failback: Declarar el fin de la fase de recuperación y coordinar el procedimiento de Vuelta a la Normalidad al sitio principal (Capítulo 11).	Proporciona la luz verde técnica al Comité para la reanudación del servicio.

9.5 Equipos de respuesta

El Nivel Táctico representa el brazo ejecutor del Plan de Contingencia y Recuperación Ante Desastres (PCRAD). Su activación se realiza únicamente por orden del Coordinador Operativo del PCRAD (Director/a de DISI), una vez que el Comité de Dirección ha declarado formalmente el estado de desastre.

9.5.1 Objetivo y composición

El objetivo primordial del Nivel Táctico es restaurar la operación de los sistemas críticos (P1/P2) dentro de los tiempos RTO predefinidos. La composición del Nivel Táctico se basa en la especialización de funciones:

9.5.2 Equipo de Recuperación Tecnológica (ERT)

Enfocado en la infraestructura (hardware, redes, sistemas operativos, bases de datos).

9.5.3 Equipo de Enlace de Procesos y Validación Funcional

Enfocado en el negocio (verificación de datos, pruebas de usuario y aprobación funcional).

9.5.4 Movilización

Todos los miembros de los equipos tácticos deben reportarse al Punto de Encuentro Alterno predefinido o trasladarse directamente al Sitio de Contingencia (DR Site), según la instrucción específica de la DISI.

9.6 Tareas del Equipo de Recuperación Tecnológica

El ERT es responsable directo de la ejecución de los Procedimientos Técnicos de Recuperación.

6. Tareas del ERT		
Rol en el ERT	**Tareas Clave**	**Sistemas de Enfoque (Ejemplos)**
Líder Técnico del ERT	Reporta al Coordinador PCRAD (DISI). Supervisa y distribuye las tareas de recuperación, asegurando el cumplimiento de la secuencia de pasos y los tiempos de recuperación.	Coordinación, Infraestructura General
Coordinación, Infraestructura General	Restablece la conectividad física y lógica en el DR Site. Configura servicios de red (VPN, DNS, Firewall) y la conexión al sitio principal.	Redes y Comunicaciones WAN/LAN
Especialista de Servidores y Sistemas Operativos	Configura y activa las máquinas virtuales, servidores y sistemas operativos replicados. Garantiza la funcionalidad del Directorio Activo (AD) y el Sistema de Gestión de PAM.	Infraestructura y sistemas operativos y software P1 y P2
Especialista de Base de Datos (DBA)	Realiza la restauración, sincronización o el Failover de las bases de datos. CRÍTICO para asegurar que el RPO (pérdida de datos) se cumpla.	Sistemas P1 y P2

6. Tareas del ERT		
Rol en el ERT	**Tareas Clave**	**Sistemas de Enfoque (Ejemplos)**
Equipo de Enlace de Procesos y Validación Funcional	Configura y realiza la puesta en marcha final de las aplicaciones P1 y P2	Sistemas P1 y P2

9.7 Tareas de los enlaces de procesos y validación funcional

El Equipo de Validación es el responsable de garantizar que los Sistemas de TIC recuperados sean funcionalmente utilizables y que los datos sean íntegros.

7. Tareas de los enlaces de procesos y validación funcional		
Fase del PCRAD	**Tarea Específica**	**Objetivo de la Tarea**
Ejecución	Validación Funcional: Ejecutar los scripts de prueba predefinidos para las transacciones críticas del negocio de su respectiva Dirección General (Ej.: registro, consulta, modificación).	Confirmar que el sistema funciona bajo contingencia.

7. Tareas de los enlaces de procesos y validación funcional		
Fase del PCRAD	**Tarea Específica**	**Objetivo de la Tarea**
	Prueba de Integridad de Datos: Verificar una muestra de datos críticos para confirmar que la información cargada en el Sitio Alterno es consistente y que se cumple con el RPO.	Limitar la pérdida de información al máximo aceptable.
Reanudación	Aprobación Operativa (Sign-Off): Emitir el visto bueno y la Aprobación de la Puesta en Producción al Coordinador PCRAD para reabrir el sistema a los usuarios finales o al público.	Es la confirmación oficial del "negocio" de que el sistema está listo para operar.
Vuelta a la Normalidad	Validación del Failback: Ejecutar las pruebas funcionales después de la migración de vuelta al sitio primario para asegurar la estabilidad final del entorno.	Mitigar riesgos para una transición segura de regreso a la infraestructura principal.

10 ANÁLISIS DE IMPACTO AL NEGOCIO

El Análisis de Impacto al Negocio (BIA) es el componente fundamental de planificación de este PCRAD. Para el Ministerio de Trabajo y Previsión Social (MINTRAB), el BIA tiene el propósito de identificar los procesos misionales críticos y los sistemas de Tecnologías de Información y Comunicación (TIC) que los soportan.

El BIA determina las consecuencias funcionales, legales y reputacionales que resultan de la indisponibilidad de estos sistemas, estableciendo así la prioridad de recuperación y los tiempos máximos aceptables de inactividad (RTO) que guiarán la respuesta del Equipo de Recuperación Tecnológica (ERT).

10.1 Criterios de medición de impacto

La clasificación de los sistemas se realiza midiendo el impacto potencial de su indisponibilidad en cuatro dimensiones críticas para el MINTRAB:

8. Criterios de medición de impacto	
Criterio	**Descripción del Impacto**
Legal y Cumplimiento	Consecuencias por incumplimiento de leyes, normativas, plazos o mandatos judiciales (Ej.: no poder recibir denuncias o registrar contratos a tiempo). Este es el criterio más alto.
Operacional y Misional	Impacto en la capacidad del MINTRAB para ejecutar sus funciones esenciales (Ej.: cese de la intermediación laboral o la supervisión de la IGT).
Financiero y Reputacional	Pérdida financiera directa o indirecta (Ej.: multas, pagos de nómina retrasados) y el daño a la imagen institucional y la confianza ciudadana.
Seguridad de la Información	Compromiso de la confidencialidad o integridad de datos sensibles (Ej.: información personal, expedientes laborales).

10.2 Clasificación de criticidad, RTO Y RPO

El MINTRAB clasifica sus sistemas de información en tres niveles de criticidad, los cuales definen los objetivos de tiempo de recuperación (RTO) y punto de recuperación (RPO).

9. Clasificación de criticidad, RTO Y RPO

Nivel	Descripción	Prioridad de Recuperación	RTO Máximo (Tiempo Aceptable de Inactividad)	RPO Máximo (Pérdida de Datos Aceptable)
P1	Crítico	Sistemas cuya indisponibilidad genera un impacto legal o social intolerable en pocas horas.	0 a 120 horas.	0 a 24 horas.
P2	Esencial	Sistemas cuya indisponibilidad afecta significativamente la eficiencia operativa y el servicio al público, pero con un plazo de tolerancia mayor.	120 a 288 horas.	48 a 72 horas.
P3	Soporte	Sistemas de apoyo administrativo. Su interrupción no detiene	288 a 480 horas.	72 a 144 horas.

9. Clasificación de criticidad, RTO Y RPO				
Nivel	**Descripción**	**Prioridad de Recuperación**	**RTO Máximo (Tiempo Aceptable de Inactividad)**	**RPO Máximo (Pérdida de Datos Aceptable)**
		inmediatamente las funciones misionales.		

11 MATRIZ DE SISTEMAS CRÍTICOS DEL MINTRAB

Esta matriz identifica los sistemas incluidos en el alcance del PCRAD y establece los objetivos de recuperación que el ERT debe cumplir.

10. Matriz de sistemas críticos del MINTRAB		
Proceso / Sistema de TIC	**Unidad Propietaria**	**Nivel de Criticidad**
Registro Electrónico de Contratos (RECIT)	Dirección General de Trabajo	P1
Legalidad Laboral	Dirección de Fomento a la Legalidad	P2
Sistemas IGT / Denuncias	Inspección General de Trabajo	P1

10. Matriz de sistemas críticos del MINTRAB		
Proceso / Sistema de TIC	**Unidad Propietaria**	**Nivel de Criticidad**
Portal Electrónico "Tu Empleo"	Dirección General de Empleo	P1
Portal Electrónico "Tu Empleo"	Dirección General de Empleo	P2
Libro Electrónico de Salarios	Dirección General de Trabajo	P2
Libro Electrónico de Salarios	Dirección General de Empleo	P1
Sistema de Gestión de PAM	Dirección de Previsión Social	P1
Correo Electrónico	Dirección de Sistemas de Información	P3
Servicios de Directorio Activo (AD)	Dirección de Sistemas de Información	P1
Sistema de Gestión de Reservas Recreativas	Dirección de Recreación del Trabajador del Estado	P3

Se establece con carácter taxativo que cualquier sistema de información, plataforma digital, base de datos o servicio informático desarrollado, administrado o alojado en la infraestructura del Ministerio de Trabajo y Previsión Social (MINTRABAJO) que no se encuentre explícitamente listado en la Matriz de Sistemas Críticos del presente capítulo, será catalogado por defecto bajo el Nivel de Criticidad P3 (Soporte).

12 CLÁUSULA DE RESPONSABILIDAD Y ÉTICA

Todo el personal que integre los comités de dirección, liderazgos operativos, equipos de recuperación tecnológica (ERT) y enlaces de validación funcional, asume el compromiso ético, legal y administrativo ineludible de velar por la absoluta confidencialidad, integridad y disponibilidad de la información institucional a la que tenga acceso antes, durante y después de la activación del presente plan. Consiguientemente, se establecen de carácter obligatorio las siguientes directrices normativas:

- **Secreto Profesional y Resguardo de Datos:** Queda estrictamente prohibido divulgar, reproducir, filtrar o sustraer cualquier tipo de información transaccional, datos de carácter personal de la ciudadanía o especificaciones técnicas de la infraestructura, de conformidad con el Protocolo de Control de Información institucional.
- **Uso Exclusivo de Activos en Contingencia:** Toda la infraestructura tecnológica, capacidad de cómputo, enlaces de comunicación y licencias de software aprovisionadas en el Sitio Alterno (DR Site) serán utilizados única y exclusivamente para garantizar la continuidad operativa del Ministerio y el restablecimiento de los servicios públicos esenciales. Queda terminantemente prohibido su uso para fines personales, comerciales o ajenos al estricto mandato de esta cartera de Estado.
- **Responsabilidad Civil y Administrativa:** El incumplimiento deliberado, negligente o fraudulento de los procedimientos descritos en este documento, así como el uso indebido de los privilegios de acceso otorgados para la atención de la crisis, será sancionado de acuerdo con lo estipulado en la legislación interna del Ministerio de Trabajo y Previsión Social, la Ley de Probidad y Responsabilidades de Funcionarios y Empleados Públicos, y demás normativas penales vigentes en la República de Guatemala.

13 ESTRATEGIA DE RECUPERACIÓN TECNOLÓGICA

La Estrategia de Recuperación Tecnológica es la respuesta técnica y planificada a los requerimientos de continuidad operacional del Ministerio de Trabajo y Previsión Social (MINTRAB), tal como fueron definidos y priorizados en el Análisis de Impacto al Negocio (BIA).

Su objetivo primordial es asegurar la continuidad de las funciones misionales vitales, mediante la provisión de la infraestructura y los mecanismos técnicos necesarios que permitan restablecer los servicios de TIC clasificados como P1 (Críticos) y P2 (Esenciales). Esta estrategia define la solución técnica que el MINTRAB ha implementado para lograr sus objetivos de RTO y RPO, minimizando el impacto legal, social y operacional de cualquier evento de desastre.

13.1 Estrategia general

La estrategia adoptada por el MINTRAB para la recuperación ante desastres es la implementación de un Sitio Alterno con replicación constante.

Sitio alterno: Un sitio de contingencia totalmente equipado con hardware, software y conectividad de red listos para tomar el control de la operación en minutos u horas. Esto es fundamental para cumplir con los RTO de los sistemas P1.

Replicación de Datos: Los datos de los sistemas P1 y P2 se replican en casi real al Sitio Alterno, minimizando la pérdida de datos y asegurando el cumplimiento de los RPO.

13.2 Componentes clave de la estrategia

13.2.1 Infraestructura del sitio alterno

El Sitio Alterno debe ser un ambiente espejo, ubicado geográficamente distante del Centro de Datos Primario para mitigar desastres regionales, y contar con la siguiente infraestructura:

- Hardware Similar: Suficiente capacidad de procesamiento (servidores) y almacenamiento (Storage) para soportar la carga operativa de todos los sistemas P1 y P2.
- Conectividad Dedicada: Enlaces de comunicación de alta velocidad dedicados (WAN) y redundantes entre el sitio primario y el DR Site para garantizar la estabilidad de la replicación.
- Servicios Esenciales: El DR Site debe contar con sistemas de energía redundantes (UPS y Generador), aire acondicionado y control de acceso.

13.2.2 Mecanismos de replicación y backup

La estrategia de replicación está diferenciada según la criticidad del sistema:

11. Mecanismos de replicación y backup		
Nivel de Criticidad	**Mecanismo de Replicación**	**Descripción Técnica**
P1 (Crítico)	Replicación Síncrona / Casi-Síncrona	Utilizado para Bases de Datos críticas y servicios de Infraestructura (AD). Mitigar riesgos que la mayoría de las transacciones se repliquen inmediatamente.

11. Mecanismos de replicación y backup		
Nivel de Criticidad	**Mecanismo de Replicación**	**Descripción Técnica**
P2 (Esencial)	Replicación Asíncrona / Backup Frecuente	Utilizado para sistemas cuya interrupción permite una pequeña pérdida de datos. La replicación ocurre en bloques programados.
P3 (Soporte)	Copias de Seguridad Diarias	Basado en el esquema de backup institucional. La recuperación se realiza cargando la última copia de seguridad.

13.2.3 Estrategia de recuperación de datos

Para los sistemas P1 y P2, el mecanismo primario para cumplir el RPO es la Replicación.

En caso de desastre, el DBA iniciará el proceso de Failover para activar la base de datos replicada en el DR Site.

Si la replicación falla o está comprometida, el mecanismo de respaldo es la Restauración del último Backup verificado y probado, reconociendo que esto puede significar un incumplimiento del RPO.

14 INFRAESTRUCTURA TECNOLÓGICA

14.1 Arquitectura del sitio primario

Este capítulo describe la configuración actual de la infraestructura de TIC del MINTRAB en su sitio de producción y la arquitectura de soporte en el Centro de Datos Alterno. El conocimiento de esta arquitectura es esencial para la ejecución de los procedimientos de recuperación.

14.2 Arquitectura del sitio de contingencia

El Centro de Datos Primario (DC Principal) es la ubicación física donde se ejecutan la totalidad de los sistemas de misión crítica y soporte del MINTRAB en condiciones normales.

Ubicación Clave: Este centro de datos está ubicado estratégicamente en el 3er nivel del edificio del Ministerio de Trabajo, dentro de las instalaciones de la Dirección de Sistemas de Información (DISI).

12. Arquitectura del sitio de contingencia		
Componente	**Configuración Clave**	**Rol en la Continuidad**
Plataforma de Virtualización	VMware vSphere / Hyper-V Cluster	Aloja todas las Máquinas Virtuales (VMs) de los sistemas P1, P2 y P3.
Almacenamiento (SAN)	Storage de Alto Rendimiento (Ej: Fibre Channel)	Proporciona el espacio de disco para todas las bases de datos y aplicaciones críticas.

12. Arquitectura del sitio de contingencia		
Componente	**Configuración Clave**	**Rol en la Continuidad**
Servidores Físicos	Servidores y nodos / Rack de alto rendimiento	Soportan los hosts de virtualización, Directorio Activo (AD) y servicios de backup.
Redes	Switching y Firewalls de Borde (Perimetrales)	Controlan el acceso interno/externo y el tráfico de datos.
Servicios Críticos	Controladores de Dominio (Active Directory), Servidores DNS.	Indispensables para la autenticación y el funcionamiento de toda la red

14.3 Esquema de replicación de datos

Para alcanzar los RPO definidos en el esquema de replicación de datos, se han implementado los siguientes mecanismos:

- Replicación a nivel de Storage: Utilizada para replicar LUNs (Unidades Lógicas de Almacenamiento) completas de los sistemas P1 entre el Storage Primario y el Storage del Centro de Datos Alterno.
- Replicación a nivel de Base de Datos: Utilizada como mecanismo de respaldo o para alta disponibilidad en bases de datos específicas, asegurando la integridad de los datos transaccionales.
- Backup Tradicional: Los sistemas P3 y los respaldos de archivos se gestionan mediante el sistema de copias de seguridad institucional, almacenadas en un repositorio aislado y accesible desde el DR Site.

15 PROCESO DE DECLARACIÓN DE DESASTRE

El Proceso de Declaración de Desastre constituye el protocolo formal y metódico que el Ministerio de Trabajo y Previsión Social (MINTRAB) utilizará para escalar un incidente grave de TIC que exceda la capacidad de respuesta de los procedimientos operativos estándar.

Este capítulo establece la cadena de mando y los umbrales de activación que transforman una falla técnica en una emergencia institucional. La correcta ejecución de este proceso es crítica, ya que autoriza la movilización del Comité de Dirección y del Equipo de Recuperación Tecnológica (ERT), así como la asignación de recursos extraordinarios para iniciar la recuperación en el Sitio de Contingencia.

El objetivo es asegurar que la activación del Plan Contingencia y Recuperación Ante Desastres (PCRAD) sea una decisión controlada, documentada y tomada al más alto nivel jerárquico del Ministerio, minimizando así la incertidumbre operativa y el riesgo legal asociado a la indisponibilidad prolongada de los servicios misionales.

15.1 Fases del proceso de activación

El Proceso de Declaración de Desastre constituye el protocolo que el Ministerio de Trabajo y Previsión Social (MINTRAB) utilizará para escalar un incidente grave de TIC que exceda la capacidad de respuesta de los procedimientos operativos estándar.

Aquí se establece la cadena de mando y los umbrales de activación que transforman una falla técnica en una emergencia institucional. La correcta ejecución de este proceso es crítica, ya que autoriza la movilización del Comité de Dirección y del Equipo de Recuperación Tecnológica (ERT), así como la asignación de recursos extraordinarios para iniciar la recuperación en el Sitio de Contingencia.

El objetivo es asegurar que la activación del Plan Contingencia y Recuperación Ante Desastres (PCRAD) sea una decisión controlada, documentada y tomada al más alto

nivel jerárquico del Ministerio de Trabajo y Previsión Social, minimizando así la incertidumbre operativa y el riesgo legal asociado a la indisponibilidad prolongada de los servicios misionales.

15.1.1 Fase 1: Detección e inicialización

Esta fase es responsabilidad del personal técnico de primera línea (Monitoreo, Soporte) de la DISI:

13. Detección e inicialización		
Paso	**Responsable**	**Acción**
Detección del Incidente	Personal de Monitoreo/Soporte DISI	Identificar la falla, confirmar su magnitud (pérdida de energía, ciberataque, indisponibilidad de sistemas P1).
Notificación Inicial	Líder de Soporte DISI	Notificar inmediatamente al Coordinador Operativo del PCRAD (Director de DISI) sobre la naturaleza del incidente.

15.1.2 Fase 2: Evaluación y notificación (coordinación táctica)

Esta fase la lidera el Director de la Dirección de Sistemas de Información (Coordinador Operativo).

14. Evaluación y notificación			
Paso	**Responsable**	**Acción**	**Resultado**
Evaluación Preliminar	Director de DISI	Analizar la magnitud del daño y el tiempo estimado de recuperación en el DC Principal.	Determinar si la recuperación puede manejarse internamente o si requiere el PCRAD.
Notificación a las autoridades Viceministeriales y Ministeriales	Director(a) de DISI	Informa del Impacto Preliminar (naturaleza, sistemas P1/P2 afectados, RTO estimado) a las autoridades.	La señora Ministra o el señor Ministro convoca a Directores de inmediato para la Sesión de Emergencia.

15.1.3 Fase 3: Declaración formal y activación operativa

Esta fase corresponde a una decisión ejecutiva adoptada en el Nivel Estratégico, mediante instrucción u orden emitida por la Máxima Autoridad del Ministerio de Trabajo y Previsión Social.

15. Declaración formal y activación operativa			
Paso	**Responsable**	**Acción**	**Consecuencia**
Decisión de Declaración	Despacho Ministerial	Declara formal del desastre basado en información vertida por la DISI	Decisión CRÍTICA. Inicia la fase de emergencia del MINTRAB.
Activación del PCRAD	Director de DISI	Emitir la orden formal para que el Equipo de Recuperación Tecnológica (ERT) se movilice al Sitio de Contingencia (DR Site).	Pone en marcha la ejecución del Procedimientos de Recuperación.
Notificación Masiva	Líder de Comunicaciones	Notificar a todo el personal relevante del MINTRAB (personal clave y usuarios) y, si es necesario, al público general, sobre la indisponibilidad de servicios.	Maneja las expectativas internas y externas.

15.1.4 Criterios de declaración formal

La Declaración Formal de Desastre solo será autorizada por el Ministro (a)o Viceministro(a) si se cumple al menos uno de los siguientes criterios:

1. RTO/RPO Comprometidos: Se ha confirmado que el tiempo de inactividad de cualquier sistema P1 superará su RTO máximo (4 horas).

2. Pérdida de Acceso Físico: El Centro de Datos Primario (3er nivel, DISI) es física o lógicamente inaccesible, o su operación es insegura (Ej: Incendio, Inundación).
3. Daño Irrecuperable: El daño a la infraestructura del Centro de Datos Principal (Storage, Servidores) es tan severo que se requiere una reconstrucción total.

15.2 Proceso de cierre de desastre

El PCRAD permanece activo hasta que el Despacho Ministerial o Viceministerial, tras la recomendación del Director de DISI y el Líder de Procesos (Validación Funcional), declara la finalización de la emergencia y autoriza el inicio del proceso de Vuelta a la Normalidad (Failback) al sitio principal.

16 PLAN DE COMUNICACIÓN Y COORDINACIÓN

Este capítulo establece los lineamientos para la gestión de la información durante la ejecución del PCRAD. El objetivo es asegurar que todos los involucrados (internos y externos) reciban información veraz, oportuna y consistente, evitando la propagación de rumores que afecten la imagen del Ministerio.

16.1 CANALES DE COMUNICACIÓN OFICIAL

Para garantizar la integridad del mensaje, se establecen los siguientes canales únicos:

- Comunicación Interna Estratégica: Sesiones presenciales o virtuales (vía plataforma de contingencia) de las autoridades Ministeriales, Viceministeriales y Directores involucrados.
- Comunicación Operativa: Grupos de mensajería instantánea encriptada específicos para el ERT y la DISI, y correo electrónico institucional (si está disponible).

- Comunicación Institucional: Portal web del MINTRAB (página de contingencia) y redes sociales oficiales.

16.2 Comunicación externa (ciudadanía y sector laboral)

El Líder de Comunicaciones (Jefe(a)de la Unidad de Comunicación Social) es el único portavoz autorizado para emitir declaraciones sobre el estado de los servicios.

16. Comunicación externa		
Público Objetivo	**Medio de Comunicación**	**Mensaje Clave**
Ciudadanía y Usuarios	Redes Sociales / Radio / Prensa	Notificar la indisponibilidad de sistemas y proporcionar alternativas o plazos estimados.
Empresas y Patronos	Correo Masivo / Portal Web	Informar sobre la situación de los sistemas con fechas legales, aclarando prórrogas legales si el Líder Legal lo autoriza.

16. Comunicación externa		
Público Objetivo	**Medio de Comunicación**	**Mensaje Clave**
Otras Entidades (Gobierno)	Oficios / Comunicación Directa	Notificar a entidades como el IGSS o SAT si existe interoperabilidad de datos afectada.

16.3 Coordinación con proveedores críticos

La DISI mantendrá un directorio actualizado de contactos de emergencia para soporte técnico externo.

17. Coordinación con proveedores críticos		
Proveedor	**Tipo de Servicio**	**Rol en la Crisis**
Proveedor de Internet (ISP)	Enlaces WAN / Internet	Asegurar la prioridad del tráfico hacia el DR Site.
Proveedor de Cloud/Data Center	Infraestructura Alterna	Soporte en la activación de recursos en el Sitio de Contingencia.
Soporte de Software	Soporte Técnico Nivel 3	Resolución de errores complejos durante la restauración de RECIT o el PAM.

16.4 Matriz de notificación (escalamiento)

En caso de desastre, se seguirá este orden de notificación:

1. Nivel 1 (Detección): El técnico de turno notifica al Subdirector/Director de la DISI.
2. Nivel 2 (Táctico): El Director de la DISI notifica al Ministro y Viceministros.
3. Nivel 3 (Estratégico): El Presidente del Comité autoriza al Líder de Comunicaciones para informar a las Direcciones Generales (IGT, Empleo, etc.) y al público.

16.5 Protocolo de control de información

Todo el personal del MINTRAB tiene estrictamente prohibido emitir juicios o información técnica sobre el desastre en redes sociales personales o medios de comunicación, para evitar fugas de información que comprometan la seguridad del Ministerio.

17 PROCEDIMIENTOS DE RECUPERACIÓN

Este capítulo contiene las guías de ejecución técnica para restaurar la plataforma tecnológica del MINTRAB. Cada procedimiento debe ejecutarse en el orden establecido para respetar las dependencias técnicas.

17.1 Secuencia general de recuperación

El ERT seguirá este orden de prelación para asegurar una restauración estable:

1. Nivel 0: Conectividad y Redes (WAN/VPN).
2. Nivel 1: Servicios Core de Infraestructura (AD, DNS, PAM).
3. Nivel 2: Capa de Datos (SQL Server/Oracle para RECIT, PEX, etc.).
4. Nivel 3: Capa de Aplicaciones (Servidores Web y Middleware).

17.1.1 Procedimiento de recuperación de infraestructura core (P1)

17.1.1.1 Servicios de identidad y acceso

- Paso 1: Verificar la conectividad entre el Centro de Datos Alterno y los Controladores de Dominio (DC) remotos.
- Paso 2: Forzar la promoción de los DCs en el sitio de contingencia como maestros de operaciones (FSMO roles) si el sitio primario es inaccesible.
- Paso 3: Activar el Sistema de Gestión para permitir que los administradores de la DISI accedan de forma segura a los servidores recuperados.
- Paso 4: Validar la autenticación de usuarios clave del equipo de validación funcional.

17.1.1.2 Procedimiento de recuperación de sistemas misionales (p1)

- Paso 1 (Base de Datos): Iniciar el Failover de las instancias de base de datos en el Centro de Datos Alterno. Verificar la integridad de la última transacción replicada (RPO).
- Paso 2 (Aplicación): Encender las Máquinas Virtuales (VMs) de los servidores de aplicaciones de los sistemas P1 en el clúster de contingencia.
- Paso 3 (Configuración): Actualizar las cadenas de conexión (Connection Strings) si las IPs del Centro de Datos Alterno difieren de las de producción.
- Paso 4 (Redirección): Actualizar los registros DNS internos para que *.MINTRAB.gob.gt apunte al Centro de Datos Alterno.

17.1.1.3 Procedimiento de recuperación de sistemas de apoyo (p2/p3)

- Paso 1: Restaurar desde la última copia de seguridad (Backup) enviada al sitio de contingencia.
- Paso 2: Validar la disponibilidad del portal de reservas para el personal del Ministerio y usuarios externos.

17.1.1.4 Tabla de verificación de salida

Antes de entregar los sistemas al Equipo de Validación Funcional, el Líder Técnico del ERT debe confirmar:

18. Tabla de verificación de salida		
Sistema	Estado del Servicio	IP / URL de Acceso
AD	[ ] Activo	Interna
RECIT	[ ] Activo	Interna
Tu Empleo	[ ] Activo	tuempleo.MINTRAB.gob.gt

18 PROCEDIMIENTOS DE RETORNO

18.1 Criterios de retorno a la normalidad

El proceso de Failback se inicia únicamente cuando se ha garantizado que las causas que originaron el desastre han sido resueltas y que la infraestructura en el 3er nivel de la DISI es estable y segura para retomar la operación.

18.2 Pasos operativos para el failback

19. Criterios de retorno a la normalidad		
Fase	**Acción Técnica**	**Responsable**
Responsable	Notificar a todos los usuarios del MINTRAB sobre la	Líder de Comunicaciones

19. Criterios de retorno a la normalidad		
Fase	**Acción Técnica**	**Responsable**
	ventana de indisponibilidad programada para el retorno.	
Cierre de Sesiones	Detener los servicios en el Centro de Datos Alterno para evitar que se sigan escribiendo nuevos datos.	ERT - Especialista
Sincronización Final	Ejecutar la última sincronización de bases de datos hacia el almacenamiento en el 3er nivel de la DISI.	ERT - DBA
Activación en DISI	Levantar los servicios y servidores en el Centro de Datos Primario.	ERT - Especialista Infra.
Redirección DNS	Actualizar nuevamente los registros DNS para que apunten a las direcciones IP originales de la red interna de la DISI.	ERT - Redes

18.3 Validación post retorno

Una vez que los sistemas están activos en el sitio primario, el Equipo de Enlace de Procesos y Validación Funcional debe realizar las mismas ejecutadas durante la crisis.

1. Verificación de Datos: Confirmar que el último registro ingresado en el Centro de Datos Alternos aparece correctamente en el sitio primario.
2. Visto Bueno Final: El Director de la DISI informa al Despacho Superior, que la operación ha retornado al 100% de normalidad.

19 MANTENIMIENTO Y PRUEBAS DEL PLAN

El Ministerio de Trabajo y Previsión Social (MINTRAB), en su calidad de entidad rectora en la promoción del empleo digno, la supervisión del cumplimiento de la legislación laboral y el desarrollo de la previsión social en Guatemala depende de manera crítica de la operatividad continua de sus sistemas de Tecnologías de Información y Comunicación (TIC). Estos sistemas constituyen un componente esencial para garantizar la prestación eficaz y oportuna de los servicios públicos bajo su competencia.

La ocurrencia de eventos disruptivos, tales como fallas graves de infraestructura tecnológica, desastres naturales o ciberataques, representa una amenaza significativa para la confidencialidad, integridad y disponibilidad de la información institucional, así como para la continuidad de los servicios brindados a la ciudadanía. Ante estos riesgos, resulta imprescindible contar con mecanismos estructurados que permitan responder de manera oportuna y efectiva.

En este contexto, el presente Plan Contingencia y Recuperación Ante Desastres (PCRAD) establece el conjunto de estrategias, procedimientos, recursos, roles y responsabilidades orientados a mitigar el impacto de incidentes mayores. Su propósito es asegurar la recuperación ordenada y eficiente de los sistemas y servicios críticos de TIC en el menor tiempo posible, garantizando así la continuidad operativa del Ministerio y el cumplimiento de su mandato legal y constitucional.

19.1 Programa de pruebas anuales

El MINTRAB realizará los siguientes tipos de pruebas se cumplen las premisas de implementación:

1. Pruebas de Escritorio (Anual): Revisión del documento y roles con los líderes de la DISI para asegurar que los contactos y procedimientos sigan vigentes.
2. Pruebas Técnicas Parciales (Semestrales): Pruebas de restauración de backups y verificación de la velocidad de replicación del enlace WAN.
3. Simulacro de Failover Completo (Anual): Activación real o simulada de los sistemas P1 en el DR Site durante un fin de semana.

19.2 Actualización del plan

La vigencia y confiabilidad del PCRAD dependen de su alineación exacta con la realidad técnica de la DISI. Por lo tanto, se establece la siguiente política de actualización:

19.2.1 Disparadores de actualización obligatoria:

El PCRAD debe someterse a revisión técnica y actualizarse de manera inmediata únicamente si ocurre alguno de los siguientes eventos:

1. Cambios Significativos en la Infraestructura: Cualquier modificación física o lógica en el Centro de Datos del 3er nivel (ej. migración de servidores, cambio de arquitectura de almacenamiento o nuevas plataformas de virtualización).
2. Hallazgos en Pruebas y Simulacros: Cuando los resultados de las pruebas anuales identifiquen fallas críticas, cuellos de botella que impidan cumplir con el RTO, o errores en las secuencias de recuperación.

19.2.2 Cláusula de inmutabilidad:

El PCRAD no sufrirá ningún cambio ni modificación en sus procedimientos si no se cumple alguno de los puntos anteriores. Esta medida garantiza que el plan se mantenga como un estándar probado y evita alteraciones arbitrarias que puedan comprometer la respuesta técnica ante una crisis real.

19.3 Requisito de certificación de premisas

Antes de iniciar cualquier simulacro o prueba de conmutación (failover), el Director de la Dirección de Sistemas de Información deberá certificar que las premisas del Capítulo 3 se encuentran vigentes.

Si alguna premisa crítica (ej. redundancia de energía en el DR Site o integridad de la réplica) no se cumple, la prueba deberá ser suspendida para evitar riesgos innecesarios a la operación institucional.

GLOSARIO

Para asegurar que todos los niveles (estratégico y táctico) comprendan el lenguaje técnico del plan, se definen los siguientes términos clave:

- **MINTRAB:** Ministerio de Trabajo y Previsión Social.
- **BIA (Análisis de Impacto al Negocio):** Proceso para determinar el impacto de la interrupción de servicios y establecer prioridades de recuperación.
- **DC Principal (Data Center Primario):** Centro de datos ubicado en el 3er nivel de la DISI donde opera la tecnología habitualmente.
- **DR Site (Sitio de Recuperación Ante Desastres):** Ubicación física alterna configurada para restaurar los servicios en caso de fallo del sitio primario.
- **ERT (Equipo de Recuperación Tecnológica):** Grupo técnico especializado encargado de ejecutar los pasos de restauración de sistemas.
- **Failback (Retorno a la Normalidad):** Proceso de transferir la operación de regreso del sitio alterno al centro de datos primario.
- **Failover (Conmutación por Error):** Proceso de activar un sistema o base de datos en el sitio alterno tras una falla.
- **Hot Site (Sitio Caliente):** Centro de datos de contingencia totalmente equipado y con datos replicados, listo para operar en poco tiempo.
- **P1 / P2 / P3:** Niveles de criticidad de los sistemas, siendo P1 el de mayor prioridad de recuperación.
- **RPO (Punto de Recuperación Objetivo):** Cantidad máxima de datos (medida en tiempo) que el Ministerio puede permitirse perder.
- **RTO (Tiempo de Recuperación Objetivo):** Tiempo máximo permitido para restaurar un sistema tras un desastre.
- **Ransomware:** es un programa malicioso que restringe el acceso a los archivos o dispositivos y exige un rescate económico para restaurarlo.

- **TIC:** Tecnologías de la Información y la Comunicación
- **Infraestructura core:** comprende los componentes esenciales y centralizados de TI (servidores, almacenamiento y redes de datos) que soportan los procesos y servicios críticos de una organización. Garantiza la máxima disponibilidad, seguridad y redundancia operativa para los sistemas de misión crítica.
- **DDoS:** ataque de denegación de servicio distribuido, conocido como DDoS (por sus siglas en inglés, Distributed Denial of Service), es un ciberataque en el que múltiples sistemas comprometidos saturan el ancho de banda o los recursos de un servidor o sitio web, dejándolo inaccesible para los usuarios legítimos.
- **Renap:** Registro Nacional de las Personas.
- **IGSS:** Instituto Guatemalteco de Seguridad Social.
- **SAT:** Superintendencia de Administración Tributaria.
- **DBA:** Administrador de Bases de Datos.
- **PAM:** Programa de Aporte Económico del Adulto Mayor
- **RECIT:** Registro Electrónico de Contratos Individuales de Trabajo
- **IGT:** Inspección General de Trabajo.