Ministerio de
Planificación Estratégica y Modernización

Gobierno de JUJUY
Cerca de la gente

PROTOCOLO
PROVINCIAL DE CIBERSEGURIDAD

Política de Planificación de Contingencias

26
CAPÍTULO

Política de Planificación de Contingencias

1.0 OBJETIVO

Garantizar que los recursos y sistemas de información normales de tecnología de la información (TI) estén disponibles durante momentos de interrupción de los servicios.

2.0 POLÍTICA

Esta política es aplicable a todos los departamentos y usuarios de recursos y activos de TI.

1. PLAN DE CONTINGENCIA

El Departamento de TI deberá:

a. Desarrollar un plan de contingencia para el sistema de información, en orientación directa y asociación con el propietario del sistema de información, que:

   i. Identifica misiones esenciales y funciones gubernamentales y requisitos de contingencia asociados.
   ii. Proporciona objetivos de recuperación, prioridades de restauración y métricas.
   iii. Aborda roles de contingencia, responsabilidades, personas asignadas con información de contacto.
   iv. Aborda el mantenimiento de misiones esenciales y funciones gubernamentales a pesar de una interrupción, compromiso o falla del sistema de información.
   v. Aborda la eventual restauración completa del sistema de información sin deterioro de los controles de seguridad originalmente planificados e implementados.
   vi. Es revisado y aprobado por el personal o roles definidos por la Repartición y la gestión del propietario del sistema de información al menos una vez al año.

b. Distribuir copias de los planes de contingencia al personal clave de contingencia, identificado por nombre y/o por función gubernamental.

c. Coordinar las actividades de planificación de contingencias con las actividades de manejo de incidentes.
d. Actualizar el plan de contingencia para abordar los cambios en la misión, el sistema de información o el entorno de operación del responsable de la Repartición y los problemas encontrados durante la implementación, ejecución o prueba del plan de contingencia.
e. Comunicar los cambios del plan de contingencia al personal clave de contingencia identificado por nombre y/o por función comercial.
f. Proteger el plan de contingencia de divulgación y modificación no autorizadas.

2. ENTRENAMIENTO DE CONTINGENCIA

El Departamento de TI deberá:

a. Proporcionar capacitación de contingencia a los usuarios del sistema de información de acuerdo con las funciones y responsabilidades asignadas.
b. Asegurar que el personal designado reciba capacitación para contingencias al menos una vez al año al asumir un rol o responsabilidad de contingencias, y cuando lo requieran cambios en el sistema de información.

3. PRUEBAS DEL PLAN DE CONTINGENCIA

TI, junto con los propietarios de los sistemas de información, deberá:

a. Probar el plan de contingencia para el sistema de información, según lo determine la naturaleza crítica de la misión de los sistemas gubernamentales al menos una vez al año.
b. Utilizar la planificación estratégica y táctica durante las pruebas para simular un sistema de información de producción para determinar la efectividad del plan y la preparación organizacional para ejecutar el plan.
c. Revisar los resultados de las pruebas del plan de contingencia.
d. Iniciar acciones correctivas, según sea necesario.
e. Coordinar las pruebas del plan de contingencia con los elementos organizacionales responsables de los planes relacionados; Los planes de contingencia para sistemas de información incluyen, por ejemplo, planes de continuidad del negocio, de recuperación de desastres, de continuidad de operaciones, de comunicación de crisis, de infraestructura crítica, de respuesta a incidentes cibernéticos y de emergencia para ocupantes.

4. SITIO DE ALMACENAMIENTO ALTERNO

TI, en orientación directa y asociación con el propietario del sistema de información, deberá:

a. Establecer un sitio de almacenamiento alternativo que incluya los acuerdos necesarios para permitir el almacenamiento y la recuperación de información de respaldo del sistema de información.
b. Asegurar que el sitio de almacenamiento alternativo proporcione controles de seguridad de la información equivalentes a las del sitio principal.
c. Identificar un sitio de almacenamiento alternativo que esté separado del sitio de almacenamiento principal para reducir la susceptibilidad a las mismas amenazas.
d. Identificar y documentar posibles problemas de accesibilidad al sitio de almacenamiento alternativo en caso de una interrupción o desastre en toda el área y describa acciones de mitigación explícitas.

5. SITIO DE PROCESAMIENTO ALTERNO

TI, en orientación directa y asociación con el propietario del sistema de información, deberá:

a. Establecer un sitio de procesamiento alternativo que incluya los acuerdos necesarios para permitir la transferencia y reanudación de las operaciones del sistema de información para misiones/funciones gubernamentales esenciales dentro del período de tiempo consistente con los objetivos de tiempo y punto de recuperación cuando las capacidades de procesamiento primario no estén disponibles.
b. Asegurar que los equipos y suministros necesarios para transferir y reanudar las operaciones estén disponibles en el sitio de procesamiento alternativo o que existan contratos para respaldar la entrega al sitio dentro del período de tiempo acordado para la transferencia/reanudación.
c. Asegurar que el sitio de procesamiento alternativo proporcione controles de seguridad de la información equivalentes a las del sitio principal.
d. Identificar un sitio de procesamiento alternativo que esté separado del sitio de procesamiento principal para reducir la susceptibilidad a las mismas amenazas.
e. Identificar posibles problemas de accesibilidad al sitio de procesamiento alternativo en caso de una interrupción o desastre en toda el área y describa acciones de mitigación explícitas.

f. Desarrollar acuerdos de sitios de procesamiento alternativos que contengan disposiciones de prioridad de servicio de acuerdo con los objetivos gubernamentales y los requisitos de disponibilidad.

6. SERVICIOS DE TELECOMUNICACIONES

El Departamento de TI deberá:

a. Establecer servicios de telecomunicaciones alternativos, incluidos los acuerdos necesarios para permitir la reanudación de las operaciones del sistema de información para misiones esenciales y funciones gubernamentales dentro de los plazos de recuperación acordados cuando las capacidades de telecomunicaciones primarias no estén disponibles en los sitios de procesamiento o almacenamiento primarios o alternativos.
b. Desarrollar acuerdos de servicios de telecomunicaciones primarios y alternativos que contengan disposiciones de prioridad de servicio de acuerdo con los objetivos de recuperación y los requisitos de disponibilidad acordados.
c. Solicitar prioridad de servicio de telecomunicaciones para los servicios de telecomunicaciones utilizados para emergencias de seguridad provincial en el caso de que los servicios de telecomunicaciones primarios y/o alternativos sean proporcionados por un proveedor común.

7. RESPALDO DEL SISTEMA DE INFORMACIÓN

TI, en orientación directa y asociación con el propietario del sistema de información, deberá:

a. Realizar copias de seguridad de la información a nivel de usuario contenida en el sistema de información definida por frecuencia consistente con el tiempo de recuperación y los objetivos de punto de recuperación.
b. Realizar copias de seguridad de la información a nivel del sistema contenida en el sistema de información definida por frecuencia consistente con el tiempo de recuperación y los objetivos del punto de recuperación.
c. Realizar copias de seguridad de la documentación del sistema de información, incluida la documentación relacionada con la seguridad, definida por frecuencia coherente con el tiempo de recuperación y los objetivos de punto de recuperación.

d. Proteger la confidencialidad, integridad y disponibilidad de la información de respaldo en las ubicaciones de almacenamiento.
e. Probar la información de respaldo para verificar la confiabilidad de los medios y la integridad de la información.

8. RECUPERACIÓN Y RECONSTITUCIÓN DEL SISTEMA DE INFORMACIÓN

TI, en orientación directa y asociación con el propietario del sistema de información, deberá:

a. Proporcionar la recuperación y reconstitución del sistema de información a un estado conocido después de una interrupción, compromiso o falla.
b. Disponer que el sistema de información implemente la recuperación de transacciones para los sistemas que estén basados en transacciones.

3.0 CUMPLIMIENTO

Los empleados que incumplan esta política pueden estar sujetos a medidas disciplinarias, así como sanciones penales, civiles y/o administrativas si correspondieren. Los no empleados, incluidos, entre otros, los contratistas, pueden estar sujetos a la rescisión de acuerdos contractuales, a la denegación de acceso a los recursos de TI y a otras acciones, así como a sanciones tanto civiles como penales.

4.0 EXCEPCIONES DE POLÍTICA

Las solicitudes de excepciones a esta política serán revisadas por el Director de Ciberseguridad (DC) y Secretaría de Innovación Pública (SIP), y/o Encargado de Seguridad de la Información. Los departamentos que soliciten excepciones deberán proporcionar dichas solicitudes al DC/SIP. La solicitud debe indicar específicamente el alcance de la excepción junto con la justificación para otorgar la excepción, el posible impacto o riesgo asociado al otorgar la excepción, las medidas de mitigación de riesgos que debe tomar el Departamento de TI, iniciativas, acciones y un cronograma para lograrlo, el nivel mínimo de cumplimiento de las políticas aquí establecidas. El DC/SIP revisará dichas solicitudes; consultar con el departamento solicitante.

5.0 HISTORIAL DE REVISIONES

Fecha	Descripción de Cambio	Participantes
09/08/2024	Revisión inicial	Alejandro Castro, Pablo Zalazar
12/08/2024	Visado, y corrección de errores	Alejandro Castro.

6.0 REFERENCIA

Publicaciones especiales (SP) del Instituto Nacional de Estándares y Tecnología (NIST):

NIST SP 800-53a – Planificación de contingencias (CP), NIST SP 800-16, NIST SP 800-34, NIST SP 800-50, NIST SP 800-84; Estándares federales de procesamiento de información (FIPS) 199 del NIST