Ministerio de
Planificación Estratégica y Modernización

Gobierno de Jujuy
Cerca de la gente

PROTOCOLO
PROVINCIAL DE CIBERSEGURIDAD

Política de Autorización y Evaluación de Seguridad

20
CAPÍTULO

Política de Autorización y Evaluación de Seguridad

1.0 OBJETIVO

Las Tecnologías de la Información (TI) y las diversas unidades gubernamentales (propietarios de la información) garantizarán los controles de seguridad en los sistemas de información y los entornos en los que operan esos sistemas, como parte de las autorizaciones de seguridad iniciales y continuas, las evaluaciones anuales, el monitoreo continuo y las actividades del ciclo de vida del desarrollo del sistema.

2.0 POLÍTICA

Esta política es aplicable a todos los departamentos y usuarios de recursos y activos de TI. Cada dependencia que mantiene o recopila activos de información debe cumplir con esta política.

1. POLÍTICA Y PROCEDIMIENTOS DE EVALUACIÓN Y AUTORIZACIÓN DE SEGURIDAD

La Repartición deberá:

a. Desarrollar, documentar y difundir a personal o roles definidos por la Repartición:
    i. Una política de evaluación y autorización de seguridad que aborda el propósito, el alcance, las funciones, las responsabilidades, el compromiso de la administración, la coordinación entre las entidades organizacionales y el cumplimiento.
    ii. Procedimientos para facilitar la implementación de la política de autorización y evaluación de seguridad y los controles de autorización y evaluación de seguridad asociados.
b. Revisar y actualizar la política y los procedimientos actuales de evaluación y autorización de seguridad en una frecuencia anual.

2. EVALUACIONES DE SEGURIDAD

La Repartición deberá:

a. Desarrollar un plan de evaluación de seguridad que describa el alcance de la evaluación, incluyendo:

   i. Controles de seguridad y mejoras de control en evaluación.
   ii. Procedimientos de evaluación que se utilizarán para determinar la eficacia del control de seguridad.
   iii. Entorno de evaluación, equipo de evaluación y roles y responsabilidades de evaluación.

b. Evaluar los controles de seguridad en el sistema de información y su entorno de operación en una frecuencia definida por la Repartición determinar en qué medida los controles se implementan correctamente, funcionan según lo previsto y producen el resultado deseado con respecto al cumplimiento de los requisitos de seguridad establecidos.
c. Producir un informe de evaluación de seguridad que documente los resultados de la evaluación.
d. Proporcionar los resultados de la evaluación del control de seguridad a individuos o roles definidos por la Repartición.

3. INTERCONEXIONES DEL SISTEMA

El Departamento de TI deberá:

a. Autorizar conexiones entre los sistemas de información mediante el uso de Acuerdos de Seguridad de Interconexión.
b. Documentar, para cada interconexión, las características de la interfaz, los requisitos de seguridad y la naturaleza de la información comunicada.
c. Revisar y actualizar Acuerdos de Seguridad de Interconexión en una frecuencia semestral.
d. Emplear una política de permitir todo, denegar por excepción, denegar todo, permitir por excepción, para permitir sistemas de información definidos por la Repartición para conectarse a sistemas de información externos.

4. PLAN DE ACCIÓN E HITOS

La Repartición deberá:

a. Desarrollar un plan de acción e hitos para el sistema de información para documentar las acciones correctivas planificadas para corregir las debilidades o deficiencias observadas durante la evaluación de los controles de seguridad y para reducir o eliminar las vulnerabilidades conocidas en el sistema.

b. Actualizar el plan de acción y los hitos existentes en una frecuencia definida por la Repartición basado en los hallazgos de las evaluaciones de los controles de seguridad, los análisis de impacto de la seguridad y las actividades de monitoreo continuo.

5. AUTORIZACIÓN DE SEGURIDAD

La Repartición deberá:

a. Designar a un funcionario, jefe de área o de departamento como autorizador del sistema de información.
b. Asegurar que el funcionario designado autorice el procesamiento del sistema de información antes de iniciar las operaciones.
c. Actualizar la autorización de seguridad en una frecuencia definida por la Repartición.

6. MONITOREO CONTINUO

El Departamento de TI deberá:

a. Desarrollar una estrategia de monitoreo continuo e implementar un programa que incluya:
    i. Establecimiento de métricas definidas por la Repartición para ser monitoreado.
    ii. Establecimiento de frecuencias definidas por la Repartición para el seguimiento y frecuencias definidas por la Repartición para evaluaciones que respalden dicho seguimiento.
    iii. Evaluaciones continuas del control de seguridad de acuerdo con la estrategia organizacional de seguimiento continuo.
    iv. Monitoreo continuo del estado de seguridad de las métricas definidas por la organización de acuerdo con la estrategia de monitoreo continuo de la organización.
    v. Correlación y análisis de información relacionada con la seguridad generada por evaluaciones y monitoreo.
    vi. Acciones de respuesta para atender resultados del análisis de información relacionada con la seguridad.
    vii. Informar del estado de seguridad de la organización y del sistema de información a personal o roles definidos por la Repartición en una frecuencia definida por la Repartición.

7. CONEXIONES DEL SISTEMA INTERNO

El Departamento de TI deberá:

a. Autorizar conexiones internas de componentes o clases de componentes del sistema de información definidos por la Repartición al sistema de información.
b. Documentar, para cada conexión interna, las características de la interfaz, los requisitos de seguridad y la naturaleza de la información comunicada.

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 la 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	Autores
19/07/24	Visado de documento.	Pablo Zalazar, Alejandro Castro
31/07/24	Revisión de Documento, corrección de errores, ajuste de formato.	Alejandro Castro

6.0 REFERENCIA

Publicaciones especiales (SP) del Instituto Nacional de Estándares y Tecnología (NIST): NIST SP 800-53a: Evaluación y autorización de seguridad (CA), NIST SP 800-12, NIST SP 800-37, NIST SP 800-39, NIST SP 800-47, NIST SP 800-100, NIST SP 800-115, NIST SP 800-137; Estándares federales de procesamiento de información (FIPS) 199 del NIST