| Política #: | Título: | Fecha de entrada en vigor: |
| --- | --- | --- |
| x.xx | Política de Planes de Contingencia | MM/DD/YYYY |

**PROPÓSITO**
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

**REFERENCIA**
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

National Institute of Standards and Technology (NIST) Special Publications (SP):
NIST SP 800-53a – Contingency Planning (CP), NIST SP 800-16, NIST SP 800-34, NIST SP 800-50, NIST SP 800-84; NIST Federal Information Processing Standards (FIPS) 199

**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:

1. Desarrollar un plan de contingencia para el sistema de información, en orientación directa y asociación con el propietario del sistema de información, que:
	1. Identifique las misiones esenciales y las funciones comerciales y los requisitos de contingencia asociados.
	2. Proporcione objetivos de recuperación, prioridades de restauración y métricas.
	3. Aborde roles de contingencia, responsabilidades, personas asignadas con información de contacto.
	4. Aborde el mantenimiento de las misiones esenciales y las funciones comerciales a pesar de una interrupción, compromiso o falla del sistema de información.
	5. Aborde la restauración eventual y completa del sistema de información sin deterioro de las salvaguardas de seguridad originalmente planificadas e implementadas.
	6. Sea revisado y aprobado por el [personal o roles definidos por la entidad] y la gerencia del propietario del sistema de información al menos una vez al año.
2. Distribuir copias de los planes de contingencia al personal clave de contingencia, identificado por su nombre y/o por su función comercial.
3. Coordinar las actividades de planificación de contingencia con las actividades de manejo de incidentes.
4. Actualizar el plan de contingencia para abordar los cambios en la misión, el sistema de información o el entorno de operación del propietario de la empresa y los problemas encontrados durante la implementación, ejecución o prueba del plan de contingencia.
5. Comunicar los cambios en el plan de contingencia al personal clave de contingencia identificado por nombre y/o por rol comercial.
6. Proteger el plan de contingencia contra la divulgación y modificación no autorizadas.
7. **CAPACITACIÓN EN CONTINGENCIA**

El Departamento de TI deberá:

1. Proporcionar capacitación en contingencia a los usuarios del sistema de información de acuerdo con las funciones y responsabilidades asignadas.
2. Asegurarse que el personal designado reciba capacitación en contingencia al menos dos veces al año para asumir un rol o responsabilidad de contingencia, y cuando lo requieran los cambios en el sistema de información.
3. **PRUEBAS DE PLANES DE CONTINGENCIA**

El departamento de TI, junto con los propietarios de los sistemas de información, deberán:

* 1. Testear el plan de contingencia para el sistema de información, según lo determine la naturaleza de misión crítica del sistema o sistemas comerciales no menos de una vez al año.
	2. Utilizar la planificación estratégica y táctica durante las pruebas para simular un sistema de información de producción para determinar la eficacia del plan y la preparación de la organización para ejecutar el plan.
	3. Revisar los resultados de las pruebas del plan de contingencia.
	4. Iniciar acciones correctivas, según sea necesario.
	5. Coordinar las pruebas de los planes de contingencia con los elementos de la organización responsables de los planes relacionados; Los planes relacionados con los planes de contingencia para los sistemas de información incluyen, por ejemplo, Planes de Continuidad del Negocio, Planes de Recuperación ante Desastres, Planes de Continuidad de las Operaciones, Planes de Comunicaciones de Crisis, Planes de Infraestructura Crítica, Planes de Respuesta a Incidentes Cibernéticos y Planes de Emergencia para los Ocupantes.
1. **SITIO DE ALMACENAMIENTO ALTERNATIVO**

El departamento de TI, en dirección directa y en asociación con el propietario del sistema de información, deberá:

* 1. Establecer un sitio de almacenamiento alternativo, incluidos los acuerdos necesarios para permitir el almacenamiento y la recuperación de la información de respaldo del sistema de información.
	2. Asegurarse de que el sitio de almacenamiento alternativo proporcione medidas de seguridad de la información equivalentes a las del sitio principal.
	3. Identificar un sitio de almacenamiento alternativo que esté separado del sitio de almacenamiento principal para reducir la susceptibilidad a las mismas amenazas.
	4. Identificar y documentar los posibles problemas de accesibilidad al sitio de almacenamiento alternativo en caso de una interrupción o desastre en toda el área y describir acciones de mitigación explícitas.
1. **SITIO DE PROCESAMIENTO ALTERNATIVO**

El departamento de TI, en dirección directa y en asociación con el propietario del sistema de información, deberá:

* 1. Establecer un sitio de procesamiento alternativo, incluidos los acuerdos necesarios, para permitir la transferencia y reanudación de las operaciones del sistema de información para misiones esenciales y funciones institucionales dentro del período de tiempo compatible con el tiempo de recuperación y los objetivos de recuperación cuando no se disponga de la capacidad de procesamiento principal.
	2. Asegurarse de que el equipo y los 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.
	3. Asegurarse de que el sitio de procesamiento alternativo proporcione medidas de seguridad de la información equivalentes a las del sitio principal.
	4. Identificar un sitio de procesamiento alternativo que esté separado del sitio de procesamiento principal para reducir la susceptibilidad a las mismas amenazas.
	5. Identificar los posibles problemas de accesibilidad al sitio de procesamiento alternativo en caso de una interrupción o desastre en toda el área y describir acciones de mitigación explícitas.
	6. Desarrollar acuerdos de sitios de procesamiento alternativos que contengan disposiciones de prioridad de servicio de acuerdo con los objetivos comerciales y los requisitos de disponibilidad.
1. **SERVICIOS DE TELECOMUNICACIONES**

El Departamento de TI deberá:

* 1. Establecer servicios de telecomunicaciones alternativos, incluidos los acuerdos necesarios, que permitan la reanudación de las operaciones del sistema de información para las misiones esenciales y las funciones institucionales dentro de los plazos de recuperación convenidos cuando las capacidades primarias de telecomunicaciones no estén disponibles en los sitios de procesamiento o almacenamiento primarios o alternativos.
	2. 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.
	3. Solicitar prioridad de servicio de telecomunicaciones para todos los servicios de telecomunicaciones utilizados para la preparación para emergencias de seguridad nacional en caso de que los servicios de telecomunicaciones primarios y/o alternativos sean proporcionados por un operador común.
1. **COPIA DE SEGURIDAD DEL SISTEMA DE INFORMACIÓN**

El departamento de TI, en dirección directa y en asociación con el propietario del sistema de información, deberá:

* 1. Realizar copias de seguridad de la información a nivel de usuario existente en el sistema de información a una frecuencia coherente con los objetivos de tiempo de recuperación y punto de recuperación.
	2. Realizar copias de seguridad de la información a nivel de sistema en el sistema de información a una frecuencia coherente con el tiempo de recuperación y los objetivos de punto de recuperación.
	3. Realizar copias de seguridad de la documentación del sistema de información, incluida la documentación relacionada con la seguridad, a una frecuencia coherente con el tiempo de recuperación y los objetivos del punto de recuperación.
	4. Proteger la confidencialidad, integridad y disponibilidad de la información de copia de seguridad en las ubicaciones de almacenamiento.
	5. Testear la información de copia de seguridad para verificar la confiabilidad de los medios y la integridad de la información.
1. **RECUPERACIÓN Y RECONSTITUCIÓN DE SISTEMAS DE INFORMACIÓN**

El departamento de TI, en dirección directa y en asociación con el propietario del sistema de información, deberá:

1. Proporcionar la recuperación y reconstitución del sistema de información a un estado conocido después de una interrupción, compromiso o fallo.
2. Establecer que el sistema de información implemente la recuperación de transacciones para los sistemas que se basan en transacciones.

**CUMPLIMIENTO**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Los empleados que infrinjan esta política pueden estar sujetos a medidas disciplinarias apropiadas que pueden incluir el despido, así como a sanciones civiles y penales. Los no empleados, incluidos, entre otros, los contratistas, pueden estar sujetos a la rescisión de los acuerdos contractuales, la denegación de acceso a los recursos de tecnología de la información (TI) y otras acciones, así como a sanciones civiles y penales.

**EXCEPCIONES A LA POLÍTICA**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Las solicitudes de excepciones a esta política serán revisadas por el Director de Seguridad de la Información (CISO) y el Director de Información (CIO). Los departamentos que soliciten excepciones deberán proporcionar dichas solicitudes al CIO. La solicitud debe indicar específicamente el alcance de la excepción junto con la justificación para otorgar la excepción, el impacto potencial o el riesgo que conlleva el otorgamiento de la excepción, las medidas de mitigación de riesgos que debe emprender el Departamento de TI, las iniciativas, acciones y un marco de tiempo para lograr el nivel mínimo decumplimiento de las políticas establecidas en este documento. El CIO revisará dichas solicitudes; consultar con el departamento solicitante.

**DEPARTAMENTOS RESPONSABLES**
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Jefe de la Oficina de Información y Propietarios de Sistemas de Información

**FECHA DE PUBLICACIÓN/FECHA DE REVISIÓN**
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

| Fecha de publicación: | MM/DD/YYYY |
| --- | --- |
| Fecha de revisión: | MM/DD/YYYY |