República Argentina - Poder Ejecutivo Nacional
Año de la Grandeza Argentina

Anexo

Número: IF-2026-43001297-APN-CNC#JGM

CIUDAD DE BUENOS AIRES
Miércoles 29 de Abril de 2026

Referencia: ANEXO I: REGLAMENTO TÉCNICO PARA LA ELABORACIÓN E IMPLEMENTACIÓN DE POLÍTICAS DE PLANES DE CONTINGENCIAS, PLANES DE CONTINGENCIA Y CENTROS DE PROCESAMIENTO DE DATOS DE RESPALDO

ANEXO I:

REGLAMENTO TÉCNICO PARA LA ELABORACIÓN E IMPLEMENTACIÓN DE POLÍTICAS DE PLANES DE CONTINGENCIAS, PLANES DE CONTINGENCIA Y CENTROS DE PROCESAMIENTO DE DATOS DE RESPALDO

CAPÍTULO 1: Política de Planes de Contingencias

Cada sujeto alcanzado elaborará una Política de Planes de Contingencias.

El documento definirá su propósito, el alcance, roles y responsabilidades, describirá cómo ha de funcionar la coordinación entre áreas, y así mismo establecerá un mecanismo de actualización de dicha política que será a la vez periódico y reactivo a eventos allí definidos. Dicha política contemplará los procedimientos para implementar la misma.

Un activo necesario para este fin es el inventario de sistemas del sujeto alcanzado. La política y el proceso asociado deberán contemplar un mecanismo para generar el inventario de sistemas, su clasificación por criticidad (de cada ítem en el inventario) y su proceso de actualización; y también incluye la creación de los planes de contingencia (de cada ítem en el inventario) y su actualización.

Deberá asimismo definir un responsable (autoridad designada) del desarrollo de la Política de Planes de Contingencia y procedimientos asociados, así como mecanismos para actualizar la política y procedimientos periódicamente y en respuesta a eventos allí definidos.

1.1. Inventario y Clasificación

La Política de Planes de Contingencias incluirá la definición de roles y responsabilidades en la confección del

inventario de sistemas, así como de la clasificación de sistemas según criticidad. El inventario enumera los sistemas en un único formato. Deberá actualizarse periódicamente en períodos no mayores a un año y ante eventos relevantes (p.ej., adquisiciones, cambios). Cada sistema se encuentra definido de manera unívoca, describiendo sus funcionalidades de negocio y aquellas para la misión del sujeto alcanzado. Cada sistema deberá ser clasificado por la criticidad de disponibilidad según la metodología de la sección precedente titulada Categorización de Sistemas por Niveles de Criticidad.

El inventario deberá enumerar los sistemas y sus dependencias (aplicaciones, datos, infraestructura, proveedores), y para cada uno deberá describir lo siguiente (ver ejemplos en Tabla 1 abajo):

1. Una estimación del impacto de interrupciones por dimensiones: seguridad/vida, continuidad de servicios al ciudadano, impacto económico/operativo, legal/regulatorio y reputacional.
2. Un nivel de criticidad (Alto/Medio/Bajo) según impacto y tolerancias según lo instruye la Sección 1.2.
3. Valores de RTO (tiempo de recuperación objetivo) y RPO (punto de recuperación objetivo) para el sistema consistentes con la Tabla 2 abajo.
4. Una priorización del orden de recuperación del sistema y los recursos necesarios.

El inventario deberá ser aprobado por la autoridad designada.

Sistema/Proceso	Impacto de interrupción prolongada	RTO	RPO	Nivel de Criticidad
Plataforma de Autenticación Ciudadana	Indisponibilidad impide validar identidad a nivel nacional y afecta múltiples servicios públicos en línea.	4 horas	15 minutos	Alto
Servicio Web Municipal	Afecta trámites en un municipio; existen alternativas presenciales temporales.	24 horas	3 horas	Medio
Sistema de Gestión Interna	Impacto limitado a procesos administrativos; retrasos manejables con trabajo manual temporal.	2 días	24 horas	Bajo

Tabla 1: Ejemplo de inventario

1.2. Categorización de Sistemas por Niveles de Criticidad

Con el fin de dirigir eficazmente los esfuerzos de recuperación y dimensionar apropiadamente las medidas de contingencia, se establece una clasificación de sistemas en tres niveles de criticidad (Alto, Medio, Bajo). Esta categorización se basa en el impacto potencial que tendría una interrupción en la disponibilidad del sistema en cuestión, siguiendo criterios inspirados en estándares internacionales (por ejemplo, la clasificación de impacto de la norma federal FIPS 199 de EE.UU.[1]):

- **Nivel Alto:** Incluye a los sistemas cuya indisponibilidad tendría efectos severos o catastróficos para el país en términos de las operaciones, los activos o individuos.

  Por ejemplo, seguridad, orden público, economía, salud pública o el bienestar general, que pudieran dejar indisponibles funciones principales del sujeto alcanzado que afecten negativamente a sus activos o individuos. Un desastre que afecte a estos sistemas críticos podría interrumpir ampliamente la prestación de servicios esenciales o comprometer la seguridad nacional. Ejemplos: centros de cómputos centrales de ministerios claves, proveedores de energía eléctrica o telecomunicaciones, sistemas bancarios de pago de alcance nacional.

- **Nivel Medio:** Corresponde a sistemas cuya operación, si bien no provocaría un colapso nacional en caso de interrupción, sí generaría efectos adversos graves en la prestación de servicios o en sectores económicos/sanitarios/regionales importantes.

  La indisponibilidad de sus sistemas podría afectar el funcionamiento de los sujetos alanzados, causando perjuicios significativos a la población o a la economía en dicho ámbito. Se considera que el impacto de un incidente sería grave pero manejable a corto plazo, requiriendo esfuerzos importantes de recuperación sin llegar al nivel crítico nacional. Ejemplos: organismos descentralizados, empresas de servicios regionales, o bases de datos con información sensible de alcance acotado (p.ej. registros provinciales, hospitales de referencia, operadores logísticos de transporte público).

- **Nivel Bajo (No Crítico):** Incluye los sistemas de información que, en caso de desastre, tendrían un impacto limitado y acotado. Una caída prolongada de estos sistemas podría ocasionar inconvenientes menores o retrasos en trámites/servicios no vitales, sin comprometer la seguridad ni funciones esenciales. El efecto adverso se considera tolerable o de baja intensidad, manejable mediante medidas alternativas temporales. No obstante, incluso en este nivel es necesario contar con planes de recuperación, aunque más simplificados, para reinstaurar las operaciones en plazos aceptables. Ejemplos: sujetos con funciones administrativas internas, bases de datos de consulta pública no crítica, o sistemas duplicados cuyo fallo no interrumpe servicios al ciudadano de forma inmediata.

CAPÍTULO 2: Plan de Contingencia y Plan de Recuperación ante Desastres (PRD)

En esencia, un Plan de Contingencias describe cómo se recuperarán sistemas, datos y servicios críticos en caso de un evento adverso, garantizando la continuidad operativa y minimizando el impacto en la misión del sujeto alcanzado y en la sociedad.

De acuerdo con lineamientos internacionales, como los de NIST en EE.UU.[2], el Plan de Recuperación ante Desastres (PRD) es parte integral de la planificación de contingencia de Tecnologías de la Información (TI) y debe coordinarse con otros planes de continuidad.

2.1. Requisitos Mínimos de un Plan de Contingencia

Todo Plan de Contingencia, sin importar el sujeto alcanzado o su criticidad, deberá contener ciertos elementos mínimos obligatorios que aseguren su efectividad. Estos requisitos mínimos se alinean con estándares internacionales de continuidad de TI y buscan que cada organización "replique" al menos las prácticas fundamentales de recuperación. A continuación, se enumeran los componentes esenciales que todo Plan de Contingencia debe incluir:

- **Alcance:** declaración formal del compromiso del sujeto alcanzado con la continuidad de operaciones de TI, aprobada. Debe definir el alcance del Plan.
- **Análisis de Impacto al Negocio (BIA):** resumen de las conclusiones del análisis de impacto al negocio realizado, identificando los procesos críticos, los sistemas de apoyo, y las consecuencias de una interrupción prolongada. Aquí se documentarán los Objetivos de Tiempo de Recuperación (RTO) máximos permitidos para cada función esencial, y el Objetivo de Punto de Recuperación (RPO) o pérdida máxima de datos tolerable. Estos parámetros guiarán todas las estrategias del plan. También se priorizarán los sistemas en orden de restauración.
- **Estrategia de Respaldo y Recuperación:** descripción de la arquitectura de recuperación seleccionada. Debe detallar el tipo de solución adoptada –por ejemplo, sitio "espejo" en tiempo real, sitio caliente, tibio o frío– justificando su idoneidad respecto a los RTO/RPO requeridos.
    - el Centro de Procesamiento de Datos de Respaldo designado (ubicación, características de infraestructura) y
    - Incluye la planificación de recursos redundantes: enlaces de comunicación alternativos, alimentación eléctrica de emergencia, capacidad de cómputo y almacenamiento suficiente en el sitio de respaldo, mecanismos de replicación de datos (sincrónicos para datos críticos de alta categoría, asincrónicos o mediante backups periódicos para menores niveles).
- **Organización, Roles y Responsabilidades:** identificación del equipo de respuesta y recuperación de TI. Debe listar los nombres y cargos de las personas clave autorizadas a declarar un desastre y activar el plan, los responsables de coordinar las tareas de recuperación, los equipos técnicos asignados a restaurar cada sistema y los enlaces de comunicación internos y externos. Se incluirá información de contacto de emergencia (24x7) de todos los actores relevantes y, de ser aplicable, datos de proveedores de soporte. Se incluirá una lista de escalamiento que asegure que todos los roles están cubiertos.
- **Procedimientos de Activación, Conmutación y Recuperación:** guías paso a paso (*playbooks*) para llevar a cabo la recuperación en distintos escenarios de desastre. Deben cubrir al menos: activación del PRD; conmutación al sitio alternativo; recuperación de sistemas y datos (incluida restauración desde backups); y retorno a la normalidad una vez superada la contingencia. Estos playbooks deben ser específicos para cada tipo de incidente relevante (por ejemplo, ransomware vs. destrucción física)[3].
- **Coordinación con otras áreas:** Se indicará las interacciones con otras áreas, incluyendo reporte de incidentes, comunicaciones, actualizaciones y configuración de sistemas de manera que queden incorporados en el plan.
- **Medidas de Seguridad en la Recuperación:** pautas para mantener o restaurar los controles de seguridad lógica en el entorno de recuperación (autenticación, firewalls, monitorización, cifrado). Debe coordinarse con el plan de respuesta a incidentes de ciberseguridad, cuidando evidencia forense y evitando alertar a atacantes. En seguridad física, prever controles durante el desastre (personal de seguridad adicional, verificación de identidad, etc.).
- **Registro y Documentación de Incidencias:** bitácora cronológica de eventos, decisiones y medidas

durante una conmutación. Cuando se trate de un servicio de colocación, la documentación deberá incluir planos eléctricos y mecánicos, y políticas de mantenimiento. Archivar resultados de pruebas del plan de contingencia y evidencias (informes de backup, reportes de replicación, etc.).

- **Programa de Pruebas:** detalla la frecuencia y tipo de pruebas del plan (failover a sitio alterno, simulacros de recuperación de datos, tabletop), con periodicidad mínima anual para pruebas integrales. Tras cada ejercicio, se deberá labrar un informe de resultados, incluyendo métricas y plan de remediación. Cuando se opte por un servicio de colocación, se sumarán resultados de pruebas FAT/SAT, y registros de auditorías de continuidad operativa.[4]
- **Revisión y Aprobación:** La política de planes de contingencia incluirá un mecanismo para la revisión y aprobación de los planes.
- **Actualización y Mejora Continua:** este Plan deberá incluir objetivos de actualización periódica y ante ciertos eventos (p.ej., fallas en la ejecución de un plan o prueba) que incorporen mejoras surgidas de las pruebas y otros ejercicios.

2.2. Requisitos Específicos para los Sujetos Alcanzados Según su Criticidad

Si bien todos los planes comparten una base común, la descripta en la sección antecedente, los sistemas deberán cumplir requisitos técnicos adicionales acordes al potencial impacto mayor de un incidente según el nivel de criticidad definido.

A continuación, se sintetizan las exigencias mínimas adicionales y mejores prácticas recomendadas.

Aspecto Clave	Alta	Media	Baja
Centro de Respaldo	Tier 3 o compromete tier 3 en el plazo de veinte (20) meses desde la entrada en vigencia del presente documento, y a una distancia no menor de 1500km	Tier 3 o compromete tier 3 en el plazo de veinte (20) meses desde la entrada en vigencia del presente documento, y a una distancia no menor de 1500km	
Estrategia de recuperación	Sitio alternativo en caliente (hot site) o tibio (worm site)	Sitio alternativo en frío (cold site), operativo mediante procesos manuales.	Copias de Seguridad.
Objetivos de Recuperación	RTO < 4 horas; RPO < 1 hora.	RTO <24 horas; RPO < 4 horas.	RTO entre 1 y 5 días.
Pruebas Periódicas	Al menos una prueba	Al menos una prueba	Pruebas de

del PRD	completa anual. Tabletop semestrales, pruebas de recuperación de backups offline, tests de failover de redes.	completa anual. Tabletop trimestrales, pruebas de recuperación de backups offline.	consistencia de copias de seguridad tomando muestras de archivos.

Tabla 2: Requisitos para Sistema por Criticidad

Sitio en caliente: operativo casi en tiempo real, con replicación continua de sistemas críticos y conmutación rápida automática o semi-automática).

Sitio en tibio: copias de seguridad incrementales, con snapshots, infraestructura configurada por software.

CAPÍTULO 3: Requisitos Técnicos Mínimos para el Centro de Procesamiento de Datos de Respaldo

Ubicación Geográfica y Condiciones del Sitio. El Centro de Datos de Respaldo (DRP) deberá estar ubicado dentro del territorio de la República Argentina, a una distancia geográfica significativa del centro de datos principal —al menos mil quinientos (1.500) kilómetros—, con el objetivo de evitar la exposición simultánea a eventos disruptivos o desastres que afecten la región del sitio primario. La selección de la ubicación deberá considerar criterios de independencia geográfica y de infraestructura, sin que ello implique excluir regiones por la sola presencia de riesgos naturales, sino gestionarlos adecuadamente mediante análisis de vulnerabilidad y medidas de mitigación documentadas. Asimismo, deberá garantizar disponibilidad de energía eléctrica, telecomunicaciones y transporte de datos que aseguren la operación continua del DRP[5].

Conectividad Redundante de Fibra Óptica. Deberán existir al menos dos enlaces de comunicaciones independientes entre el centro de datos principal y el Centro de Datos de Respaldo, preferentemente utilizando fibra óptica tendida por rutas físicas diferenciadas. Cada enlace deberá poseer capacidad suficiente para replicación en tiempo real y, de ser posible, contratarse a diferentes proveedores para evitar puntos únicos de falla. Se recomienda un enlace alternativo adicional (satelital o radioenlace) para contingencias extremas.

Suministro Eléctrico y Climatización Resilientes. El Centro de Datos de Respaldo deberá contar con doble acometida energética (cuando sea factible), UPS adecuadas y generadores con autonomía suficiente para sostener la operación (≥ 24–48 h)[6]. Los sistemas de climatización deberán ser redundantes y, en ubicaciones frías, podrá implementarse free cooling. Controlar humedad para evitar condensación o estática.

Infraestructura de Hardware Compatible y Dimensionada. El equipamiento debe ser compatible con el del Centro de Datos Principal (arquitecturas, hipervisores, SO, middleware) y con recursos suficientes para soportar los servicios críticos. Para datos críticos: replicación sincrónica cuando el RPO sea cercano a cero; si no es viable, replicación asíncrona con RPO documentado y aceptado por el sujeto alcanzado. ISO 22300 define RPO como la

pérdida máxima de datos tolerable[7].

Seguridad Física y Lógica Equivalente. Aplicar al sitio alterno controles equivalentes a producción: accesos, CCTV, perímetro, detección y extinción de incendios; y en lo lógico, firewalls, IDS/IPS, autenticación robusta, segmentación, cifrado y monitoreo (SIEM). NIST SP 800-53, control CP-7(3), exige seguridad equivalente en el sitio alternativo.

Certificación Tier 3. Además, antes de cumplidos los veinte (20) meses de la entrada en vigencia del presente documento el Centro de Datos de Respaldo deberá certificarse como Tier 3. A saber:

Desde el inicio de las operaciones, el Centro de Datos de Respaldo (DRP) deberá ajustarse a los requerimientos técnicos y de infraestructura correspondientes al nivel Tier 3, conforme a la norma ANSI/TIA-942 y las guías del Uptime Institute, garantizando así una disponibilidad anual de 99,982 % y la capacidad de realizar mantenimiento concurrente sin interrupción del servicio.

La certificación formal del nivel TIER 3 deberá obtenerse dentro de un plazo máximo de veinte (20) meses a partir de la entrada en vigencia del presente documento[8].

- Mantenibilidad concurrente: Todos los componentes críticos (energía, climatización, conectividad) deben poder aislarse o retirarse sin interrumpir las operaciones del centro de datos[9].
- Redundancia eléctrica (N+1): Se requiere una arquitectura con múltiples rutas de distribución (A/B), UPS redundantes y generadores que aseguren alimentación continua durante mantenimiento o fallas.
- Redundancia de climatización (N+1): Los sistemas HVAC deberán incluir unidades redundantes y trayectos de aire o refrigerante alternativos que permitan mantener condiciones ambientales seguras sin interrupciones[10].
- Conectividad diversa: Deberá contar con al menos dos enlaces de telecomunicaciones de proveedores distintos, tendidos por rutas físicas independientes hasta el sitio, con capacidad suficiente para replicación en tiempo real[11].
- Protección contra incendios: Se exigirá detección temprana (por ejemplo, VESDA) y sistemas automáticos de supresión con agentes limpios o agua nebulizada, de acuerdo con las normas locales y NFPA 75/76[12].
- Seguridad física y lógica: Deberán aplicarse controles equivalentes a los del centro principal: accesos por capas, CCTV, autenticación multifactor, segmentación de red y monitoreo continuo de incidentes[13].

CAPÍTULO 4: Contribuciones del Centro Nacional de Ciberseguridad

La Autoridad de Aplicación podrá:

- Emitir guías y formularios de Análisis de Impacto al Negocio (BIA, por sus siglas en inglés) estandarizados para asistir en la categorización de criticidad de sistemas.
- Dictar resoluciones complementarias y aclaratorias a fin de que los sujetos alcanzados puedan implementar sus políticas y planes de contingencia eficientemente.
- Publicar un calendario de entrenamientos invitando a integrantes de los sujetos alcanzados a participar.
- Ser el órgano de consulta y estar a disposición para acompañar a los distintos sujetos alcanzados en sus procesos de elaboración de políticas, planes, inventarios, así como la ejecución de los mismos.

[1]FIPS 199, “Standards for Security Categorization of Federal Information and Information Systems” (NIST, 2004).

[2]NIST Special Publication 800-34 Rev.1, “Contingency Planning Guide for Federal Information Systems” (2010).

[3] NIST Special Publication 800-184, “Guide for Cybersecurity Event Recovery” (2016).

[4] ISO/IEC 27031:2011; ISO 22301:2019.

[5]NIST SP 800-34 Rev.1; ISO/IEC 27031:2011; ISO 22301:2019.

[6] ISO/IEC 22301:2019, Seguridad y resiliencia – Sistemas de gestión de la continuidad del negocio – Requisitos.

[7] ISO 22300:2021, Seguridad y resiliencia – Vocabulario (definiciones de RPO/RTO).

[8] Uptime Institute, Tier Standard: Topology (2018); ANSI/TIA-942:2023.

[9] Uptime Institute, Tier Classification System, Sección 3.2.

[10] ANSI/TIA-942:2023, Sección 7.2; ASHRAE TC9.9 (2021).

[11] ANSI/TIA-942:2023, Sección 10.3; ISO/IEC 27031:2011.

[12] NFPA 75:2023; ANSI/TIA-942:2023, Sección 9.4.

[13] NIST SP 800-53 Rev.5, Control CP-7(3)

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
Date: 2026.04.29 09:08:09 -03:00

Ariel Waissbein
Director Ejecutivo
Centro Nacional de Ciberseguridad
Jefatura de Gabinete de Ministros

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
Date: 2026.04.29 09:08:10 -03:00