Ministerio de
Planificación Estratégica y Modernización

Gobierno de JUJUY
Cerca de la gente

PROTOCOLO
PROVINCIAL DE CIBERSEGURIDAD

Política de Respuesta a Amenazas de Seguridad Informática

25
CAPÍTULO

Política de Respuesta a Amenazas de Seguridad Informática

1.0 OBJETIVO

El propósito de esta política es definir la responsabilidad de la Repartición en la respuesta a amenazas de seguridad que afecten la confidencialidad, integridad y/o disponibilidad de los recursos de tecnología de la información (TI).

2.0 POLÍTICA

Esta política es aplicable a todos los departamentos y todos los sistemas de información.

1. RESPUESTA DE EMERGENCIA INFORMÁTICA

a. Se establecerá un Equipo de Respuesta a Emergencias Informáticas (EREI). El EREI estará dirigido por el Director de Ciberseguridad (DC) o quien designe el MPEyM
b. El EREI estará compuesto por representantes de todas las Unidades de Organización.
c. El EREI deberá comunicar información de seguridad, pautas para los procesos de notificación, identificar posibles riesgos de seguridad y coordinar respuestas para frustrar, mitigar o eliminar amenazas de seguridad a los recursos de TI.
d. Tras la activación de EREI por parte del DC, todos los responsables de Seguridad de la Información y otros representantes de EREI deberán informar directamente al DC durante la activación de EREI.

2. RESPUESTA DE EMERGENCIA INFORMÁTICA

Cada Repartición establecerá el/los responsable/s de la repartición designados para responder a incidentes y/o coordinar la respuesta a las amenazas de seguridad a los recursos de TI dentro de la Unidad de Organización.

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	Participan tes
09/08/2024	Revisión inicial	Alejandro Castro, Pablo Zalazar
12/08/2024	Visado, y corrección de errores	Alejandro Castro.

6.0 REFERENCIA

Publicación especial (SP) del Instituto Nacional de Estándares y Tecnología (NIST): NIST SP 800-61: Guía de manejo de incidentes de seguridad informática