Ministerio de
Planificación Estratégica y Modernización

Gobierno de JUJUY
Cerca de la gente

PROTOCOLO
PROVINCIAL DE CIBERSEGURIDAD

Política de Respuesta a Incidentes

27
CAPÍTULO

Política de Respuesta a Incidentes

1.0 OBJETIVO

Garantizar que la Tecnología de la Información (TI) identifique, contenga, investigue, solucione, informe y responda adecuadamente a los incidentes de seguridad informática.

2.0 POLÍTICA

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

1. ENTRENAMIENTO DE RESPUESTA A INCIDENTES

La Repartición con el acompañamiento del MPEYM debe:

a. Proporcionar capacitación en respuesta a incidentes a los usuarios del sistema de información de acuerdo con las funciones y responsabilidades asignadas:

   i. Dentro de un período de tiempo definido por la Repartición de asumir un rol o responsabilidad de respuesta a incidentes.
   ii. Cuando lo requieran cambios en el sistema de información, y en una frecuencia definida por la Repartición después de eso.

2. PRUEBAS DE RESPUESTA A INCIDENTES

La Repartición debe:

a. Probar la capacidad de respuesta a incidentes del sistema de información. En una frecuencia definida por la Repartición usando una asignación de pruebas definidas por Repartición para determinar la efectividad de la respuesta al incidente y documentar los resultados.
b. Coordinar las pruebas de respuesta a incidentes con los contactos de la Repartición responsables de los planes relacionados: de continuidad del negocio, de contingencia, de recuperación de desastres, de continuidad de operaciones, de comunicación de crisis, de infraestructura crítica y de emergencia para ocupantes.

3. MANEJO DE INCIDENTES

La Repartición debe:

a. Implementar una capacidad de manejo de incidentes de seguridad que incluya preparación, detección y análisis, contención, erradicación y recuperación.
b. Coordinar las actividades de manejo de incidentes con las actividades de planificación de contingencias.
c. Incorporar las lecciones aprendidas de las actividades de manejo de incidentes en curso en los procedimientos de respuesta a incidentes, capacitación y pruebas/ejercicios, e implementar los cambios resultantes en consecuencia.

4. SEGUIMIENTO DE INCIDENTES

La Repartición debe:

a. Emplear mecanismos automatizados para ayudar en el seguimiento de incidentes de seguridad y en la recopilación y análisis de información sobre incidentes.

5. INFORME DE INCIDENTE

La Repartición debe:

a. Exigir al personal que informe los incidentes de seguridad sospechosos a la capacidad de respuesta a incidentes dentro de un período de tiempo definido por la Repartición. Se sugiere que sea de manera inmediata y hasta dentro de las **primeras 24 horas**.
b. Reportar información sobre incidentes de seguridad a las autoridades o encargados definidos por la Repartición.

6. ASISTENCIA DE RESPUESTA A INCIDENTES

La Repartición debe:

a. Proporcionar un recurso de soporte de respuesta a incidentes, integral a la capacidad de respuesta a incidentes, que ofrezca asesoramiento y asistencia a los usuarios del sistema de información para el manejo y notificación de incidentes de seguridad.

7. PLAN DE RESPUESTA A INCIDENTES

La Repartición debe:

a. Desarrollar un plan de respuesta a incidentes en donde:
    i. La Repartición proporcione una hoja de ruta para implementar su capacidad de respuesta a incidentes.
    ii. Describa la estructura de la capacidad de respuesta a incidentes.
    iii. Proporcione un enfoque de alto nivel sobre cómo la capacidad de respuesta a incidentes encaja en el sistema general de la Repartición.
    iv. Cumpla con los requisitos únicos de la Repartición, que se relacionan con la misión, el tamaño, la estructura y las funciones.
    v. Defina incidentes reportables.
    vi. Proporcione métricas para medir la capacidad de respuesta a incidentes dentro de la Repartición.
    vii. Defina los recursos y el apoyo de gestión necesarios para mantener y madurar eficazmente una capacidad de respuesta a incidentes.
    viii. Sea revisado y aprobado por el personal o roles definidos por la Repartición.

b. Distribuir copias del plan de respuesta a incidentes al personal de respuesta a incidentes definido por la Repartición (identificado por nombre y/o por función).
c. Revisar el plan de respuesta a incidentes en una frecuencia definida por la Repartición.
d. Actualizar el plan de respuesta a incidentes para abordar los cambios del sistema o los problemas encontrados durante la implementación, ejecución o prueba del plan.
e. Comunicar los cambios en el plan de respuesta a incidentes al personal de respuesta a incidentes definido por la Repartición (identificado por nombre y/o por función).
f. Proteger el plan de respuesta a incidentes de divulgación y modificación no autorizadas.

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
12/08/2024	Revisión inicial	Alejandro Castro, Pablo Zalazar
13/08/2024	Visado, y corrección de errores	Alejandro Castro.

6.0 REFERENCIA

Publicación especial (SP) del Instituto Nacional de Estándares y Tecnología (NIST): NIST SP 800-53a: respuesta a incidentes (IR), NIST SP 800-16, NIST SP 800-50, NIST SP 800-61, NIST SP 800-84, NIST SP 800-115