Ministerio de
Planificación Estratégica y Modernización

Gobierno de JUJUY
Cerca de la gente

PROTOCOLO
PROVINCIAL DE CIBERSEGURIDAD

Política de Planificación

28
CAPÍTULO

Política de Planificación

1.0 OBJETIVO

Garantizar que los recursos y sistemas de información de tecnología de la información (TI) se planifiquen con controles de seguridad efectivos y mejoras de control que reflejen las leyes, órdenes gubernamentales, directivas, regulaciones, políticas, estándares y directrices nacionales y provinciales aplicables.

2.0 POLÍTICA

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

1. PLAN DE SEGURIDAD DEL SISTEMA

El Departamento de TI deberá:

a. Desarrollar un plan de seguridad para cada sistema de información que:

   i. Sea consistente con la arquitectura gubernamental de la Repartición.
   ii. Defina explícitamente el límite de autorización para el sistema.
   iii. Describa el contexto operativo del sistema de información en términos de misiones y procesos.
   iv. Proporcione la categorización de seguridad del sistema de información, incluida la justificación de respaldo.
   v. Describa el entorno operativo para el sistema de información y las relaciones o conexiones con otros sistemas de información.
   vi. Proporcione una descripción general de los requisitos de seguridad del sistema.
   vii. Identifique cualquier superposición relevante, si corresponde.
   viii. Describa los controles de seguridad implementados o planificados para cumplir con esos requisitos, incluida una justificación de las decisiones de adaptación.
   ix. Sea revisado y aprobado por el funcionario autorizado o representante designado antes de la implementación del plan.

b. Distribuir copias del plan de seguridad y comunicar los cambios posteriores al plan al personal autorizado y/o unidades de negocio.

c. Revisar el plan de seguridad del sistema de información al menos una vez al año.
d. Actualizar el plan para abordar cambios en el sistema de información/ entorno de operación o problemas identificados durante la implementación del plan o las evaluaciones de control de seguridad.
e. Proteger el plan de seguridad contra divulgación y modificación no autorizadas.

2. REGLAS DE COMPORTAMIENTO

El Departamento de TI deberá:

a. Establecer y poner a disposición de las personas que requieran acceso al sistema de información, las reglas que describen sus responsabilidades y el comportamiento esperado con respecto a la información y el uso del sistema de información.
b. Recibir un reconocimiento firmado de dichas personas, indicando que han leído, comprendido y se comprometen a respetar las reglas de conducta, antes de autorizar el acceso a la información y al sistema de información.
c. Revisar y actualizar las normas de conducta.
d. Exigir a las personas que hayan firmado una versión anterior de las reglas de conducta que lean y renuncien cuando se revisen y actualicen las reglas de conducta.

3. ARQUITECTURA DE SEGURIDAD DE LA INFORMACIÓN

El Departamento de TI deberá:

a. Desarrollar una arquitectura de seguridad para el sistema de información que:
    i. Describa la filosofía general, los requisitos y el enfoque que se debe adoptar con respecto a la protección de la confidencialidad, integridad y disponibilidad de la información organizacional.
    ii. Describir cómo la arquitectura de seguridad de la información se integra y respalda la arquitectura gubernamental.
    iii. Describir cualquier supuesto de seguridad de la información y dependencia de servicios externos.
b. Revisar y actualizar la arquitectura de seguridad de la información al menos una vez al año, para reflejar las actualizaciones en la arquitectura gubernamental.

c. Asegurar que los cambios planificados en la arquitectura de seguridad de la información se reflejen en el plan de seguridad, las operaciones de seguridad y las compras/adquisiciones.

4. ENFOQUE DE DEFENSA EN PROFUNDIDAD

El Departamento de TI deberá:

a. Diseñar una arquitectura de seguridad utilizando un enfoque de defensa en profundidad que:

   i. Asigne controles de seguridad a ubicaciones definidas y capas arquitectónicas de la Repartición.
   ii. Garantizar que los controles de seguridad asignados funcionen de manera coordinada y se refuercen mutuamente.

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
19/08/2024	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 seguridad (PL), NIST SP 800-12, SP NIST 800-18, NIST SP 800-100